Graphical User Interface User Manual

EX Series Secure WAN Manager

Document No.: D-020-01-00-0002

Ver. 3.1 4/20/2011

Headquarters

A10 Networks, Inc.
2309 Bering Dr.
San Jose, CA 95131

Tel: 408 325 8668 (main)
Tel: 408 325 8676 (support)
Fax: 408 325 8666

www.a10networks.com

Information in this document is subject to change without notice.

Trademarks

A10 Networks, the A10 logo, ACOS, aFleX, aFlow, aGalaxy, aVCS, aXAPI, IDaccess, IDSENTRIE, IP to ID, SmartFlow, SoftAX, VirtualADC, Virtual Chassis, and VirtualN are trademarks or registered trademarks of A10 Networks, Inc. All other trademarks are property of their respective owners.

Patents Protection

A10 Networks products including all AX Series products are protected by one or more of the following US patents and patents pending: 7716378, 7675854, 7647635, 7552126, 20090049537, 20080229418, 20080040789, 20070283429, 20070271598, 20070180101

Confidentiality

This document contains confidential materials proprietary to A10 Networks, Inc. This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside A10 Networks, Inc. without prior written consent of A10 Networks, Inc. This information may contain forward looking statements and therefore is subject to change.

A10 Networks Inc. Software License and End User Agreement

Software for all AX Series products contains trade secrets of A10 Networks and its subsidiaries and Customer agrees to treat Software as confidential information.

Anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not:

1) reverse engineer, reverse compile, reverse de-assemble or otherwise translate the Software by any means

2) sublicense, rent or lease the Software.

Disclaimer

The information presented in this document describes the specific products noted and does not imply nor grant a guarantee of any technical performance nor does it provide cause for any eventual claims resulting from the use or misuse of the products described herein or errors and/or omissions. A10 Networks, Inc. reserves the right to make technical and other changes to their products and documents at any time and without prior notification.

No warranty is expressed or implied; including and not limited to warranties of non-infringement, regarding programs, circuitry, descriptions and illustrations herein.

Environmental Considerations

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

Further Information

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks, Inc. location which can be found by visiting www.a10networks.com.

End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING A10 NETWORKS OR A10 NETWORKS PRODUCTS, OR SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

A10 NETWORKS IS WILLING TO LICENSE THE PRODUCT (EX Series) TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, THEN A10 NETWORKS IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND DO NOT DOWNLOAD, INSTALL OR USE THE PRODUCT.

The following terms of this End User License Agreement ("Agreement") govern Customer's access and use of the Software, except to the extent there is a separate signed agreement between Customer and A10 Networks governing Customer's use of the Software

License. Conditioned upon compliance with the terms and conditions of this Agreement, A10 Networks Inc. or its subsidiary licensing the Software instead of A10 Networks Inc. ("A10 Networks"), grants to Customer a nonexclusive and nontransferable license to use for Customer's business purposes the Software and the Documentation for which Customer has paid all required fees. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) specifically pertaining to the product or products and made available by A10 Networks in any manner (including on CD-Rom, or on-line).

Unless otherwise expressly provided in the Documentation, Customer shall use the Software solely as embedded in or for execution on A10 Networks equipment owned or leased by Customer and used for Customer's business purposes.

General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and A10 Networks retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of A10 Networks, its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Accordingly, except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

a. transfer, assign or sublicense its license rights to any other person or entity, or use the Software on unauthorized or secondhand A10 Networks equipment
b. make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same

c. reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction

d. disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of A10 Networks. Customer shall implement reasonable security measures to protect such trade secrets.

Software, Upgrades and Additional Products or Copies. For purposes of this Agreement, "Software" and “Products” shall include (and the terms and conditions of this Agreement shall apply to) computer programs, including firmware and hardware, as provided to Customer by A10 Networks or an authorized A10 Networks reseller, and any upgrades, updates, bug fixes or modified versions thereto (collectively, "Upgrades") or backup copies of the Software licensed or provided to Customer by A10 Networks or an authorized A10 Networks reseller.

OTHER PROVISIONS OF THIS AGREEMENT:

a. CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE OR ADDITIONAL COPIES

b. USE OF UPGRADES IS LIMITED TO A10 NETWORKS EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LEASEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED

c. THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Term and Termination. This Agreement and the license granted herein shall remain effective until terminated. All confidentiality obligations of Customer and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement

Export. Software and Documentation, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software and Documentation.

Trademarks. A10 Networks, the A10 logo, ACOS, aFleX, aFlow, aGalaxy, aVCS, aXAPI, IDaccess, IDsentrie, IP-to-ID, SoftAX, Virtual Chassis, and VirtualN are trademarks or registered trademarks of A10 Networks, Inc. All other trademarks are property of their respective owners.

Patents Protection. A10 Networks products including all AX Series are protected by one or more of the following US patents and patents pending: 7716378, 7675854, 7647635, 7552126, 20090049537, 20080229418, 20080040789, 20070283429, 20070271598, 20070180101.

Limited Warranty

Disclaimer of Liabilities. REGARDLESS OF ANY REMEDY SET FORTH FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL A10 NETWORKS OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE PRODUCT OR OTHERWISE AND EVEN IF A10 NETWORKS OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

In no event shall A10 Networks' or its suppliers' or licensors' liability to Customer, whether in contract, (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim or if the Software is part of another Product, the price paid for such other Product.

Customer agrees that the limitations of liability and disclaimers set forth herein will apply regardless of whetherCustomer has accepted the Software or any other product or service delivered by A10 Networks. Customer acknowledges and agrees that A10 Networks has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

The Warranty and the End User License shall be governed by and construed in accordance with the laws of the State of California, without reference to or application of choice of law rules or principles. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement shall remain in full force and effect. This Agreement constitutes the entire and sole agreement between the parties with respect to the license of the use of A10 Networks Products unless otherwise supersedes by a written signed agreement.

About This Document

This document describes use of the A10 Networks EX Series Secure WAN Manager network appliances using its graphical user interface. Descriptions of all available options are provided, along with examples and other information useful in configuration and usage.

System Description

FIGURE 1 The EX Series Secure WAN Manager

The EX Secure WAN Manager provides the following major features:

- Identity Based Bandwidth Usage Reporting
- Identity Based Applications Logging and Reporting
- Bandwidth Management and QoS
- Link Load Balancing
- Firewall and Server Load Balancing
- Cache Redirection
- Network Intrusion Prevention
- Layer 3 support (RIP and OSPF)

- Transparent Layer 2 Connectivity Support
- High Availability Software and Hardware Redundancy

For more information, see "Major Features" on page 33.

Introduction

The EX Series Secure WAN Manager provides various types of interfaces for configuration and management:

- Serial interface (RS-232 port)
- Command Line Interface (CLI) accessible using Telnet or Secure Shell (version 1 or version 2)
- Graphical User Interface (GUI)

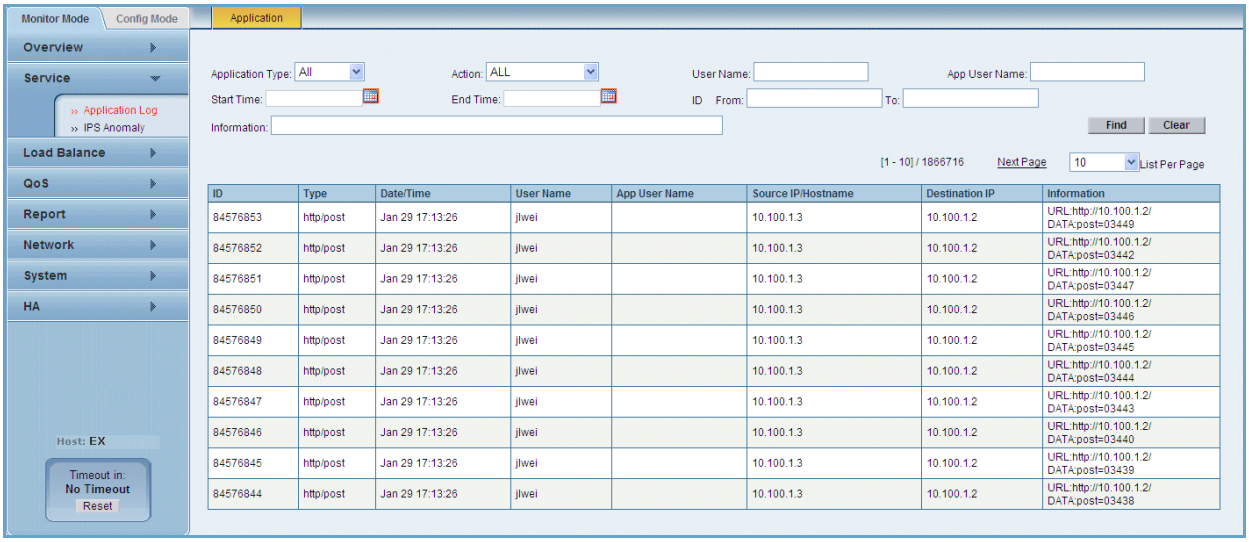
This guide describes the GUI.

The Graphical User Interface

The EX Series Secure WAN Manager GUI enables you to manage it with a Web browser. The GUI runs as a Web server on the EX appliance.

Figure 2 shows an example of the GUI. This is a page in the application log, which shows the QoS classes (applications) used in the traffic flowing through the EX appliance.

FIGURE 2 The EX Secure WAN Manager Graphical User Interface



The GUI consists of the following components:

- Module buttons – used to select a feature area (module) on the EX appliance
- Menu bars – move the cursor over a menu to view its sub-commands (note not all menus will have sub-commands)
- Main display area – where configuration is performed and management information is displayed

Save, Logout, and Help

The banner at the top of the GUI shows the hostname of the accessed EX Secure WAN Manager to the right of the A10 Networks logo. It also has the following option buttons:

- Save – Saves configuration changes in the running configuration to the startup configuration file. If the running configuration has unsaved changes, this button flashes red. Click to save the changes.
- Logout – Ends your Web GUI session and closes the browser window.
- Help – Displays online help. (See "Online Help" on page 31.)

Figure 3 shows the option buttons.

FIGURE 3 Banner with Save, Logout, and Help Buttons

Viewing Tips

On many workstations, you can use "ctrl + scroll-wheel" and "ctrl + +/-" to zoom the text displayed size within the browser.

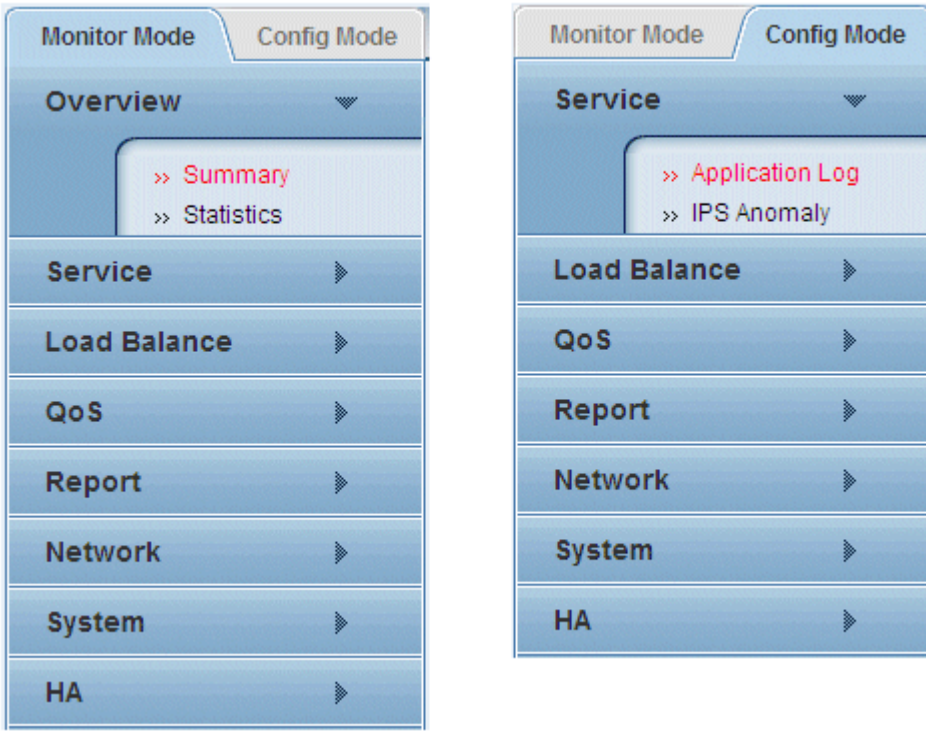
Browser add-ons and extensions are available with similar functionality, such as Image Zoom for Firefox.

Microsoft Windows users can use its Magnifier to enlarge screens, text and graphics in the GUI or in Help by selecting Start > Accessories > Accessibility > Magnifier. Other operating systems have similar features.

Module Buttons

The left panel has large buttons for selecting the main functional modules (features) of the EX Secure WAN Manager, as shown in Figure 4.

FIGURE 4 Module Buttons for Monitor Mode and Config Mode



The buttons appear on two tabs:

- Monitor Mode (left tab)
- Config Mode (right tab)

After you click a module button, hyperlinks to the options within that module are displayed. Click an option hyperlink to display the information or input fields for that option. The active hyperlink within a selected module appears in red text.

Note: Selecting a module button does not automatically select any options available under the button. The display area continues to contain the information for the previously selected option until you select a new option.

In this guide, paths used to navigate to a specific button and option are shown as follows: Mode > Button > Option

For example, to navigate to the application log screen shown in Figure 2, use the following path:

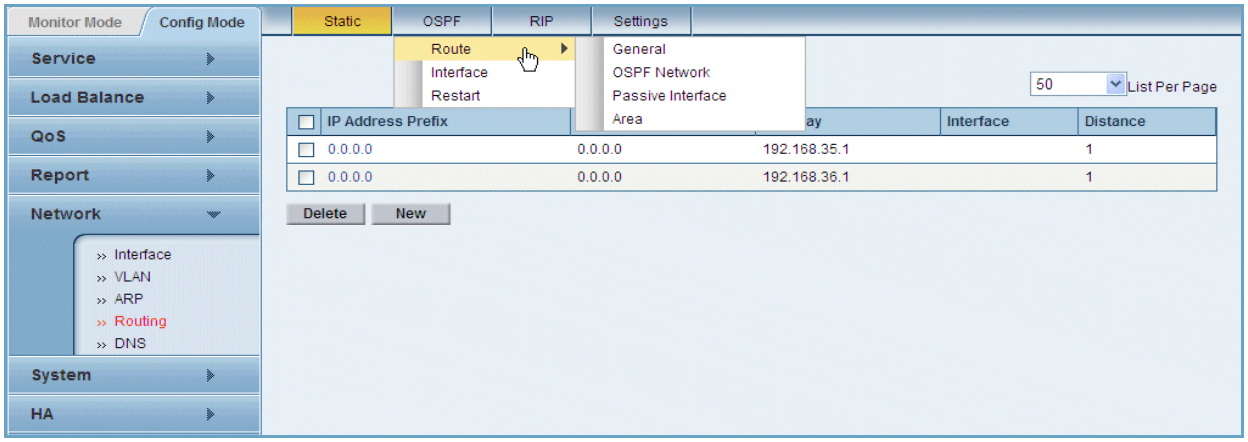
Monitor Mode > Service > Application Log

Menu Bar

The top panel contains the menu bar. Menus change depending on which module is active. Some menu options display tables or configuration tabs. Other menu options display pull-down menus of actions or of additional options. The active menu bar item is highlighted.

Figure 5 shows the menu bar for the Config Mode > Network > Routing option. In this example, the submenus under OSPF > Route are shown. (The module buttons and the display area containing the route table also are shown.)

FIGURE 5 Example Menu Bar



For simplicity, the paths for selecting actions or further options from a menu option are shown using the same nomenclature as used for options selected under a button. For example, to display the configuration tab for an OSPF network route:

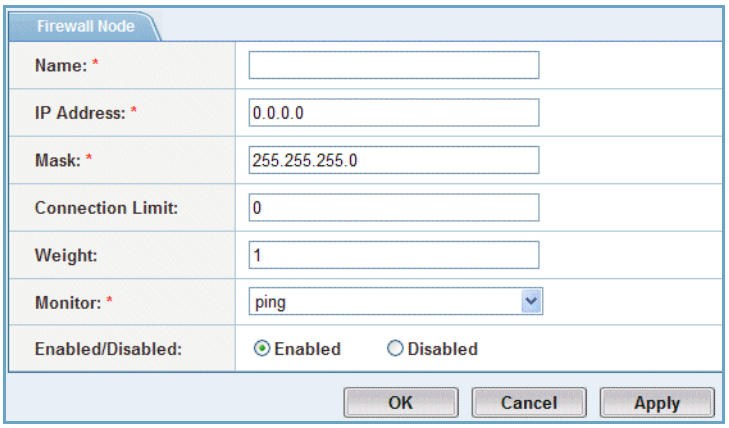
1. Select Config Mode > Network > Routing.

2. From the menu bar, select OSPF > Route > OSPF Network.

Configuration Tabs

The GUI uses tabs for configuration. A tab contains input fields for a configuration item. For example, you use a tab to configure settings for a firewall to be included in a load-balancing configuration. (See Figure 6.)

FIGURE 6 Example Configuration Tab



To display a configuration tab:

1. Select the Config option to access the tabular display for the configuration item.

2. Display settings for an item that is already configured, or display a tab for configuring a new item:

   - To display the configuration settings for an existing item, click on the item name. A configuration tab showing the item's settings is displayed.
   - To configure a new item, click the New button located under the table.

For example, to access the Firewall Node tab shown in Figure 6:

1. Select Config Mode > Load Balance > Firewall. A table listing the configured firewall nodes is displayed.

2. Click New.

Action Buttons

Most configuration tabs have the following action buttons:

- OK – Adds the new item to the EX appliance running configuration and re-displays the table that lists the configured items.

Note: This action does not save configuration changes. To save changes, you must write them to the startup configuration file. Select the Save option in the upper right corner of the EX appliance GUI window. (See "Save, Log-out, and Help" on page 18.)

- Cancel – Cancels configuration of the new item and re-displays the table that lists the configured items.
- Apply – Adds the new item to the EX appliance running configuration but leaves the configuration tab displayed. This option is useful when you want to configure more than one item and you do not need to verify configuration until the last item is configured.

Tabular Displays

Data and configured items are displayed in tables such as the ones shown in Figure 7 and Figure 8.

FIGURE 7 Example Tabular Display – Monitor

Name	Bytes		Packets		Connections		Status	Report
	Received	Sent	Received	Sent	Current	Total		
fw1	19.0K	21.6K	124	108	0	36	Running	
fw2	37.3K	65.2K	368	318	0	36	Running	

FIGURE 8 Example Tabular Display – Config

Name	IP Address/Mask	Connection Limit	Weight	Monitor	Enabled
fw1	192.168.10.2/24	0	1	ping	
fw2	192.168.10.3/24	0	1	ping	

Delete New

Generally, Monitor displays show statistics whereas Config displays show configuration information. Some Monitor displays also have a Report column, which contains icons you can click on to display graphs of the statistics. (See "Statistics and Graphs" on page 24.)

Each tabular display has columns that list the names of the configuration items. In some of the Config tabular displays, the names of the configuration items are hyperlinks. You can click on the name of a configuration item to display a configuration tab for the item. (See "Configuration Tabs" on

page 21.) You also can perform actions on configuration items by selecting the checkboxes next to the item names, then clicking an action button. (See "Action Buttons" on page 23.)

Action Buttons

Most tabular displays for configuration items have the following action buttons:

- New – Displays a configuration tab to add a new item. (Figure 6 on page 21 shows an example.)
- Delete – Deletes the selected configuration items. To perform this action, click on the checkboxes next to the items you want to delete, then click Delete.

These buttons are located under the table.

A few displays have other action buttons. These are described in the operational procedures in later chapters.

Action Icons

Action icons are small buttons for performing actions on items selected in a table. Table 1 shows the action icons used in the EX appliance GUI.

TABLE 1 Action Icons

Enable	Disable	View Report	Edit Report
			

You can display more information for an action icon by placing the cursor over the icon.

Navigation Controls

If a table has more items than can be displayed in a single page, the GUI displays page navigation controls.

FIGURE 9 Table Navigation Controls

The Summary Buttons (Start, Left, Right, and End) provide browser-like navigation through the pages of table rows.

The numbers in brackets indicate the entry numbers displayed on the current page. The number following the forward slash indicates the total number of entries that match the display criteria (display filters).

The List Per Page drop-down list specifies how many rows to display on a single page. You can select one of the following: 50, 10, 20, 100, Show All. The default is 50.

Display Filters

Many tables also provide options to filter the display to show only the entries you want to see. The Name field allows you to quickly find specific entries. To find a single entry, type the entire name string in the Name field and click Find.

To find multiple, similar entries, you can use a glob pattern, which is part of the name along with one or both of the following wildcards:

- ? – Matches on any single character.
- * – Matches on any string of characters.

When you click Find, the table is re-displayed showing only those entries that match the filter.

Note: The name of this field often is specific to the type of data or configuration items displayed. For example, on the list of QoS classes, the field is called Class Name.

Some displays have additional fields for filtering the display based on names or categories. For example, the Application Log (displayed by selecting Monitor Mode > Service > Application Log) has all the following fields for filtering the display:

- Application Type
- App User Name
- User Name
- Action
- Information
- Start Time
- End Time

For displays with additional fields, the operational procedures in later chapters describe the fields.

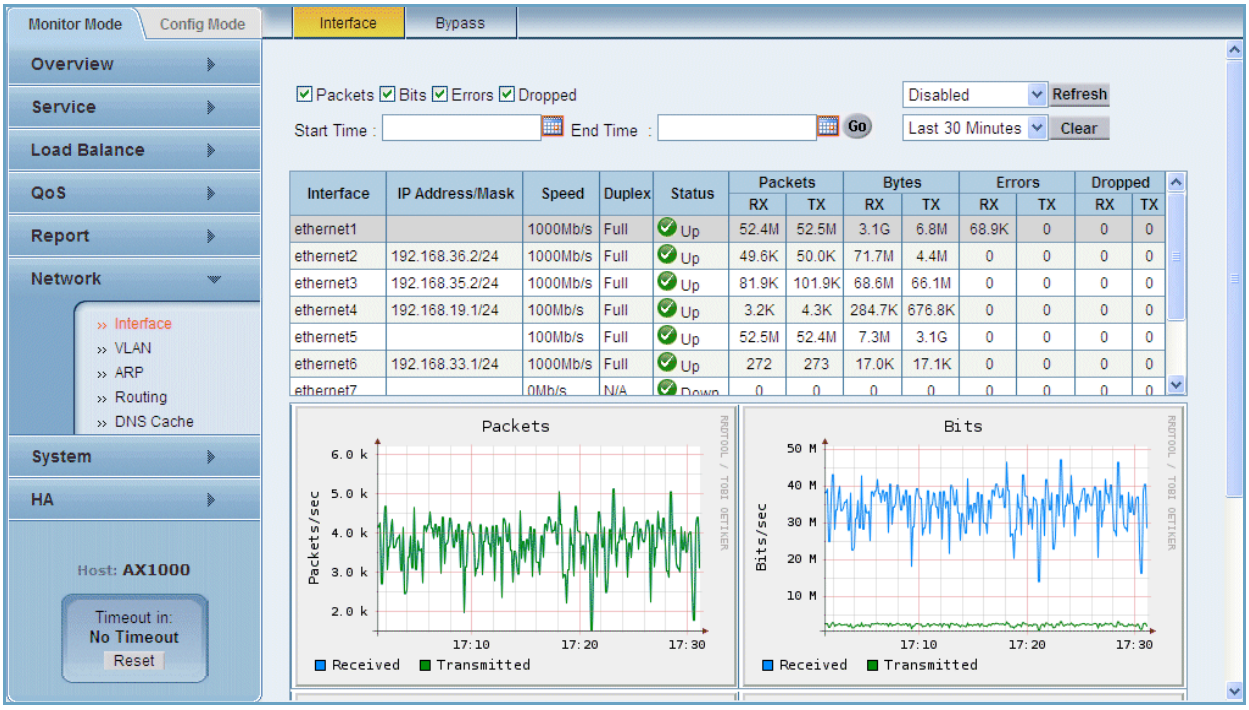
Statistics and Graphs

Statistics are available in both tabular and graph displays.

Interface Statistics

Figure 10 shows an example of the Interface statistics, which are displayed on the same page with both a table and graphs. To display them, select Monitor Mode > Network > Interface.

FIGURE 10 Interface Statistics Example



Load-Balancing and Traffic Statistics

Statistics for load-balancing and traffic features also are displayed in tables and graphs, but the tables and graphs are on separate pages. To display statistics in a table, select a Monitor option for Load Balancing or Traffic.

To display a graph, do one of the following:

- Select a Monitor option for Load Balancing or Traffic.

  Then, select Statistics > *option* on the menu bar, where *option* is the type of configuration item for which you want to display statistics.

- Click the click the icon in the Report column of a statistics table.

For example, to display statistics for a link group:

1. Select Monitor Mode > Load Balance > Link.
2. To display the statistics in a table, select Link Group on the menu bar.

3. To display the statistics in a graph, do one of the following:

- On the menu bar, select Statistics > Link Group.
- If the statistics are already displayed in a table, click on the following icon in the Report column: 

When graphs for a configuration item are displayed, you can easily select another item of the same type to graph. For example, if you are displaying graphs for a firewall group, you can select a different firewall group from the pull-down list at the top of the display.

Graph Display Options

You can modify the data refresh rate and the time span for statistics.

You also can disable or re-enable display of individual graphs. To disable display of a graph, click the check box next to the graph name to clear the checkbox. For example, to disable display of the Bytes graph in Figure 10, click the Bytes checkbox to clear it.

The other display options are described in the following sections.

Data Refresh

Statistics counters start incrementing from 0 after the most recent reboot or the most recent clear performed by an administrator.

To refresh the display with the latest counter values, click Refresh. You also can enable automatic refresh by selecting the refresh rate from the pull-down list next to the Refresh button. You can select one of the following refresh rates:

- 10 seconds
- 20 seconds
- 30 seconds
- 60 seconds
- 180 seconds
- 300 seconds
- Disabled

For example, to automatically refresh the counters once a minute, select 60 from the pull-down list. By default, automatic refresh is disabled.

To clear the counters, click Clear.

Time Span

The horizontal (x) axis of each graph shows the time span of the data in the graph. The same time span is used for all four graphs.

To change the time span, do one of the following:

- Select a new span from the pull-down list to the left of the Start Time field. The spans you can select range from 10 minutes to 30 days.
- Use the calendars to select specific start and end dates and times.

To select a date and time using the calendars:

1. Click  (the calendar icon) next to Start Time or End Time.

   (They must be selected separately.)

2. Select the month and year.
   - To scroll through years, click double brackets (<< or >>).
   - To scroll through months, click a single bracket (< or >).

3. Select the day of the month.

   To change the day of the week that starts each week, click the day (Mon, Tue, and so on).

4. Select the time. Place the cursor over the hours or minutes counter and do one of the following:
   - To select a later time, click on the hours or minutes counter to scroll forward.
   - To select an earlier time, hold Shift and click on the hours or minutes counter to scroll backward.

5. Click **x** in the upper right corner of the calendar to save the settings and close the calendar.

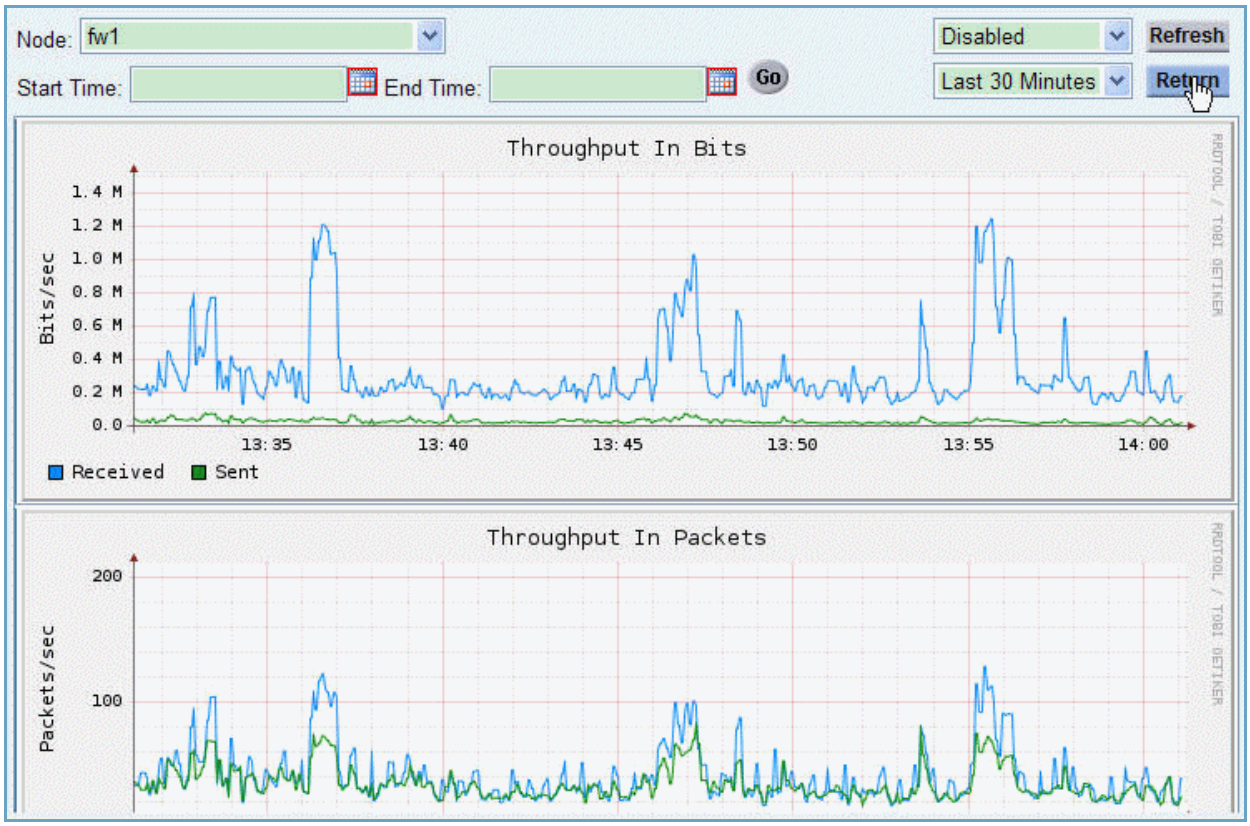
   The date and time you selected appear in the Start Time or End Time field.

6. Click Go to redraw the graphs using the new time span.

Return to the Tabular Display

The Statistics pages for Load Balancing and Traffic have a Return button. Click this button to return to the tabular display of the statistics.

FIGURE 11 The Return Button



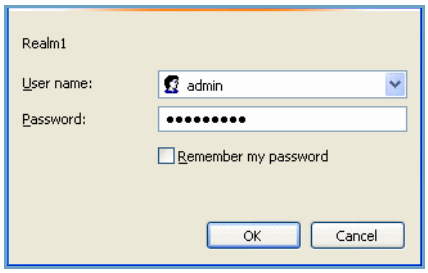
Login

To access the GUI:

1. In a Web browser, enter **https://***ip-addr*, where *ip-addr* is the IP address of the unit.

   A login dialog appears, as shown in Figure 12.
2. Enter a valid user name and password and click OK.
   - Default user name: **admin**
   - Default password: **a10**

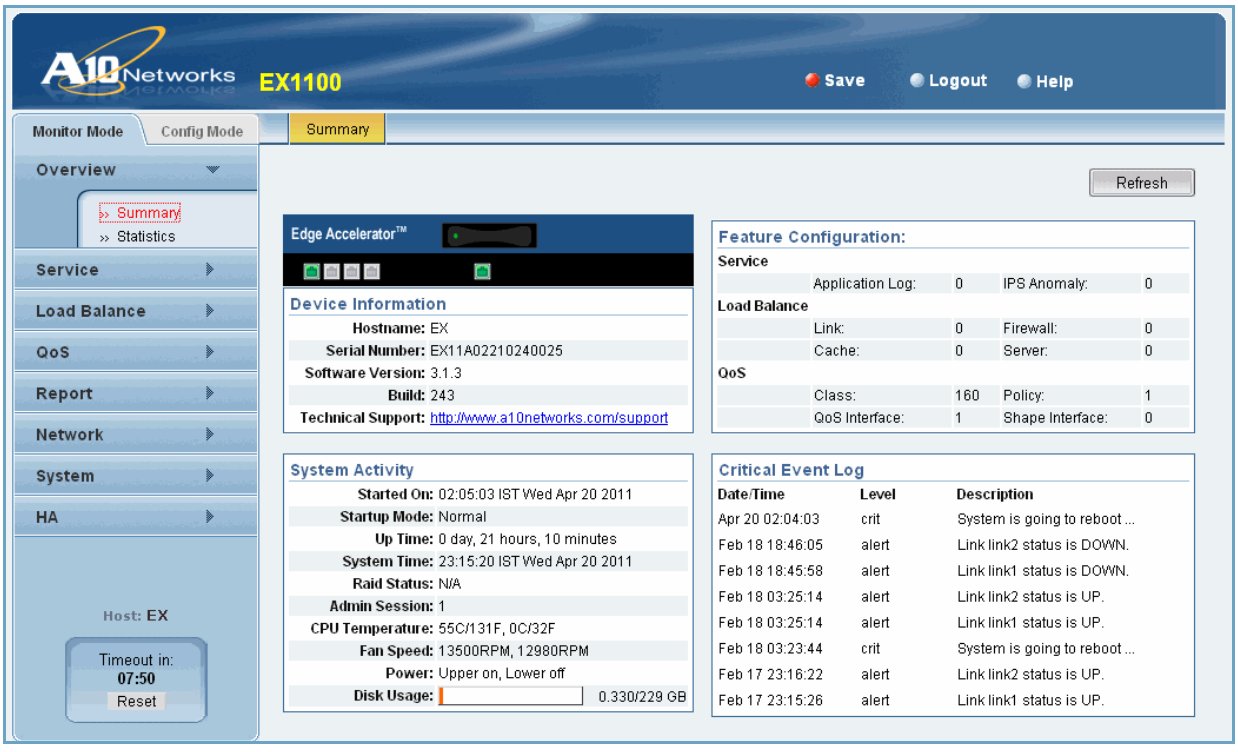
FIGURE 12 Login



Note: The EX Secure WAN Manager has a default admin user name and password. A10 Networks recommends that you change the admin name and password when you first deploy the switch, for obvious network security reasons. (See "Admin Accounts" on page 248.)

After successful login, the Summary screen is displayed, as shown in Figure 13. The Summary screen provides a high-level view of the EX appliance configuration and status.

FIGURE 13 Monitor Mode > Overview > Summary



(For more information about this screen, see "Display the System Summary" on page 261.)

Login Requirements

An IP address must be configured on the EX appliance and the browser must be able to reach the EX appliance over the network.

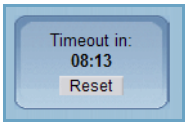
The EX Secure WAN Manager GUI has been tested with and is supported on the following Web browsers:

- Internet Explorer versions 6 and 7
- Firefox versions 1 (1.5.0.6), 2, and 3

Web Timeout

Web Timeout is used to prevent accidental blockage of the admin access. The timeout counter indicates the amount of time remaining before the GUI is automatically closed. The timeout counter is displayed in the Web Timeout window, which is located at the bottom left of the display.

FIGURE 14 Web Timeout window



To reset the timer, click the Reset button. Clicking any EX appliance button or menu option also resets the timer.

Caution: After the Web timer expires, the EX appliance ends the GUI session and closes the browser window. No warning or confirmation message appears. If you are configuring something, any unsubmitted configuration input data is lost. To submit configuration input data, click Apply or OK on the configuration page.

Online Help

The EX Secure WAN Manager provides online help. To access the help, click the Help button at the top right of the display. (See "Save, Logout, and Help" on page 18.)

The online help opens. You can select topics from the left-most column.

Deployment

This chapter describes the major product features and instructions to prepare the EX Secure WAN Manager for management access by the GUI.

Major Features

The EX Secure WAN Manager is a WAN optimization and load-balancing switch. The EX appliance enables you to manage precious WAN bandwidth with the following features:

- Identity based bandwidth usage reporting and applications logging. (See "Dynamic Identity-Management Integration" on page 243, "Reports" on page 177, "Traffic Information" on page 173, and "Display the Application Log" on page 46.)
- Traffic Monitoring and Logging – EX appliance monitors traffic and organizes it by class. You can log traffic and display statistics. (See "Application Log" on page 39.)
- Intrusion Prevention System (IPS) – EX appliance can detect, log, and take action against many types of intrusions. (See "IPS Anomaly Filters" on page 47.)
- Load Balancing – EX appliance can balance traffic across multiple WAN links based on a variety of criteria including Firewall Load Balancing (FWLB), Cache Load Balancing (CLB) and Server Load Balancing (SLB). (See "Load Balancing" on page 59.)
- Quality of Service – EX appliance provides rate limiting, rate shaping, and marking. (See "Traffic Analysis and Quality of Service" on page 123.)
- Layer 2 and 3 Support – EX appliance can operate as a Layer 2 or Layer 3 device, and supports multiple VLANs as well as RIP and OSPF routing. (See "Network Settings" on page 203.)
- System Management – EX appliance provides extensive management features including logging options, SNMP support, and admin access-control options. (See "System Settings" on page 237.)
- High Availability (HA) – EX appliances can be configured in pairs, with one unit providing service while the other operates in standby mode, ready to take over if the primary unit becomes unavailable. (See "High Availability" on page 267.)

Definition of *Connections*

Most EX Secure WAN Manager features, including the load-balancing features, operate based on connections. On the EX appliance, a *connection* is a set of packets that have the same protocol and address information. For example, a TCP or UDP connection consists of packets that have the same values for all the following:

- IP protocol (ex: TCP or UDP)
- Source IP address
- Source protocol port
- Destination IP address
- Destination protocol port

In general, the EX appliance makes QoS and load balancing decisions for the first packet in a new connection, and applies those same decisions to subsequent packets in the same connection.

Some features distinguish between inbound connections and outbound connections.

- *Inbound connection* – A connection is inbound if its first packet is received on an external EX appliance interface. An *external interface* is one connected to the Internet.
- *Outbound connection* – A connection is outbound if its first packet is received on an internal EX appliance interface. An *internal interface* is one connected to the private network.

A packet in a connection is a *forward packet* if it flows in the same direction as the first packet of the connection, while a *reverse packet* is a packet that flows in the reverse direction.

Provisioning the EX Secure WAN Manager

To prepare an EX Secure WAN Manager for configuration and management, perform the following tasks:

1. Configure IP connectivity.
2. Change the password for the admin account.
3. Set the system date, time, and timezone.

You must use a serial connection to the Command Line Interface (CLI) to configure IP connectivity. An IP connection is required in order for a browser to be able to log onto the EX appliance GUI. Other provisioning steps can be performed using the CLI or the GUI.

Configure IP Connectivity

Before you can use the GUI to access the EX Secure WAN Manager, you must use the CLI to configure an IP interface and, if needed, a default route. After you configure IP connectivity, you can use a Web browser to log in to the GUI and continue provisioning.

To configure an IP interface:

1. Attach a PC to the EX appliance serial interface.
2. Log on to the EX appliance CLI.
3. Configure the interface.

Note: To access the EX appliance CLI, the PC must have a terminal emulation application (for example, HyperTerminal).

Attach a PC to the EX Secure WAN Manager Serial Interface

1. Using the supplied RS-232 cable, connect the EX Secure WAN Manager RS-232 serial port to the PC's COM1 or COM2 port.
2. Power on the PC and EX appliance, if they are not already on.
3. On the PC, set the terminal emulation application to use the following modem settings:
   - for 9600 baud
   - 8-N-1 (8 bits - no parity - 1 stop bit)

   When the serial connection is established, the login prompt is displayed on the terminal.

Log In to the EX Secure WAN Manager CLI

1. Log in to the EX Secure WAN Manager with the default user name (*admin*) and password (*a10*).

```
login as: admin
Using keyboard-interactive authentication.
Password:a10
[type ? for help]
```

2. Enable the privileged EXEC level by typing **enable** and pressing the enter key. There is no default password (one can be assigned).

```
EX appliance>enable
Password:(press the enter key only)
EX appliance#
```

3. Enable the configuration mode by typing **config** and pressing enter.

```
EX appliance#config
EX appliance(config)#
```

Configure an IP Interface

Using the CLI, you can configure an IP interface to be a management interface, a data interface, or both.

Here are the CLI commands for configuring each the IP address.

1. In the factory default configuration, Ethernet port 4 has the IP address 192.168.1.10/24.

2. The admin can use either a console connection or use another PC with IP address 192.168.1.x/24, and connect the PC to Ethernet port 4

3. Assuming the admin wants to configure the IP address for Ethernet port 1, IP address 192.168.2.228 and 255.255.255.0, shown below, are only examples.

   - Note: Out of the box, Ethernet port 4 has the IP address 192.168.1.10/24. The admin can *not* assign IP address 192.168.1.x/24 to any port other than Ethernet port 4, unless the IP address on Ethernet port 4 is removed or changed to another subnet.

```
EX appliance(config)#interface ethernet 1
EX appliance(config-if:ethernet1)#ip address 192.168.2.228 /24
```

4. Verify the interface IP address change:

```
EX appliance(config-if:ethernet1)#show this
interface ethernet 1
 speedduplex auto
 ip address 192.168.2.228 255.255.255.0
 permit ssh http ping
```

Change the Admin Password

The EX Secure WAN Manager configuration contains an admin account by default:

- username: *admin*
- Password: *a10*

To ensure that you always have access to the device, this account cannot be deleted. However, you can change the password. A10 Networks recommends that you change the admin password as soon as possible to secure access to the device.

To change the admin password and configure other admin settings, select Config Mode > System > Admin.

(See "Admin Accounts" on page 248.)

Set the System Date, Time and Time Zone

Most of the statistics displayed in the GUI have time stamps. To ensure that the time stamps are accurate, set the system time and date.

To set time and date parameters, select Config Mode > System > Time.

(See "Configure Time Settings" on page 250.)

Service Options

This chapter describes how to configure and use the service options:

- Application Log
- IPS Anomaly Filters

Application Log

The application log lists usage events for the following chat, email, and file management applications:

- Chat applications:
  - AOL Instant Messenger (AIM)
  - Yahoo Instant Messenger (YIM)
  - MSN Messenger (MSNIM)
  - Tencent Instant Messenger (QQ)
- File management applications:
  - File Transfer Protocol (FTP)
  - Network File System (NFS)
  - Common Internet File System (CIFS)
- Email applications:
  - Post Office Protocol (POP3)
  - Simple Mail Transfer Protocol (SMTP)
- Web applications:
  - Hypertext Transfer Protocol (HTTP)

For each application, you can select specific actions to log. For example, you can enable logging of chat applications as well as any file transfers.

You also can configure archiving of application logs to a remote server, in one of the following formats: HTML, PDF, CSV, or XML.

Configure Application Logging

Application logging is connection-based. The EX Secure WAN Manager logs events for specific combinations of source and destination IP

addresses, applications, and actions. These criteria are defined by application log filters.

By default, no log filters are defined and therefore no application events are logged.

To enable application logging:

1. Configure an application log filter.
2. Optionally, configure an alias.
3. Select the applications to log.
4. Optionally, change selection of actions to log for individual applications.
5. Optionally, configure archiving of application logs to a remote server.

Configure an Application Log Filter

An application log filter contains a list of host or network IP addresses to either include or exclude for application logging purposes.

1. Select Config Mode > Service > Application Log.
2. On the menu bar, select Filter, if not already selected.
3. Click the New button. The Filter tab appears.
4. In the Name field, enter a name for the filter.
5. In the IP and Mask fields, enter an IP address and network mask.

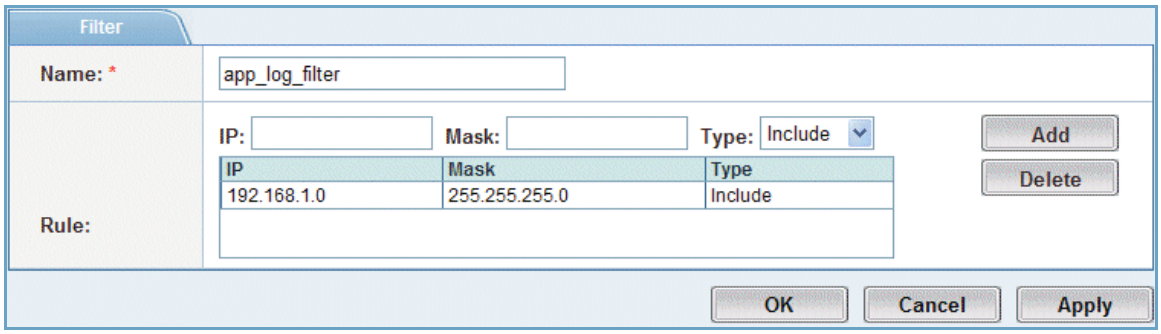
   You can enter an individual host address or a subnet address. The network mask indicates whether the address is for a host or a subnet.

   To filter on all IP addresses, enter IP: 0.0.0.0, Mask: 0.0.0.0.
6. From the Type pull-down list, select whether to include or exclude the address in the log.
7. Click Add.

   The address appears in the Rule list.
8. Repeat step 5 through step 7 for each address.
9. Click OK. The new filter appears in the filter table.
10. Go to "Configure an Alias" on page 41.

Figure 15 shows the Filter tab.

FIGURE 15 Config Mode > Service > Application Log – Filter Tab



Configure an Alias

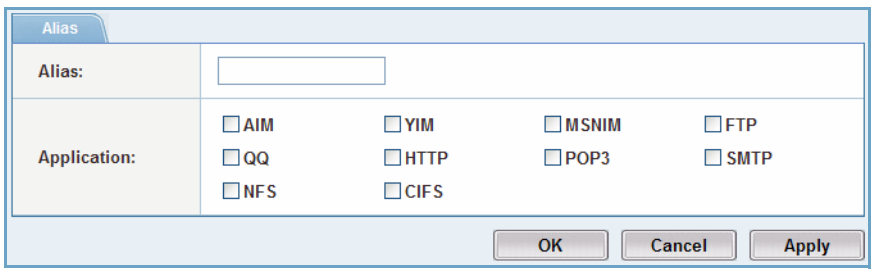
An alias is a string that represents a list of applications that can be logged. You can use aliases when configuring application logging. You also can use aliases to filter the display of application log entries.

To configure an application alias:

1. Select Config Mode > Service > Application Log if not already selected.
2. On the menu bar, select Alias.
3. Click the New button. The Alias tab appears.
4. In the Alias field, enter a string.
5. In the Application list, select the applications you want to map to the alias.
6. Click OK. The new alias appears in the alias table.
7. Go to "Select Applications To Log" on page 42.

Figure 16 shows the Alias tab.

FIGURE 16 Config Mode > Service > Application Log – Alias Tab



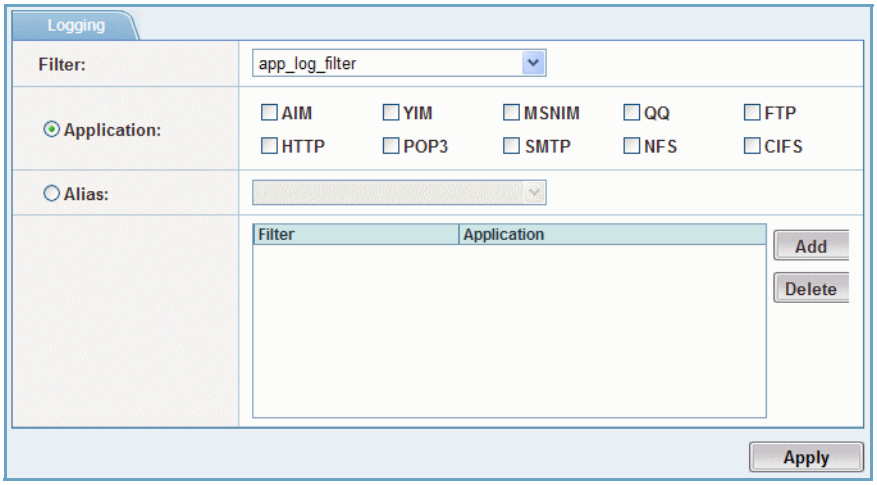
Select Applications To Log

By default, no applications are selected in a new application log filter. To select them:

1. Select Config Mode > Service > Application Log, if not already selected.
2. On the menu bar, select Logging. The Logging tab appears.
3. From the filter pull-down list, select the filter.
4. Select the applications to log:
   - To select individual applications, click on the checkboxes next to them in the Application list.
   - To select applications by selecting an alias, click the Alias radio button to activate the pull-down list. Select the alias from the list.
5. Click Add. The filter and application names or alias appear in the list.
6. Repeat step 3 through step 5 for each filter.
7. Click Apply.
8. Go to "Select Actions To Log" on page 43.

Figure 17 shows the Logging tab.

FIGURE 17 Config Mode > Service > Application Log – Logging Tab



Select Actions To Log

Most actions are logged by default. To view or change the set of actions to be logged, use the following procedure.

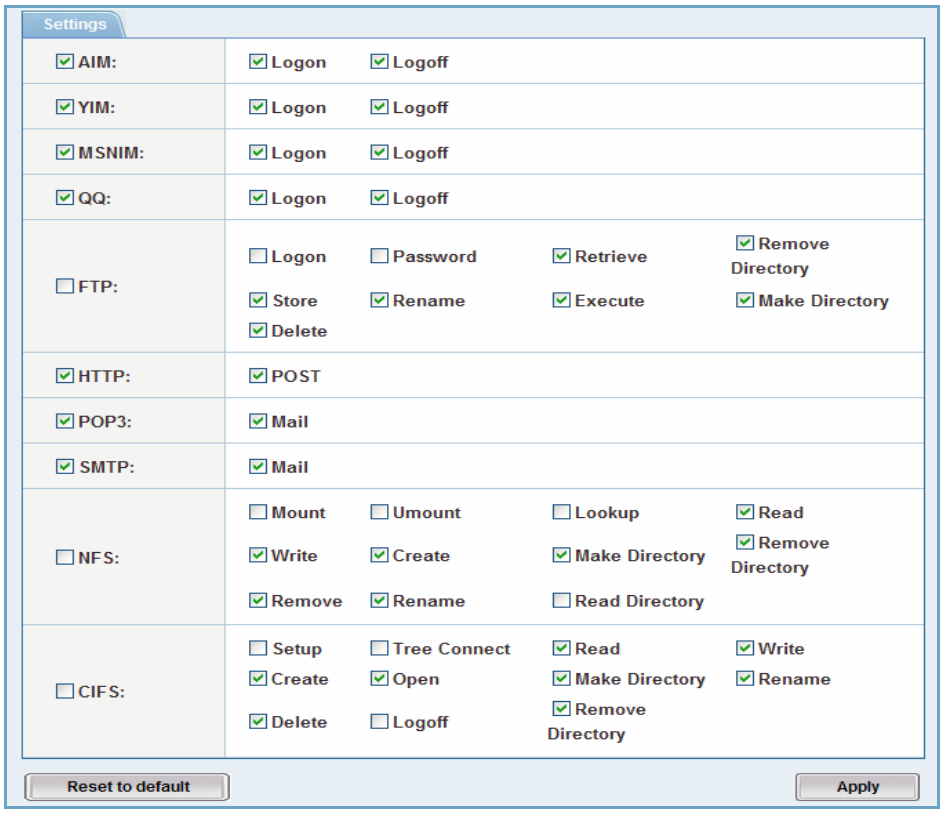
Note: Logging for specific actions is enabled or disabled on a global basis. If you disable or enable logging of a specific action, the change affects all application log filters that log the application that uses that action.

To display the list of logged actions or to change the actions to be logged:

1. Select Config Mode > Service > Application Log, if not already selected.
2. On the menu bar, select Settings. The Settings tab appears.
3. To globally disable or re-enable logging of an application, select or deselect the application.
4. To globally disable or enable logging of an action, select or deselect the action.
5. Click Apply.

Figure 18 shows the Settings tab.

FIGURE 18 Config Mode > Service > Application Log – Settings Tab



If you need to reset all the settings to their default values, click the Reset To Default button at the bottom of the tab.

Configure Archiving of Application Logs to a Remote Server

By default, when the application log buffer becomes full, the EX appliance discards the oldest entries to make room for new ones. To retain the discarded log entries, you can archive them to a remote server.

Application log archive files are named using the following convention:

`applog_archive-`*`yyyy-mm-dd-hh-mm-ss`*`.tar`

To display the list of logged actions or to change the actions to be logged:

1. Select Config Mode > Service > Application Log, if not already selected.

2. On the menu bar, select Archive. The Archive tab appears.

3. In the Application section, select the applications for which to archive logs. By default, all applications are deselected.

4. In the Protocol section, select the file transfer protocol and protocol port.

5. In the Host field, enter the IP address of the remote server.

6. In the Location field, enter the directory path for the remote server relative to the home directory for the file transfer protocol. For example, if the file transfer protocol is FTP and the FTP home directory is \FTPhome, leave " / " in the field to copy files to \FTPhome.

7. In the User and Password fields, enter the username and password for the administrator who has write access on the remote server.

8. To change the number of minutes between archive operations, edit the number in the Interval field.

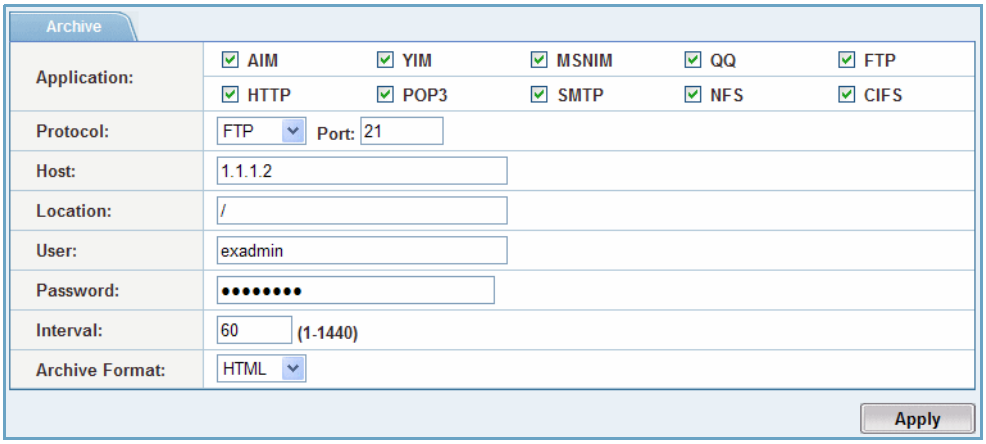
Note: Beginning in EX Release 3.0, archiving will only occur when the interval expires. Even without archiving, the most recent 1,000,000 application logs will not be lost.

9. Select the desired format from the Archive Format drop-down list:
   - HTML
   - PDF
   - CSV
   - XML

10. Click Apply.

Figure 19 shows the Archive tab.

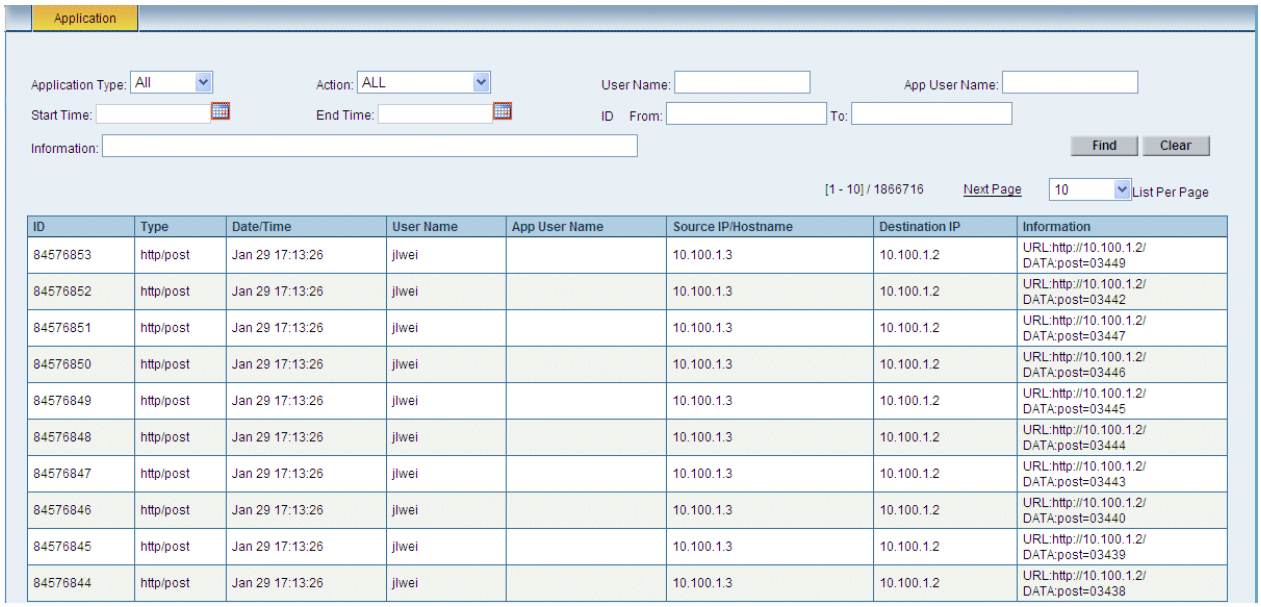
FIGURE 19 Config Mode > Service > Application Log – Archive Tab



Display the Application Log

To display the application log, select Monitor Mode > Service > Application Log.

FIGURE 20 Application Log



ID	Type	Date/Time	User Name	App User Name	Source IP/Hostname	Destination IP	Information
84576853	http/post	Jan 29 17:13:26	jlwei		10.100.1.3	10.100.1.2	URL:http://10.100.1.2/ DATA:post=03449
84576852	http/post	Jan 29 17:13:26	jlwei		10.100.1.3	10.100.1.2	URL:http://10.100.1.2/ DATA:post=03442
84576851	http/post	Jan 29 17:13:26	jlwei		10.100.1.3	10.100.1.2	URL:http://10.100.1.2/ DATA:post=03447
84576850	http/post	Jan 29 17:13:26	jlwei		10.100.1.3	10.100.1.2	URL:http://10.100.1.2/ DATA:post=03446
84576849	http/post	Jan 29 17:13:26	jlwei		10.100.1.3	10.100.1.2	URL:http://10.100.1.2/ DATA:post=03445
84576848	http/post	Jan 29 17:13:26	jlwei		10.100.1.3	10.100.1.2	URL:http://10.100.1.2/ DATA:post=03444
84576847	http/post	Jan 29 17:13:26	jlwei		10.100.1.3	10.100.1.2	URL:http://10.100.1.2/ DATA:post=03443
84576846	http/post	Jan 29 17:13:26	jlwei		10.100.1.3	10.100.1.2	URL:http://10.100.1.2/ DATA:post=03440
84576845	http/post	Jan 29 17:13:26	jlwei		10.100.1.3	10.100.1.2	URL:http://10.100.1.2/ DATA:post=03439
84576844	http/post	Jan 29 17:13:26	jlwei		10.100.1.3	10.100.1.2	URL:http://10.100.1.2/ DATA:post=03438

By default, entries for all applications are displayed. You can filter the display by selecting an application or alias from the Application Type pull-down list. You also can filter by user name, application user name, date, and information.

Note: An IDsentrie network appliance is required to provide the user names. (See "Identity-Management Integration" on page 242.)

IPS Anomaly Filters

The Intrusion Prevention System (IPS) detects and takes action against attempts to intrude upon or disrupt the network. IPS also can log the attempts and their origins in the EX Secure WAN Manager system log.

By default, IPS is disabled. You can enable IPS to check for the following types of intrusions:

- Invalid or suspect IP packet formations or options (sanity checks)
- TCP SYN floods
- ICMP, TCP, or UDP packet floods
- Address sweeps
- Excessive connection requests
- Protocol port scans
- ICMP attacks
- TCP or UDP protocol port numbers higher than a specified maximum

The IPS intrusions that the EX Secure WAN Manager can protect against are described in Table 2 on page 48.

TABLE 2 IPS Options

IPS Category	IPS Option	Description
Sanity Check[1]	IP Land	Protects against spoofed SYN packets containing the same IP address as the source and destination. Flooding a system with such empty connections can overwhelm the system, causing Denial of Service (DoS).
	TCP Syn Frag	Protects against floods of TCP SYN fragments. During this type of attack, the targeted host stores the fragments in order to reassemble them and presumably complete the connections. Eventually, the SYN fragments for uncompleted connections fill the host's memory buffer, causing the host to stop working properly. When this option is selected, matching packets are dropped by default. However, you can select one of the following responses instead: • Reset Client – Drops the packet, sends a reset to the client, and removes the session from the EX appliance session table. • Reset Server – Drops the packet, sends a reset to the server, and removes the session from the EX appliance session table. • Reset – Drops the packet, sends a reset to both the client and the server, and removes the session from the EX appliance session table. • Clear Session – drops the packet and removes the session from the EX appliance session table, but does not send a reset to either the client or the server.
	TCP Check Flag	Protects against TCP packets with the following flag settings, which typically are used by attackers for reconnaissance: • No flags set • FIN flag only • SYN and FIN flags • FIN with no ACK • FIN, SYN, and ACK When this option is selected, matching packets are dropped by default. However, you can select one of the following responses instead: • Reset Client – Drops the packet, sends a reset to the client, and removes the session from the EX appliance session table. • Reset Server – Drops the packet, sends a reset to the server, and removes the session from the EX appliance session table. • Reset – Drops the packet, sends a reset to both the client and the server, and removes the session from the EX appliance session table. • Clear Session – drops the packet and removes the session from the EX appliance session table, but does not send a reset to either the client or the server.
	ICMP Broadcast Echo Request	Protects against ICMP echo requests sent to a subnet broadcast address. Echo replies from hosts in the network can be used by an attacker to gather information about the network.

TABLE 2 IPS Options (Continued)

IPS Category	IPS Option	Description
Sanity Check (cont.)	UDP Broadcast Echo Request	Protects against UDP echo requests sent to a subnet broadcast address. Echo replies from hosts in the network can be used by an attacker to gather information about the network.
	ICMP Broadcast	Protects against ICMP broadcast packets, which are used by attackers for reconnaissance of target networks and hosts.
	IP Record Route Option	Protects against packets that record the route used to forward them. Attackers can use route information to learn about the address scheme and topology of a target network.
	IP Strict Source Route Option	Protects against packets that specify each hop to use for forwarding to the destination. Attackers can use information in messages sent by routers to learn about the address scheme and topology of a target network.
	IP Security Option	Protects against packets containing the IP security option, which is obsolete. Because the option is no longer used, packets containing the option are most likely from malicious sources.
	IP Loose Source Route Option	Protects against packets that specify an IP address that must be used as one of the hops to reach the destination. Attackers can use information in messages sent by routers to learn about the address scheme and topology of a target network.
	IP Option	Protects against all packets containing any IP option.
	IP Malformed Option	Protects against packets with incomplete or malformed options in the header. This type of packet is always invalid and should not be forwarded.
	IP Timestamp Option	Protects against packets that use the timestamp option. This option is rarely used, therefore its presence can indicate a malicious source.
	IP Stream Option	Protects against packets that use the stream option. This option is obsolete, therefore its presence can indicate a malicious source.
	IP Fragment	Protects against fragmented packets. Fragmented packets can be used to attack hosts running IP stacks that have known vulnerabilities in their fragment reassembly code.

TABLE 2 IPS Options (Continued)

IPS Category	IPS Option	Description
TCP Syn Flood	TCP Syn Flood	Enables transaction rate limiting to protect against TCP SYN floods. An attacker causes a TCP SYN flood by sending TCP SYN (connection) requests to a host faster than the host can acknowledge them, causing DoS on the host. Generally, the source IP address of the TCP SYN packets is spoofed. To configure TCP SYN protection, you specify the following: • Threshold – Maximum number of TCP SYN packets to the same destination IP address that are allowed within the specified interval. If this number or more TCP SYN packets are received for the same destination within the interval, the EX appliance creates a SYN cookie. • Interval – Number of milliseconds during which that number of TCP SYN packets specified by one less than the threshold value are allowed for the same destination IP address. • Action – Specifies whether TCP SYN floods are logged in the IPS Anomaly log.
Flood	ICMP Flood TCP Flood UDP Flood	Protects against ICMP echo floods, TCP packet floods, and UDP packet floods. These types of attacks slow down target systems. To configure flood protection, select ICMP, TCP, or UDP and specify the following. (Flood protection is individually configurable for each packet type.) • Threshold – Maximum number of ICMP echo, TCP, or UDP packets to the same destination IP address that are allowed within the specified interval. • Interval – Number of milliseconds during which the number of ICMP echo, TCP, or UDP packets specified by the threshold are allowed for the same destination IP address. Within interval, (threshold -1) packets are allowed to pass. • Hold Time – Number of seconds to withhold ICMP echo, TCP, or UDP packets addressed to the destination, after the threshold is exceeded. ICMP echo, UDP or TCP packets addressed to the destination are dropped during the hold period. • Action – Specifies whether packet floods of the specified type are logged in the IPS Anomaly log.

TABLE 2 IPS Options (Continued)

IPS Category	IPS Option	Description
Address Sweep	ICMP UDP	Protects against reconnaissance attempts using ICMP or UDP sweeps. An ICMP sweep is a series of ICMP echo requests sent to a range of IP addresses. When a host replies to the request, this confirms the host's IP address to the hacker. Similarly, a UDP sweep is a series of UDP packets from the same source but to different IP addresses, within the specified interval. Because this traffic pattern is unusual, it is considered to be a signature of reconnaissance for an attack. If the EX appliance receives more than 5 ICMP echo or UDP packets from the same source to different destinations, within the specified interval, the EX appliance drops further ICMP echo or UDP packets from that source for the period specified by the hold time. To configure address sweep protection, select ICMP or UDP and specify the following. (Address sweep protection is individually configurable for each packet type.) • Interval – Number of milliseconds during which no more than 5 ICMP echo or UDP packets are allowed from the same source to different destinations. The threshold is 6 packets and cannot be configured. • Hold Time – Number of seconds to withhold ICMP echo or UDP packets from the same source, after the threshold is exceeded. ICMP echo or UDP packets from the same source are dropped during the hold period. • Action – Specifies whether address sweeps of the specified type are logged in the IPS Anomaly log.

TABLE 2 IPS Options (Continued)

IPS Category	IPS Option	Description
Exceed Rate	Source Destination	The exceed rate is calculated by the session. If a single source connects to a single destination several times, there are more than one sessions, and this can be considered as the exceed rate. This provides traffic rate limiting to protect against attacks such as Distributed DoS (DDoS) attacks and mass distribution attacks such as the Nimda virus. During a DDoS attack, the same destination IP address receives an unusually high number of connection requests at the same time from different source IP addresses or ports. Similarly, mass distribution of connections from the same source to multiple destinations can indicate an attack. To configure traffic rate limiting, select Source or Destination and specify the following. (Source and destination traffic rate limiting are individually configurable.) • Threshold – Maximum number of connections from multiple sources to the same destination, or from a single source to multiple destinations, that are allowed within the specified interval. • Interval – Number of milliseconds during which the number of connections specified by the threshold are allowed. Within interval, (threshold - 1) connections are allowed. • Hold Time – Number of seconds to withhold new connections after the threshold is exceeded. Connection attempts are dropped during the hold period. • Action – Specifies whether this type of anomaly is logged in the IPS Anomaly log.
Port Scanning	Port Scanning	Protects against reconnaissance attempts using protocol port scans. During a port scan, an attacker sends a series of packets with the same source and destination IP addresses, but to different TCP or UDP ports. An attacker can determine the applications that are running on the destination host based on its replies to the packets. To configure protection against protocol port scans, specify the following: • Interval – Number of milliseconds during which no more than 6 TCP or UDP ports can be addressed in packets from the same source and addressed to the same destination IP address. The threshold is 6 packets and cannot be configured. • Hold Time – Number of seconds to withhold further TCP or UDP packets with the same pair of source and destination IP addresses, after the threshold is exceeded. TCP or UDP packets with the same IP address pair are dropped during the hold period. • Action – Specifies whether protocol port scans are logged in the IPS Anomaly log.

TABLE 2 IPS Options (Continued)

IPS Category	IPS Option	Description
ICMP Attacks	Ping of Death	Protects against jumbo IP packets longer than the maximum valid IP packet size (65535 bytes). Packets longer than 65353 bytes can cause DoS, with symptoms such as halting or restarting on the target host. Generally, this type of attack occurs in conjunction with fragmented packets, where the attacker sends the last fragment with an offset such that the ping packets are longer than 65535 bytes, causing 16-bit variables to overflow.
	Type/Code	Specifies the valid ranges of ICMP type and code values. Some combinations of ICMP type and code (subtype) that can be used to gain information about a host or network. Attackers can use the information to attack the network. For example, an ICMP timestamp message (type 13) elicits a timestamp reply from Unix systems, but not from Microsoft systems, therefore indicating to the attacker the types of systems in the network. If the type or the code in the packet is larger than the configured Type/Code, the packet will be dropped. Those packets for which type and code are both smaller than the configured Type/Code, are allowed to pass.
IP Max Protocol-Known		Logs all packets whose protocol numbers are higher than the specified maximum number.

1. For all Sanity Check options, when the option is enabled, packets that match the option are dropped and logged by default.

Configure Intrusion Prevention System (IPS)

By default, no IPS anomalies are detected or logged. To configure IPS:

1. Configure an IPS group (optional - a default group can also be used).
2. Bind the group to one or more of the EX Secure WAN Manager switch's ethernet interfaces.

An IPS group takes effect only when you bind it to an interface. An interface can be bound to only one IPS group.

Configure an IPS Group

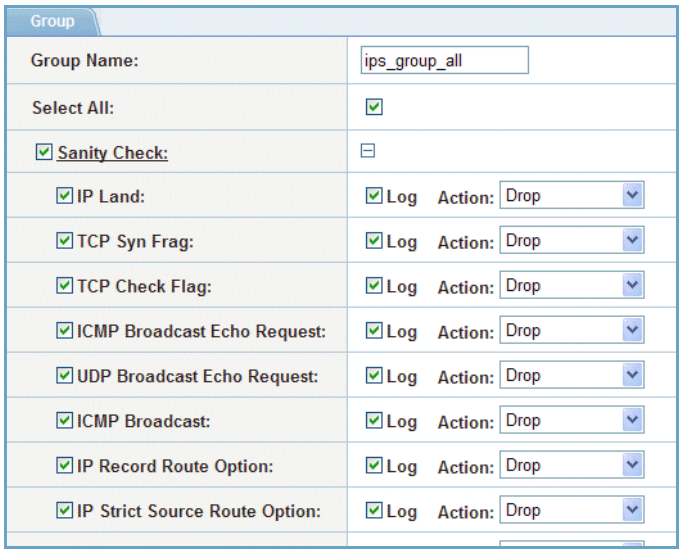
1. Select Config Mode > Service > IPS Anomaly.
2. On the menu bar, select Group, if not already selected.
3. Click the New button. The Group tab appears.

4. In the Name field, enter a name for the IPS group.
5. Select the IPS anomalies to counteract and log.
   - To select all IPS anomalies, use the Select All checkbox.
   - To select a subset of anomalies, use the checkbox next to each one.

   Most anomalies have configurable options.

   (For information on anomalies and their configurable options, see Table 2 on page 48.)
6. Click OK. The new IPS group appears in the IPS group table.
7. Go to "Bind an IPS Group to an Interface" on page 54.

FIGURE 21 Config Mode > Service > IPS Anomaly – Group Tab



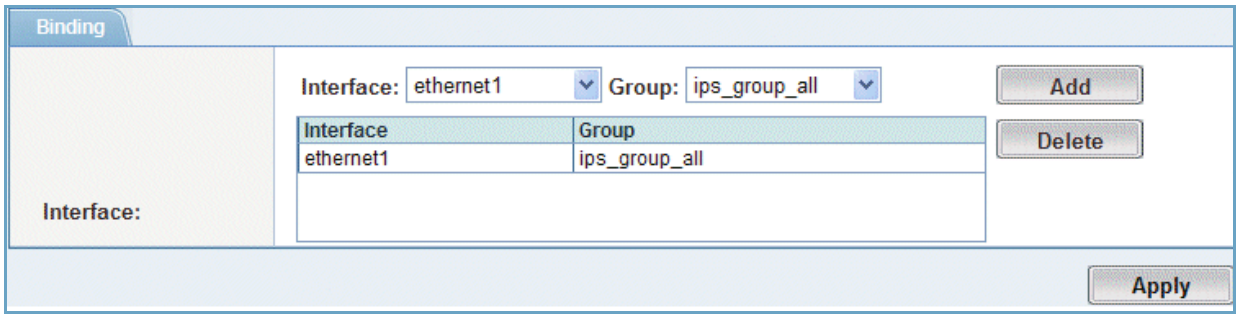
Bind an IPS Group to an Interface

1. Select Config Mode > Service > IPS Anomaly, if not already selected.
2. On the menu bar, select Binding.
3. From the Interface pull-down menu, select one of the EX Secure WAN Manager ethernet interfaces.
4. From the Group pull-down menu, select an IPS group.
5. Click Add.
6. Repeat step 3 through step 5 for each additional interface.

7. Click Apply. The IPS group immediately takes effect on the interfaces you selected.

Figure 22 shows the Binding tab.

FIGURE 22 Config Mode > Service > IPS Anomaly – Binding Tab



Display IPS Anomaly Statistics

To display IPS anomaly statistics, select Monitor Mode > Service > IPS Anomaly.

Display IPS Anomaly Log Entries

IPS anomalies are logged in the EX Secure WAN Manager system log.

Note: For an IPS anomaly to be logged, logging must be enabled for the anomaly. To verify whether logging is enabled for an anomaly, display the IPS groups in which detection of the anomaly is enabled.

To display IPS anomaly log entries:

1. Select Monitor Mode > Service > IPS Anomaly.
2. On the menu bar, select IPS Log.

To filter the list:

1. To filter based on log message text, enter the text string in the Description field.
2. To filter based on message date, use the Start Time and End Time fields to specify the date range.
   a. Click the calendar icon next to Start Time to select the start date and time.
   b. To specify the end date and time, click the calendar icon next to End Time to select them.
3. Click Find.

To export the IPS log:

1. Click Export. The browser displays a file management dialog.
2. Click OK (Firefox) or Save (Internet Explorer), navigate to the save location, and click Save.

To clear the log, click Clear.

Hold an IP Address

You can configure the EX Secure WAN Manager to drop all traffic from a specific host or subnet IP address. Optionally, you also can log the dropped traffic.

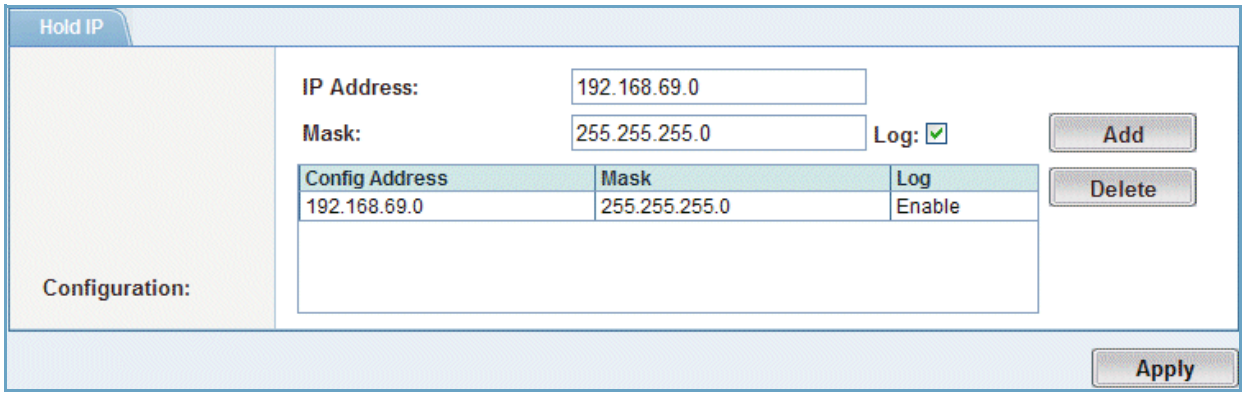
To hold traffic:

1. Select Config Mode > Service > IP Anomaly.
2. On the menu bar, select Hold IP. The Hold IP tab is displayed.
3. In the IP Address and Mask fields, enter the host or subnet address you want to hold. All traffic from the held address is dropped.
4. To generate a log entry when traffic from this address is dropped, select Log.
5. Click Add.
6. Repeat step 3 though step 5 for each host or subnet address to hold.
7. Click Apply.

If you enable logging, the EX appliance generates IPS log entries for held IP addresses. To simplify management, events for held IP addresses are summarized and logged once a minute per source IP address.

Figure 23 shows the Hold IP tab.

FIGURE 23 Config Mode > Service > IPS Anomaly – Hold IP Tab



Load Balancing

This chapter describes the load-balancing features, how to configure them, and how to monitor their operation.

Types of Load Balancing

The EX Secure WAN Manager can perform the following types of load balancing:

- Link Load Balancing (LLB) – Traffic is distributed among multiple WAN links.
- Firewall Load Balancing (FWLB) – Traffic is balanced among a group of firewalls.
- Cache Load Balancing (CLB) – Traffic is redirected to one or more cache switches and balanced among them.
- Server Load Balancing (SLB) – Traffic addressed to a virtual IP address is balanced among a group of real servers.
- Trunk load balancing (link aggregation) – Traffic is load balanced across a set of physical Ethernet interfaces based on the selected load-balancing method.

To configure load balancing, you configure individual links (for LLB) or nodes (FWLB, CLB, SLB), and then configure groups to define how traffic will be balanced among those links or nodes.

You also can configure health monitors to regularly verify the availability of links, servers, or individual applications.

Link Load Balancing

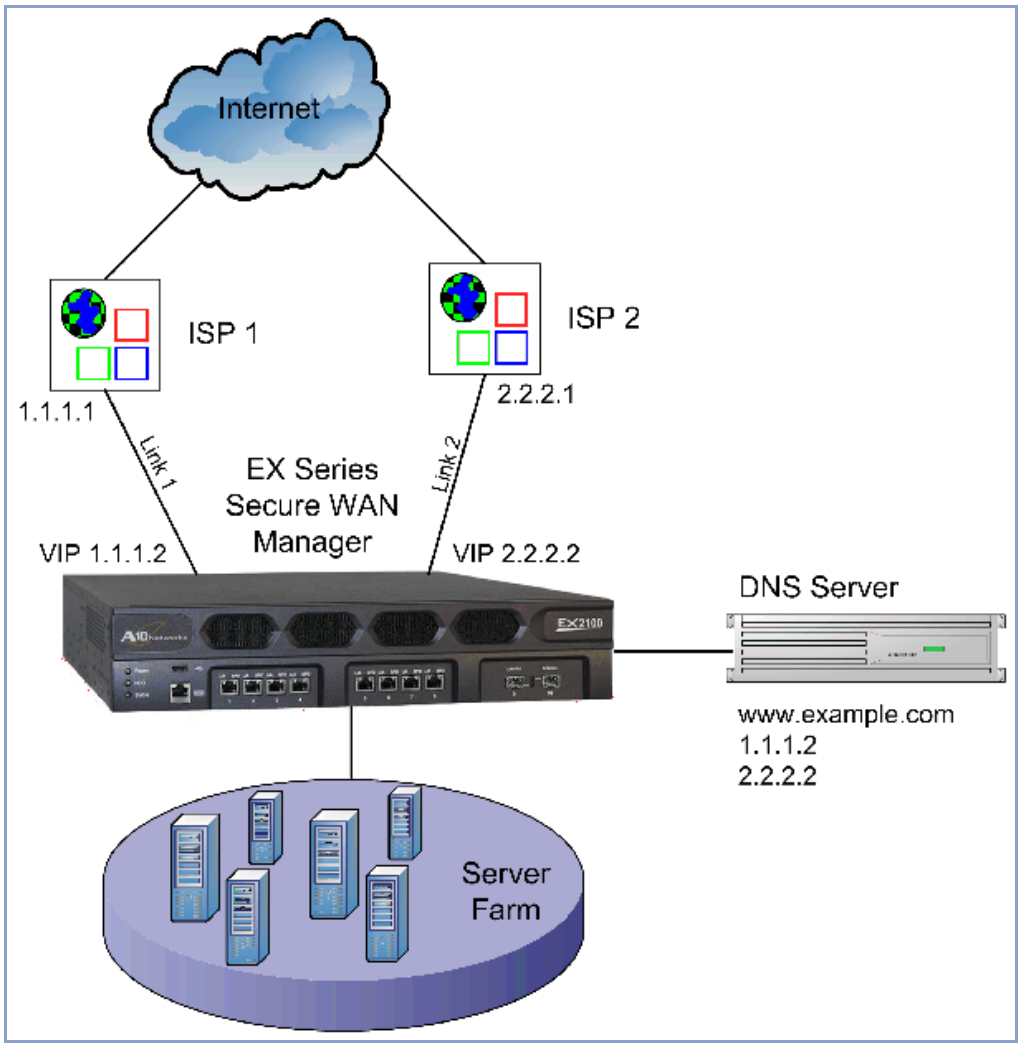
The EX Secure WAN Manager can balance traffic loads across groups of logical WAN links. The strategies used to perform the load balancing differ for inbound and outbound traffic.

Note: The Link Load Balancer (LLB) should have a direct connection to the gateway. This means the LLB should be either directly connected to the interface of the EX appliance or should be connected through a Layer 2 switch – a Layer 3 router will not suffice.

Inbound LLB

When inbound link load balancing is configured, the EX Secure WAN Manager receives connection requests from the public Internet. These requests for services on the internal network (shown as the Server Farm in Figure 24 below) are load balanced across the two available ISP links.

FIGURE 24 Inbound LLB



In this example, two virtual IP addresses (VIPs) are configured on the EX appliance: 1.1.1.2 and 2.2.2.2.

Each VIP corresponds to a link (Link 1 or Link 2), and both VIPs refer to the same server farm on the internal side of the EX appliance.

Services are provided by the server farm. Clients can access these services over the Internet via the domain name: *www.example.com*. The DNS server resolves the domain name into the two VIPs, 1.1.1.2 and 2.2.2.2.

To perform inbound LLB, the EX appliance monitors the reverse part of inbound DNS connections (on UDP port 53).

The DNS server resolves the domain name to a link group on the EX appliance. Inbound traffic arrives at the EX appliance, where the device chooses one of the links within the link group, (which in our example has only two links). This link selection process is based upon the load balancing algorithm chosen by the administrator.

The EX appliance then re-orders the IP addresses in the DNS reply to place the one that corresponds to the selected link on the top of the IP address list. Subsequent requests from the client will use the selected link based on the modified DNS reply.

Note: The DNS LLB method requires the DNS traffic to and from the client to pass through the EX appliance. If the DNS server is in the same internal network as the servers the client is trying to access (as shown in Figure 24), you only need to bind the domain name to the LLB group.

If the DNS server is not in the internal network, you can configure the EX appliance to act as a proxy for the DNS server for the domain to be load balanced. In this case, a client DNS request for the domain is sent to the EX appliance, which sends the request to the DNS server. When the EX appliance receives the reply from the DNS server, it sends a reply to the client. If required by LLB, the EX appliance re-orders the IP addresses in the reply before sending the reply to the client.

Alternate Subnets

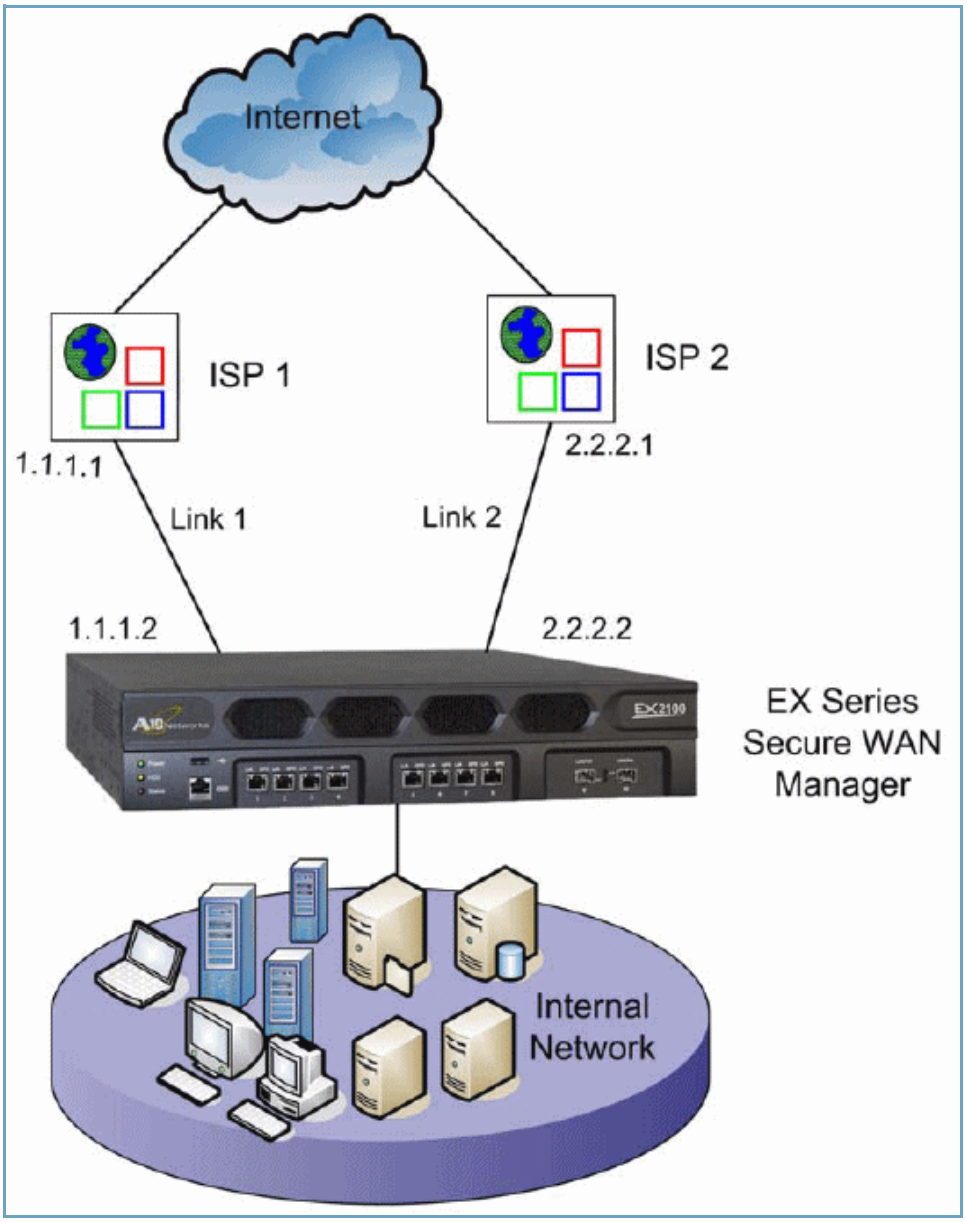
To load balance inbound traffic for content servers that are not in the same subnets as the EX appliance's LLB links, you can use alternate subnets. When you configure an alternate subnet address on an LLB link, the EX appliance will use the link for inbound client traffic sent to the alternate subnet. Without alternate subnets, the EX appliance load balances client traffic addressed to the subnets the LLB links are in.

You can configure a maximum of 8 alternate subnets on each LLB link.

Outbound LLB

For outbound traffic, from the private network to the Internet, the EX Secure WAN Manager selects a link based on the load-balancing algorithm enabled for the link group. For example, if the round robin algorithm is enabled, the EX appliance simply selects the next link in the group. Figure 25 shows an example outbound LLB configuration.

FIGURE 25 Outbound LLB



A connection qualifies for outbound LLB if both the following conditions are true:

- The next hop of the first packet is one of the links configured on the EX appliance.

  For a Layer 2 (bridged) packet, the next hop is identified by the destination MAC address. For a Layer 3 (routed) packet, the EX appliance looks in its IP route table for the next hop.

- The packet's destination IP address is not in the link's neighborhood.

  An IP address is in a link's neighborhood if the address is within the subnet identified by the IP address and network mask configured on the link.

To perform outbound LLB, the EX appliance does the following:

- Selects a link group based on the result of QoS classification of the first packet of a new connection.
- Selects a link within the group based on the load-balancing algorithm.
- Makes the link persistent for the connection. You can configure LLB sessions to persist based on source IP address or destination IP address.
  - Source-IP persistence – After the EX appliance uses the load-balancing algorithm to select a link for the first packet of a session, the EX appliance uses the same link for all subsequent packets *from* the same IP address. Typically, source-IP persistence is used to accommodate websites that hold state information. Otherwise, a client behind a firewall might use different links to the same site, preventing the web application from working correctly.
  - Destination-IP persistence – After the EX appliance uses the load-balancing algorithm to select a link for the first packet of a session, the EX appliance uses the same link for all subsequent packets *to* the same IP address.

Session Persistence

Source-IP persistence is recommended, if allowed by your deployment. However, if the EX appliance is placed after a firewall that acts as a NAT gateway, all outbound traffic comes from a single source IP address. LLB will always select the same link for all traffic, defeating the purpose of LLB. You can use destination-IP persistence instead.

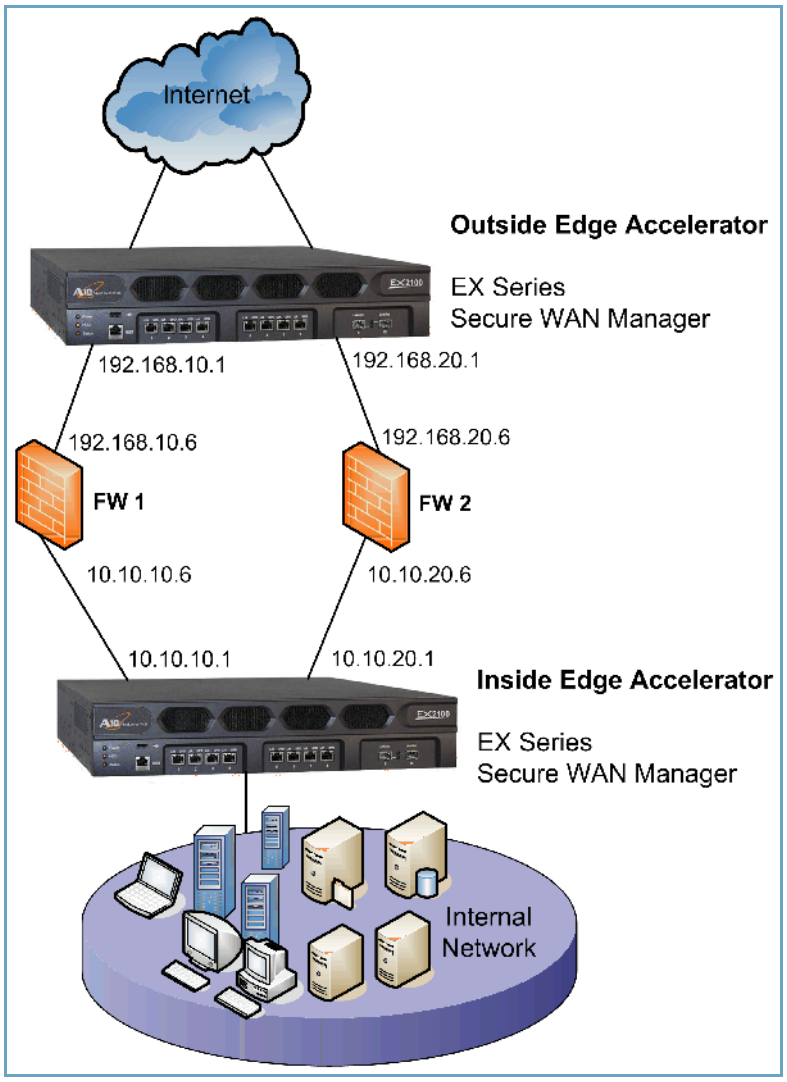
Destination-IP persistence helps maintain use of the same link to the same destination, allowing web applications to continue to work properly even though the client IP addresses are hidden by NAT.

For both types of persistence, a persistent link selection ages out after a configurable period.

Firewall Load Balancing (FWLB)

A pair of EX Secure WAN Manager devices, one deployed on each side of a group of firewalls, can load balance sessions through those firewalls. Figure 26 shows an example of FWLB topology.

FIGURE 26 Firewall Load Balancing (FWLB)



Note: FWLB requires the firewalls to be directly connected to the EX appliance. The firewalls can not be separated from the EX appliance by a router but they can be separated by a Layer 2 switch.

FWLB is performed using a pair of EX appliance units:

- Inside EX Secure WAN Manager – This load balances outbound connections across the firewalls.
- Outside EX Secure WAN Manager – This load balances inbound connections across the firewalls.

To perform inbound or outbound FWLB, the EX appliance does the following:

- Selects a firewall group based on the result of QoS classification of the first packet of a new connection.
- Selects a firewall node (a firewall) within the group based on the load-balancing algorithm.

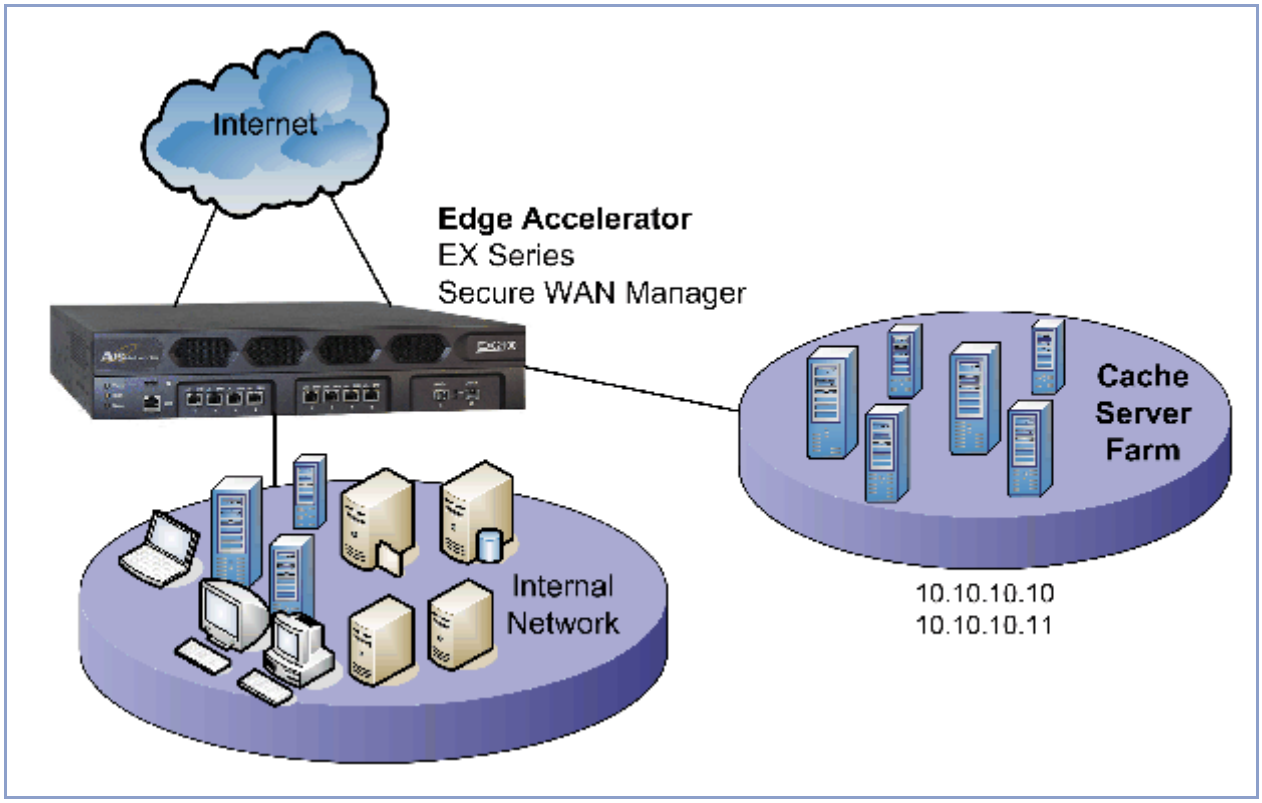
You can configure the EX appliance to use the same firewall for subsequent packets to or from a given IP address, by enabling persistence. Sessions are persistent based on source IP address or destination IP address, depending on configuration. A persistent firewall selection ages out after a configurable period.

Cache Load Balancing (CLB)

Cache Load Balancing (CLB) enables you to redirect traffic to a group of caches. The EX Secure WAN Manager supports transparent cache server redirect. CLB is supported for inbound and outbound connections. Figure 27 shows an example of redirect CLB.

Note: CLB requires the cache servers to be directly connected to the EX appliance, or connected through a Layer 2 switch. The cache servers cannot be separated from the EX appliance by a router.

FIGURE 27 Redirect Cache Load Balancing (CLB)



To perform transparent CLB, the EX appliance does the following:

- Selects a cache group based on the result of QoS classification of the first packet of a new connection.
- Selects a cache node (cache server) within the group based on the load-balancing algorithm.

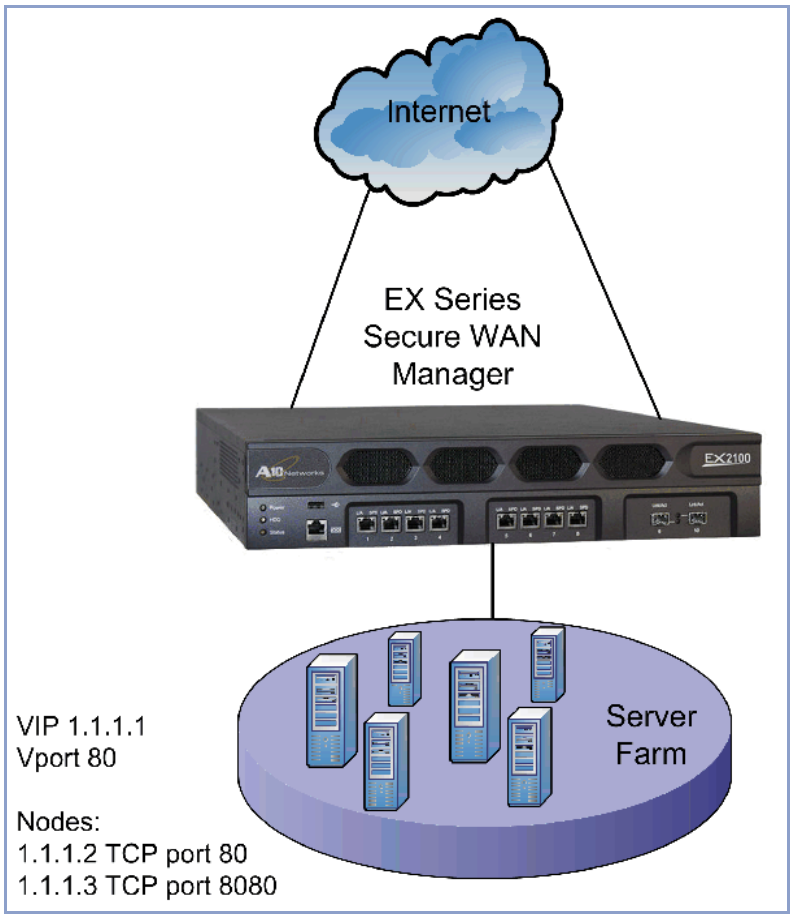
The EX appliance does not change the source or destination address information in the packet. The cache server is responsible for all address changes and replies to clients.

Server Load Balancing (SLB)

Server Load Balancing balances traffic across a server farm (service group). Clients send traffic to a virtual IP address and protocol port, and the EX appliance balances the traffic across a group of real servers/ports containing the content for the virtual address and port. The EX appliance selects the real server/port based on the load balancing methods configured in the service group.

The servers do not need to be directly connected to the EX appliance. They can be connected through a switch or router. Figure 28 shows an example of SLB.

FIGURE 28 Server Load Balancing (SLB)



When the EX Secure WAN Manager receives a packet for a new connection to a virtual port configured on the EX appliance, the EX appliance does the following:

- Selects the service group that is bound to the virtual port of the packet.
- Selects a member (a server node or a server port) within the group based on the load-balancing algorithm.

  Translates the packet's destination IP address from the VIP into the server node's real IP address; and if the selected member is a server port, the EX appliance also translates the packet's destination port into the selected port number.

After a server is selected for a connection, new connections from the same source IP address to the same destination IP address and protocol port number are forwarded to the same server.

SLB can be used to load balance connections from external clients (clients on the Internet) and from internal clients (clients in the same network as the servers.)

Health Monitor Methods

Before sending traffic to a node, the EX Secure WAN Manager verifies that the node is still available (healthy) by sending a health check to the node. The EX appliance supports Layer 3, Layer 4, and Layer 7 health methods. Health monitors can also be used to test LLB links. By default, routing information is used to determine LLB link health.

(For a detailed list of health methods, see Table 8 on page 106.)

Layer 3 Health Method

A health check using the Layer 3 health method is an ICMP echo request (ping) addressed to a specific IP address. The link or node passes the check if an echo reply is received. Layer 3 health checks do not verify the availability of specific QoS classes. Layer 3 health checks are often used to verify the health of WAN links.

To test a path through multiple links, you can configure a transparent ping to an alias address, which is the address at the other end of the link.

Layer 4 Health Method

Health checks using Layer 4 health methods are addressed to a specific IP address and a specific QoS class (TCP or UDP application port). The criteria for passing the check depend on the port reachability.

Layer 7 Health Method

Some health methods allow you to specify application-specific information that must be present on the target node in order for the node to pass the health check. For example, you can configure a HTTP health check to send an HTTP GET or HEAD request. The target node passes the health check only if its reply contains specific page content or specific meta-information from the page header.

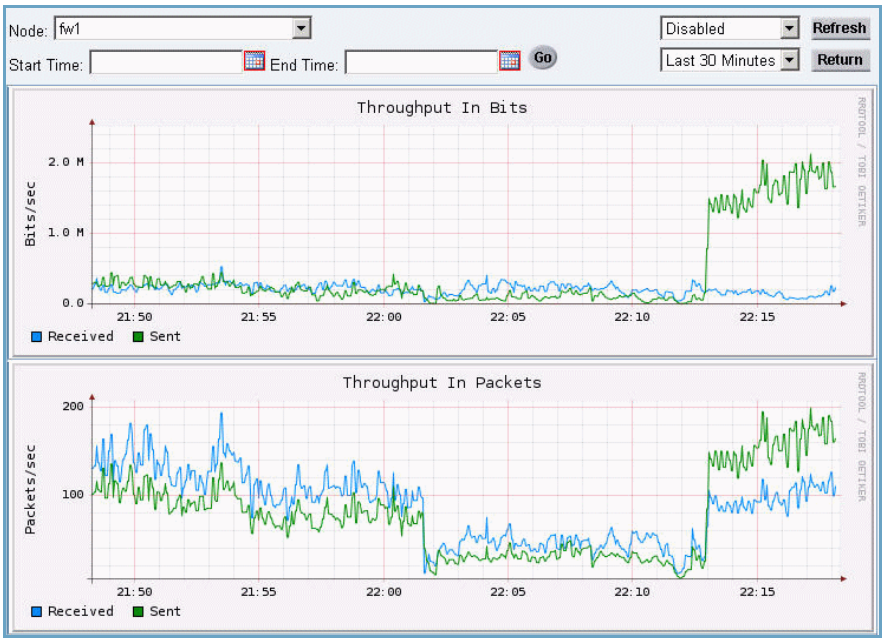
Statistics and Graphs

Load-balancing statistics are available in tabular or graph form. The tables contain a separate row for each link, node, or group. The graphs show traffic activity for a single link, node, or group. Figure 29 and Figure 30 show examples of each type of display.

FIGURE 29 Load-Balancing Statistics – Tabular View

Name	Bytes		Packets		Connections		Status	Report
	Received	Sent	Received	Sent	Current	Total		
fw1	13.5K	19.6K	155	137	0	20	Running	
fw2	40.8K	62.6K	295	171	0	75	Running	

FIGURE 30 Load-Balancing Statistics – Graphs



(See also "Display Load-Balancing Statistics" on page 116.)

Load Balancing Parameters

The following sections list the configurable LLB parameters.

Group Parameters

Table 3 lists the parameters you can configure for load-sharing groups.

TABLE 3 Configurable Parameters for Load-Sharing Group

Parameter	Description	Supported Values
Name	String to uniquely identify the group.	1 to 31 alphanumeric characters. Spaces (internal blanks) are allowed and do not require quotation marks.
Default Group (LLB only)	LLB group into which new LLB links are automatically placed. The user must explicitly specify a default group.	Any configured LLB group.

TABLE 3 Configurable Parameters for Load-Sharing Group (Continued)

Parameter	Description	Supported Values
Algorithm	Method used to balance traffic among the links or nodes. You can select an algorithm that best fits the capacities of the links or nodes in the group. **Note:** Round Trip Time and Bandwidth Usage algorithms are not available for FWLB/CLB/SLB.	One of the following: • Round Robin (default) • Least Connection • Bandwidth Usage • Bandwidth Price • Round Trip Time • Weighted Round Robin • Weighted Least Connection (For descriptions, see "Load-Balancing Algorithms" on page 73.)
Persistence	Option that always sends traffic for a given connection to the same link or server. • When persistence is enabled (On) – After the link or node is selected for the first packet in a connection, traffic for the same or similar connections (in terms of IP address or protocol port) is sent to the same link or node. • When persistence is disabled (Off) – Each new connection is forwarded to a link or node based on the load-balancing algorithm. Different connections can be sent to different links or nodes.	One of the following: • On • Off (default) When persistence is enabled, the age time can be 60-86400 seconds. The value must be divisible by 10. The default is 60 seconds. When persistence is enabled, source-IP persistence is used by default. For LLB and FWLB sessions, destination-IP persistence is also supported.
Members	List of links, nodes, or server protocol ports in a load-balancing group. • For LLB – Links in the group • For FWLB – Firewall nodes in the group • For CLB – Cache servers in the group • For SLB – Either server nodes or server protocol ports. An SLB service group can contain either a set of servers or a set of individual ports, not both.	List of configured links or nodes
Type	Type specifies the service group member type: if it's "Any", a service group member is an SLB node; "TCP", a member is a TCP port of an SLB node; "UDP", a member is a UDP port of an SLB node. Ports should be configured using the "Port" tab in the SLB node configuration form.	One of the following: • TCP • UDP • Any Default: Any

TABLE 3 Configurable Parameters for Load-Sharing Group (Continued)

Parameter	Description	Supported Values
Binding (LLB, FWLB, and CLB)	Set of QoS classes (TCP and UDP applications) for which to load balance. For each class, you can specify a priority. If traffic matches more than one class, in different link groups, the link group with the highest priority for a matching class is selected. For example, if the http class is bound to two link groups, LLBGroup1 and LLBGroup2, and the class has priority 1 in LLBGroup1 and priority 512 in LLBGroup2, the EX appliance will select LLBGroup1 for traffic in the http class.	You can select any of the well-known QoS classes that are recognized by the EX appliance. For LLB and FWLB, you can check the "Default class" checkbox, which is a virtual class that matches all traffic. The priority value of a class can be 1-512. The highest priority is 1. The default is 256.

Individual Link or Node Parameters

Table 4 lists the parameters you can configure for individual links or nodes.

TABLE 4 Configurable Parameters for Individual Links and Nodes

Parameter	Description	Supported Values
Name	String to uniquely identify the link or node.	1 to 31 alphanumeric characters. Spaces (internal blanks) are allowed and do not require quotation marks.
IP Address and Mask	IP address and network mask. • LLB Link – IP address of the EX appliance connection to the Internet. • FWLB node – IP address of the firewall interface connected to the EX appliance. • CLB node – IP address of the cache interface connected to the EX appliance. • SLB node – IP address of the real server's interface connected to the EX appliance. Note: LLB link, FWLB node, and CLB node, must be directly connected to the EX appliance.	Standard 32-bit address and mask in dotted decimal notation. For example: 10.10.10.10 255.255.255.0.
Bandwidth (LLB only)	Maximum amount of bandwidth to allow on an LLB link.	1 to 8000000 (8 million) Kbps Default: 1000 Kbps
Connection Limit	Maximum number of concurrent connections to allow on the link or node.	0 to 1000000 (1 million) Default: 0 (unlimited)
Price	Bandwidth price to assign to link or link group.	1 to 10000
Weight	Number representing the link's or node's capacity relative to the other links or nodes in the group.	1 to 255 Default: 1
Monitor	Health check periodically sent to the link destination or node to verify its availability.	(See "Health Monitor Methods" on page 68.)

TABLE 4 Configurable Parameters for Individual Links and Nodes (Continued)

Parameter	Description	Supported Values
State	Administrative state of the link or node.	Enabled (default) / Disabled
NAT Pool (LLB only)	Source IP addresses to use when forwarding internal traffic on the WAN links. The EX appliance replaces the source IP address of traffic from an internal host with one of the addresses in the NAT pool. The NAT pool ensures that return traffic for an outbound connection always uses the same link.	Standard 32-bit address in dotted decimal notation. For example: 10.10.10.10
Port (LLB)	Ethernet port number.	Physical Ethernet port number or Virtual Ethernet (VE) number
Port (SLB)	TCP or UDP port number. You can load balance among SLB nodes even if they use different protocol port numbers for the same QoS class. (However, the protocol must be the same on all nodes in a service group; either TCP or UDP.) This setting is optional. If you do not specify a protocol and port number for the node, the node can be used in service groups set to Any (rather than TCP or UDP).	1 to 65535 (any valid TCP or UDP protocol port number)

Load-Balancing Algorithms

Table 5 lists load-balancing algorithms supported by the EX Secure WAN Manager.

TABLE 5 Load-Balancing Algorithms

Type	Description	Valid with...			
		LLB	FWLB	CLB	SLB
Round Robin	Each link or node in the load-balancing group is used sequentially, in rotation. The first link or node is selected for the first new connection, the second link or node is selected for the second new connection, and so on until all links or nodes have been selected. Then selection starts over again with the first link or node.	Yes	Yes	Yes	Yes
Least Connection	The link or node that currently has the fewest connections is selected.	Yes	Yes	Yes	Yes
Bandwidth Usage	The link with the most bandwidth available is selected. Bandwidth availability is calculated based on the percentage of the link's maximum allowed bandwidth that is currently in use. The maximum bandwidth is specified in the link's configuration on the EX appliance.	Yes	No	No	No
Round Trip Time	The link with the shortest round-trip-time between the EX appliance and the destination is used. The round-trip time is based on the time it takes for a packet to reach its destination and for its response to return.	Yes	No	No	No

TABLE 5 Load-Balancing Algorithms (Continued)

Type	Description	Valid with...			
		LLB	FWLB	CLB	SLB
Weighted Round Robin	Links or nodes are selected based on a combination of round robin and weight. Weight is an administratively assigned number that indicates a link's or node's performance relative to the other links or nodes in the group. The default weight is 1. A higher number indicates a higher capacity to serve connections. For example, a node with weight 3 is more likely to be selected than a node with weight 1 because it has three times the capacity of a node with weight 1. This load-sharing algorithm ensures that better performing links or nodes receive statistically more connections, while slower links or nodes still receive some connections.	Yes	Yes	Yes	Yes
Weighted Least Connection	Links or nodes are selected based on a combination of current connections and weight. This load-sharing algorithm ensures that links or nodes with higher capacity for new connections receive statistically more connections, while slower links or nodes still receive some connections.	Yes	Yes	Yes	Yes
Bandwidth Price	Links are selected based on their bandwidth tier price settings and their current bandwidth usage. The cheapest link will be selected. If more than one link are currently of the same price, this method functions as "Bandwidth usage" method.	Yes	No	No	No

Link Load Balancing (LLB)

Use the procedures in the following sections to configure LLB.

Configure LLB

To configure LLB:

1. Configure health methods to check the availability of links. (See "Health Monitor" on page 104.)
2. Optionally, you can configure IP address pools. This may be particularly helpful if the EX appliance will perform source NAT for outbound traffic for any of the traffic classes on external links.
3. Configure external links. (These are the WAN links to the ISP or the Internet.)
4. Configure DNS policies for inbound LLB.

5. Configure a link group, add the external links to it, and bind a QoS class (or the default QoS class) to the group.
6. Optionally, change global parameters (default LLB group, RTT settings, and DNS settings).
7. Configure default routes to the ISP gateways.

Configure External Links

To configure an external link:

1. Select Config Mode > Load Balance > Link.
2. On the menu bar, select Link, if not already selected.
3. Click the New button. The General tab appears. (See Figure 31.)
4. In the Name field, enter a name for the link.
5. To specify the Ethernet interface on which outbound traffic on the link can be sent, select the interface from the Port drop-down list.

   If you select an interface, outbound traffic on the link is sent only on the selected interface. Otherwise, outbound traffic for the link can be sent on any interface that is connected to the next hop.

   Selecting the interfaces for LLB links enables you to configure multiple links with the same subnet but different interfaces.
6. In the Gateway and Mask fields, enter the IP address and subnet mask of the next hop to the ISP or Internet.
7. Configure load-balancing settings:
   a. In the Bandwidth field, specify the maximum transmission speed to allow on this link.

      You can specify from 1 to 8000000 (8 million) Kbps.
   b. In the Connection Limit field, specify the maximum number of connections that can be active on the link at the same time.

      You can specify from 0 (unlimited) to 1000000 (1 million). The default is 0 (unlimited).
   c. For weighted load-balancing algorithms, specify this link's weight relative to other links in the same link group.

      You can specify from 1 to 255. The default is 1.

8. From the Monitor pull-down list, select the health monitor to use for checking the health of the link.

   If you have not configured the health monitor yet, you still can finish configuration of the link and select the monitor later.

9. To use source NAT, enable it for the link by selecting Enabled next to Source NAT.

   On the NAT tab, you can specify, you can specify the traffic classes for which to perform source NAT, and the IP address pools from which to allocate the source IP addresses. The NAT tab is described in step 11.

10. Select the link state (Enabled or Disabled).

11. To configure NAT:

    a. Click the NAT tab.

    b. In the Class drop-down list, select a class name.

    c. In the IP Pool drop-down list, you can optionally select an IP address pool.
    Note: An IP address pool is optional when configuring NAT. If you enable NAT without configuring an IP address pool, the IP address of the corresponding interface will be used when doing source NAT.

    d. Select the NAT checkbox to enable source NAT for the class.

       For this class' traffic, the EX Secure WAN Manager replaces the internal host's real IP address with a NAT address from the pool before forwarding the traffic.

       If you do not select the NAT checkbox, NAT will be disabled for the class, but the class will still be added to the list.

    e. Click Add.

    f. Repeat these steps for each traffic class for which you want to provide source NAT.

12. To configure the link's bandwidth price:

    - Click the Price Bandwidth tab.
    - Input bandwidth tier and price in the input field, or use the radio buttons to specify special bandwidth tier "unlimited" and price "prepaid", then click Add.
    - Repeat for each bandwidth tier you want to add.

13. To load balance inbound client traffic based on a destination subnet that is different from the subnet the link is in, enter the destination subnet in the Alternate Subnet field.

14. Click OK. The new link appears in the load-balancing link table.

15. Go to "Configure a Link Group" on page 80.

FIGURE 31 LLB Link – General Tab

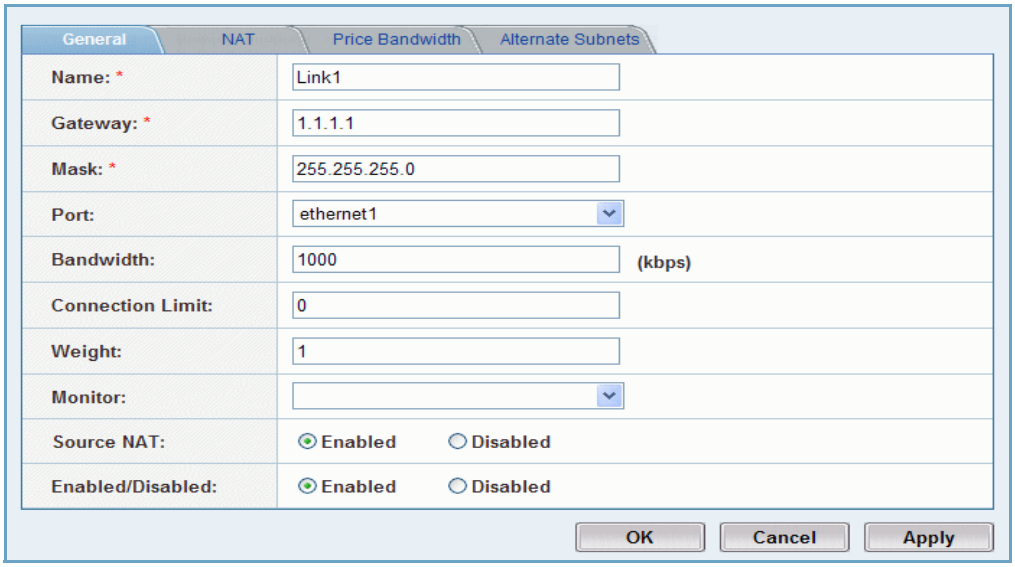


FIGURE 32 LLB Link – NAT Tab

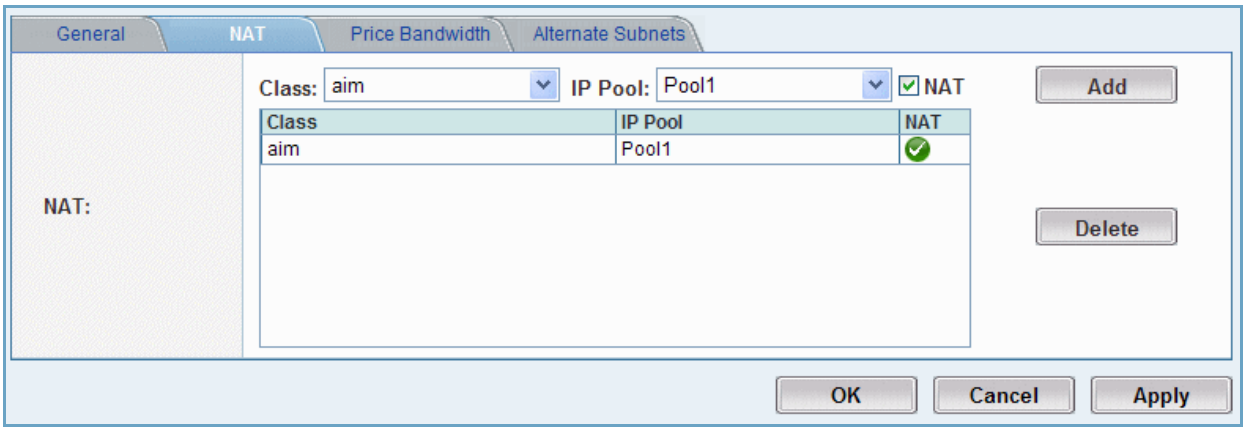


FIGURE 33 LLB Link – Price Bandwidth Tab

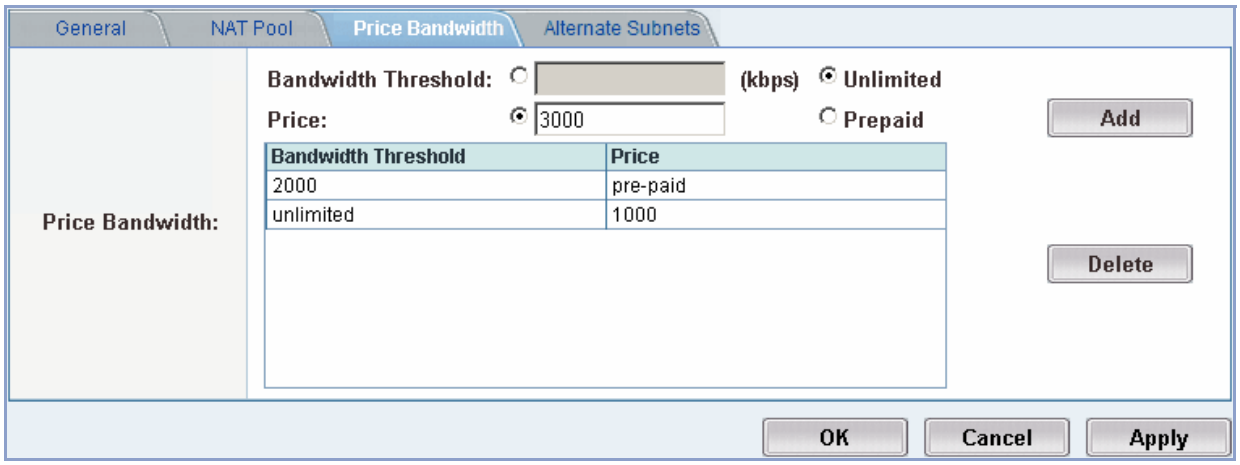
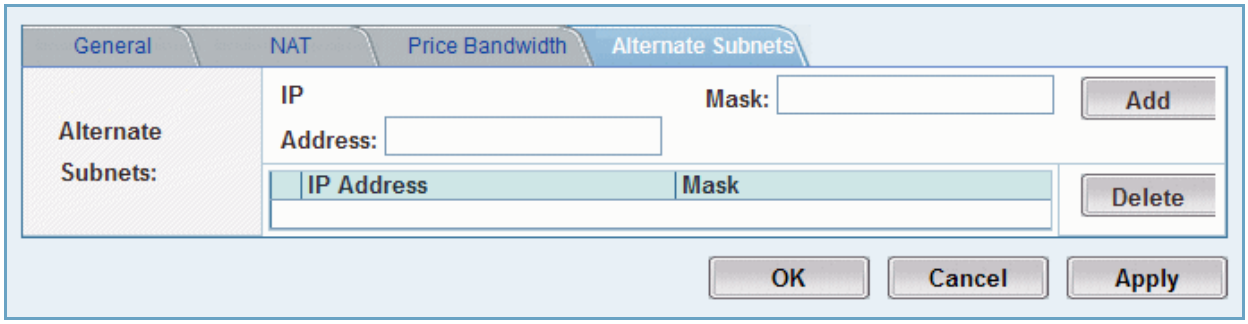


FIGURE 34 LLB Link – Alternate Subnets Tab



Configure a DNS Policy for Inbound LLB

The EX Secure WAN Manager can modify DNS replies to suggest use of a preferred IP address, so that the following inbound connection initiated by a client will be destined for the suggested IP address and go through the selected link.

Using the DNS policy, the EX appliance re-orders the IP addresses in replies to inbound DNS requests for the specified domain names and hosts, so that the IP address of the next link in the load-balancing rotation is placed at the top of the list. The client therefore uses the same link for subsequent traffic on the connection. (For more information about this type of LLB, see "Inbound LLB" on page 60.)

Note: If the DNS server is located outside the network, you also need to configure the EX appliance to act as a proxy for the DNS server, for the load-balanced domain. See "Configure Domain Based Proxies" on page 235.

To implement this type of inbound LLB:

1. Configure the DNS policy by specifying the domain names and host names for which to load balance return traffic.
2. When configuring link groups, bind the policies to the groups. (See "Configure a Link Group" on page 80.)

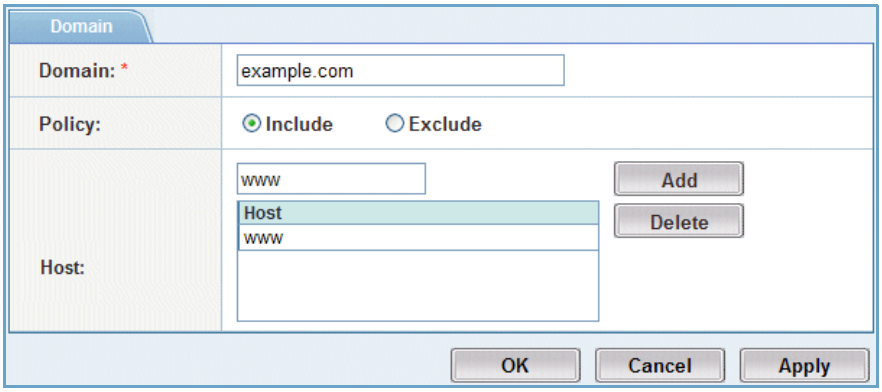
Note: You must configure the DNS policy before you configure the link group. Otherwise, the policy will not be available to select when you configure the group.

Configuring a DNS Policy

To configure a DNS policy for inbound LLB:

1. Select Config Mode > Load Balance > Link.
2. On the menu bar, select Domain. The list of configured domain policies appears.
3. Click New. The Domain tab appears. (See Figure 35.)
4. In the Domain field, type the domain name for which you want to load balance traffic.
5. Select whether to include (default) or exclude the hosts listed in the Host list in DNS load-balancing decisions.
   - Include – Domain policy "include" means an FQDN is considered matching only when it matches the *domain and one* of its hosts.
   - Exclude – Domain policy "exclude" means an FQDN is considered matching only when it matches the *domain and none* of its hosts.
6. Enter the host name in the field above the host name list and click Add. The host appears in the list. Repeat for each host name for which you want to balance traffic.
7. Click OK. The domain appears in the list.

FIGURE 35 LLB – Domain Tab



Configure a Link Group

Note: If you plan to apply a DNS domain policy to the group, you must configure the DNS policy first. (See "Configure a DNS Policy for Inbound LLB" on page 78.)

To configure a link group:

1. Select Config Mode > Load Balance > Link.
2. On the menu bar, select Link Group.
3. Click the New button. The Link Group tab appears. (See Figure 36.)
4. In the Name field, enter a name for the link group.
5. From the Algorithm pull-down list, select the load-balancing algorithm to use. (For descriptions, see "Load-Balancing Algorithms" on page 73.)
   - Round Robin
   - Least Connection
   - Bandwidth Usage
   - Bandwidth Price
   - Round Trip Time (If you select this algorithm, see "Configure Global LLB Settings" on page 84 after you complete this procedure.)
   - Weighted Round Robin
   - Weighted Least Connection

6. Select whether load-balanced flows are persistent.
   - Persistent On – The same link will be used for all connections with the same IP address within the age period.

     When persistence is enabled, the default session timeout (age) is 60 seconds. To change the timeout, edit the value in the Age field. The value must be divisible by 10; for example 120 is valid but 125 is not valid. The default is 60 seconds.

     Persistence is based on source IP address by default. To base persistence on destination IP address instead, select the Destination checkbox.
   - Persistent Off – A new link will be selected for each new connection.

7. From the pull-down list, select a link, then click Add. Repeat for each link.

8. To specify the QoS classes (applications) to load balance, click the Bind Classes tab and go to step 10. (See Figure 38.)

Note: Only Layer 4 classes are supported.

9. Select the QoS classes to load balance. If you select specific QoS classes, the EX appliance load balances traffic only for those classes.
   a. To load balance on all traffic, check the Default Class checkbox. Otherwise, select QoS class from the pull-down list.
   b. To change the priority of the class in this link group, edit the value in the Priority field.
   c. Click Add. Repeat for each class.

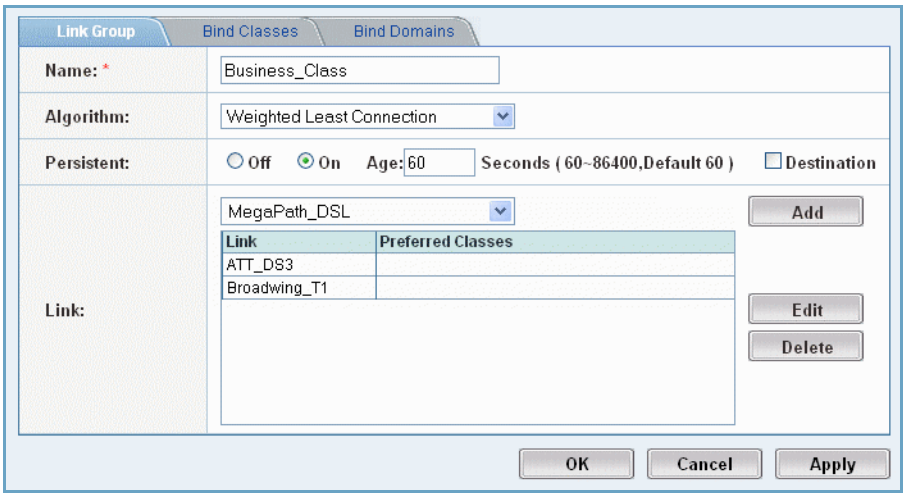
10. To apply a DNS policy for inbound LLB, click the Bind Domains tab and go to step 11. (See Figure 39.)

    Otherwise, to save the link group without applying a DNS policy, go to step 12.

11. Select the DNS domains for which to load balance return traffic for inbound LLB:
    a. Select the domain from the pull-down list.
    b. Click Add. Repeat for each class.

12. Click OK. The new link group appears in the link group table.

FIGURE 36 LLB Group – Link Group Tab



To edit an existing link:

Select the link in the Link section of the Link Group tab, then click the Edit button. The Preferred Classes tab appears, as seen in Figure 37, where you can select a class from the pull-down list and then click the Add button to add a new preferred class to the list. You can also select an existing preferred class form the list and then click the Delete button to remove it. Click the Return button o return to the Link Group tab and continue editing.

FIGURE 37 Edit Preferred Class Links

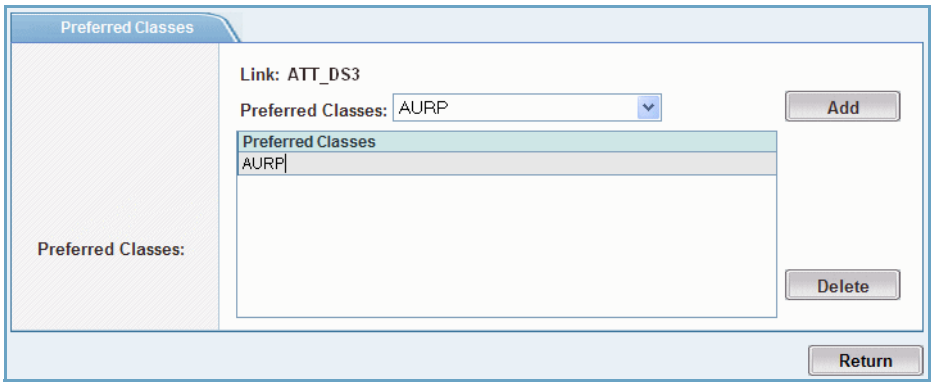


FIGURE 38 LLB Group – Bind Classes Tab

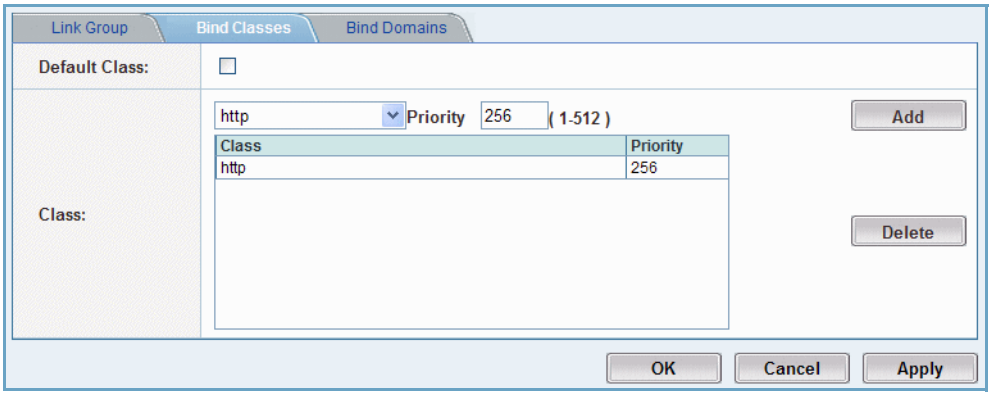
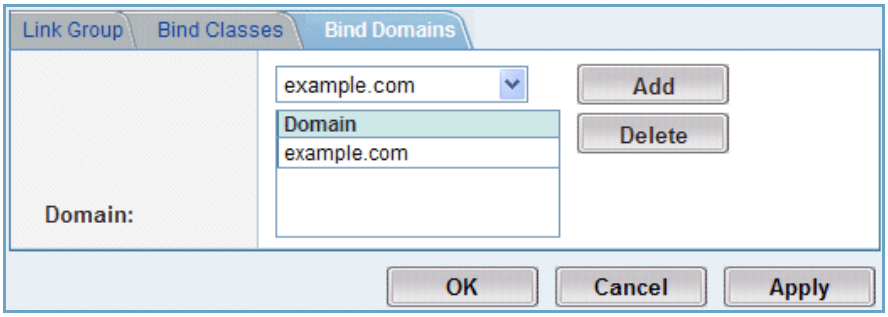


FIGURE 39 LLB Group – Bind Domains Tab



Configure Global LLB Settings

This section describes how to configure the parameters described in Table 6.

TABLE 6 Configurable Global LLB Parameters

Parameter	Description	Supported Values
Proximity mask	Mask used for round-trip-time (RTT) collection. The Round Trip Time (RTT) algorithm selects a link based on the time it takes for packet to reach its destination and for its response to return. Generally, a packet can reach its destination using any of the links in a link group. However, the RTTs for the links can differ. When RTT is the load balancing algorithm used for a link group, the EX Secure WAN Manager selects the link with the shortest RTT. The EX Secure WAN Manager gets RTTs from TCP handshakes that occur over the links. • For outbound sessions, the RTT is the time between when the EX appliance sends a TCP SYN and when the SYN ACK is received. • For inbound sessions, the RTT is the time between when the EX appliance sends the SYN ACK and when the ACK is received. The EX appliance does not actively send traffic to obtain RTT values. Instead, the EX appliance uses the TCP exchange times for real traffic between internal and external devices. The proximity mask specifies the granularity of RTT entries in the cache. Depending on the proximity mask, the EX appliance can use the same RTT entry for multiple destinations. For example, if the proximity mask is 255.255.0.0, then separate RTT entries are used for destinations 192.168.10.10 and 192.141.10.10. However, a single entry is used for destinations 192.168.10.10 and 192.168.20.10. The default proximity mask is 255.255.240.0. The RTT settings are global for all links on the EX appliance. **Note:** A10 Networks recommends not to set the proximity mask to 255.255.255.255. Using this level of granularity uses a lot of system resources without providing significantly more useful information than less specific masks.	Valid subnet mask or mask length Default: 20 bits: /20 or 255.255.240.0
RTT agetime	Number of seconds RTT entries can remain unused before they are removed from the RTT cache. The EX appliance caches the RTT times.	60-1800 seconds 300 seconds

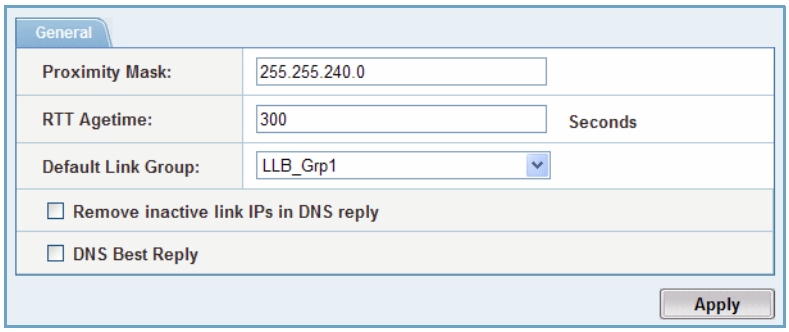
TABLE 6 Configurable Global LLB Parameters (Continued)

Parameter	Description	Supported Values
Default link group	Link group to which LLB links are automatically bound.	Name of a configured link group Default: not set
Remove inactive link IPs from DNS replies	Removes all answers associated with down links from the DNS reply. If all links are down, the reply will consist of 0 answers.	Enabled or disabled Default: disabled
Include only the best IP in DNS replies	Removes all but the best IP from the DNS answer. DNS reply contains at most 1 IP or answer. The best IP is never associated with an inactive link.	Enabled or disabled Default: disabled

1. Select Config Mode > Load Balance > Link.
2. On the menu bar, select Settings.
3. To configure RTT settings:
   - In the Proximity Mask field, edit the mask value.
   - In the RTT Agetime field, edit the number of seconds.
4. To set a default link group, select the group from the Default Link Group drop-down list.
5. To configure DNS settings:
   - To remove inactive link IPs from DNS replies, select the Remove inactive link IPs in DNS reply option.
   - To include only the best IP in DNS replies, select the DNS Best Reply option.
6. Click Apply.

Note: Links that were already assigned to the previous default link group remain in that link group. The links are not automatically moved to the new default link group.

FIGURE 40 Config > Load Balance > Link > Settings



Configure Default Routes to the ISP Gateways

For information about configuring default routes, see "Static Routes" on page 214.

Firewall Load Balancing (FWLB)

Use the procedures in the following sections to configure FWLB.

Configure FWLB

To configure FWLB:

1. Configure health methods to check the paths through the firewalls. (See "Health Monitor" on page 104.)
2. Configure firewall nodes.
3. Configure a firewall group and add the firewall nodes to it.
4. Enable FWLB.

Configure Firewall Nodes

Note: The EX Secure WAN Manager must be directly connected to the firewall nodes. You cannot connect them through a router, but you can connect them through a layer 2 switch.

To configure a firewall node:

1. Select Config Mode > Load Balance > Firewall.
2. On the menu bar, select Firewall Node, if not already selected.
3. Click the New button. The Firewall Node tab appears. (See Figure 41.)
4. In the Name field, enter a name for the firewall node.
5. In the IP Address and Mask fields, enter the IP address and network mask of the firewall node's interface with the EX appliance.
6. Configure load-balancing settings:
   a. In the Connection Limit field, specify the maximum number of connections through the EX appliance to this node that can be active at the same time.

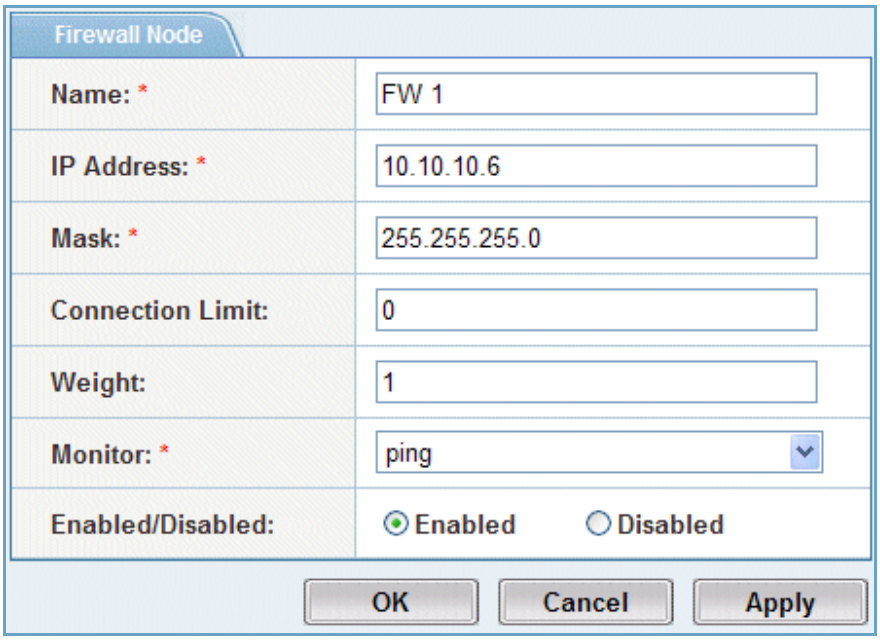
      You can specify from 0 (unlimited) to 1000000 (1 million). The default is 0 (unlimited).

   b. For weighted load-balancing algorithms, specify this node's weight relative to other nodes in the same firewall group.

      You can specify from 1 to 255. The default is 1.
7. From the Monitor pull-down list, select the health monitor to use for checking the health of the firewall node.

   If you have not configured the health monitor yet, you still can finish configuration of the node and select the monitor later.
8. Select the firewall node state (Enabled or Disabled).
9. Click OK. The new node appears in the firewall node table.
10. Go to "Configure a Firewall Group" on page 88.

FIGURE 41 FWLB Node – Firewall Node Tab



Configure a Firewall Group

To configure a firewall group:

1. Select Config Mode > Load Balance > Firewall.
2. On the menu bar, select Firewall Group.
3. Click the New button. The Firewall Group tab appears. (See Figure 42.)
4. In the Name field, enter a name for the firewall group.
5. From the Algorithm pull-down list, select the load-balancing algorithm to use. (For descriptions, see "Load-Balancing Algorithms" on page 73.)
   - Round Robin
   - Least Connection
   - Weighted Round Robin
   - Weighted Least Connection

6. Select whether load-balanced flows are persistent.
   - Persistent ON: The same FWLB node will be used for all connections from the same client IP in a persistent period.

     When persistence is enabled, the default session timeout is 60 seconds. To change the timeout, edit the value in the Age field. The value must be divisible by 10; for example 120 is valid but 125 is not valid. The default is 60 seconds.
   - Persistent OFF: New FWLB node will be selected for each new connection.

     Persistence is based on source IP address by default. To base persistence on destination IP address instead, select On next to Persistent by Destination.

7. From the pull-down list, select a firewall node, then click Add. Repeat for each firewall node.

8. To specify the QoS classes (applications) to load balance, click the Binding tab and go to step 9. (See Figure 43.)

Note: Only Layer 4 classes are supported.

9. Select the QoS classes to load balance. If you select specific QoS classes, the EX appliance load balances traffic only for those classes.
   a. To load balance on all traffic, check the Default class checkbox.
   b. To add a recognized QoS class to the firewall group, select the class from the pull-down list and click Add. Repeat for each class.

10. Click OK. The new firewall group appears in the firewall group table.

11. Go to "Enable FWLB" on page 90.

FIGURE 42 FWLB Group – Firewall Group Tab

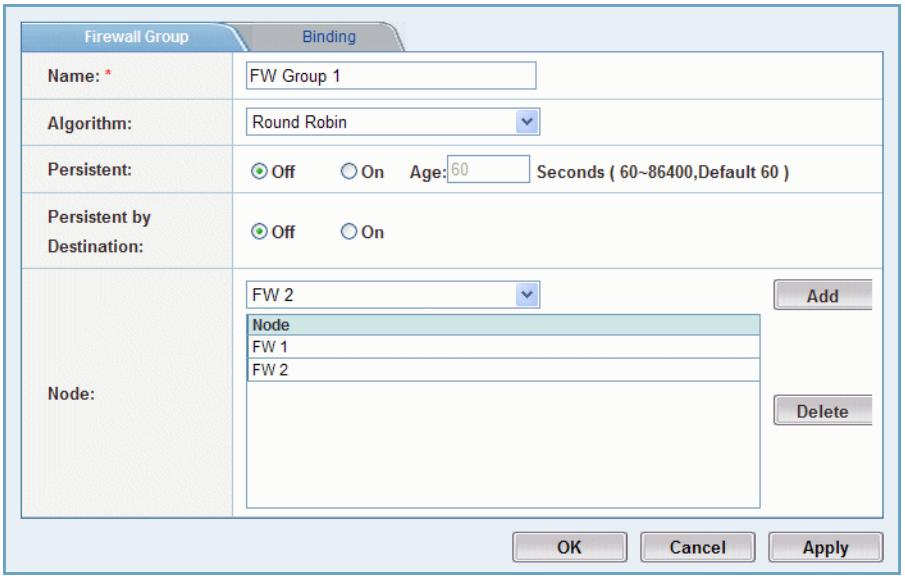
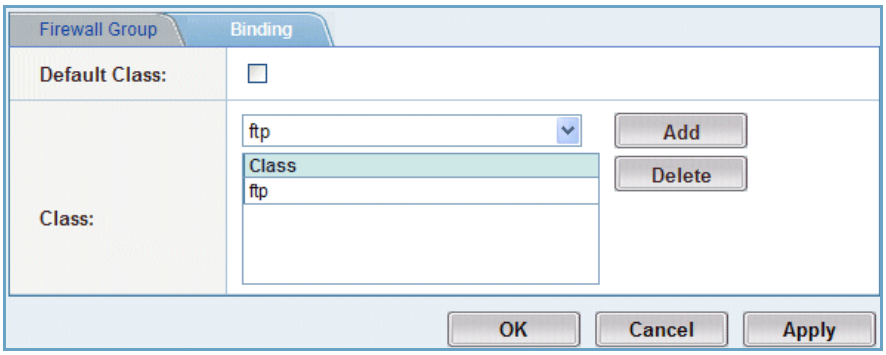


FIGURE 43 FWLB Group – Binding Tab



Enable FWLB

FWLB requires an EX Secure WAN Manager to be placed on each side of the firewall nodes. An EX appliance is required on the external side that is unprotected, and another EX appliance is required on the internal side that is protected by the firewall nodes.

On each EX appliance, to enable FWLB, you must specify the following:

- EX appliance's location (inside or outside)
- Address of the peer EX appliance on the other side of the firewall nodes

To enable FWLB:

1. Select Config Mode > Load Balance > Firewall.
2. On the menu bar, select Settings. The Enable tab is displayed. (See Figure 44.)
3. Select the location:
   - Inside – The EX appliance is connected to the internal, protected side of the firewalls.
   - Outside – The EX appliance is connected to the external, unprotected side of the firewalls.
   - None – The EX appliance currently is not enabled to perform FWLB.
4. To specify the FWLB peer:
   a. Click Peer to display the tab. (See Figure 45.)
   b. In the IP Address and Mask fields, enter the IP address and network mask of the EX appliance on the other side of the firewall nodes.
5. Click Apply.

FIGURE 44 FWLB Settings – Enable Tab

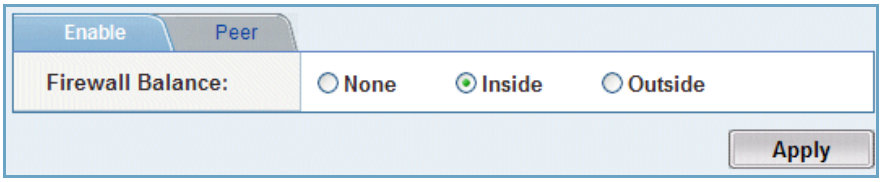
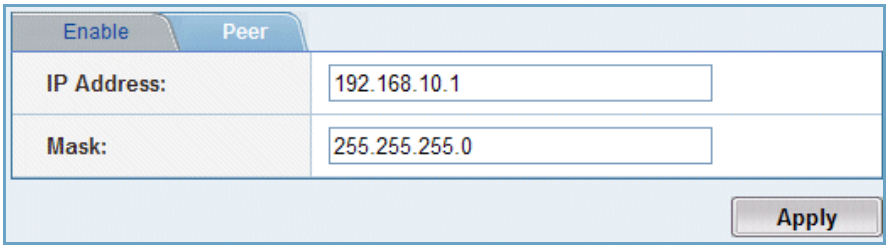


FIGURE 45 FWLB Settings – Peer Tab



Cache Load Balancing (CLB)

Use the procedures in the following sections to configure CLB.

Configure CLB

To configure CLB:

1. Configure health methods to check the availability of the caches. (See "Health Monitor" on page 104.)
2. Configure cache nodes.
3. Configure a cache group and add the cache nodes to it.

Configure Cache Nodes

To configure a cache node:

1. Select Config Mode > Load Balance > Cache.
2. On the menu bar, select Cache Node, if not already selected.
3. Click the New button. The Cache Node tab appears. (See Figure 46.)
4. In the Name field, enter a name for the cache node.
5. In the IP Address and Mask fields, enter the IP address and network mask of the cache node's interface with the EX appliance.
6. Configure load-balancing settings:
   a. In the Connection Limit field, specify the maximum number of connections through the EX appliance to this node that can be active at the same time.

      You can specify from 0 (unlimited) to 1000000 (1 million). The default is 0 (unlimited).

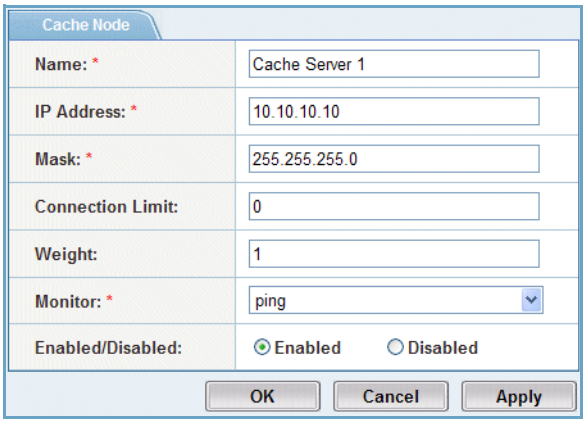
   b. For weighted load-balancing algorithms, specify this node's weight relative to other nodes in the same cache group.

      You can specify from 1 to 255. The default is 1.
7. From the Monitor pull-down list, select the health monitor to use for checking the health of the cache node.

   If you have not configured the health monitor yet, you still can finish configuration of the node and select the monitor later.

8. Select the cache node state (Enabled or Disabled).
9. Click OK. The new node appears in the cache node table.
10. Go to "Configure a Cache Group" on page 93.

FIGURE 46 CLB Node – Cache Node Tab



Configure a Cache Group

To configure a cache group:

1. Select Config Mode > Load Balance > Cache.
2. On the menu bar, select Cache Group.
3. Click the New button. The Cache Group tab appears. (See Figure 47.)
4. In the Name field, enter a name for the cache group.
5. From the Algorithm pull-down list, select the load-balancing algorithm to use. (For descriptions, see "Load-Balancing Algorithms" on page 73.)
   - Round Robin
   - Least Connection
   - Weighted Round Robin
   - Weighted Least Connection

6. Select whether load-balanced flows are persistent.
   - Persistent ON: The same CLB node will be used for all connections from the same client IP in a persistent period.

     When persistence is enabled, the default session timeout is 60 seconds. To change the timeout, edit the value in the Age field. The value must be divisible by 10; for example 120 is valid but 125 is not valid. The default is 60 seconds.
   - Persistent OFF: New CLB node will be selected for each new connection.

7. From the pull-down list, select a cache node, then click **Add**. Repeat for each cache node.

8. To specify the QoS classes (applications) to load balance, click the Binding tab and go to step 9. (See Figure 48.)

Note: Only Layer 4 classes are supported.

9. Select the QoS classes to load balance. The v load balances traffic only for the selected classes.

   To add a recognized QoS class to the cache group, select the class from the pull-down list and click Add. Repeat for each class.

10. Click OK. The new cache group appears in the cache group table.

FIGURE 47 CLB Group – Cache Group Tab

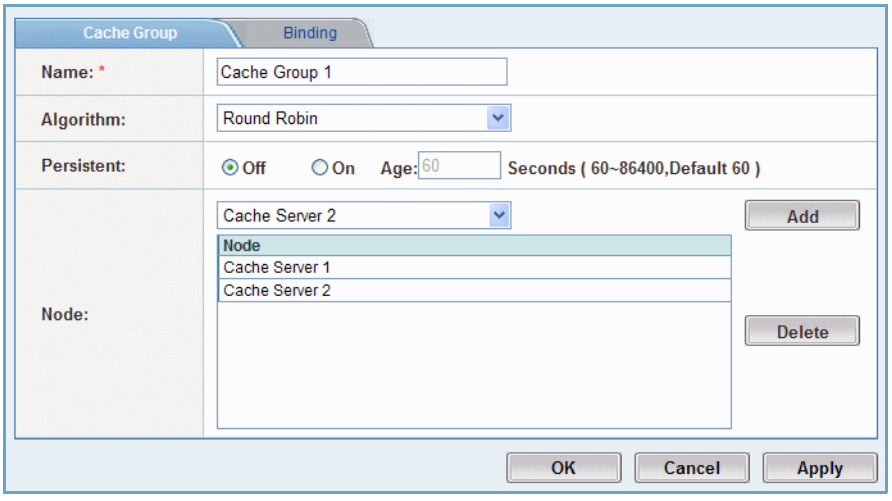
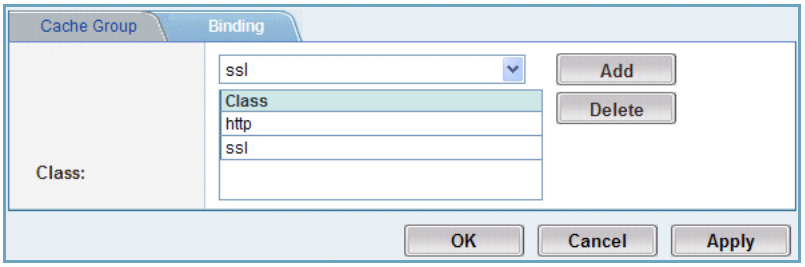


FIGURE 48 CLB Group – Binding Tab



Server Load Balancing (SLB)

Use the procedures in the following sections to configure SLB.

Configure SLB

To configure SLB:

1. Configure health methods to check the availability of QoS classes (applications) on server nodes. (See "Health Monitor" on page 104.)
2. Configure the server nodes.
3. Configure a service group and add the server nodes to it.
4. Configure a virtual server and bind it to the service group.

Configure Server Nodes

To configure a server node:

1. Select Config Mode > Load Balance > Server.
2. On the menu bar, select Server Node, if not already selected.
3. Click the New button. The General tab appears. (See Figure 49.)
4. In the Name field, enter a name for the server node.
5. In the IP Address and Mask fields, enter the IP address and network mask of the server node's interface with the EX appliance.

6. Configure load-balancing settings:
   a. In the Connection Limit field, specify the maximum number of connections through the EX appliance to this node that can be active at the same time.

      You can specify from 0 (unlimited) to 1000000 (1 million). The default is 0 (unlimited).

   b. For weighted load-balancing algorithms, specify this node's weight relative to other nodes in the same server group.

      You can specify from 1 to 255. The default is 1.

7. From the Monitor pull-down list, select the health monitor to use for checking the health of the server node.

   If you have not configured the health monitor yet, you still can finish configuration of the node and select the monitor later.

8. Select the server node state (Enabled or Disabled).

9. To configure ports, click the Port tab and go to step 10.

   Otherwise, to load balance on all traffic, go to step 11.

10. Click New. The Service Group Port tab is displayed. (See Figure 50.)
    a. In the Port field, enter the protocol port number.
    b. From the Protocol pull-down list, select the port type:
       - TCP
       - UDP
    c. In the Connection Limit field, specify the maximum number of connections through the EX appliance to this port that can be active at the same time.

       You can specify from 0 (unlimited) to 1000000 (1 million). The default is 0 (unlimited).

    d. For weighted load-balancing algorithms, specify this port's weight relative to the same port on other nodes in the same server group.

       You can specify from 1 to 255. The default is 1.

    e. Select the server node state (Enabled or Disabled).
    f. Click OK. The Port tab is re-displayed. The new port appears in the list. (See Figure 51.)

11. Click OK. The new node appears in the server node table.

12. Go to "Configure a Service Group" on page 98.

FIGURE 49 SLB Node – General Tab

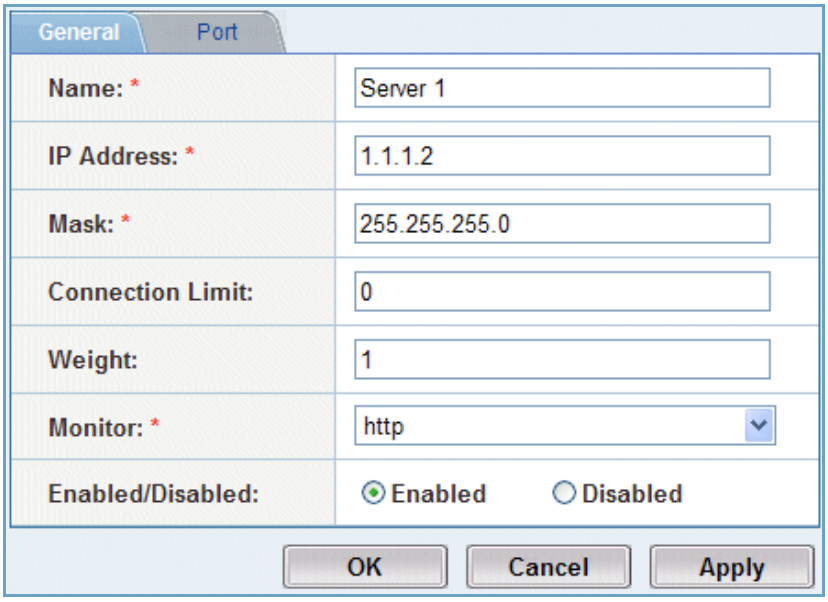


FIGURE 50 SLB Node – Service Group Port Tab

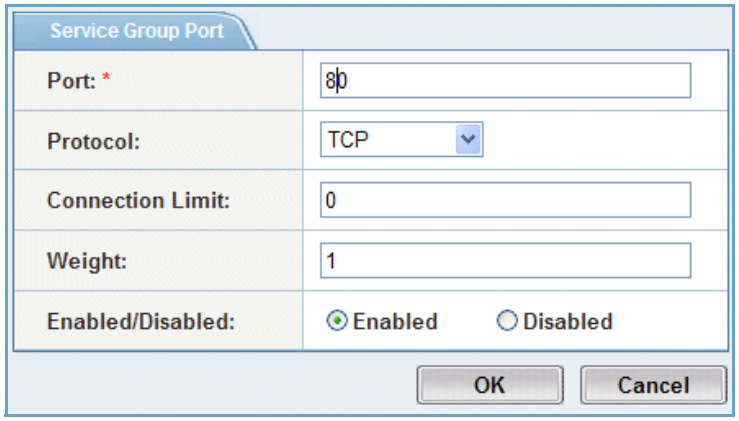
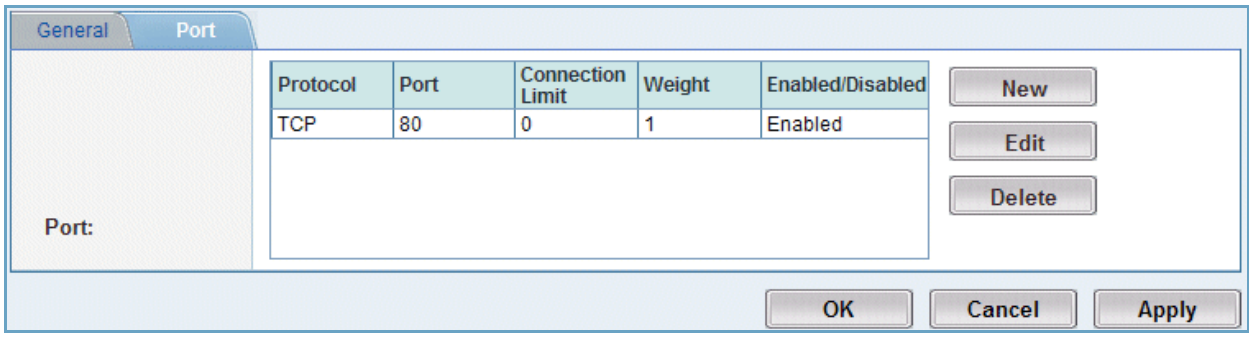


FIGURE 51 SLB Node – Port Tab



Configure a Service Group

To configure a service group:

1. Select Config Mode > Load Balance > Server.
2. On the menu bar, select Service Group.
3. Click the New button. The Service Group tab appears. (See Figure 52.)
4. In the Name field, enter a name for the service group.
5. From the Type pull-down list, select the traffic type to which SLB will apply.
   - TCP
   - UDP
   - Any

   If you select TCP or UDP, the Port drop-down list is displayed next to the Node drop-down list. When Any is selected, the Port drop-down list disappears.

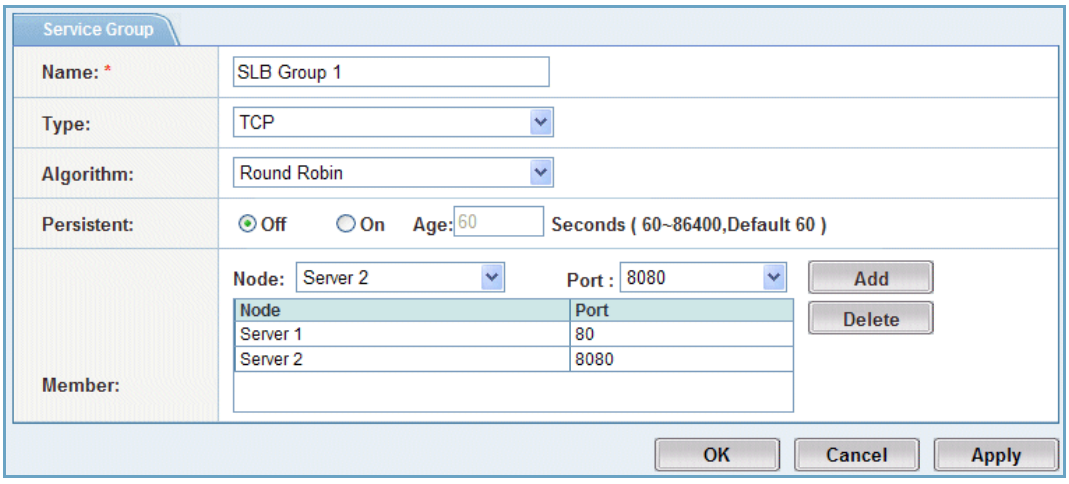
Note: All nodes in a service group must be the same type. If the nodes do not have specific port configurations, they are valid with Any. If the nodes do have specific port configurations, the port type (TCP or UDP) must be the same for all nodes in the group. Changing the Type value clears the server nodes from the Members list.

6. If you selected TCP or UDP as the Type, from the Port pull-down list, select the protocol port for which you want to load balance.

7. From the Algorithm pull-down list, select the load-balancing algorithm to use. (For descriptions, see "Load-Balancing Algorithms" on page 73.)
   - Round Robin
   - Least Connection
   - Weighted Round Robin
   - Weighted Least Connection
8. Select whether load-balanced flows are persistent.
   - Persistent ON: The same SLB node/port will be used for all connections from the same client IP and to the same virtual server IP and port in a persistent period.

     When persistence is enabled, the default session timeout is 60 seconds. To change the timeout, edit the value in the Age field. The value must be divisible by 10; for example 120 is valid but 125 is not valid. The default is 60 seconds.
   - Persistent OFF: New SLB node/port will be selected for each new connection.
9. From the pull-down list, select a server node, then click Add. Repeat for each node.
10. Click OK. The new service group appears in the service group table.
11. Go to "Configure a Virtual Server" on page 100.

FIGURE 52 SLB Group – Service Group Tab



Configure a Virtual Server

To configure a virtual server:

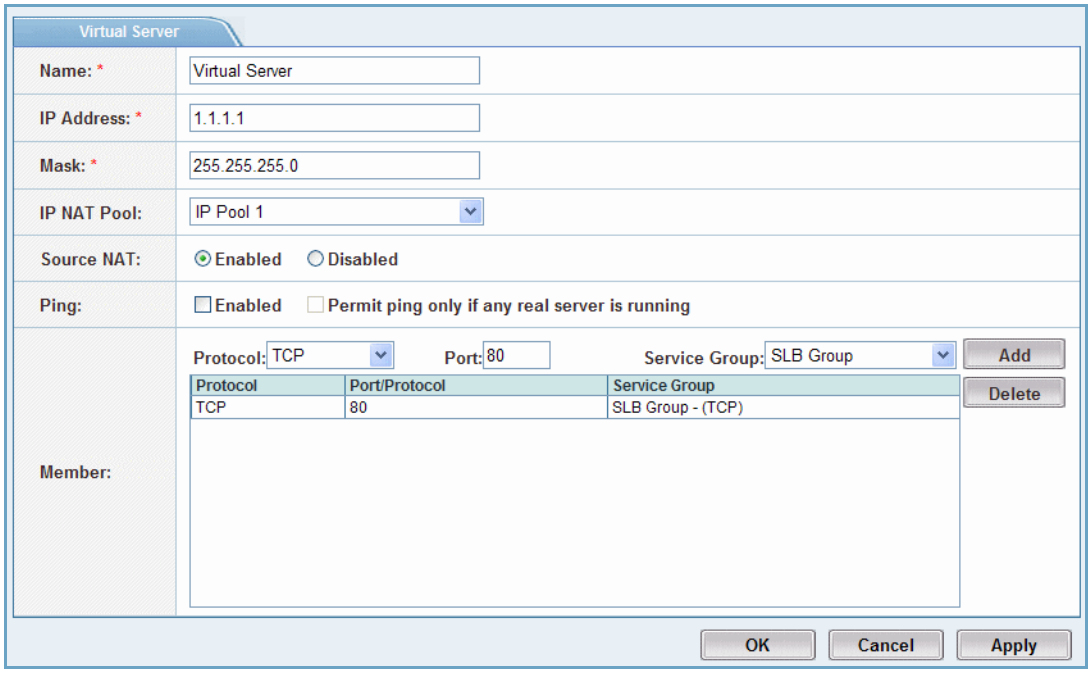
1. Select Config Mode > Load Balance > Server.
2. On the menu bar, select Virtual Server.
3. Click the New button. The Virtual Server tab appears. (See Figure 53.)
4. In the Name field, enter a name for the virtual server.
5. In the IP Address and Mask fields, enter the IP address and network mask of the virtual server.
6. To configure IP source NAT for the virtual server:
   a. In the Source NAT IP field, select an IP pool. Otherwise, to use the virtual IP address of the server as the source NAT address, leave the field blank.
   b. Select the Source NAT state (Enabled or Disabled).
7. Optionally, to enable the EX appliance to reply to ping requests sent to the VIP address, select Enabled next to Ping.

   To reply only if at least one real server is up, select Permit ping only if any real server is running. Without this option, the EX appliance replies to pings for the VIP even if all real servers are down.
8. In the Member area, select the protocol and port number to add, also select service group to bind to the member.
   a. From the Protocol pull-down list, select the protocol: TCP, UDP, or Others.
   b. In the Port field, enter the protocol port number.

Note: You can not bind a "TCP" service group to a "UDP" port, or vice versa.

   c. From the Service Group pull-down list, select the service group.
   d. Click Add.
   e. Repeat for each protocol port and service group.
9. Click OK. The new virtual server appears in the virtual server table.

FIGURE 53 SLB Virtual Server – Virtual Server Tab



Destination NAT

Destination NAT translates the destination IP address of incoming traffic before sending the traffic to a real server. The Destination NAT feature is disabled by default.

You can configure Destination NAT for:

- **Based on QoS class** – This implementation relies on QoS classes to identify traffic before forwarding to an internal IP address. Note that this method offers no support for direct port mapping.
- **Based on IP (and port)** – This implementation allows up to eight external IP addresses and ports to be mapped to a single internal IP address and port. This approach would, for example, allow you to create a mapping between port 2000 (on an external IP) with port 100 (on an internal IP).

To configure a Destination NAT entry Based on QoS Class:

1. Select Config > Load Balance > Destination NAT.
2. Select Based on QoS Class from the menu bar.

3. Click New. The Destination NAT tab appears. (See Figure 54.)

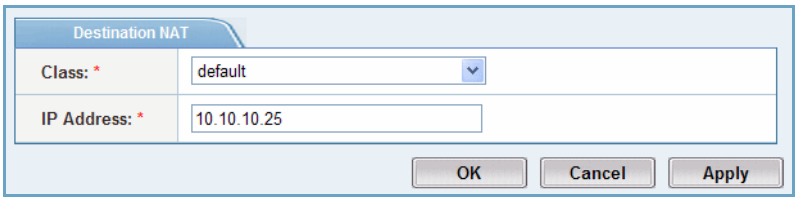
4. From the Class drop-down list, select the QoS traffic class that will use the destination NAT address. need to do inbound Destination NAT in the poll-down list of Class.

   To configure a destination NAT address for all traffic classes, assign it to the “default” traffic class.

5. In the IP address field, enter the IP address to use as the destination IP address for incoming traffic.

6. Click OK. The new destination NAT entry appears in the Destination NAT list.

FIGURE 54 Config > Load Balance > Destination NAT > Based on QoS



To configure a Destination NAT entry Based on IP:

1. Select Config > Load Balance > Destination NAT.

2. Select Based on IP from the menu bar.

3. Click New. The Destination NAT tab appears. (See Figure 55.)

4. Enter a name for the DNAT object in the Name field.

5. Enter the internal IP address, and optionally the port, to which inbound traffic from the external ports will be sent.

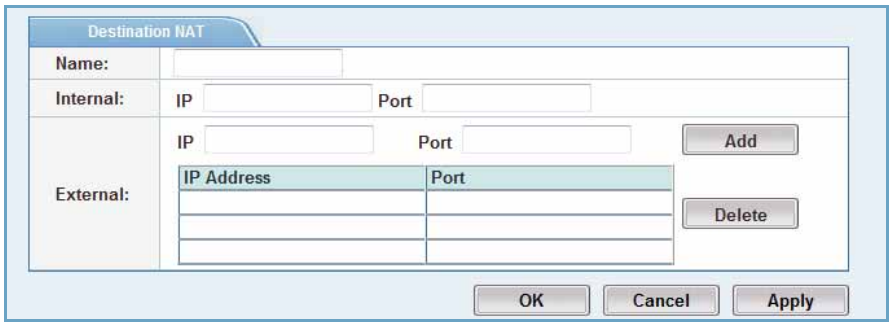
6. Enter the external IP address, and optionally the port, from which inbound traffic will be sent to the internal IP address.

7. Click the Add button to add the mapping to the DNAT object.

8. Repeat this process to create a mapping for up to 8 external IPs to one internal IP.

9. Click OK. The new destination NAT entry appears in the Destination NAT list.

FIGURE 55 Config > Load Balance > Destination NAT > Based on IP



IP Pool

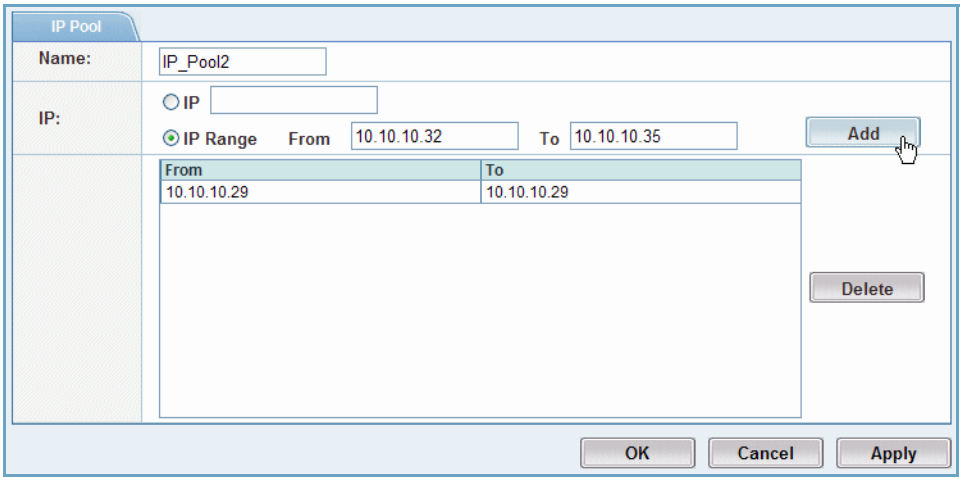
IP pools are sets of IP addresses that can be used with IP source NAT. To perform IP source NAT, the EX Secure WAN Manager translates the source address of a packet into one of the addresses in the IP pool.

To configure an IP Pool:

1. Select Config > Load Balance > IP Pool.
2. Click New. The IP Pool tab appears. (See Figure 56.)
3. In the Name field, enter a name for the IP Pool.
4. Add single addresses or address ranges:
   - To add a single address, click IP, enter the address in the IP field, and click Add.
   - To add a contiguous range of addresses, click IP Range, enter the starting adders in the From field, enter the ending address in the To field, and click Add.

   Repeat for each single address or contiguous range.
5. Click OK. The new IP Pool appears in the IP Pool list.

FIGURE 56 Config > Load Balance > IP Pool



Health Monitor

The EX Secure WAN Manager uses health monitors to periodically check the availability of servers and applications. A health monitor is a packet addressed to a link or node. You can use a Layer 3 monitor (Ping), Layer 4 monitors, or application-specific Layer 7 monitors, whose type is determined by its health method attribute.

Health monitors make load balancing more efficient. If a server or application stops responding to health checks, the EX appliance stops directing traffic to the down server or application, until it starts replying to the health checks again.

A health monitor is a required configuration parameter of every FWLB firewall, CLB cache server, and SLB server. If you plan to use a monitor other than ping, you must configure the monitor before you can assign it to a node.

The EX appliance automatically checks the health of protocol ports on SLB protocol nodes with a non-configurable monitor. These monitors are not displayed in the configuration and cannot be changed or disabled.

For LLB links, link status is automatically determined by routing information. However, you can optionally assign a health monitor to a link. In this case, the monitor is used instead of routing information to determine the link's health.

Interval, Timeout, and Retries

By default, the EX Secure WAN Manager monitors a server's health once every 30 seconds and waits 5 seconds for a reply. If the server does not reply, the EX appliance retries the monitor up to 2 more times before determining that the server is down.

The EX appliance continues to send health checks to the server even after determining that the server is down. As soon as the server is available again and successfully replies to a health check, the EX appliance starts load balancing traffic to the server again.

The table below lists the health monitor options.

TABLE 7 Health Monitor Settings

Type	Description	Supported Values
Name	Name for the health monitor.	1 to 31 alphanumeric characters.
Interval	Number of seconds between each use of the health monitor.	15 to 180 seconds Default: 30 seconds
Retry	Maximum number of times the EX appliance will send the same health check to an unresponsive server before determining that the server is down.	1 to 4 Default: 3
Timeout	Number of seconds the EX appliance waits for a reply to a health check. If the server does not respond, the EX appliance does one of the following: • Resends the check, up to the number specified by Retry. • If the maximum number of retries has already been used, marks the server Down and stops sending client traffic to the server.	1 to 12 seconds Default: 5 seconds
Method	A method commonly corresponds to a protocol, such as ICMP, TCP, HTTP, etc., each of which has protocol-relative arguments. See Table 8 on page 106.	Health method name used, 1 to 31 alphanumeric characters

Health Methods

Table 8 on page 106 lists the health method types supported by the EX Secure WAN Manager. The health methods use the well-known port numbers for each application by default. You can change the port numbers and other options when you define the health methods.

Multiple health method instances can be defined using the same method type and different parameters. Alike, multiple health monitors can use the same health method to check different links, nodes, etc.

The following health method is included in the EX appliance configuration by default:

- ping - A health method of ICMP type named ping with default parameters.

When a health monitor is in use by a link or node, the monitor cannot be removed.

TABLE 8 Health Method Types

Type	Description	Successful If...	Configuration Required on Target Server
ICMP	The EX appliance sends an ICMP echo request (ping) to the server. To check the health of a path through other devices, enable the transparent option and specify the IP address at the other end of the path as the alias address. For example, in LLB, you can verify the health of an LLB link. **Note:** This is a Layer 3 health check only. Use the following health method types to check the health of a specific application.	Target device replies with an ICMP echo reply message.	Target device must be configured to reply to ICMP echo requests. If you are checking the health of a path, all devices along the path must allow ICMP echo replies to be forwarded.
TCP	The EX appliance sends a connection request (TCP SYN) to the specified TCP port on the server.	Server replies with a TCP ACK. By default, the EX appliance responds to the SYN ACK by sending an ACK, which completes the connection setup. To configure the EX appliance to send a RST (Reset) instead, enable the Halfopen option.	Destination TCP port of the health check must be valid on the server.
UDP	The EX appliance sends a packet with a valid UDP header and a garbage payload to the specified UDP port on the server.	Server does either of the following: • Replies from the specified UDP port with any type of packet. • Does not reply at all. The server fails the health check only if the server replies with an ICMP Error message.	Destination UDP port of the health check must be valid on the server.

TABLE 8 Health Method Types (Continued)

Type	Description	Successful If...	Configuration Required on Target Server
HTTP	The EX appliance sends an HTTP GET or HEAD request to the specified TCP port and URL. • GET requests the entire page. • HEAD requests only the meta-information in the header. If a user name and password are required to access the page, they also must be specified in the health check configuration.	Server replies with OK message (200). For GET requests, the server also must reply with the requested content or meta-information in the page header. The response must include the string specified in the Expect field on the EX appliance. For HEAD requests, the EX appliance ignores the Expect field and only checks for the server reply message.	Requested page (URL) must be present on the server. Also, for GET requests, the string specified as the expected reply must be present.
HTTPS	Similar to an HTTP health check, except SSL is used to secure the connection.	Same as the successful reply to an HTTP health check.	Same requirements as for HTTP health checks. Additionally, SSL support must be enabled on the server. A certificate does not need to be installed on the EX appliance. The EX appliance always accepts the server certificate presented by the server.
FTP	The EX appliance sends an FTP login request to the specified port. If anonymous login is not used, they also must be specified in the health check configuration.	Server replies with FTP OK message or Password message. If the server sends the Password message, the EX appliance sends the password specified in the health check configuration. In this case, the EX appliance expects the server to reply with another OK message.	Requested user name and password must be valid on the server.
SMTP	The EX appliance sends an SMTP Hello message.	Server sends an OK message (reply code 250).	Server recognizes and accepts the domain of sender. If SMTP service is running and can reply to Hello messages, the server can pass the health check.

TABLE 8 Health Method Types (Continued)

Type	Description	Successful If...	Configuration Required on Target Server
POP3	The EX appliance sends a POP3 user login request with the specified user parameter.	Server replies with an OK message. The EX appliance then sends the password specified in the health check configuration. The EX appliance expects the server to reply with another OK message.	Requested user name and password must be valid on the server.
SNMP	The EX appliance sends an SNMP Get or Get Next request to the specified OID, from the specified community.	Server replies with the value of the OID.	Requested OID and the SNMP community must both be valid on the server.
DNS	The EX appliance sends a lookup request for the specified domain name.	Server sends a reply with code 0.	Domain name in the lookup request must be in the server's database.
RADIUS	The EX appliance sends a Password Authentication Protocol (PAP) request to authenticate the user name and password specified in the health check configuration.	Server sends Access Accepted message (reply code 2).	Requested user name and password must be configured in the server's user database. Likewise, the shared secret sent in the health check must be valid on the server.
LDAP	The EX appliance sends an LDAP Bind request for the specified Distinguished Name. Optionally, SSL can be enabled for the health check. The EX appliance also must send a valid password, if one is required by the server.	Server sends a reply containing result code 0.	The Distinguished Name and password sent in the health check must be configured on the LDAP server. Additionally, the password must be valid on the server. A certificate does not need to be installed on the EX appliance. The EX appliance always accepts the server certificate presented by the server.
RTSP	The EX appliance sends a request for information about the file specified in the health check configuration.	Server replies with information about the specified file.	The file must be present on the RTSP server.

TABLE 8 Health Method Types (Continued)

Type	Description	Successful If...	Configuration Required on Target Server
SIP	The EX appliance checks for SIP communication on the port designated, the default is port 5060.	Sends a SIP request to the SIP port. Expects 200 OK in response. The request is an OPTION request, not a REGISTER request.	The server must be able to respond to SIP messages.
External	The EX appliance uses a tcl script selected from the Program pull-down menu. The port can be designated and arguments can be set in the respective fields.	Server replies with information requested in the script parameters.	This depends on the script and the application being checked.

Configure a Health Check

To configure a health check:

1. Configure a health method.

   A health method specifies the service to be checked, the type of health check to perform, and the information to send in the check.

2. Configure a health monitor.

   The monitor specifies the interval, timeout, number of retries, and the health method to use.

3. Bind the health monitor to a link or node.

4. Configure required health check values on the node.

Configure a Health Method

Use the following procedure to specify the protocol-specific parameters to use in health checks. The settings for a health-check method apply to all health monitors that use the method.

(For information about specific values, see Table 8 on page 106.)

1. Select Config Mode > Load Balance > Health Monitor.

2. On the menu bar, select Health Method.

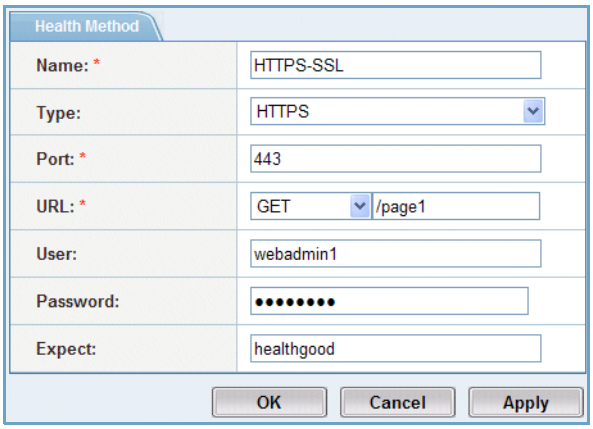
3. Click the New button. The Health Method tab appears. (See Figure 57.)

4. From the Type pull-down list, select the type of health check you want to perform. The remaining fields on the tab change based on the health-check type you select.

5. Set or select the remaining values as required for the type of health check.

6. Click OK.

FIGURE 57 Health Monitors – Health Method Tab



Configure a Health Monitor

Use the following procedure to specify the timer values and health check type for a health monitor.

(For information about specific values, see Table 7 on page 105 and Table 8 on page 106.)

1. Select Config Mode > Load Balance > Health Monitor.

2. On the menu bar, select Health Monitor, if not already selected.

3. Click the New button. The Health Monitor tab appears. (See Figure 58.)

4. In the Name field, enter a name for the monitor.

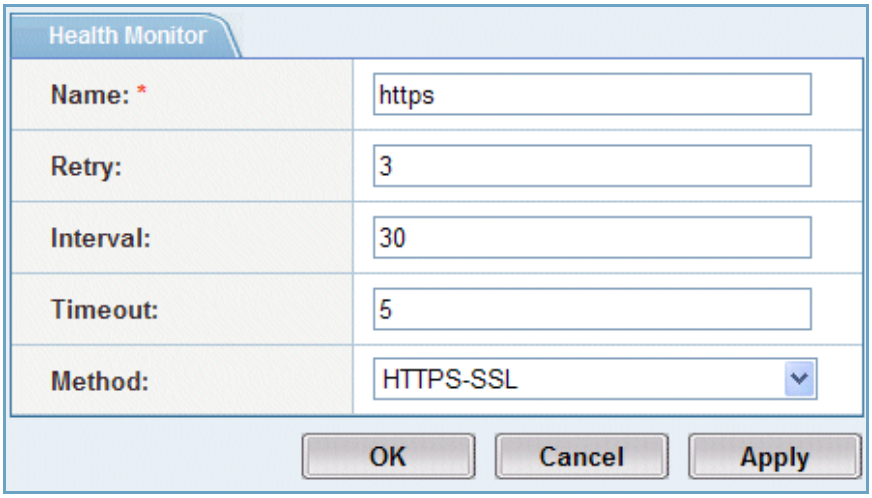
5. To change the number of retries, edit the number in the Retries field.

6. To change the interval between health checks, edit the number in the Interval field.

7. To change the number of seconds the EX appliance waits for the server to reply, edit the number in the Timeout field.

8. From the Method pull-down list, select the type of health check you want to perform.

FIGURE 58 Health Monitors – Health Monitor Tab



Bind a Health Monitor to a Link or Server

Health monitors take effect only when you bind them to a link or a server. The configuration procedures elsewhere in this chapter describe how to bind a health monitor to a link or node while you are configuring it.

If you have already configured the link or node, you can select it to open the configuration tabs, then select the health method.

To Bind a Health Monitor to an LLB Link

1. Select Config Mode > Load Balance > Link.
2. On the menu bar, select Link, if not already selected.
3. In the link table, select the link.

   The configuration tab for the link appears.
4. From the Monitor pull-down list, select the health monitor to use for checking the health of the link.
5. Click Apply or OK.

To Bind a Health Monitor to an FWLB Link

1. Select Config Mode > Load Balance > Firewall.
2. On the menu bar, select Firewall Node, if not already selected.
3. In the firewall node table, select the node.

   The configuration tab for the node appears.
4. From the Monitor pull-down list, select the health monitor to use for checking the health of the firewall node.
5. Click Apply or OK.

To Bind a Health Monitor to a CLB Link

1. Select Config Mode > Load Balance > Cache.
2. On the menu bar, select Cache Node, if not already selected.
3. In the cache node table, select the node.

   The configuration tab for the node appears.
4. From the Monitor pull-down list, select the health monitor to use for checking the health of the cache node.
5. Click Apply or OK.

To Bind a Health Monitor to an SLB Link

1. Select Config Mode > Load Balance > Server.
2. On the menu bar, select Server Node, if not already selected.
3. In the server node table, select the node.

   The configuration tab for the node appears.
4. From the Monitor pull-down list, select the health monitor to use for checking the health of the server node.
5. Click Apply or OK.

Configure Required Health Check Values on the Node

Some health checks require configuration on the target node. For example, health check of a Web node uses a GET or HEAD request for a specific URL. For the node to pass the health check, the requested page (URL) must

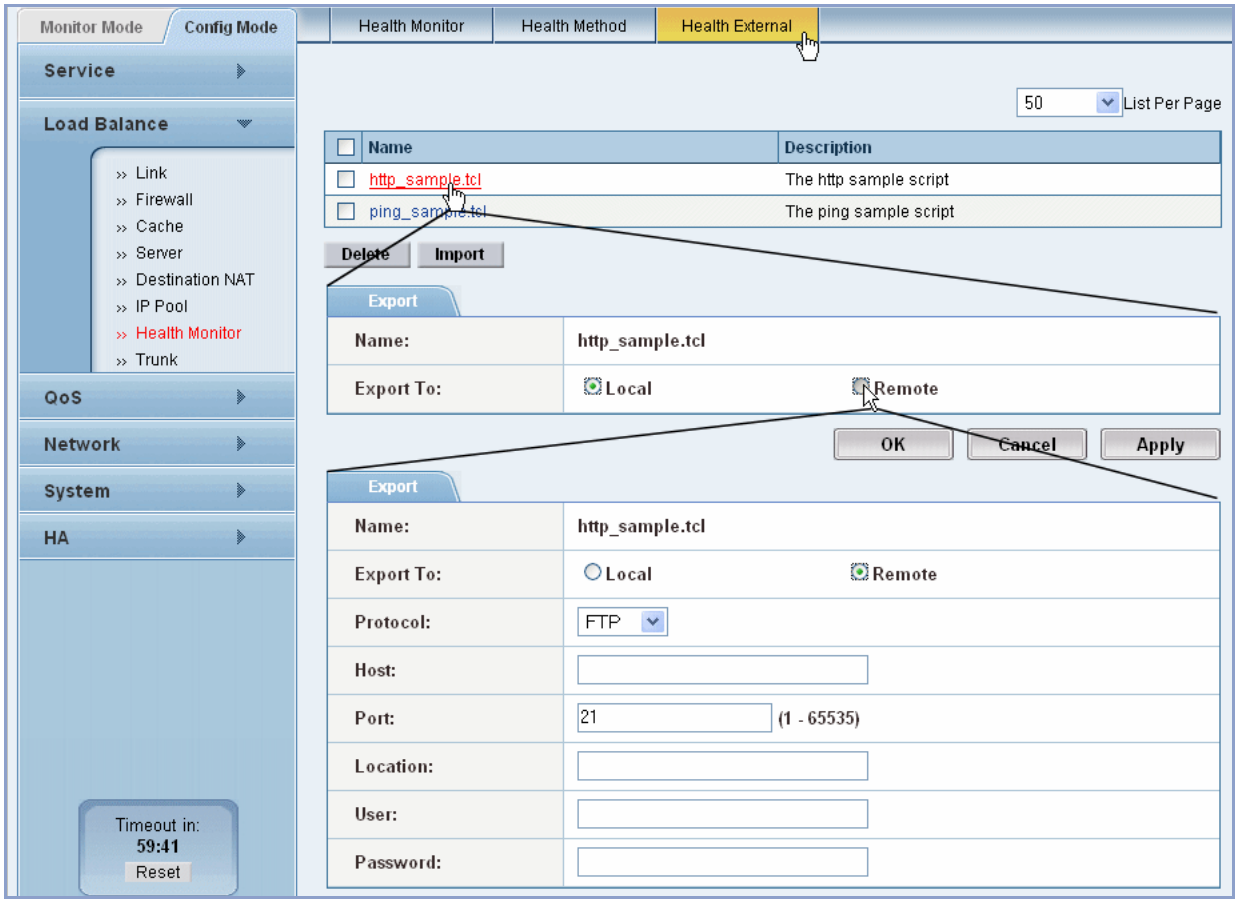
be on the node and the expected string reply must be present in the body or header of the page.

The node requirements are listed in Table 8 on page 106. To configure a node, consult the documentation for the node.

Health External - Import, Export or Delete Health Monitor Scripts

Health Monitor TCL scripts can be deleted or imported and exported to and from the EX Secure WAN Manager. Export steps are shown. To import, first click the Import button and enter the parameters of the script to import.

FIGURE 59 Health Monitor > Health External - Import, Export, or Delete



Trunking

You can configure a static trunk to aggregate load-balancing links. A trunk is a set of multiple physical Ethernet ports that use as a single, higher-capacity logical interface. A trunk interface has the combined capacity of all the physical interfaces in the trunk.

The EX appliance supports a maximum of 4 trunks. Each trunk can contain a maximum of 8 physical Ethernet interfaces. An Ethernet interface can be a member of only a single trunk.

When you add an Ethernet interface to a trunk, the following settings are replaced with those set on the trunk:

- IP address
- MAC address
- Speed configuration
- Mode (duplex, half-duplex, and so on)
- MTU size

Operations such as setting an IP interface or VLAN are performed on the lead member of the trunk, which is the lowest-numbered interface. For example, to configure an IP interface on a trunk containing ports 1-4, add the interface to port 1.

Trunk Load Balancing Methods

To optimize use of a trunk interface, the EX appliance load balances traffic among the physical interfaces in the trunk. Table 9 lists the trunk load-balancing methods supported by the EX appliance. A trunk can support a single load-balancing method. The load-balancing method is used or all unicast traffic sent on the trunk.

TABLE 9 Load Balance Trunk Load Balancing Methods

Load Balancing Method	Unicast Traffic Is Load-Balanced Based On...
src-mac	Source MAC address
dst-mac	Destination MAC address
src-dst-mac	Source and destination MAC addresses
src-ip	Source IP address
dst-ip	Destination IP address
src-dst-ip	Source and destination IP addresses
src-port	Source Layer 4 protocol port
dst-port	Destination Layer 4 protocol port

TABLE 9 Load Balance Trunk Load Balancing Methods (Continued)

Load Balancing Method	Unicast Traffic Is Load-Balanced Based On...
src-dst-port	Source and destination Layer 4 protocol ports
vlanID	VLAN ID
src-ip-port	Source IP protocol port
dst-ip-port	Destination IP protocol port
src-dst-ip-port	Source and destination IP protocol ports
src-ip-vlan	Source IP address and VLAN ID
dst-ip-vlan	Destination IP address and VLAN ID
src-dst-ip-vlan	Source and destination IP address and vlan ID
src-ip-port-vlan	Source IP address, source Layer 4 protocol port, and VLAN ID
dst-ip-port-vlan	Destination IP address, source Layer 4 protocol port, and VLAN ID
src-dst-ip-port-vlan	Source and destination IP address, source Layer 4 protocol port, and VLAN ID

Multicast traffic is load balanced as follows:

- Multicast traffic that includes Layer 4 information – load balanced based on source IP address, source Layer 4 protocol port, destination IP address, and destination Layer 4 protocol port
- Multicast traffic without Layer 4 information – load balanced based on source and destination IP addresses
- Non-IP multicast traffic – load balanced based on source and destination MAC addresses

Notes

- It is recommended not to use an HA interface in a trunk. If an interface in a trunk is also configured for High Availability (HA), HA operations can change interface settings such as MAC address and IP address. In this case, the interface's HA settings may conflict with the trunk settings.
- When configuring a trunk, be careful if adding the management interface to the trunk. If you add the interface your GUI or CLI management session is using to a trunk, your management session will end and you will lose management access on that interface.

Configure Trunk

To configure a load-balancing trunk:

1. Select Config > Load Balance > Trunk.
2. In the Number field, enter the trunk number, 1-4.

3. Select the load balancing method from the Load balance method drop-down list. (See Table 9 on page 114.)
4. Add Ethernet interfaces to the trunk:
   a. Select an interface from the drop-down list and click Bind.
   b. Repeat for each interface to be added to the trunk.
5. Select the Enable checkbox.
6. Click Apply or OK.

Display Trunk Information

To display trunk information, select Monitor > Load Balance > Trunk. Configuration and status information as well as traffic statistics are displayed.

Display Load-Balancing Statistics

You can display statistics and graphs for the following:

- LLB links and link groups
- FWLB nodes and groups
- CLB nodes and cache groups
- SLB nodes and groups

Statistics are available in tabular or graph form. The tables contain a separate row for each link, node, or group. The graphs show traffic activity for a single link, node, or group.

Tabular Displays

Display Link or Node Statistics

For individual link or node statistics, select one of the following:

- Monitor Mode > Load Balance > Link
- Monitor Mode > Load Balance > Firewall
- Monitor Mode > Load Balance > Cache

- Monitor Mode > Load Balance > Server
- Monitor Mode > Load Balance > Trunk

Display Group Statistics

For group statistics, select one of the following:

- Monitor Mode > Load Balance > Link, followed by the Link Group menu bar option
- Monitor Mode > Load Balance > Firewall, followed by the Firewall Group menu bar option
- Monitor Mode > Load Balance > Cache, followed by the Cache Group menu bar option
- Monitor Mode > Load Balance > Server, followed by the Service Group menu bar option

Column Descriptions

Both the link table and the link group table have counters for bytes, packets, and connections.

The link table also has a Status column, which can have one of the following values:

- Up / Running – The link or node is up. For LLB, the value is “Up”. For CLB, FWLB, and SLB, the value is “Running”.
- Down / Stopped – The link or node is down. For LLB, the value is “Down”. For CLB, FWLB, and SLB, the value is “Stopped”.
- Incomplete – The configuration has not been completed by the administrator. All the following are required to complete a link’s configuration:
  - IP address and network mask
  - Gateway address and network mask
  - NAT address. The NAT address must be in the same subnet as the gateway address.

The Report column enables you to display graphs for an individual link, node, or group. To display a graph, click  . (See “Graphs” on page 118.)

Data Refresh

Statistics counters start incrementing from 0 after the most recent reboot or the most recent clear performed by an administrator.

To refresh the display with the latest counter values, click Refresh. You also can enable automatic refresh by selecting the refresh rate from the pull-down list next to the Refresh button. For example, to automatically refresh the counters once a minute, select 60 from the pull-down list. By default, automatic refresh is disabled.

To clear the counters, click Clear.

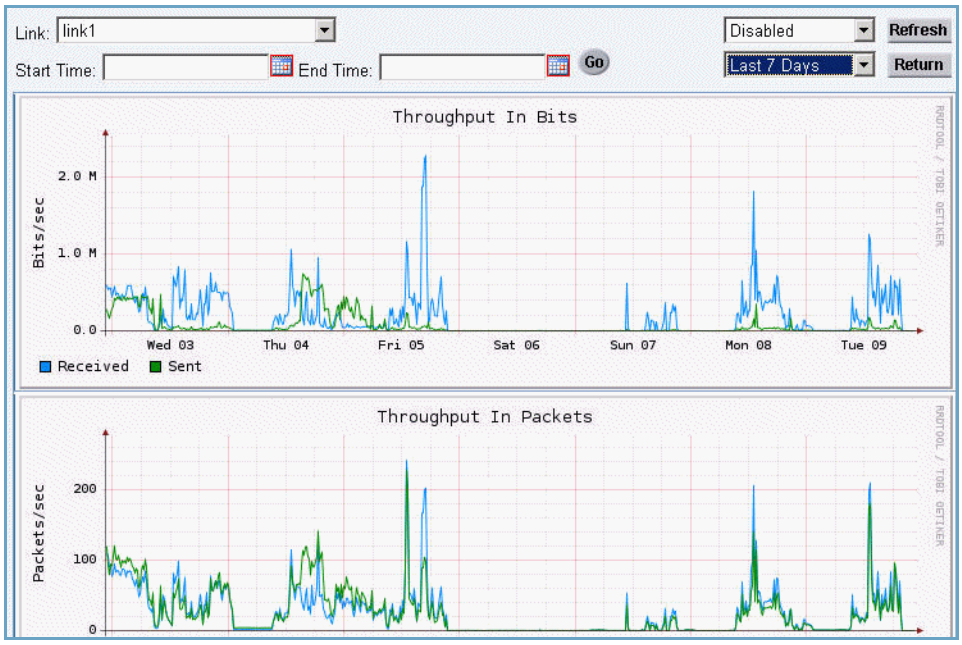
Graphs

For any load-balancing link, node, or group, you can display graphs of the following statistics:

- Throughput in Bits – Number of bits forwarded to the link, node, or group by the EX appliance.
- Throughput In Packets – Number of packets forwarded to the link, node, or group by the EX appliance.
- Active Connections – The number of traffic flows currently using the link, node, or group.
- New Connections – This is the rate, or number of new connections per second the EX appliance set up on the link, node, or group.

Figure 60 shows an example of Link statistics.

FIGURE 60 Load-Balancing Statistics - Link



All four graphs are displayed in the same window. To view the graphs, scroll up or down.

Note: In the legends for the vertical axes of graphs, “m” means 1/1000, whereas “M” means 1000000. “K” or “k” means 1000.

Displaying Graphs

To display statistics in a graph, do one of the following:

- If you are already viewing the statistics in a table, click in the Report column.
- Navigate to the monitor options for the type of load balancing for which you want to display a graph (for example, Monitor Mode > Load Balance > Link).

  Next, select one of the following options from the menu bar:
  - Statistics > Link
  - Statistics > Link Group
  - Statistics > Firewall Node
  - Statistics > Firewall Group
  - Statistics > Cache Node

- Statistics > Cache Group
- Statistics > Server Node
- Statistics > Service Group

When graphs for a configuration item are displayed, you can easily select another item of the same type to graph. For example, if you are displaying graphs for a firewall group, you can select a different firewall group from the pull-down list at the top of the display.

Time Span

The horizontal (x) axis of each graph shows the time span of the data in the graph. The same time span is used for all four graphs.

To change the time span, do one of the following:

- Select a new span from the pull-down list to the left of the Start Time field. The spans you can select range from 10 minutes to 30 days.
- Use the calendars to select specific start and end dates and times.

To select a date and time using the calendars:

1. Click  (the calendar icon) next to Start Time or End Time.

   (They must be selected separately.)

2. Select the month and year.
   - To scroll through years, click double brackets (<< or >>).
   - To scroll through months, click a single bracket (< or >).
3. Select the day of the month.

   To change the day of the week that starts each week, click the day (Mon, Tue, and so on).

4. Select the time. Place the cursor over the hours or minutes counter and do one of the following:
   - To select a later time, click on the hours or minutes counter to scroll forward.
   - To select an earlier time, hold Shift and click on the hours or minutes counter to scroll backward.
5. Click **x** in the upper right corner of the calendar to save the settings and close the calendar.

   The date and time selected appear in the Start Time or End Time field.

   Click Go to redraw the graphs using the new time span.

Data Refresh

Data refresh works the same as it does for tabular displays. (See "Data Refresh" on page 118.)

Return to the Tabular Display

To display the tabular view of the statistics, click Return.

Traffic Analysis and Quality of Service

This chapter describes how to configure Quality of Service (QoS) and how to display traffic statistics.

QoS Features

The EX Secure WAN Manager QoS features enable you to control the bandwidth consumption and priority of traffic.

You can configure the following types of QoS:

- Rate Shaping – Rate shaping guarantees a specific amount of bandwidth to an interface or individual QoS class, and specifies the maximum amount of bandwidth the interface or QoS class can consume. Rate shaping buffers packets that have exceeded a configured threshold and sends them at a later time.
- Rate Limiting – Rate limiting *polices* the bandwidth use of a QoS class by enforcing a specified maximum rate and taking action against traffic that exceeds the rate. Unlike rate shaping, rate limit does not buffer packets. Instead, packets that exceed a configured threshold are typically dropped.
- Marking – Priority marking changes the Diffserv Control Point (DSCP) values in the IP packet headers of a QoS class to change their forwarding priority throughout the network. Marking changes the priority used for packet routing in EX appliance internally.
- Drop – You can configure the EX appliance to drop all traffic of a specific class.

QoS Classes

The EX Secure WAN Manager manages traffic based on QoS classes. A QoS class consists of rules. Rules consist of Layer 7 application protocols and some field values in the IP header, for example, source IP address, source port, etc.

QoS classes are used to monitor and classify traffic. Once classified, the traffic can then be managed with rate shaping, rate limiting, and marking.

The EX appliance is configured by default with more than one-hundred QoS classes for a large set of well-known applications. You can modify or

delete classes and even add new classes. (For the complete list of QoS classes configured on the EX appliance, select Config Mode > QoS > Class.)

Attributes of QoS Classes

Attributes that define a QoS class on the EX Secure WAN Manager are shown in Table 10.

TABLE 10 QoS Class Attributes

Parameter	Description
Name	String to uniquely identify the class. For well-known classes, the well-known names are used. (For example: ftp, http, yim, and so on.) For the complete list of QoS classes configured on the EX appliance select: Config Mode > QoS > Class.
Category	High-level description of the type of QoS class. The EX appliance uses the following categories: • Application • Database • DirectoryService • Email • File • Games • IP-Protocol • Messaging • Misc • Multimedia • Others • P2P • Security • Session • VOIP • Vlan • extif • intif • subnet
Rules List	Match criteria that defines the traffic in the class. (See "Traffic Class Rules" on page 127.)

The *Others* Class

In addition to the set of QoS classes for well-known applications, the EX Secure WAN Manager also has a class called *others*. The *others* is used for traffic whose applications do not match any of the default applications in the pre-configured QoS classes.

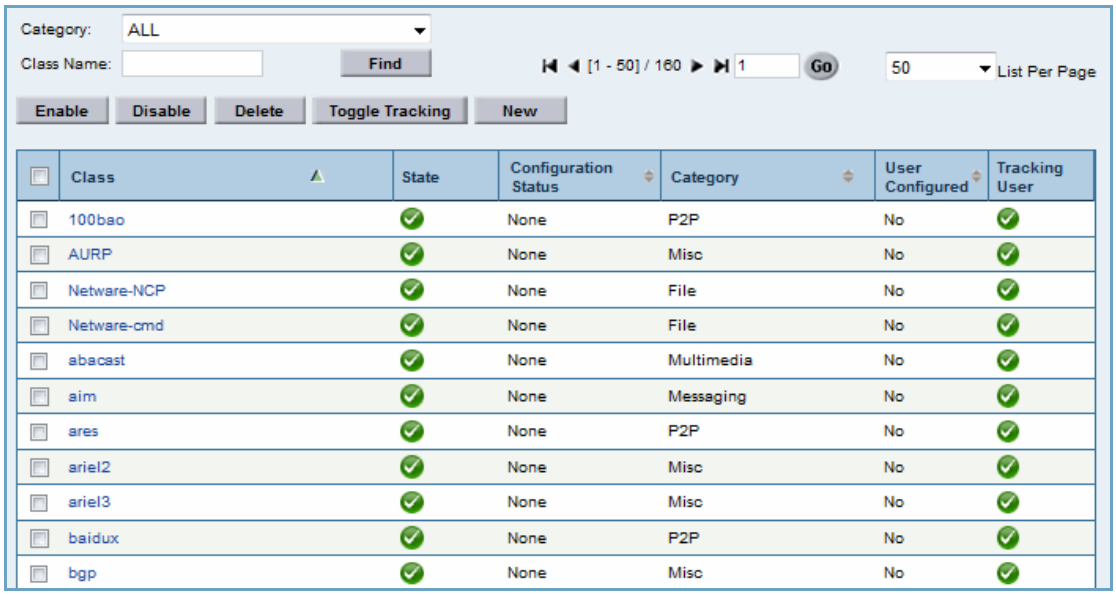
In traffic monitoring, statistics are listed individually for each class and for the *others* class.

Display QoS Classes

To display the configured QoS classes:

1. Select Config Mode > QoS > Class.
2. On the menu bar, select Class, if not already selected. The list of configured classes appears. (See Figure 61.)
3. To display the configuration for a class, click on the name in the Class column. The Class tab appears. (See Figure 62 on page 127.)
4. To display details for a rule, select the rule, then click Edit. The Rule tab appears. (See Figure 63 on page 130.)
5. When you are finishing viewing the rule's configuration, click Cancel to return to the Class tab.
6. When you are finished viewing the class configuration, click Cancel again to return to the class list.

FIGURE 61 QoS Class Table



The State column indicates whether QoS classification features are enabled for the QoS class.

- – Classification features are enabled.
- – Classification features are disabled.

To change the state, select the checkbox next to the class name and click Disable or Enable.

Note: If the class is disabled, the class will seem to not exist and the traffic will not be classified.

The Toggle Tracking button is used to enable or disable tracking users. Select the checkbox next to the class name and click the Toggle Tracking button to change the user tracking state for the class. The Tracking User column indicates whether the users are currently being tracked for the class.

- – Tracking User is enabled.
- (blank) – Tracking User is disabled.

The Configuration Status can be one of the following:

- None – The class is not used in a QoS policy.
- Policy defined – The class is used in a QoS policy.

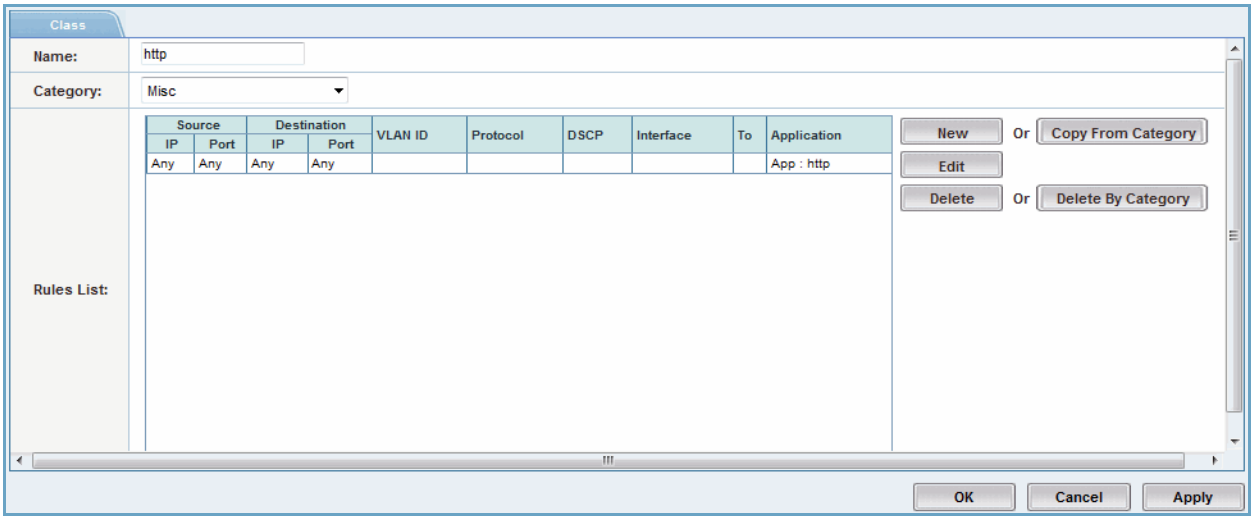
Click the Category menu to display the existing Categories, which include the default Categories and any newly added Categories.

Default categories cannot be deleted, but you can delete user-defined Categories by selecting the checkbox to the left of their name and then the clicking the Delete button.

You can add a new Category by clicking the New button.

To edit an existing Category, click on the Category name under the Name heading to open the Category tab.

FIGURE 62 QoS class – Configuration Details



This example shows the default configuration for the http QoS class. The class has one rule that matches on all sources and destinations.

Traffic Class Rules

Rules are used to specify the traffic that matches a class. The preconfigured traffic classes have preconfigured rules. You can modify the rules that

define a class' traffic. You also can configure new traffic classes and the rules that define them.

Each rule contains the following information:

- Source IP – You can specify one of the following:
  - IP address and mask – Host or subnet IP address. If specifying an individual host address, enter mask 255.255.255.255.
  - Category – Configured list of Categories. To configure a Category, see "Category" on page 131.
  - IP List – Configured list of IP addresses. To configure an IP list, see "IP List" on page 131.
  - ID Group – Configured list of user IDs. To configure an ID group, see "ID Group" on page 132.
  - Domain Group – Configured list of domain names. To configure a domain group, see "Domain Group" on page 132.
  - Abuser Criteria – Configured list of traffic thresholds that indicate abuse of network resources. To configure abuser criteria, see "Abuser Criteria" on page 133.

  By default, the source IP is included in the class. To exclude the source IP from the class instead, select the Except checkbox.
- Source MAC – You can enter a MAC address.
- Source Port – You can specify an individual protocol port number or select a configured list of port numbers. To configure a port list, see "Port List" on page 131.

  By default, the source port is included in the class. To exclude the source port from the class, select the Except checkbox.
- Destination IP – The options are the same as those for Source IP.

  By default, the Destination IP is included in the class. To exclude the Destination IP from the class, select the Except checkbox.
- Destination MAC – You can enter a MAC address.
- Destination Port – The options are the same as those for Source port.
- VLAN ID – Local VLAN the traffic is on. The local VLAN is a VLAN configured on the EX appliance. To be available for selection when configuring a policy, the VLAN must already be configured on the EX appliance.
- Protocol – IP protocol number or Layer 4 protocol (ICMP, TCP, or UDP).
- DSCP – DiffServ Code Point; ranges from AF11 to AF43, or CS1 to CS7; other options include EF or *others*.

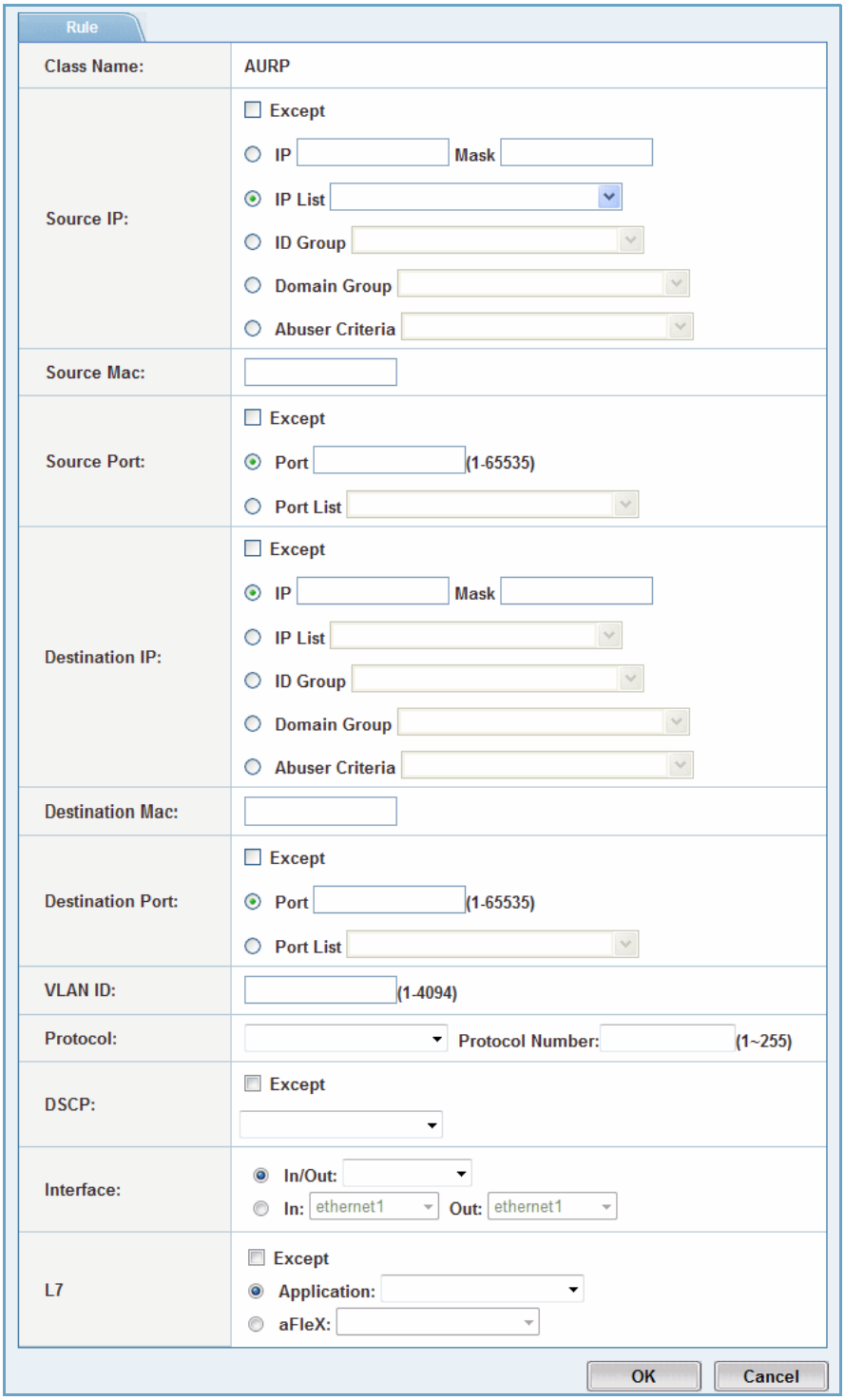
By default, the DSCP is included in the class. To exclude the DSCP from the class, select the Except checkbox.

- Interface – You can either specify a single interface for both incoming and outgoing traffic; or specify two separate interfaces, one for incoming traffic and the other for outgoing traffic.
- L7 – Type of application traffic. You can specify one of the following:
  - Application – for a well-known QoS class recognized by the EX appliance, the application name is the same as the QoS class name.
  - aFleX – A script that defines the application traffic. See "aFleX Script" on page 133.

  By default, the L7 application and aFleX traffic are included in the class. To exclude either of these, select the Except checkbox.

A valid QoS class has at least one rule. An empty rule matches on all valid sources and destinations. You can narrow the scope of a QoS class by modifying or deleting this rule and adding rules for specific sources and destinations.

FIGURE 63 QoS Class – Rule Configuration Details



Category

To configure a Category:

1. Select Config Mode > QoS > Class.
2. On the menu bar, select Category.
3. Click the New button.
4. Enter a name for the category in the Name field.
5. (Optional) Enter a brief summary in the Description field.
6. Use the arrow buttons (<<) to include traffic classes into this Category, or use the or (>>) arrow button to remove classes, as desired.
7. Click Apply to configure another Category, or click OK to finish.

IP List

To configure an IP list:

1. Select Config Mode > QoS > Class.
2. On the menu bar, select IP List.
3. Click New.
4. Enter a name for the list in the Name field.
5. To add an individual IP address to the list, select IP, enter the address in the IP field, and click Add. The address appears in the list. Repeat for each individual address to add.
6. To add a range of IP addresses, select IP Range. Enter the lowest address in the range in the From field. In the To field, enter the highest address in the range. Click Add. The range appears in the list. Repeat for each address range to add.
7. Click Apply to configure another IP list, or click OK to finish.

Port List

To configure a port list:

1. Select Config Mode > QoS > Class.
2. On the menu bar, select Port List.
3. Click New.

4. Enter a name for the list in the Name field.
5. To add an individual protocol port to the list, select Port, enter the port in the Port field, and click Add. The port appears in the list. Repeat for each individual port to add.
6. To add a range of ports, select Port Range. Enter the lowest port number in the range in the From field. In the To field, enter the highest port number in the range. Click Add. The range appears in the list. Repeat for each port range to add.
7. Click Apply to configure another port list, or click OK to finish.

ID Group

To configure an ID group:

1. Select Config Mode > QoS > Class.
2. On the menu bar, select ID Group.
3. Click New.
4. Enter a name for the group in the Name field.
5. Enter a user ID in the entry field and click Add. Repeat for each user to add.
6. Click Apply to configure another ID group, or click OK to finish.

Domain Group

To configure a domain group:

1. Select Config Mode > QoS > Class.
2. On the menu bar, select Domain Group.
3. Click New.
4. Enter a name for the group in the Name field.
5. Enter a domain name in the Domain Name field and click Add. Repeat for each domain name to add. The EX appliance performs a DNS lookup on the domain name to obtain the IP addresses.

   Wildcard characters ***** and **?** are supported.
6. Click Apply to configure another domain group, or click OK to finish.

aFleX Script

You can use aFleX scripts to specify traffic signatures for Layer 7 traffic classes that are not already recognized by the EX appliance.

To add an aFleX policy:

1. Select Config Mode > QoS > Class.
2. On the menu bar, select aFleX.
3. Click New.
4. Enter a name for the script the Name field.
5. Enter the script syntax in the Definition field. For syntax information, see the *EX Series aFleX Reference*.
6. Click Apply. The EX appliance checks the syntax and displays error messages to indicate any syntax errors.
7. After all syntax errors have been corrected, click OK.

Abuser Criteria

Abuser criteria provide a means to identify traffic flows and network users (IP addresses) that are abusing network resources.

Abuser criteria enable you to proactively manage available bandwidth and control bandwidth utilization in cases where application protocol (traffic class) classification is unable to do so.

A set of abuser criteria consists of thresholds that define when a user's traffic is considered abusive, and when the traffic is no longer abusive. Each set of abuser criteria consists of the following parameters:

- Status – Indicates whether the set of abuser criteria is active (enforced).
- Period – Indicates the minimum number of minutes a user (IP address) remains on the abuser list after being added to it. The action taken by the EX appliance on users in the abuser list is specified in the QoS policy for the traffic class. The period can be 1-3600 minutes (2-1/2 days). The default is 5 minutes.
- Scope – Indicates the traffic classes to which the abuser criteria apply. By default, a set of abuser criteria applies to all traffic classes.
- Fall In thresholds – Specifies the upper thresholds allowed for a user's traffic before the traffic is considered to be abusive.
- Fall Out thresholds – Specifies the upper thresholds an abuser's traffic must remain at or below before the user is removed from the abuser list.

Specifying fall-out thresholds is optional. The fall-in thresholds are used by default.

You can define fall-in and fall-out thresholds for each of the following:

- Long-lived connections – A long-lived connection is one that is active longer than the maximum number of minutes allowed. You can specify the maximum number of minutes a connection can be active before it becomes long-lived, 5-1440 minutes. You also can specify the maximum number of concurrent long-lived connections (1-200) allowed per user within the specified duration.
- New connections – Maximum number of new connections allowed (1-10000), for the specified duration (1-1440 minutes).
- New-connection rate – Maximum number of new connections per second (1-200), for the specified duration (1-60 minutes).
- Traffic rate – Maximum traffic rate (1-8000000 kbps), for the specified duration (1-1440 minutes). You can specify the traffic direction (inbound or outbound). By default, the threshold applies to both directions.

  You can specify the maximum allowed percentage (1-100) of large packets. A packet is considered to be long if it is equal to or greater than the length you specify (256, 512, or 1024 bytes). If you specify a percentage, the default large packet size is 1024.

Note: You also can manually add or remove individual IP addresses in the abuser list.

To add abuser criteria:

1. Select Config Mode > QoS > Class.
2. On the menu bar, select Abuser Criteria.
3. Click New.
4. Enter a name for the criteria in the Name field.
5. Specify the status of the criteria, Enabled or Disabled. The criteria are enforced only if they are enabled.
6. In the Period field, enter the minimum number of minutes an abuser IP address remains on the abuser list.
7. In the Scope field, select the traffic classes to which to apply the criteria. To apply the criteria to all traffic classes, select All. To exclude a class

from enforcement of the criteria, select the class, then select the Except checkbox.

8. To configure the entry thresholds that indicate network abuse is occurring:
   a. Click the Fall In tab.
   b. Enter the threshold values.
9. To configure the exit thresholds that indicate network abuse is no longer occurring:
   a. Click the Fall Out tab.
   b. Enter the threshold values.
10. Click Apply to configure another set of abuser criteria, or click OK to finish.

Modify or Add a QoS Class

To modify or add a QoS class:

1. Select Config Mode > QoS > Class.
2. On the menu bar, select Class, if not already selected. The list of configured classes appears.
3. To modify an existing class, click on the name in the Class column. The Class tab appears.

   To add a new class, click New. (The New button is located at the bottom of the display.) The Class tab appears.
4. If you are adding a new class, enter a name in the Name field.

Note: If you edit the name of a class that is already configured, the EX appliance does not change the class. Instead, the EX appliance creates a new class.

5. From the Category pull-down list, select the category for the class.
6. To modify a rule for an existing class, select the rule and click Edit. The Rule tab appears.

   To add a new rule, click New. The Rule tab appears.

7. Enter the rule information. (See "Traffic Class Rules" on page 127.)

   If you are not editing or adding any rules, go to step 11.

   For any field, to match on all values, leave the field blank.

8. Click OK to return to the Class tab. The new or modified rule appears in the rules list.

9. To copy rules from existing classes based on category:
   a. Click Copy From Category. A class list appears.
   b. Select the category. By default "All" is selected. The list is modified to display only the classes in the selected category.
   c. Select individual classes by clicking the checkbox next to each class name. To select all the displayed classes, click the checkbox at the top of the list.
   d. Click Return. The rules for those classes appear in the Rule List for the class you are configuring.

10. To delete rules from the class you are configuring based on category:
    a. Click Delete By Category. A class list appears.
    b. Select the category. By default "All" is selected. The list is modified to display only the classes in the selected category.
    c. Select individual classes by clicking the checkbox next to each class name. To select all the displayed classes, click the checkbox at the top of the list.
    d. Click Return. The rules for those classes are deleted form the Rule List for the class you are configuring.

11. Click OK to save the class changes. The class table is displayed. If you add a new class, the class appears in the table.

Delete a QoS Class

To delete a QoS class:

1. Select Config Mode > QoS > Class.

2. On the menu bar, select Class, if not already selected. The list of configured classes appears.

3. Click on the checkbox next to the class name to select the class.

4. Click Delete.

Layer 7 Application List for EX Secure WAN Manager

TABLE 11 L7 Application List for EX Secure WAN Manager

	Application	Comment
Database	**MSSQL**	MS SQL 2000, 2005
	Oracle (and by database)	Oracle 8.0, 10.0
DirServ	**LDAP**	ldap3
	RADIUS	RADIUS protocol
Email	**IMAP**	Internet Message Access Protocol
	POP3	Post Office Protocol
	SMTP	Simple Mail Transport Protocol
File	**CIFS-SMB**	Common Internet File System Protocol
	NFS	Network File System Protocol
	TFTP	Trivial File Transport Protocol
Messaging	**AOL-AIM-ICQ**	America Online Instant Messenger
	fetion	China Mobile Instant Messaging Service
	GoogleTalk	Google talk service
	MSN-Messenger	Microsoft MSN Messenger
	QQ	Tencent Instant Messenger
	YahooMsg	Yahoo Instant Messaging Service
Misc	**Exchange**	Microsoft Exchange
	FTP	File Transport Protocol
	HTTP	Hyper Text Transport Protocol
	HTTP.HOST	Host name for HTTP header
	HTTP.USER-AGENT	User agent name for HTTP header
	HTTP.CONTENT-TYPE	Content type for HTTP body
	HTTP.CONTENT	HTTP payload
	HTTP.RANGE	Range for HTTP header
	HTTP.URL	URL for HTTP
	HTTP.HEADER	Any other HTTP header
	Lotus	Lotus
	VNC	Virtual Network Computing

TABLE 11 L7 Application List for EX Secure WAN Manager

	Application	Comment
Multimedia	**Abacast**	AbaCast online audio/video service
	flv	Adobe Flash Video player
	iTunes	Apple iTunes music player
	MSMMS	Windows Media Server
	QuickTime	Apple QuickTime media player
	RTSP	Real Time Streaming Protocol, using it to block Real.com Online radio
	YouTube	YouTube
Peer to Peer	**100bao**	P2P protocol
	Ares	P2P protocol
	BaiduX	P2P protocol
	BitTorrent and BitSpirit	BitTorrent and BitSpirit protocol
	Cspace	P2P protocol
	Dijjer	P2P protocol
	DirectConnect	P2P protocol
	eDonkey-eMule	eDonkey P2P protocol
	FreeCast	P2P protocol
	FurthurNet	P2P protocol
	Gnutella	Gnutella P2P protocol
	Huntmine	P2P protocol
	iMesh	P2P protocol
	Kazaa and Kazaa Lite	P2P protocol
	Krawler	P2P protocol
	Kugoo	P2P protocol
	Lime Wire	P2P protocol
	OpenNAP	P2P protocol
	POCO	P2P protocol
	PPLive	P2P online media
	PPStream	P2P online media
	QQLive	P2P protocol
	TVAnts	P2P online media
	Share	P2P protocol
	Share EX2	P2P protocol
	sopcast	P2P protocol
	SoulSeek	P2P protocol
	UUSee	P2P protocol
	WinMX	P2P protocol
	Xunlei	P2P protocol

TABLE 11 L7 Application List for EX Secure WAN Manager

	Application	Comment
Session	**remote-desktop**	Microsoft Remote Desktop Protocol
	Telnet	Telnet protocol
VOIP	**H.323Q931**	H323 Q931
	H.323ras	H323 RAS
	Megaco	Media Gateway Control (H.248)
	MGCP	Media Gateway Control Protocol
	RTP	Realtime Transport Protocol
	RTCP	Realtime Transport Control Protocol
	SIP	Session Initial Protocol, VOIP related
	Skinny (SCCP)	Cisco's Skinny client control protocol
	Skype	A popular voip client
	T.120	T.120
Security	**SSL**	Secure Socket Layer Protocol
	SSH	Secure Shell Remote Login Protocol

Layer 4 Application List for EX Secure WAN Manager

TABLE 12 L4 Application List for EX Secure WAN Manager

	Application	Comment
DirServ	**RRP**	Registry Registrar Protocol
	bootps	Bootstrap Protocol, server.
	Bootpc	Bootstrap Protocol, client.
	finger	The Finger User Information Protocol.
	whois	Whois and Network Information Lookup Service Whois++
	tacacs	Login host protocol
	ident	Identification Protocol
	crs	Microsoft Content Replication Service
	dns	Domain Name System
	kerberos	The Network Authentication Protocol.
	ldaps	LDAP over SSL

TABLE 12 L4 Application List for EX Secure WAN Manager

	Application	Comment
Email	**biff**	UNIX new mail notification
	imaps	IMAP over SSL
	pop3s	POP-3 over SSL
	smtps	SMTP over SSL (TLS)
File	**netbios-ns**	NETBIOS Name Service
	netbios-dgm	NETBIOS Datagram Service
	netbios-ssn	NETBIOS Session Service
	Netware-NCP	Netware 5 Core Protocol
	Netware-cmd	Netware 5 - Compatibility Mode Drivers service group
	fujitsu-dev	Fujitsu Device Control
	rsync	UNIX remote file synchronization protocol
Session	**matip-type-a**	Mapping of Airline Traffic over Internet Protocol, Type A
	matip-type-b	Mapping of Airline Traffic over Internet Protocol, Type B
	cvspserver	CVS client/server operations
	rexec	remote process execution
	who	Maintains data bases for who's logged on a local net and the average load of the machine
	login	Maintains data bases for who's logged on a local net and the average load of the machine
	rtelnet	Remote Telnet Service
	telnets	telnet over TLS/SSL
	stun	Simple traversal of UDP over NATs (STUN)
Messaging	**irc**	Internet Relay Chat Protocol.
	Ircs	irc over TLS/SSL

TABLE 12 L4 Application List for EX Secure WAN Manager

	Application	Comment
Misc	**gopher**	Internet Gopher
	uucp	Unix To Unix Copy
	ntp	Network Time Protocol.
	rpc2portmap	Coda portmappe
	sunrpc	Remote Procedure Call Protocol
	ariel2	Infotrieve document delivery system
	ariel3	Infotrieve document delivery system
	shell	UNIX remote shell command
	AURP	AppleTalk Update-based Routing Protocol
	snmp	Simple Network Management Protocol
	snmptrap	Simple Network Management Protocol traps
	router	Routing Information Protocol
	bgp	Border Gateway Protocol
	nntp	Network News Transfer Protocol
	nntps	Network News Transfer Protocol over ssl
	echo	Echo Protocol
	daytime	Daytime Protocol.
	syslog	syslog Protocol
	printer	Line Printer Daemon Protocol
	ipp	Internet Printing Protocol.
	time	Time Protocol
	dhcp-client	Dynamic Host Configuration client Protocol
	dhcp-server	Dynamic Host Configuration server Protocol
	sftp	Simple File Transfer Protocol
	lotus	Lotus Application Protocol
Security	**isakmp**	Internet Security Association and Key Management Protocol
	Socks	Protocol for sessions traversal across firewall securely

Traffic Policies

The EX appliance offers two methods of applying Traffic Policies (1) Easy QoS Mode and (2) Advanced QoS Mode.

- **Easy QoS Mode** – Offers a simplified, GUI-based way to configure QoS policies. For more details, See "Easy QoS Mode" on page 142.
- **Advanced QoS Mode** – Offers a more powerful, CLI-based method of configuring QoS policies, although it is not as intuitive for new users. For more details, See "Advanced QoS Mode" on page 150.

Easy QoS Mode

Easy QoS Mode simplifies all settings related to QoS policy and QoS interface configuration. This newer approach is based on a hierarchical tree structure, and with it, you can (1) create a traffic class to identify specific types of traffic, and (2) identify an action to be applied to traffic that matches the class.

By default, new EX appliances are deployed in Easy QoS Mode while existing deployments, (which were deployed in Advanced QoS Mode), will remain in Advanced QoS Mode.

Note: QoS configuration files created in Advanced QoS Mode are incompatible with those created in Easy QoS Mode. Thus, A10 strongly recommends that users who have configured their systems in Advanced QoS Mode should remain in Advanced QoS Mode.

Easy QoS Mode, which can only be executed via the GUI and ***not*** the CLI, simplifies the configuration of QoS policies by removing the concepts of "ingress" and "egress", and it QoS policies are no longer required to be bound to QoS Interfaces. This is in contrast to Advanced QoS Mode, which requires users to define a QoS policy before binding it to a QoS interface.

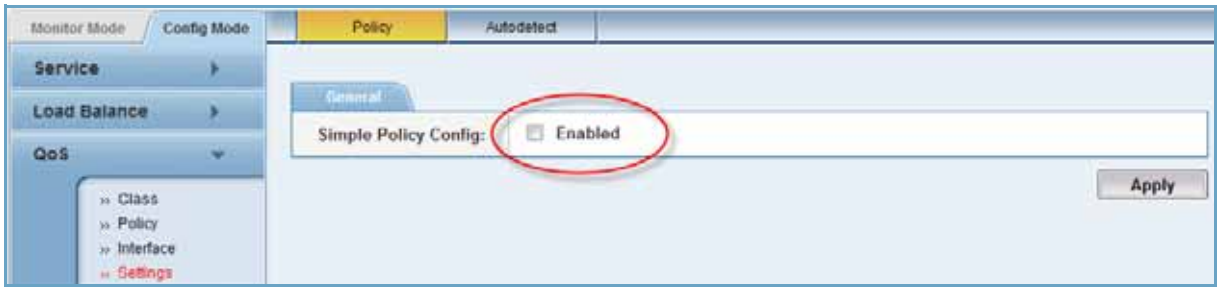
Enabling Easy QoS Mode

If you are in Advanced QoS Mode and wish to enable Easy QoS Mode, follow the procedure below **after checking with A10 Networks Technical Support:**

1. Select Config Mode > QoS > Settings.
2. Select Policy from the menu bar (if not already selected).

   A window similar to the one shown below appears:

FIGURE 64 Config > QoS > Settings > Policy



3. Select the Enabled checkbox next to Simply Policy Config to enable Easy QoS Mode.
4. Click Apply to submit your changes, and click the flashing red Save button to save your changes to the startup-config file.

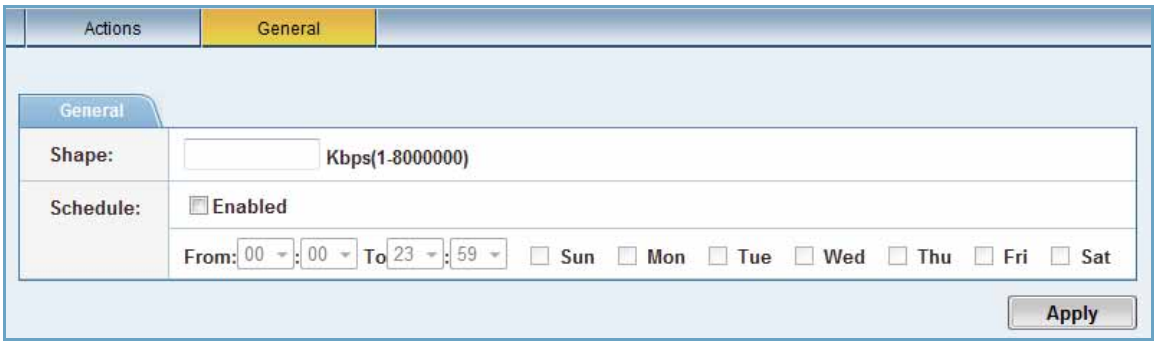
Easy QoS Mode is now enabled, and you will notice that the Policy and Interface hyperlinks that appear under the QoS module button (in Advanced QoS Mode) are replaced with a hyperlink that says Simple Policy.

Configuring the General tab:

To configure the General tab, follow the procedure below:

1. Select Config Mode > QoS > Simple Policy.
2. Select General from the Menu bar. A window similar to the one shown below appears:

FIGURE 65 Config > QoS > Simple Policy



a. In the Shape field, enter a value ranging from 1 - 8000000 Kbps. Shaping applies to egress traffic and guarantees a specific amount of bandwidth for forwarding traffic.

b. Select the Enabled checkbox to enable scheduling.

c. Enter the hours during which the policy will be active in the From and To fields (e.g. 9:00 – 17:00).

d. Use the checkboxes to determine which days of the week the policy will be active (e.g. Mon – Fri).

3. Click Apply to submit your changes, and then click the flashing red Save button to save your changes to the startup-config file.

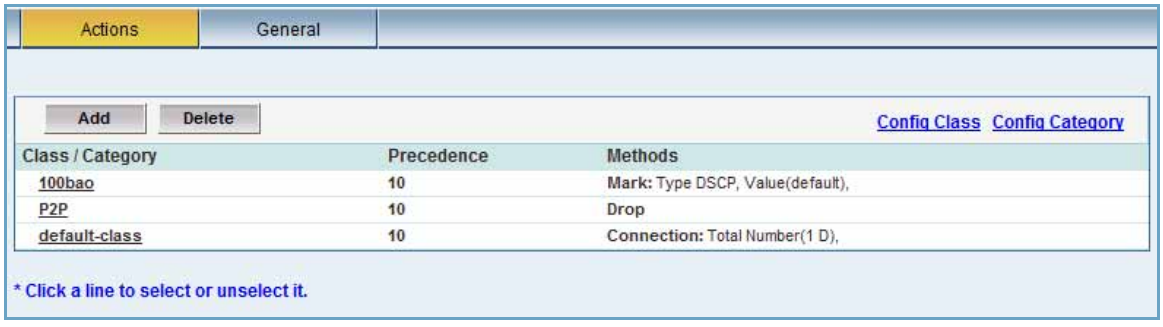
Configuring Action Groups

To add an Action group:

1. Select Config Mode > QoS > Simple Policy.

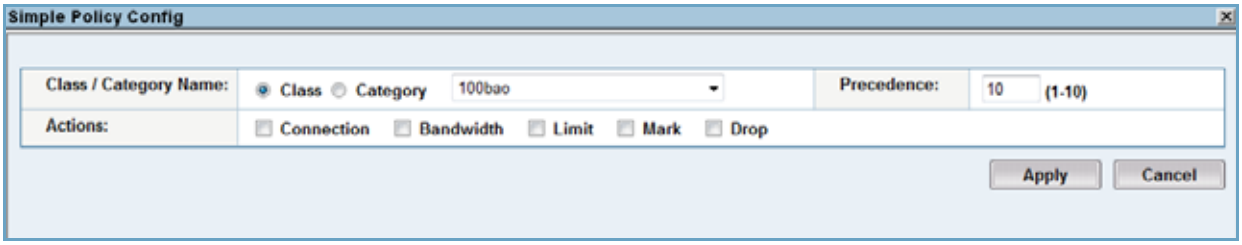
2. Select Actions from the menu bar. A window similar to the one shown below appears, listing Action Groups.

FIGURE 66 Config > QoS > Simple Policy > Actions



3. Click the Add button to configure a new Action Group.
   A window similar to the one shown below appears.

FIGURE 67 Config > QoS > Simple Policy > Actions (Add)



Note: If you do not select one of the Action checkboxes, then the Action associated with this Policy (configured below) will be at the top of the hierarchy. If you select one of the action checkboxes, then the new Action Group will appear as a sub-level action belonging to one of the higher level Action Groups.

4. Select the Class or Category radio button, and then click the drop-down menu and select the desired class or category for which traffic will be classified.

5. Enter a value (1 – 10) in the Precedence field. The default value is 10. Entering 1 will cause this Action Group to receive the highest (or most preferred) precedence.

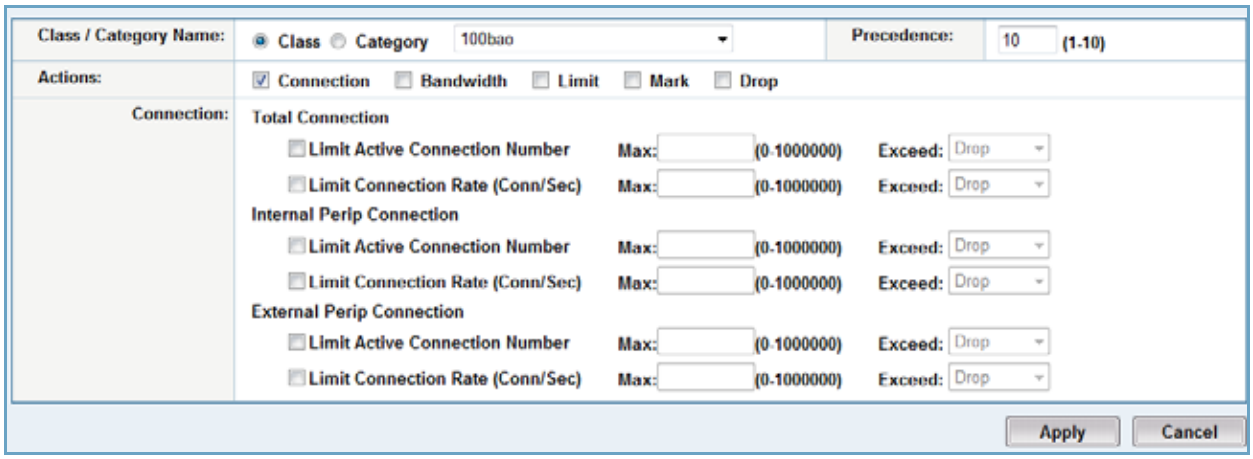
Note: The EX appliance compares traffic against the match criteria within an Action Group, taking action based upon the first positive match. Action Groups that have a lower Precedence will vet traffic before Action Groups that have a higher Precedence. Therefore, if your goal is to prevent P2P traffic, then you should create an Action Group based on the "P2P" category and assign that Action Group a Precedence of 1.

6. Select the desired Actions checkbox. Options are:
   - Connection – Limit traffic based on connection usage.
   - Bandwidth – Limit traffic based on bandwidth usage.
   - Limit – Apply rate limiting to police the bandwidth used by traffic of a certain QoS class of category by enforcing a specified maximum rate.
   - Mark – Change the DSCP value in the IP packet headers to change their forwarding priority throughout the network or routing through the EX appliance.
   - Drop – Drop traffic that matches the criteria in the Action Group.

   Each of these options are discussed in further detail below.

If selecting the **Connection** action, sub-options are shown in the window below:

FIGURE 68 Config > QoS > Simple Policy > Add > Connection

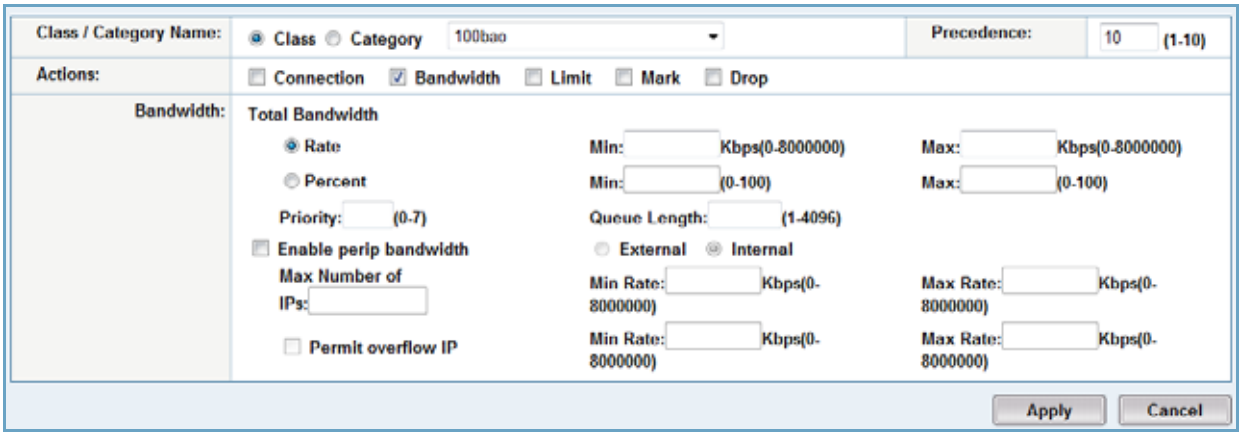


- Total Connection:
  - Limit Active Connection Number – select this checkbox to limit the aggregate connections for this class or category.
  - Limit Connection Rate – select this checkbox to limit the connections per second for this class or category.
- Internal Perip Connection:
  - Limit Active Connection Number – select this checkbox to limit the connections for this class or category for a specific internal IP address.
  - Limit Connection Rate – select this checkbox to limit the connections per second for this class or category for a specific internal IP address.
- External Perip Connection:
  - Limit Active Connection Number – select this checkbox to limit the connections for this class or category for a specific external IP address.
  - Limit Connection Rate – select this checkbox to limit the connections per second for this class or category for a specific external IP address.
- Max:
  - Enter the value that will determine the limit on Active Connections or Connections per Second for aggregate, or for an internal or external IP address.

- Exceed:
  - Select the action that should occur for traffic that exceeds this maximum configured value. Options are drop or reject.

  If selecting the **Bandwidth** action, sub-options are shown in the window below:

FIGURE 69 Config > QoS > Simple Policy > Add > Bandwidth



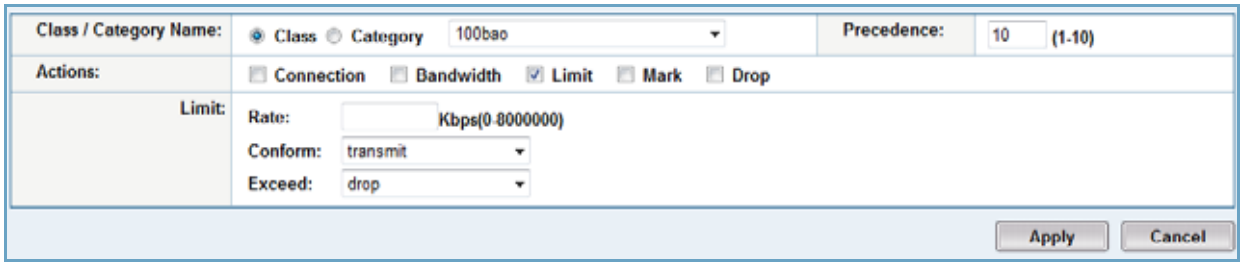
- Total Bandwidth:
  - Rate – select this radio button to set limits based on Kbps for the total amount of bandwidth available.
    - Min – Minimum amount of bandwidth, measured in Kbps, reserved for the QoS class/category. This rate is guaranteed to be available for forwarding matching traffic.
    - Max – Maximum bandwidth, measured in Kbps, allowed for matching traffic.
  - Percent – select this radio button to limit the total bandwidth based on a percentage of bandwidth available to this class/category.
    - Min – Minimum amount of bandwidth, measured as a percentage of the total available bandwidth, reserved for the QoS class/category. This rate is guaranteed to be available for forwarding matching traffic.
    - Max – Maximum amount of bandwidth, measured in percentage of total available bandwidth, reserved for the QoS class/category.
  - Priority – Enter a priority value ranging from 0–7 to give this class/category priority over other classes/categories for receiving shared bandwidth. If more than one QoS class/category is sharing bandwidth, the class with higher priority is given access to the bandwidth first.

- Queue Length – Enter a value ranging from 1–4096. This value represents the maximum number of packets the EX appliance will hold in its forwarding buffers when the Max-Rate interval has been exceeded. Packets are forwarded when bandwidth becomes available. If the queue is full, additional packets are dropped.

- Enable perip bandwidth – Select this checkbox to enable the configuration options for setting bandwidth controls on a per-IP basis.
  - External or Internal – Select the desired radio button to determine whether the IP address is internal or external. External refers to an outside IP address connected to an external interface. Internal refers to an inside IP address that is connected to an internal interface on the EX appliance.
  - Max Number of IPs – Number of IP addresses for which bandwidth will be guaranteed. Bandwidth is allocated in equal portions up to the Max Rate. Additional IP addresses can get bandwidth only if "Permit overflow IP" is enabled.
    - Min Rate – Amount of bandwidth, measured in Kbps, reserved for the Max Number of IPs.
    - Max Rate – Maximum bandwidth, measured in Kbps, allowed for the Max Number of IP addresses.
  - Permit overflow IP
    - Min Rate – Amount of bandwidth guaranteed for additional IP addresses.
    - Max Rate – Maximum bandwidth allowed for additional IP addresses.

  If selecting the **Limit** action, sub-options are shown in the window below:

FIGURE 70 Config > QoS > Simple Policy > Add > Limit



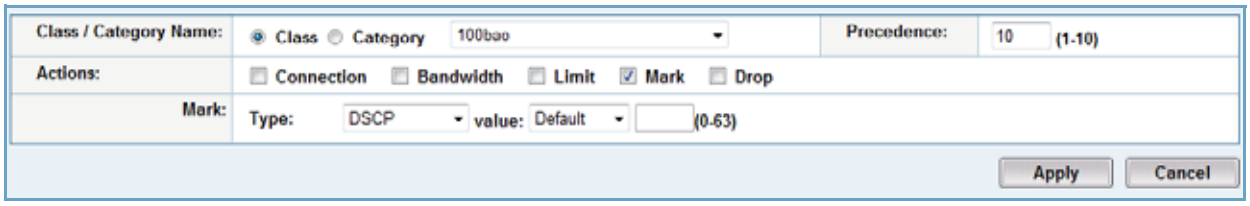
- Rate – Set the average rate allowed for the traffic that matches this category/class. Enter a value from 0 to 8,000,000 Kbps. This is sometimes called the committed information rate (CIR).

- Conform – For traffic that falls within the configured limit, click the drop-down menu and select the desired action. Options are transmit, drop, or set-dscp-transmit.

- Exceed – For traffic that exceeds the configured limit, click the drop-down menu and select the desired action. Options are transmit, drop, or set-dscp-transmit.

  If selecting the **Mark** action, sub-options are shown in the window below:

FIGURE 71 Config > QoS > Simple Policy > Add > Mark

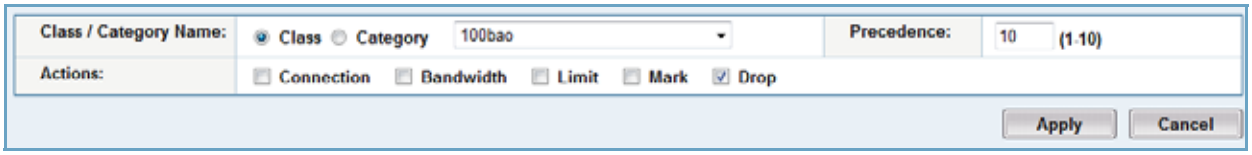


- Type: Type of marking to perform. You can mark DSCP values.
  - Select DSCP, if not already selected.
- Value: Priority value to set in packet headers of matching traffic before forwarding.
  - Select any one of the following well-known values: default, AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43, EF, others.

    Selecting *others* enables the additional input field where you can enter a numeric value from 0 to 63.

  If selecting the **Drop** action, sub-options are shown in the window below:

FIGURE 72 Config > QoS > Simple Policy > Add > Drop



- Drop:
  - Drop all traffic of that matches this class or category.

7. When done configuring Action Groups, click Apply to submit your changes. The new action group is listed under the Action tab. If desired, click the flashing red Save button to save your changes to the startup-config file.

Details:

- You can delete an Action Group by clicking on it to highlight it, and then click the Delete button.
- You can add a new action by clicking the Add button. If there are no other Action Groups, the new Action Group will appear at the top level of the hierarchy. If Action Groups have already been created, then the new Action Group may appear as a sub-level action belonging to one of the higher level Action Groups.
- You can add to the EX appliance's predefined classes by clicking the Config Class hyperlink at the upper right (to display the Config Class window), and then clicking the New button.

Advanced QoS Mode

Advanced QoS Mode offers a more powerful method of configuring QoS policies. This CLI-based approach to QoS Policy configuration requires you to define a QoS Policy and a QoS Interface, and then you must bind the QoS Policies to the QoS Interfaces. Although this method offers a more granularity in how QoS Policies are applied, it may not be as intuitive for new users. For that reason, new deployments are installed in Easy QoS Mode.

Note: Users with existing systems in Advanced QoS Mode who would like to switch to "Easy QoS Mode" must clear their existing "Advanced QoS Mode" configuration, enable Easy QoS Mode, and then re-configure.

Background

QoS Policies enable you to manage traffic on an individual QoS class or category basis. You can use policies to perform the following management functions:

- Shape traffic (offer minimum bandwidth guarantees)
- Rate limit traffic (policing traffic)
- Mark traffic priority (DSCP)
- Automatically drop traffic

A traffic policy (or QoS policy) is a set of one or more action groups. An action group defines the actions that will be taken upon traffic that matches the filtering criteria (or rules) within a QoS class.

You can apply traffic policies to QoS Interfaces, where a QoS Interface is defined as a type of virtual interface that groups together one or more physical ports. Each QoS Interface can have one ingress policy and one egress policy. The ingress policy applies to traffic received on the interface. The egress policy applies to traffic to be forwarded on the interface.

Table 13 lists the parameters you can configure for policy action groups.

TABLE 13 Policy Action-Group Parameters

Parameter	Description	Supported Values
Class / Category	QoS class or Category to which the policy applies.	Any one of the configured QoS classes. (See "Display QoS Classes" on page 125.)
Precedence	Numeric value used to prioritize the action groups within a policy. Before comparing traffic against a policy, the EX appliance internally reorders the action groups based on precedence. The EX Secure WAN Manager then compares the traffic against the action groups, and takes the action specified in the first policy group that matches the QoS class in the traffic.	1 to 10 Default: 10 The highest (most preferred) precedence is 1.

TABLE 13 Policy Action-Group Parameters (Continued)

Parameter	Description	Supported Values
Connection	Configure connection limits for a class or category based upon total number of connections or connections per-IP address. This limit on the number of connections is defined within the QoS policy and is bound to a QoS class. Selecting the Connection checkbox enables configuration of the following connection sub-options. **Total Connection:** • Limit Active Connection Number checkbox – Selecting this option will limit the total number of connections for this class. • Limit Connection Rate checkbox – Selecting this option will limit the number of connections per second that will be allowed for this class. • Max field – Enter the upper threshold for the number of connections. • Exceed drop-down menu – Select the action (drop or reject) that should occur when the threshold is exceeded. **Internal Per-IP Connection:** • Limit Active Connection Number checkbox – Selecting this option will limit the total number of connections for this IP address. • Limit Connection Rate checkbox – Selecting this option will limit the number of connections per second that will be allowed for this IP address. • Max field – Enter the upper threshold for the number of connections for this IP address. • Exceed drop-down menu – Select the action (drop or reject) that should occur when the threshold is exceeded. **External Per-IP Connection:** • Limit Active Connection Number checkbox – Selecting this option will limit the total number of connections for this IP address. • Limit Connection Rate checkbox – Selecting this option will limit the number of connections per second that will be allowed for this IP address. • Max field – Enter the upper threshold for the number of connections for this IP address. • Exceed drop-down menu – Select the action (drop or reject) that should occur when the threshold is exceeded.	Total Connection parameters: • Limit Active Connection Number – 0 to 1,000,000 • Limit Connection Rate – 0 to 1,000,000 Conn/Sec Internal PerIP Connection parameters: • Limit Active Connection Number – 0 to 1,000,000 • Limit Connection Rate – 0 to 1,000,000 Conn/Sec External PerIP Connection parameters: • Limit Active Connection Number – 0 to 1,000,000 • Limit Connection Rate – 0 to 1,000,000 Conn/Sec

TABLE 13 Policy Action-Group Parameters (Continued)

Parameter	Description	Supported Values
Bandwidth	Configure rate shaping. You can configure total bandwidth limits for a class or category, as well as bandwidth limits on a per-IP basis. Bandwidth limits for a class apply to all traffic for the class, and limits for a category apply to all classes within that category. Per-IP limits apply to individual users (IP addresses) of the class. Selecting the Bandwidth checkbox enables the configuration options for bandwidth rate shaping. **Total Bandwidth** You can configure rate-based shaping *or* percentage-based shaping. Rate-based parameters: • Min Rate – Amount of bandwidth, measured in Kbps, reserved for the QoS class. This rate is guaranteed to be available for forwarding matching traffic. • Max Rate – Maximum bandwidth, measured in Kbps, allowed for matching traffic. For shape and bandwidth, all related packets will queue up. The ingress packet is queued to the tail, and queued packets are sent out at the rate that the class or interface can use. After the maximum rate has been reached within a one-second interval, any additional packets for the matching class received in that interval are queued. (See Queue Length below.) Percentage-based parameters: • Min Percent – The minimum amount of bandwidth, measured in percentage of total available bandwidth, reserved for the QoS class. This rate is guaranteed to be available for forwarding matching traffic. • Max Percent – The maximum amount of bandwidth, measured in percentage of total available bandwidth, reserved for the QoS class.	Rate-based parameters: • Min-Rate – 0 to 8,000,000 (8 million) Kbps • Max-Rate – 0 to 8,000,000 (8 million) Kbps Percentage-based parameters: • Min Percent – 0 to 100 • Max Percent – 0 to 100

TABLE 13 Policy Action-Group Parameters (Continued)

Parameter	Description	Supported Values

Bandwidth (cont.)	Parameters applicable to both types of total bandwidth shaping:
	• Priority – Preference of this class over other classes for receiving shared bandwidth. If more than one QoS class shares bandwidth, the class with higher priority is given access to the bandwidth first.
	• Queue Length – Maximum number of unforwarded packets the EX appliance will hold in its forwarding buffers. Packets enter the queue when the Max-Rate within a one-second interval is exceeded.
	During the following one-second interval, the EX appliance forwards the queued packets when bandwidth is available. If the queue is full, any additional packets over the Max-Rate are dropped until packets already in the queue are forwarded.
	Per-IP Bandwidth
	Per-IP bandwidth shaping sets bandwidth guarantees and limits for individual IP flows within a traffic class, and dynamically allocate bandwidth equally among active flows.
	Selecting "Enable perip bandwidth" enables the configuration options for the feature.
	• External / Internal – Traffic direction to which this action group applies:
	  • External – Outside IP address connected to an EX external interface.
	  • Internal – Inside IP address connected to an EX internal interface.
	• Max Number of IPs – Number of IP addresses for which bandwidth will be guaranteed. Bandwidth is allocated in equal portions up to the Max Rate to all IP addresses up to the maximum. Additional IP addresses can get bandwidth only if "Permit overflow IP" is enabled.
	• Min Rate – Amount of bandwidth, measured in Kbps, reserved for the Max Number of IPs.
	• Max Rate – Maximum bandwidth, measured in Kbps, allowed for the Max Number of IPs.
	By default, bandwidth is guaranteed only for the number of IP addresses specified by Max Number of IPs. You can enable allocation of bandwidth for additional (overflow) IP addresses.
	Permit overflow IP parameters:
	• Min Rate – Amount of bandwidth guaranteed for additional IP addresses.
	• Max Rate – Maximum bandwidth allowed for additional IP addresses.
		Parameters applicable to both types of total bandwidth shaping:
		• Priority – 0 to 7
		Queue Length – 0 to 4,096 packets
		Traffic direction – Internal or External
		Max Number of IPs – 0-65,535 or blank (unlimited)
		Min Rate – 0-8,000,000 or blank
		Max Rate – 0-8,000,000 or blank (unlimited)
		Permit overflow IP parameters:
		• Min Rate – 0-8,000,000 or blank
		• Max Rate – 0-8,000,000 or blank (unlimited)

TABLE 13 Policy Action-Group Parameters (Continued)

Parameter	Description	Supported Values
Drop	Drops traffic that matches the action group.	Enabled or disabled (indicated by selecting the checkbox)

Limit	Configures rate limiting (policing).
	Selecting the Limit checkbox enables the following configuration fields:
	• Rate – Average rate allowed for the traffic. This is sometimes called the *committed information rate* (CIR).
	• Conform – Action to take for conforming traffic.
	• Exceed – Action to take for non-conforming traffic.
	You can enforce the traffic rate for a class by setting different actions for conforming and non-conforming traffic. For example, you can set the Conform action to transmit and set the Exceed action to set-dscp-transmit or drop.
	The set-dscp-transmit actions mark the DSCP priority value in a packet before forwarding it. For example, you can remark non-conforming traffic to the lowest priority. This still allows the traffic to be forwarded, but only when bandwidth is not in use by conforming traffic of other classes.
	The drop action discards the non-conforming packet without forwarding it.
		• Rate – 0 to 8,000,000 (8 million) Kbps
		• Conform – one of the following:
		  • transmit
		  • drop
		  • set-dscp-transmit (mark DSCP, then transmit)
		• Exceed – Same options as Conform

Mark	Configures marking of priority values in the packet headers of matching traffic.
	Selecting the Mark checkbox enables the following configuration fields:
	• Type – Type of marking to perform. You can mark DSCP priority values.
	• Value – Priority value to set in the packet headers of matching traffic before forwarding. The values you can select depend on the priority type you select.
		• Type – DSCP
		• Value:
		  • DSCP – Any one of the following well-known values, or a numeric value from 0 to 63:
		  routine, priority, AF11, AF12, AF13, immediate, AF21, AF22, AF23, flash, AF31, AF32, AF33, flash-override, AF41, AF42, AF43, critical, EF, internet-work-control, network-control.
		The *others* selection displays an additional input field where you can enter a numeric value from 0 to 63.

Policy	Additional policy to apply to matching traffic.	Any configured policy.

Configure Rate Shaping

Shaping guarantees a specific amount of bandwidth for forwarding traffic. You can configure rate shaping on an interface basis or, using a policy, on a class basis. Shaping applies to egress traffic.

Configuration of shaping on an interface basis is simpler than configuration on a class basis, whereas class-based shaping provides finer control than interface-based shaping.

- Interface-based shaping – When configured on an interface basis, shaping applies to all traffic on the interface, regardless of class. You can configure shaping on a physical interface or on a QoS Interface. You can specify the minimum amount of bandwidth to guarantee for all egress traffic on the interface.
- Policy-based shaping – When applied by a policy, shaping applies only to the QoS classes specified in the policy. You can specify the minimum amount of bandwidth to guarantee for individual QoS classes. You also can adjust maximum rate, burst, and queue settings.

Note: Before you can configure shaping on a QoS interface, either directly or through a policy, you must configure the QoS interface first. (See "Configure QoS Interfaces" on page 164.)

Configure Shaping for All Classes on an Interface

To configure shaping for all QoS classes on an interface, see "Configure QoS Interfaces" on page 164.

Configure Shaping for an Individual Class

To configure shaping for an individual class:

1. Configure a policy, with an action group to be shaped.
2. Apply the policy as an egress policy to one or more QoS interfaces. (See "Configure QoS Interfaces" on page 164.)

Configure a Rate-Shaping Policy

1. Select Config Mode > QoS > Policy.
2. On the menu bar, select Policy, if not already selected. The list of configured policies appears.
3. To configure a new policy, click New. The Policy tab appears.

   To add a rule to an existing policy, click on the policy name. The Policy tab appears.

4. In the Name field, enter a name for the policy.

   The name can be from 1 to 31 alphanumeric characters long. Spaces (internal blanks) are allowed and do not require quotation marks.

5. To add a new rule, click New. The Action Group tab appears. (See Figure 73.)

   To edit an existing rule, select the rule and click Edit. The Action Group tab appears.

6. Select the Class or Category radio button, and then use the drop-down menu to select the desired QoS class or Category.

7. Select the Bandwidth checkbox to display the configuration fields.

8. Configure the shaping parameters by selecting either Rate or Percentage based:

   - **For Rate Based**

   a. In the Min Rate field, enter the amount of bandwidth you want to reserve for the class.

   b. In the Max Rate field, enter the maximum amount of bandwidth allowed for matching traffic. Packets received after the Max Rate has been reached are sent to the queue.

   - **For Percentage Based**

   a. In the Min-Percent field, enter the minimum percentage of bandwidth you want to reserve for the class.

   b. In the Max Percent field, enter the maximum percentage of bandwidth allowed for matching traffic. Packets received after the Max Percent has been reached are sent to the queue.

   - **For either Rate Shaping or Percent Based**

   c. In the Priority field, specify the priority to give this class when sharing bandwidth with other classes.

   d. In the Queue Length field, enter the maximum number of packets the EX appliance can queue for traffic that exceeds the Max-Rate.

   (For more information about the shaping parameters, see Table 13 on page 151.)

9. To configure marking in the same rule, select the checkbox next to Marking. (For information about marking parameters, see Table 13 on page 151.)

10. To apply an additional policy to traffic that matches the QoS class related to the Action Group, click the checkbox next to Policy and select the policy from the pull-down list.

11. Click OK. The Policy tab reappears with the new rule in the Action Group List. (See Figure 74.)

12. Click OK to complete the policy configuration.

13. Go to "Configure QoS Interfaces" on page 164.

FIGURE 73 Action Group Tab – Bandwidth (Shaping)

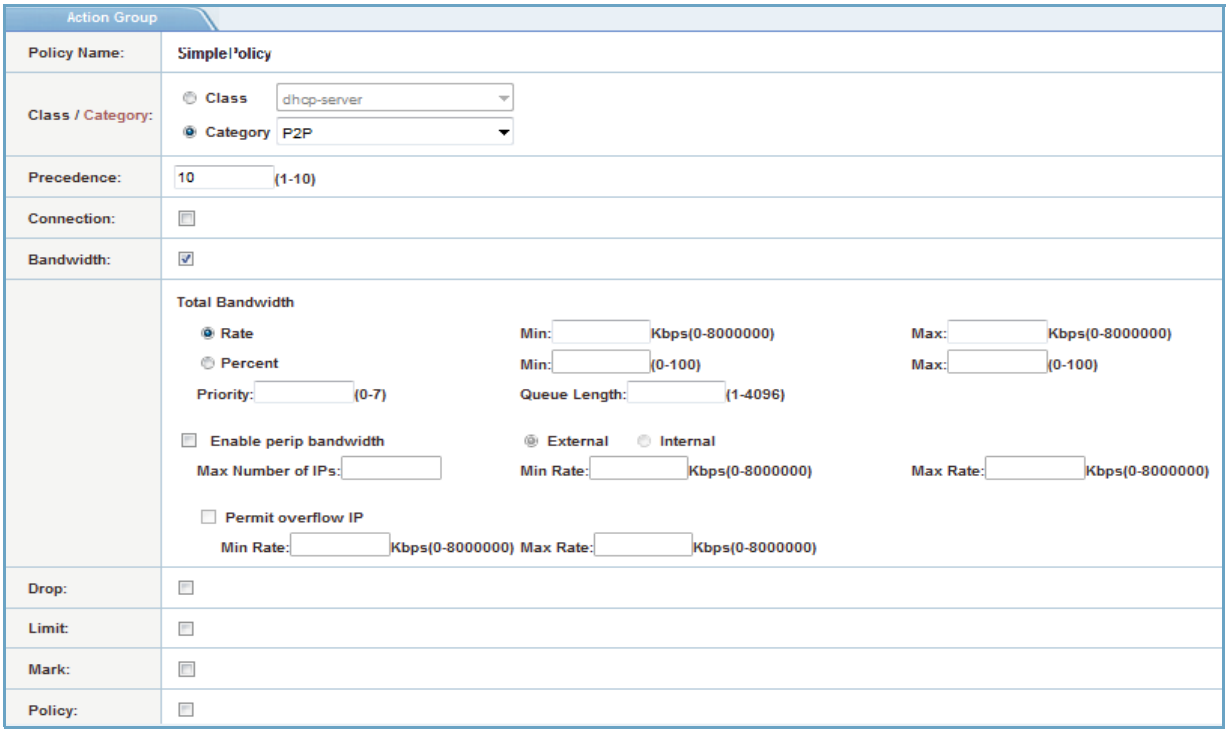
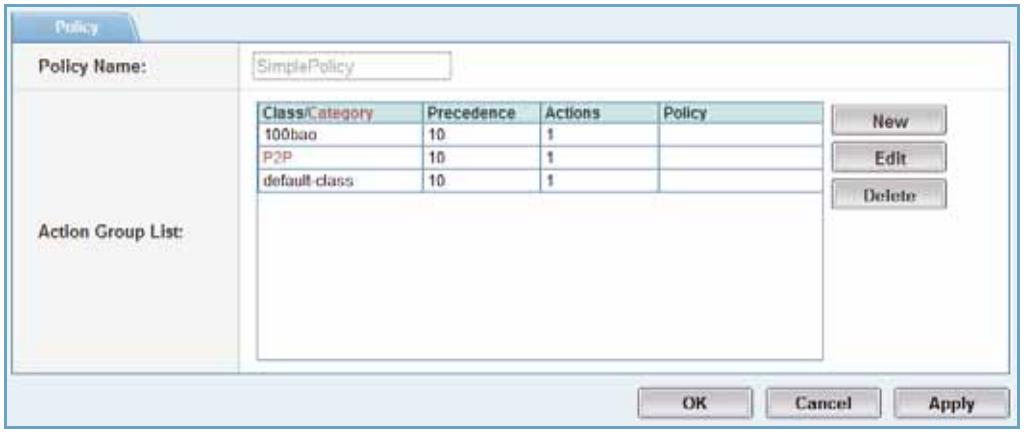


FIGURE 74 Policy Tab – Bandwidth (Shaping) Policy



Configure Rate Limiting

Rate limiting controls the rate of ingress traffic on a QoS interface. You can configure rate limiting on an individual class basis.

Note: Before you can configure rate limiting on a QoS interface, you must configure the QoS interface first. You cannot configure rate limiting directly on a physical interface.

To configure rate limiting:

1. Select Config Mode > QoS > Policy.
2. On the menu bar, select Policy, if not already selected. The list of configured policies appears.
3. To configure a new policy, click New. The Policy tab appears.

   To add a rule to an existing policy, click on the policy name. The Policy tab appears.
4. In the Name field, enter a name for the policy.

   The name can be from 1 to 31 alphanumeric characters long. Spaces (internal blanks) are allowed and do not require quotation marks.
5. To add a new rule, click New. The Action Group tab appears.

   To edit an existing rule, select the rule and click Edit. The Action Group tab appears.
6. From the Class pull-down list, select the QoS class.
7. Select the Limit checkbox to display the configuration fields. (See Figure 75.)
8. Configure the rate limiting parameters:
   a. In the Rate field, enter the maximum rate to allow the QoS class on the interface.
   b. From the Conform pull-down list, select the action to take for traffic that is at or under the specified rate.
   c. From the Exceed pull-down list, select the action to take for traffic that is over the specified rate.

   (For more information about the shaping parameters, see Table 13 on page 151.)

9. To configure marking in the same rule, select the checkbox next to Marking. (For information about marking parameters, see Table 13 on page 151.)

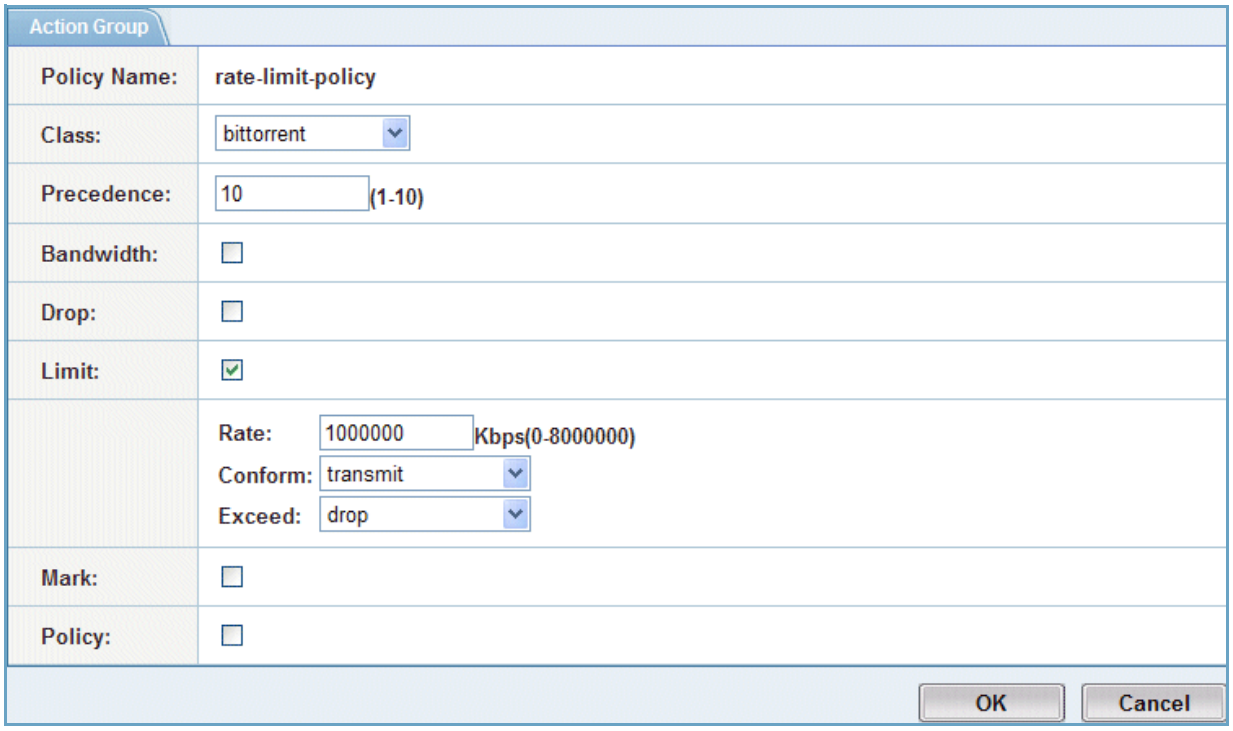
10. To apply an additional policy to traffic that matches the QoS class related to the Action Group, click the checkbox next to Policy and select the policy from the pull-down list.

11. Click OK. The Policy tab reappears with the new rule in the Action Group List.

12. Click OK to complete the policy configuration.

13. Go to "Configure QoS Interfaces" on page 164.

FIGURE 75 Action Group Tab – Rate Limiting



Configure Traffic Marking

To configure traffic marking:

1. Select Config Mode > QoS > Policy.
2. On the menu bar, select Policy, if not already selected. The list of configured policies appears.
3. To configure a new policy, click New. The Policy tab appears.

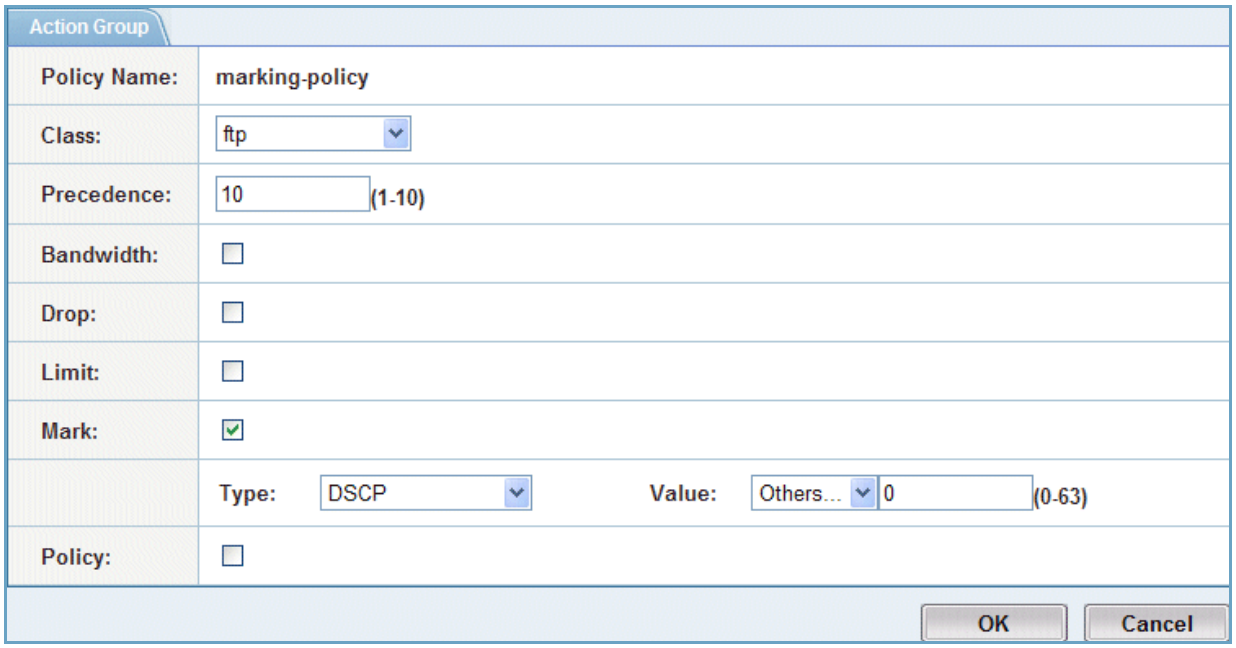
   To add an Action Group to an existing policy, click on the policy name. The Policy tab appears.
4. In the Name field, enter a name for the policy.

   The name can be from 1 to 31 alphanumeric characters long. Spaces (internal blanks) are allowed and do not require quotation marks.
5. To add a new Action Group, click New. The Action Group tab appears.

   To edit an existing Action Group, select the rule and click Edit. The Action Group tab appears.
6. From the Class pull-down list, select the QoS class.
7. Select the Mark checkbox to display the configuration fields. (See Figure 76.)
8. Configure the marking parameters:
   a. From the Type pull-down list, select the type of marking to perform.
   b. From the Value pull-down list, select the value to mark in egress traffic before forwarding it.

   (For more information about the marking parameters, see Table 13 on page 151.)
9. To apply an additional policy to traffic that matches the QoS class related to the Action Group, click the checkbox next to Policy and select the policy from the pull-down list.
10. Click OK. The Policy tab reappears with the new rule in the Action Group List.
11. Click OK to complete the policy configuration.
12. Go to “Configure QoS Interfaces” on page 164.

FIGURE 76 Action Group Tab – Marking



Drop Traffic

To drop traffic:

1. Select Config Mode > QoS > Policy.
2. On the menu bar, select Policy, if not already selected. The list of configured policies appears.
3. To configure a new policy, click New. The Policy tab appears.

   To add an Action Group to an existing policy, click on the policy name. The Policy tab appears.
4. In the Name field, enter a name for the policy.

   The name can be from 1 to 31 alphanumeric characters long. Spaces (internal blanks) are allowed and do not require quotation marks.
5. To add a new Action Group, click New. The Action Group tab appears.

   To edit an existing Action Group, select the rule and click Edit. The Action Group tab appears.

6. From the Class pull-down list, select the QoS class.
7. Select the Drop checkbox.
8. To apply an additional policy to traffic that matches the QoS class relate to the Action Group, click the checkbox next to Policy and select the policy from the pull-down list.
9. Click OK. The Policy tab reappears with the new rule in the Action Group List.
10. Click OK to complete the policy configuration.
11. Go to "Configure QoS Interfaces" on page 164.

Include Sub-Policies

A policy can include sub-policies. In this case, the policy includes the policy actions in the sub-policy.

Note: If traffic creates a positive match at both the policy level and the sub-policy level, then the actions associated with the policy will be applied to the traffic first, followed by the actions associated with the sub-policy.

To include a sub-policy in a policy:

1. Select Config Mode > QoS > Policy.
2. On the menu bar, select Policy, if not already selected. The list of configured policies appears.
3. To configure a new policy, click New. The Policy tab appears.

   To add an Action Group to an existing policy, click on the policy name. The Policy tab appears.
4. In the Name field, enter a name for the policy.

   The name can be from 1 to 31 alphanumeric characters long. Spaces (internal blanks) are allowed and do not require quotation marks.
5. To add a new Action Group, click New. The Action Group tab appears.

   To edit an existing Action Group, select the rule and click Edit. The Action Group tab appears.
6. From the Class pull-down list, select the QoS class.
7. Select the Policy checkbox.

8. Select the policy from the pull-down list.
9. Click OK. The Policy tab reappears with the new rule in the Action Group List.
10. Click OK to complete the policy configuration.
11. Go to "Configure QoS Interfaces" on page 164.

QoS Interface

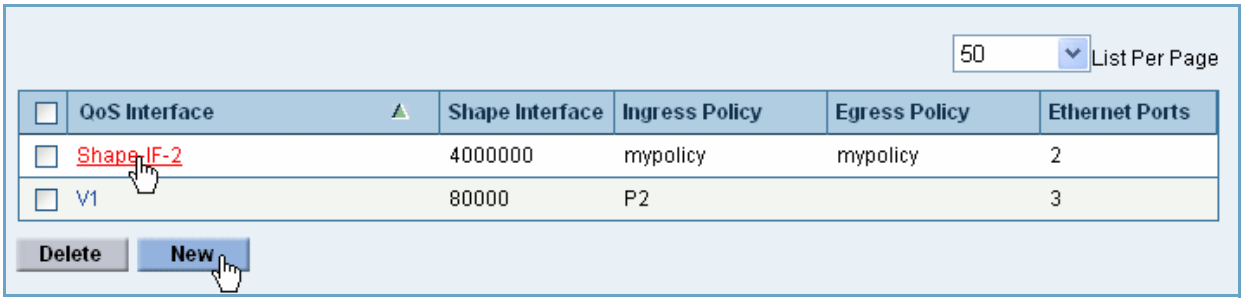
A QoS interface is a type of virtual interface that groups together one or more physical ports. Policies, as well as shaping, can be applied to QoS interfaces.

Configure QoS Interfaces

The Config > QoS > Interface tab displays a list of all currently configured QoS Interfaces and allows you to create new ones. It also displays each QoS Interface's respective shape rate, ingress and egress policies, and the index of ethernet port bindings.

The QoS Interface list is alphabetically ordered by name. It can toggle between ascending and descending order by clicking the small up/down arrowhead at the right side of the QoS Interface heading.

FIGURE 77 Config > QoS > Interface



To apply a QoS Policy to a QoS Interface and set its shape interface rate:

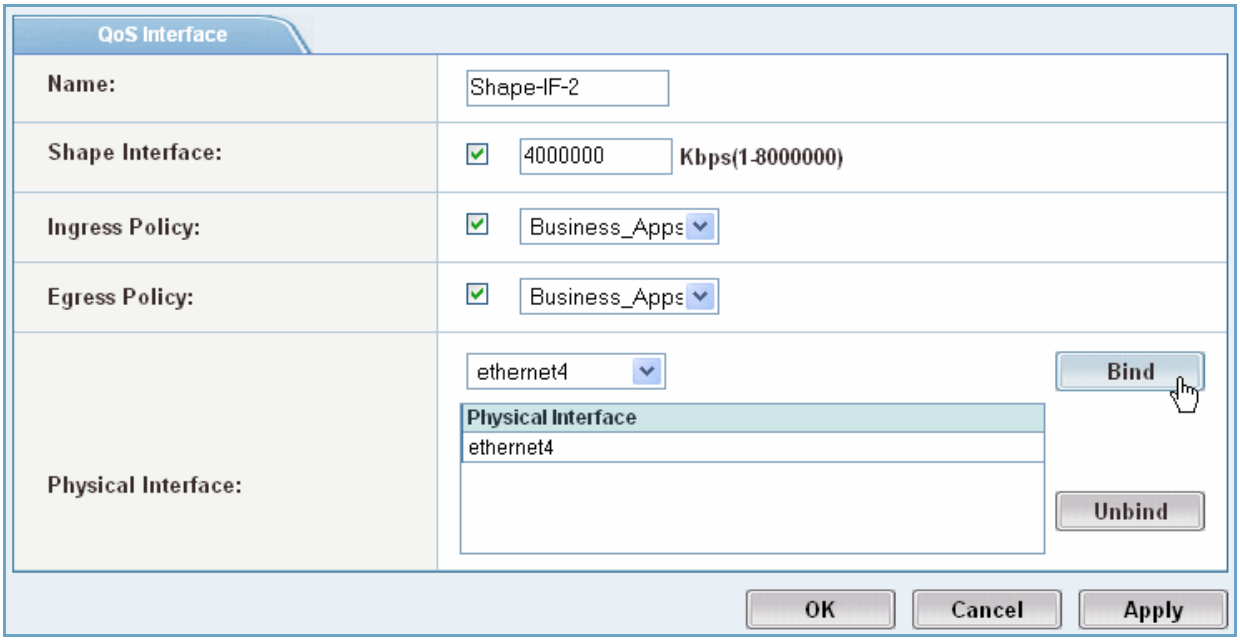
1. Select Config Mode > QoS > Interface. (See Figure 77.) The list of configured QoS Interfaces is displayed. The QoS Interface tab lets you modify listed interface configurations or add new QoS interfaces.

   a. To assign ingress/egress policies to a configured QoS Interface, click on the interface name. The QoS Interface tab is displayed along with its current settings. (See Figure 78.) Go to step 2b.

   b. To configure a new QoS Interface, click New. The QoS Interface tab is displayed. (See Figure 78.)

   Here, you set the rate of the Shape Interface and apply Policies (see "Configure a Rate-Shaping Policy" on page 156) to QoS Interfaces. Policies do *not* take effect until you apply them to an interface. One policy can apply to each traffic direction.

FIGURE 78 QoS Interface Tab



2. To shape an interface:

   a. In the Name field, enter a name for the new interface.

   b. To set the Shape Interface rate, check the Shape Interface checkbox, then enter its rate.

   c. To apply a policy to traffic that is received on the QoS Interface, select the Ingress Policy checkbox. A drop-down list of the configured policies is activated. Select the policy from the list.

d. To apply a policy to traffic to be forwarded on the QoS Interface, select the Egress Policy checkbox. A drop-down list of the configured policies is activated. Select the policy from the list.

3. To bind the newly configured QoS interface to an ethernet interface or to add an ethernet interface to an existing QoS interface, select the ethernet interface from the drop-down list and click Bind. The selected ethernet interface appears in the list.

Note: If the policy selected to apply on egress has bandwidth actions, the QoS Interface must have been shaped.

4. To remove an ethernet interface from the QoS Interface, select the interface in the Physical Interface list and click Unbind. Deleted ethernet interfaces no longer appear in the list.

5. Click OK.

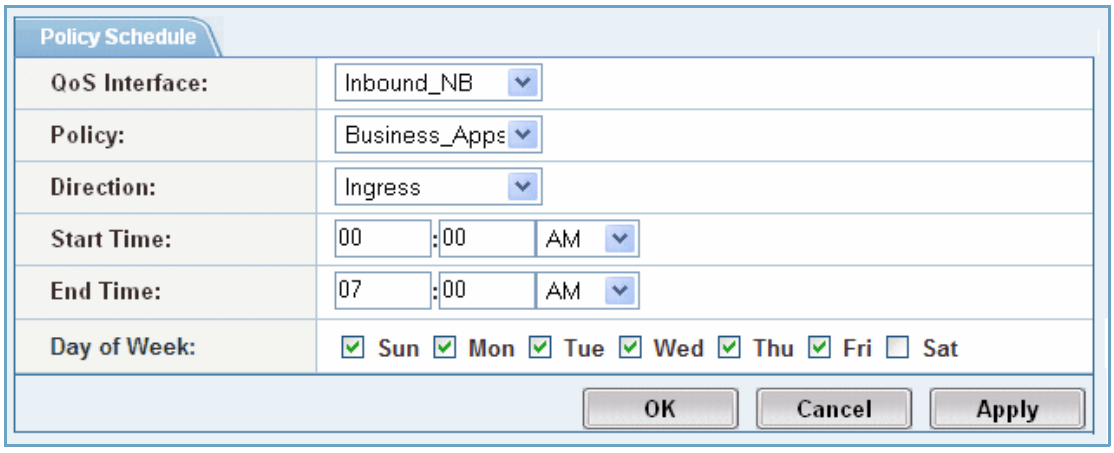
Policy Schedule

Click the Policy Schedule menu to display the existing Policy Schedules.

You can delete existing policy schedules by checking the checkbox left of their name and then the clicking the Delete button.

You can add new policies by clicking the New button.

FIGURE 79 Policy Schedules



To edit an existing policy, click on the policy name under the QoS Interface heading to open the Policy Schedule tab. The following parameters can be set for the selected Policy Schedule and for new Policy Schedules:

- QoS Interface selection
- Policy selection
- Ingress or Egress Direction selection
- Start and End times
- Days of the week

Click Apply to apply the changes to the current configuration and remain on this screen. Click Cancel to rescind all changes made in the current window. Click OK to apply all changes to the current configuration and return to the previous screen. Click Save to save the current configuration to the CompactFlash backup memory that restores on system boot and remain on this screen.

IP List

IP list is a group of IP addresses that can be used for source IP or destination IP in QoS class Match rules. Click on the IP List menu to open the IP List tab and to add new or delete existing IP addresses or IP ranges.

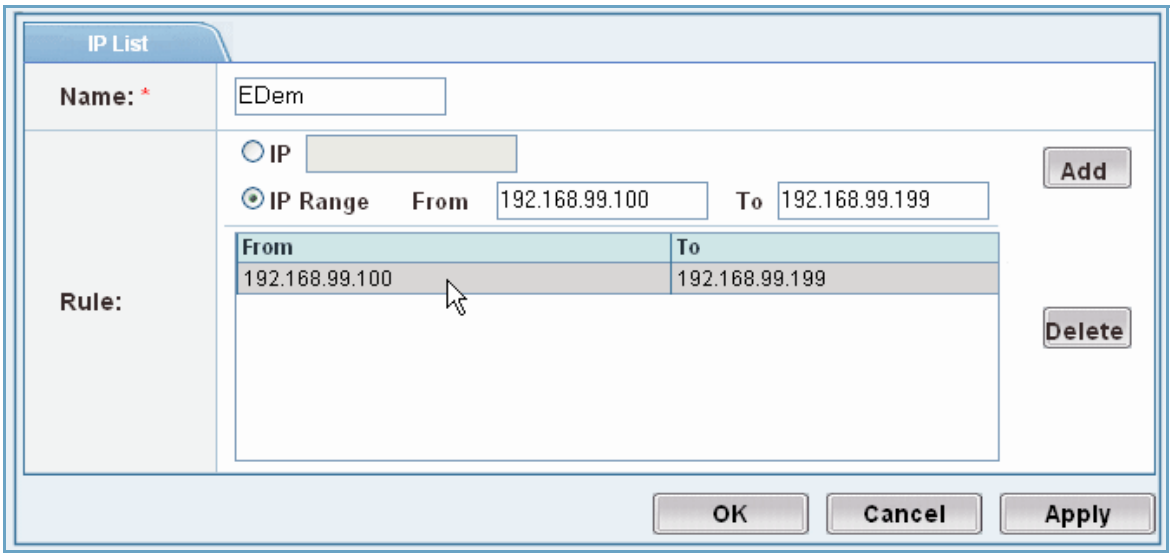
Select the New button to create a new IP list.

Select the checkbox for an IP List Name and then click the Delete button to delete it.

Click on an IP List Name to open the IP List tab where Rules containing the IP addresses and/or IP address ranges can be added to and/or deleted from the selected IP.

Note: Rules can NOT be edited. If you want to change the IP address or range for a selected Rule, delete it and add it again with the revised address(es).

FIGURE 80 IP List



Click Apply to apply the changes to the current configuration and remain on this screen. Click Cancel to rescind all changes made in the current window. Click OK to apply all changes to the current configuration and return to the previous screen. Click Save to save the current configuration to the CompactFlash backup memory that restores on system boot and remain on this screen.

IP Limit

An IP Limit specifies the following limits for the IP addresses in an IP address list:

- Maximum rate – Maximum bandwidth, measured in Kbps, allowed for traffic on an IP address.
- Connection limit – Maximum rate of new connections allowed for each client in the IP address list.

Click Config Mode > QoS > IP Limit display the existing IP limit configurations.

You can delete existing IP limits by checking the checkbox left of their names and then clicking the Delete button.

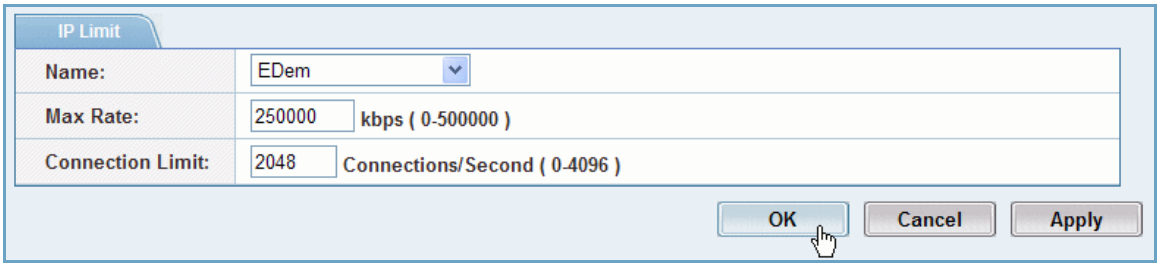
You can add a new IP limit configuration by clicking the New button.

To edit an existing IP limit, click on the IP limit configuration name under the Name heading.

Click Apply to apply changes to the current configuration and remain on this screen. Click Cancel to recall all changes made in the current window.

Click OK to apply all changes to the current configuration and return to the previous screen.

FIGURE 81 Config Mode > QoS > IP Limit



ID Group

ID group is a group of IDs that can be used for source IP or destination IP in QoS class Match rules.

ID is the user ID on IDsentrie, It will translate to IP address when a user login occurs. The IP address will be used for QoS class classify if the ID group is used for source IP or destination IP in Qos class match Rules.

Click Config Mode > QoS > ID Group ID Group to display the existing ID Groups.

You can delete existing ID Groups by checking the checkbox left of their name and then clicking the Delete button.

You can add a new ID Group by clicking the New button.

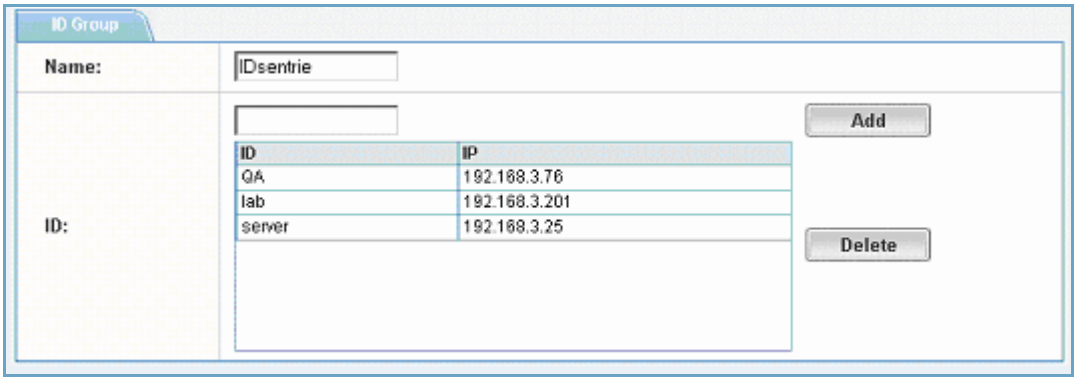
To edit an existing ID Group, click on the ID Group name under the Name heading to open the ID Group tab. The following parameters can be set for the selected ID Group:

- Name
- ID

Click Apply to apply changes to the current configuration and remain on this screen. Click Cancel to recall all changes made in the current window.

Click OK to apply all changes to the current configuration and return to the previous screen.

FIGURE 82 Config Mode > QoS > ID Group



Settings

The Config > QoS > Settings option offers two options:

- Policy – This menu option allows you to toggle between Easy QoS Mode and Advanced QoS Modes. See "Toggling Between Easy QoS Mode and Advanced QoS Mode" on page 171.
- Autodetect – This option allows you to enable or disable autodetection of QoS classes for the following:
  - VLANs
  - Ethernet interfaces (includes internal and external interfaces)
  - Internal subnets
  - IP Protocols
    Note: By selecting this checkbox, traffic that used to be classified under the "Others" class, such as non-TCP and non-UDP traffic (e.g. ICMP and OSPF) will be classified under the more specific "IP-Protocol" class.

  See "Configuring Autodetection of QoS Classes" on page 172.

Toggling Between Easy QoS Mode and Advanced QoS Mode

If you are in Advanced QoS Mode and wish to enable Easy QoS Mode, please follow the procedure below, **but only after checking with A10 Networks Technical Support for guidance.**[1]

1. Select Config Mode > QoS > Settings.
2. Select Policy from the menu bar (if not already selected).

   A window similar to the one shown below appears:
3. Select the Enabled checkbox next to Simply Policy Config to enable Easy QoS Mode.
4. Click Apply to submit your changes, and then click the flashing red Save button to save your changes to the startup-config file.

1. One possible issue that can occur when transitioning to Advanced Mode is as follows. When in Easy QoS Mode, the system will automatically create a QoS interface that includes all physical interfaces when you submit the first Simple Policy Action. If you have configured a QoS interface that includes one or more physical interfaces (while in Advanced QoS Mode), switching to Easy QoS Mode will fail because of this conflict. Therefore, we suggest backing up your QoS interface configurations and then removing them from the system before attempting to transition your system to Easy QoS Mode.

Easy QoS Mode is now enabled, and you will notice that the Policy and Interface hyperlinks that appear under the QoS module button (in Advanced QoS Mode) are replaced with a hyperlink that says Simple Policy.

See "Enabling Easy QoS Mode" on page 143 for more details.

Configuring Autodetection of QoS Classes

Classes are split into system-defined "auto-created" classes and user-defined "normal" classes. Deploying the EX appliance in a complicated network may result in too many auto-created classes (based on internal-subnet and IP-Protocol traffic).

By default, autodetection is enabled for most classes (with the exception of internal subnets). If this causes the creation of an excessive number of auto-created classes, you can use the Max Class Number field to set an upper limit on the number of auto-created classes in order to prevent them from using all of the available classes and potentially crowding out your ability to set up manual or "normal" classes.

To enable or disable autodetection for a specific interface type:

1. Select Config > QoS > Settings.
2. On the menu bar, select Autodetect, if not already selected.
3. Select the checkbox next to the interface type to enable autodetection for that interface type, or clear the checkbox to disable autodetection.
4. Enter a value in the Max Class Number field to limit the number of classes that can be auto-created. This max limit varies based on EX model number, and the valid range appears in parentheses near the field.
5. Click Apply.

Details:

- To avoid naming conflicts between user-created classes and auto-created class, some auto-created classes will have the prefix: "sys_"
- For auto-created classes based on IP protocol, the class name will not be prefixed with "sys_" but rather with the common IP protocol name, such as "icmp". If there is no common protocol name associated with the IP protocol, then the protocol number will be used such as "ip-proto-64" as the class name.

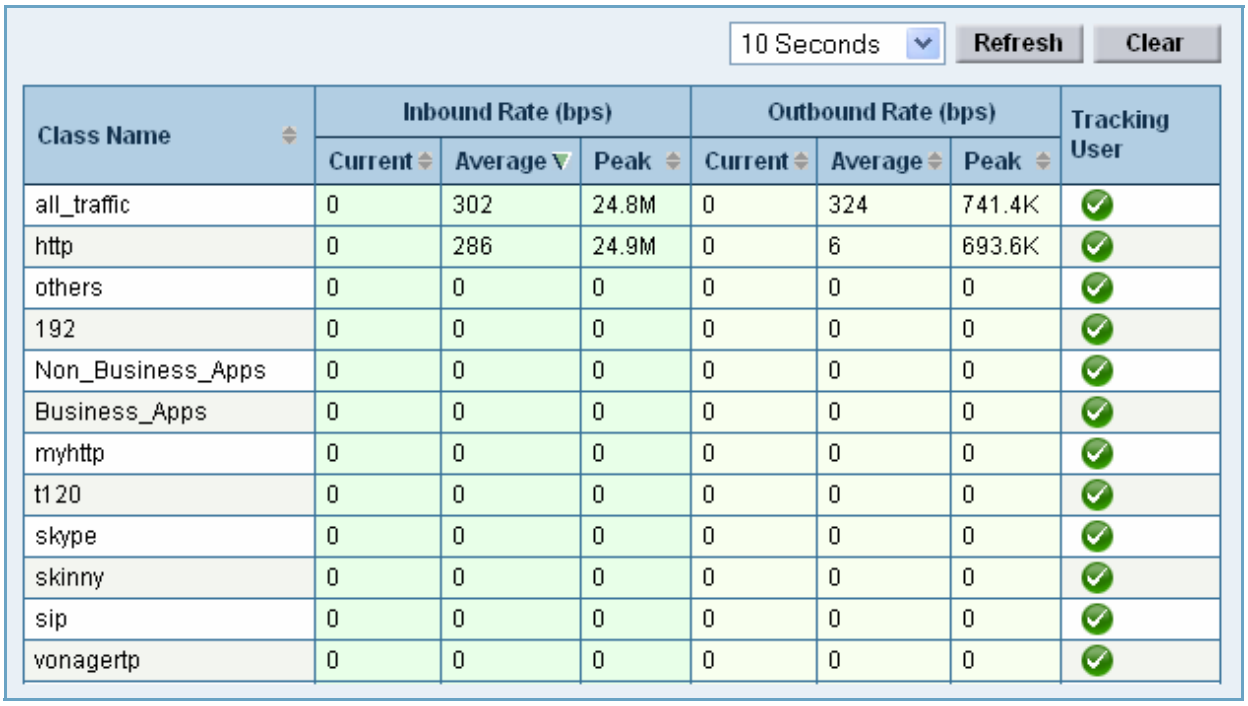
Traffic Information

The following sections describe how to display traffic and QoS statistics.

Class Statistics

To display QoS class statistics, select Monitor Mode > QoS > Class.

FIGURE 83 QoS class Statistics – Tabular Display



Class Name	Inbound Rate (bps)			Outbound Rate (bps)			Tracking User
	Current	Average	Peak	Current	Average	Peak	
all_traffic	0	302	24.8M	0	324	741.4K	
http	0	286	24.9M	0	6	693.6K	
others	0	0	0	0	0	0	
192	0	0	0	0	0	0	
Non_Business_Apps	0	0	0	0	0	0	
Business_Apps	0	0	0	0	0	0	
myhttp	0	0	0	0	0	0	
t120	0	0	0	0	0	0	
skype	0	0	0	0	0	0	
skinny	0	0	0	0	0	0	
sip	0	0	0	0	0	0	
vonagertp	0	0	0	0	0	0	

In this simplified example, the EX Secure WAN Manager displays statistics for HTTP traffic and for *others* traffic (traffic that is not for one of the classes listed in the class table).

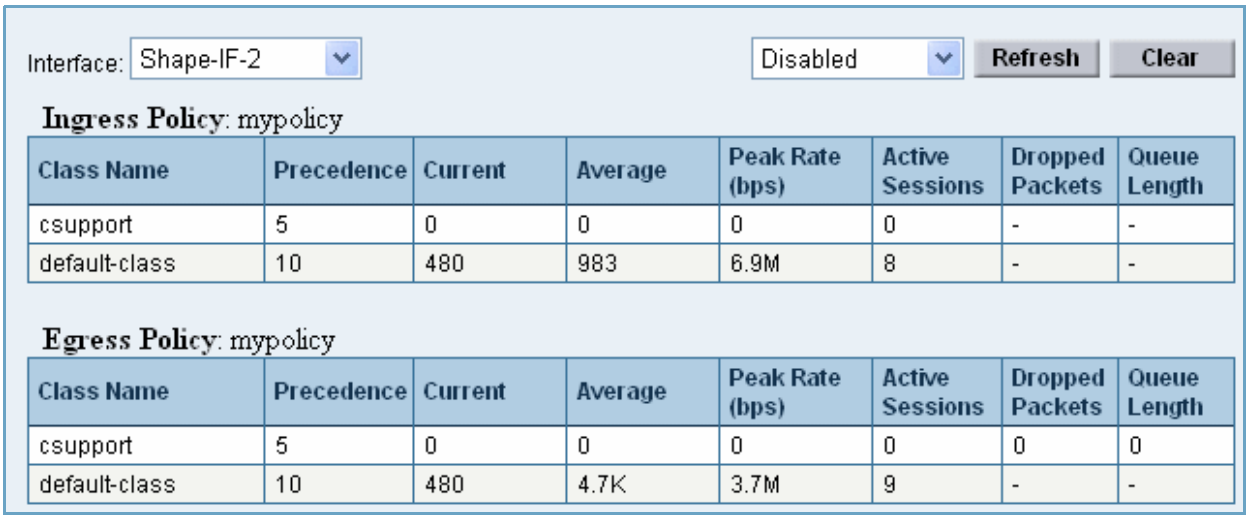
Policy Statistics

To display policy statistics for a QoS interface:

1. Select Monitor Mode > QoS > Policy.
2. From the Interface pull-down list, select the QoS interface. Statistics for the selected interface appear.

Statistics are listed separately for the interface's ingress and egress policies.

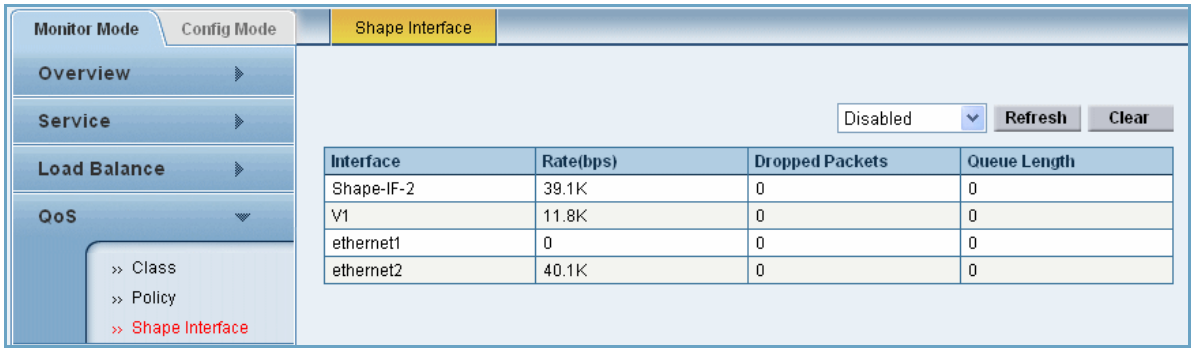
FIGURE 84 Monitor > QoS > Policy



Rate Shaping Statistics

To display statistics for rate shaping, select Monitor Mode > QoS > Shape Interface.

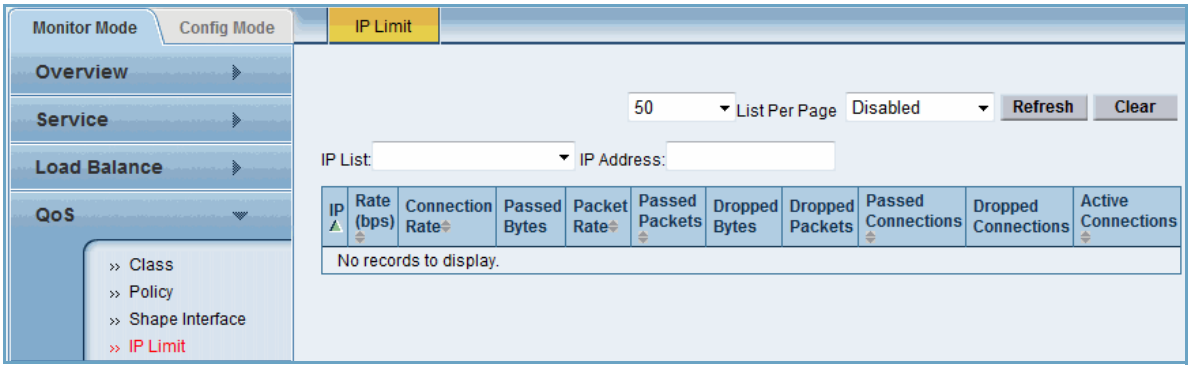
FIGURE 85 Monitor > QoS > Shape Interface



IP Limit Statistics

To display statistics for IP limiting, select Monitor Mode > QoS > IP Limit.

FIGURE 86 Monitor > QoS > IP Limit



Reports

This chapter describes the EX Secure WAN Manager reporting options.

Overview

The Monitor and Config modes each provide report features.

Monitor Mode Report Features

Monitor mode provides the following report options:

- Overview – Provides at-a-glance traffic information.
- Generate – Enables you to configure and generate reports. You can save report configurations to the favorites list. You also can locally save report output on the EX appliance and export the output. Reports can be generated in HTML, PDF, XML or CSV format.
- Favorite – Provides access to saved (“favorites”) report configurations. You can generate new on-demand reports from saved report configurations, and you also can schedule reports to be generated automatically.
- Stored – Provides access to saved report output.

Config Mode Report Features

Config mode provides the following report options:

- View – Configures “views”, which are named sets of QoS categories. Views simplify report configuration by enabling you to include multiple classes in a report. When you select a view for a report, all the classes in all the categories included in the view are included in the report. Views are configurable.
- Alert – Configures email alerts. The alerts are based on configurable network use thresholds.
- General – Configures email addresses for report and alert recipients, allows you to transfer a report file to a remote device using FTP, TFTP, RCP, or SCP, and provides access to report history information.

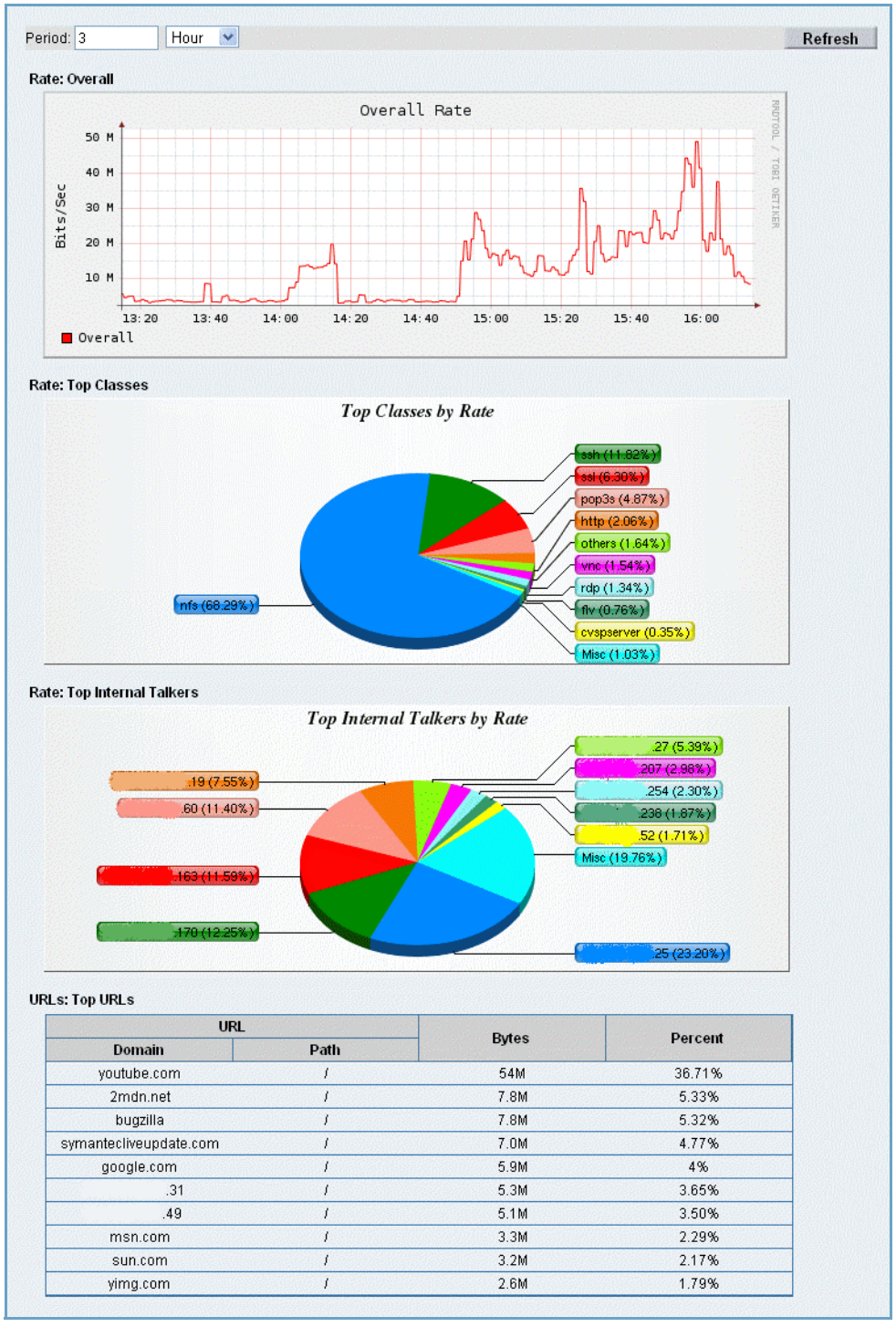
Display Traffic Overview Graphs

The Monitor > Report > Overview option provides at-a-glance traffic information with the following graphs:

- Overall Rate – Shows the traffic rate, in bits per second.
- Top Classes by Rate – Shows the most active traffic classes.
- Top Internal Talkers by Rate – Shows the most active internal IP addresses.
- Top URLs – Shows the most active URLs.

Figure 87 shows an example of the overview graphs.

FIGURE 87 Monitor > Report > Overview



URL		Bytes	Percent
Domain	Path		
youtube.com	/	54M	36.71%
2mdn.net	/	7.8M	5.33%
bugzilla	/	7.8M	5.32%
symantecliveupdate.com	/	7.0M	4.77%
google.com	/	5.9M	4%
.31	/	5.3M	3.65%
.49	/	5.1M	3.50%
msn.com	/	3.3M	2.29%
sun.com	/	3.2M	2.17%
yimg.com	/	2.6M	1.79%

Configure and Generate Reports - Monitor Mode

The Monitor > Report > Generate option enables you to configure and generate the following types of reports:

- Traffic
- TCP Performance
- URL
- Abuser
- Others
- Alert

All report output is shown in the EX appliance GUI. Report types can be exported in one of the following formats: HTML, PDF, XML, or CSV. The Alert log can be exported in PDF, XML, or CSV format but not HTML.

The default time period for all report types is the most recent 3 hours. The following time period increments are also supported:

- Minute
- Hour
- Day
- Week
- Month

By default, the end period of a report is the current date and time when the report output is generated. This means the report will be generated for the prior 3 hours unless you specify an earlier date and time.

All report configuration pages except Alert have the following buttons:

- Generate – Generates report output using the selected report configuration settings. After clicking, a progress bar appears, displaying the percentage complete for the generated report.
- Hide / More – Hides the report configuration fields. When you click Generate, the settings are automatically hidden and the button name becomes More. Click More to redisplay the report configuration fields.
- Add to Favorite – Adds the report configuration to the Favorite page.

The buttons on the Alert page are described in “Alert” on page 193.

Traffic

Traffic reports show graphs and statistics for the following:

- Traffic rate
- Number of connections
- Packet size distribution

For each type of graph, you can display the following:

- Traffic Overall
- Top 10 Classes
- Top 10 Categories
- Top 10 Internal Talkers
- Top 10 External Talkers

The Traffic Overall option is enabled by default. The Top 10 Classes, Top 10 Categories, and Top 10 Talkers options are disabled by default. For the Top 10 options, you can specify how many classes, categories, or talkers to include. The default for each is 10.

By default, statistics are shown for all classes, categories, internal talker IPs, and external talker IPs. You can narrow the scope of the report by specifying any of the following:

- Specific classes
- Specific internal talker IP
- Specific external talker IP

Statistics for all (both) inbound and outbound connection and packet directions are shown. For traffic rate, you can change the direction to inbound or outbound connections only. For packet distribution, you can change the connection direction and packet direction individually, to inbound or outbound.

Figure 88 shows the default traffic report settings.

FIGURE 88 Monitor > Report > Generate > Traffic - default report configuration options

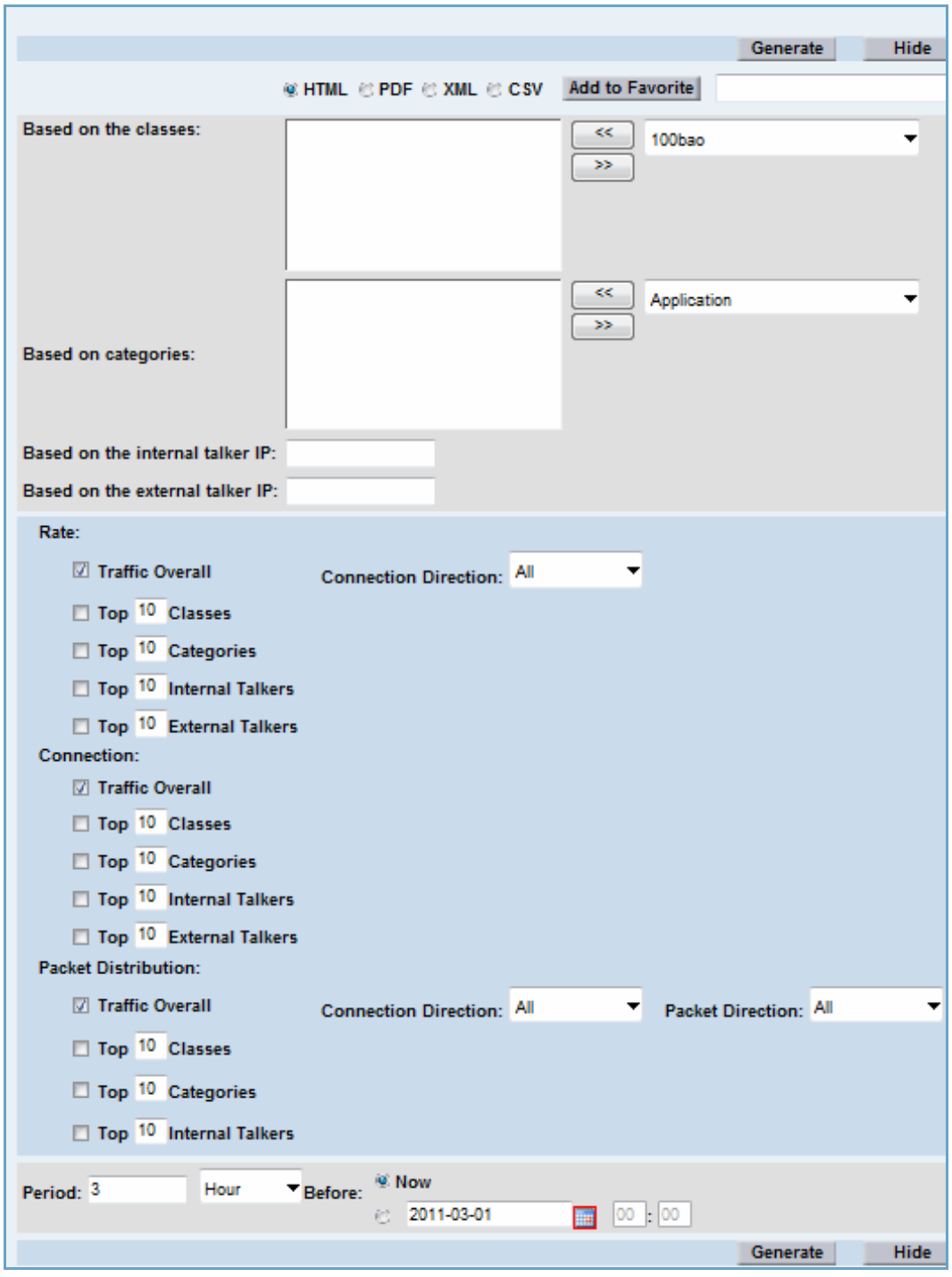


Figure 89 shows output using the default report settings.

FIGURE 89 Monitor > Report > Generate > Traffic - report output

TCP Performance

TCP performance reports shows graphs and statistics for the following:

- Efficiency
- Round-trip-time (RTT)
- Connection health (Conn-Health)

By default, statistics are shown for all classes, and for both packet and connection directions. You can narrow the scope of the report by selecting individual classes, and by selecting inbound or outbound for the packet or connection direction.

Figure 90 shows the default TCP performance report settings.

FIGURE 90 Monitor > Report > Generate > TCP Performance - default report configuration options

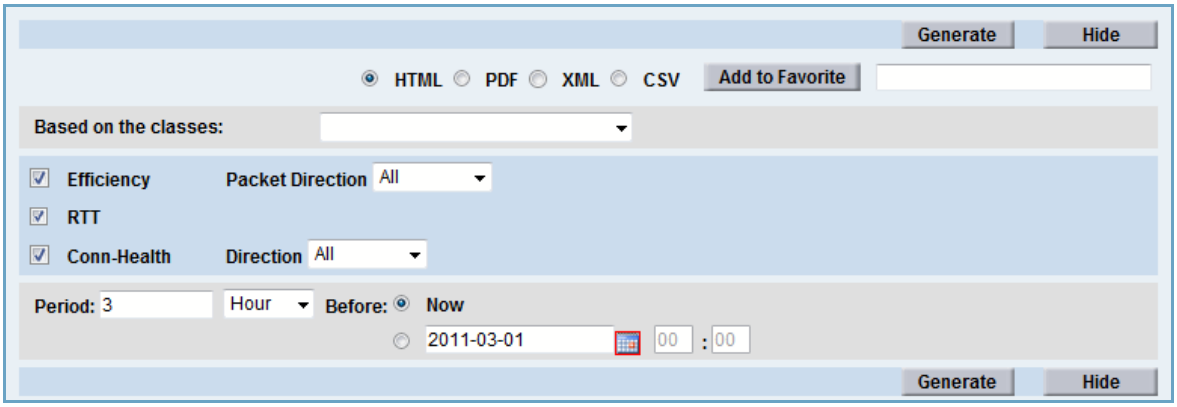


Figure 91 and Figure 92 show output using the default report settings.

FIGURE 91 Monitor > Report > Generate > TCP Performance - report output (1 of 2)

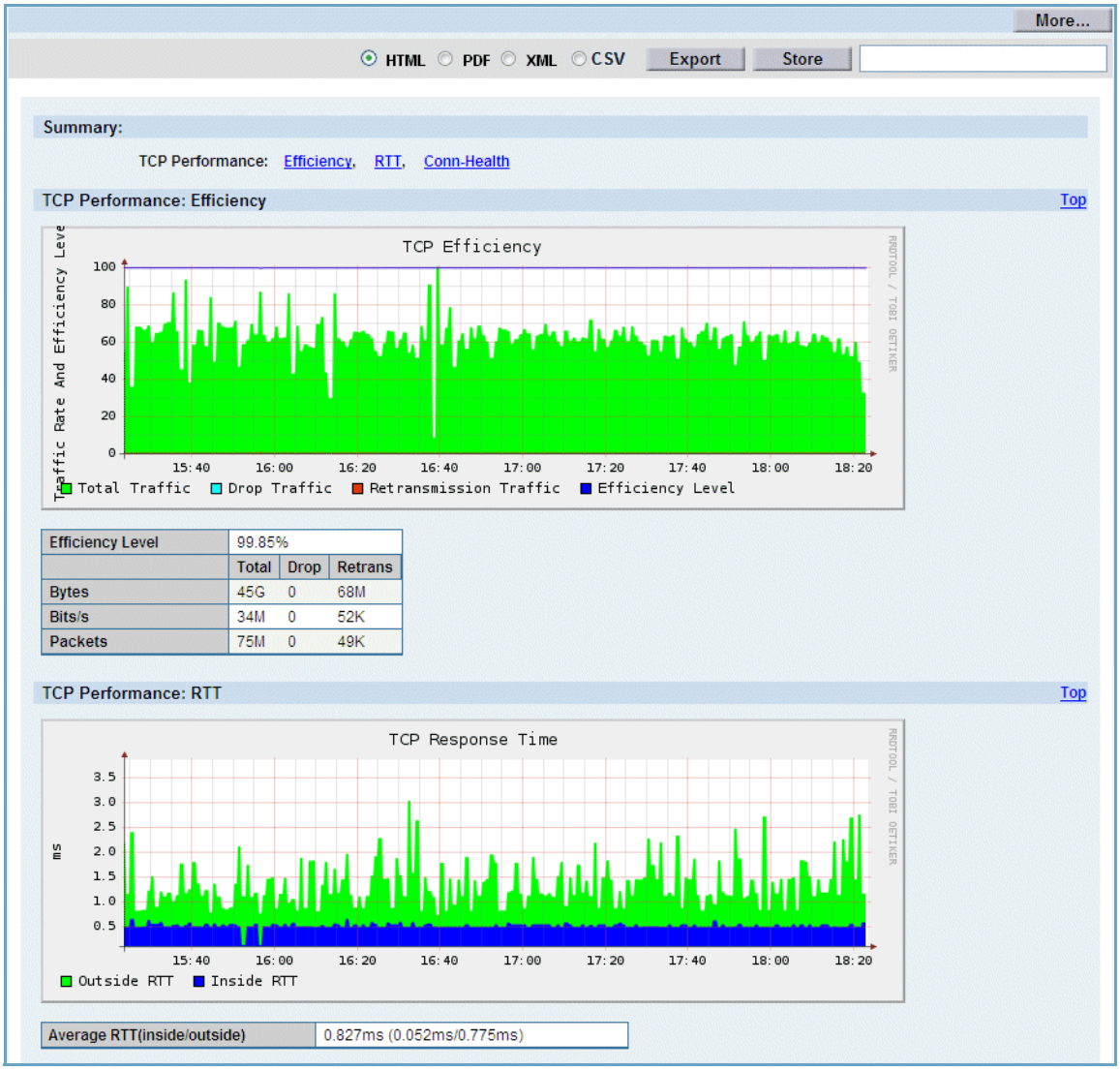
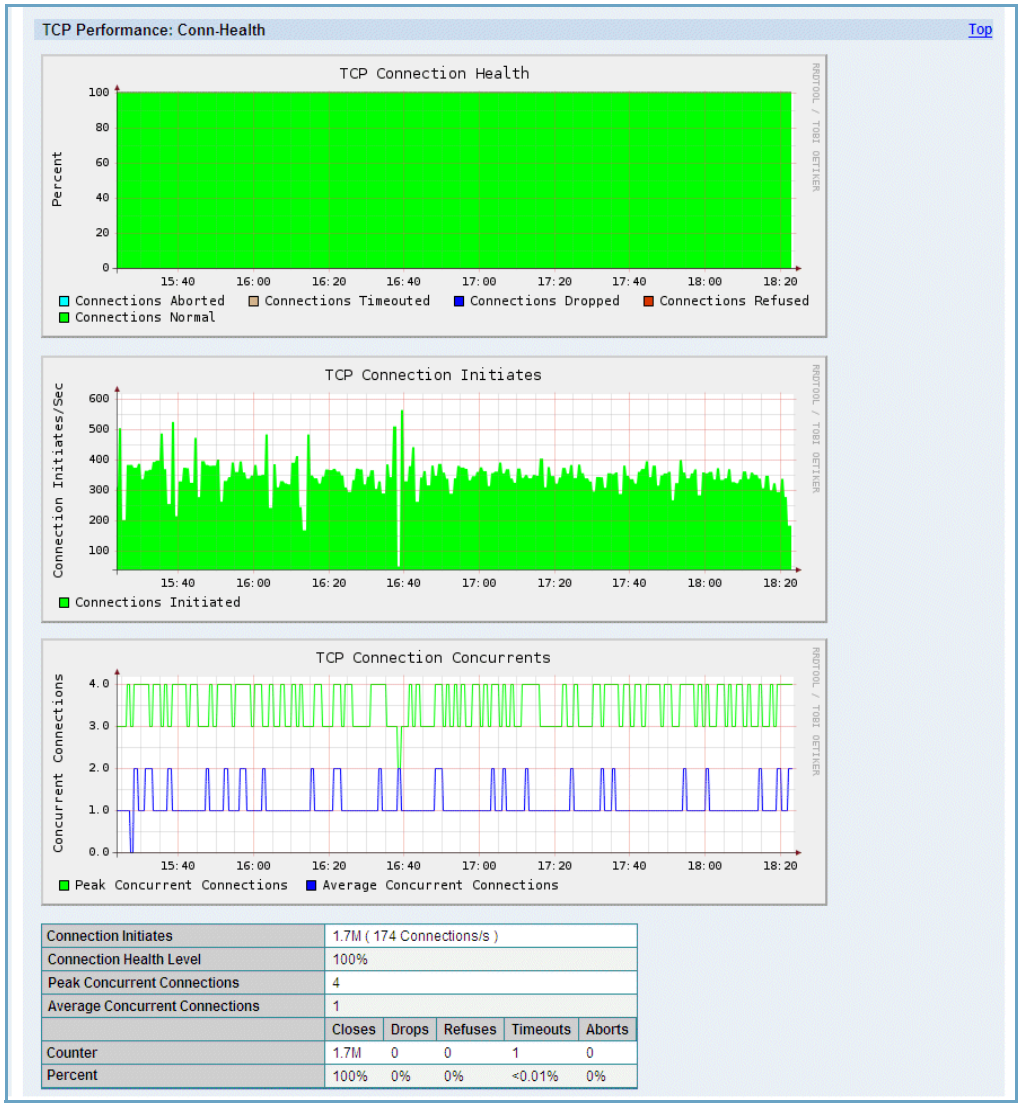


FIGURE 92 Monitor > Report > Generate > TCP Performance - report output (2 of 2)



Connection Initiates	1.7M (174 Connections/s)				
Connection Health Level	100%				
Peak Concurrent Connections	4				
Average Concurrent Connections	1				
	Closes	Drops	Refuses	Timeouts	Aborts
Counter	1.7M	0	0	1	0
Percent	100%	0%	0%	<0.01%	0%

URL

URL reports show the URLs accessed by internal talkers during the report period, and lists the most active internal talker IP addresses.

By default, overall statistics are displayed, as well as the 10 most active URLs and the 10 most active internal talkers.

You can narrow the scope of the report by entering a specific URL string. internal talker IP, or both. You also can change the number of URLs or talker IPs listed in the report output.

Figure 93 shows the default URL report settings.

FIGURE 93 Monitor > Report > Generate > URL - default report configuration options

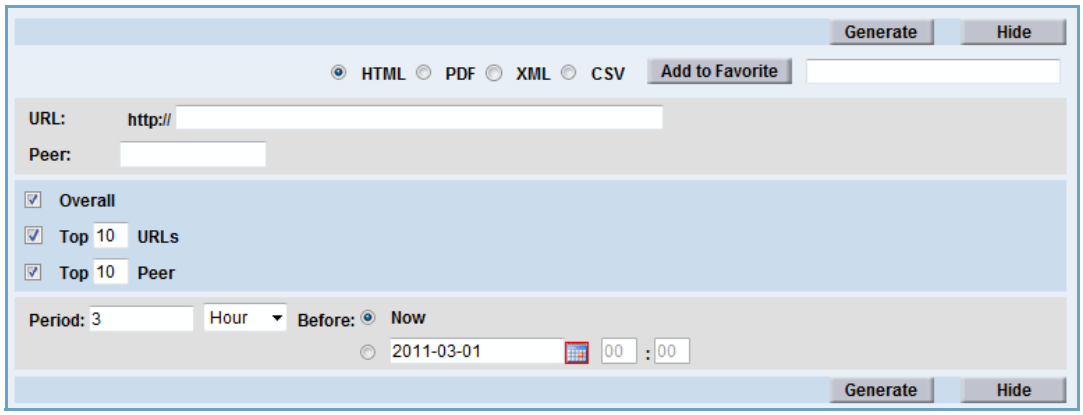
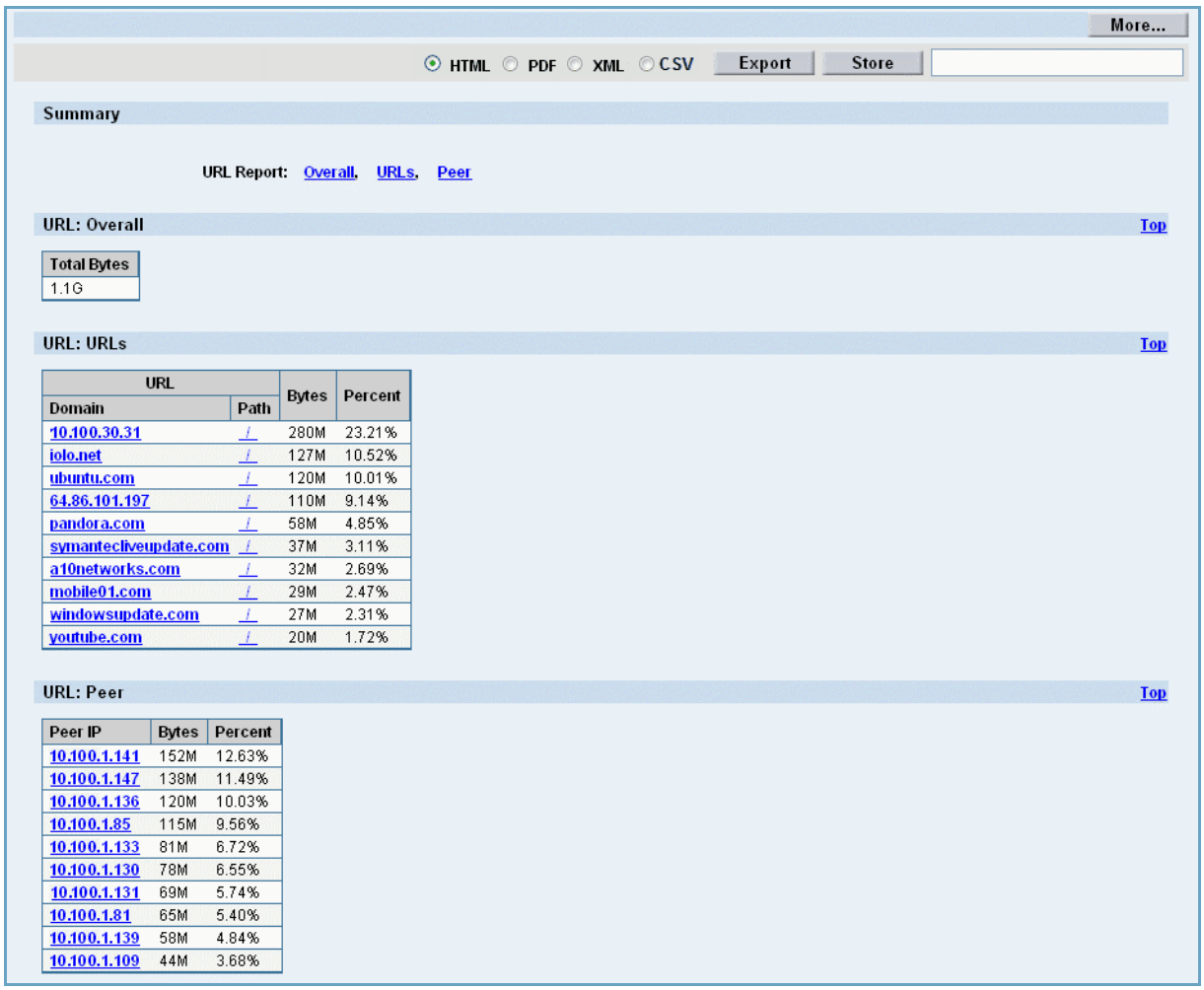


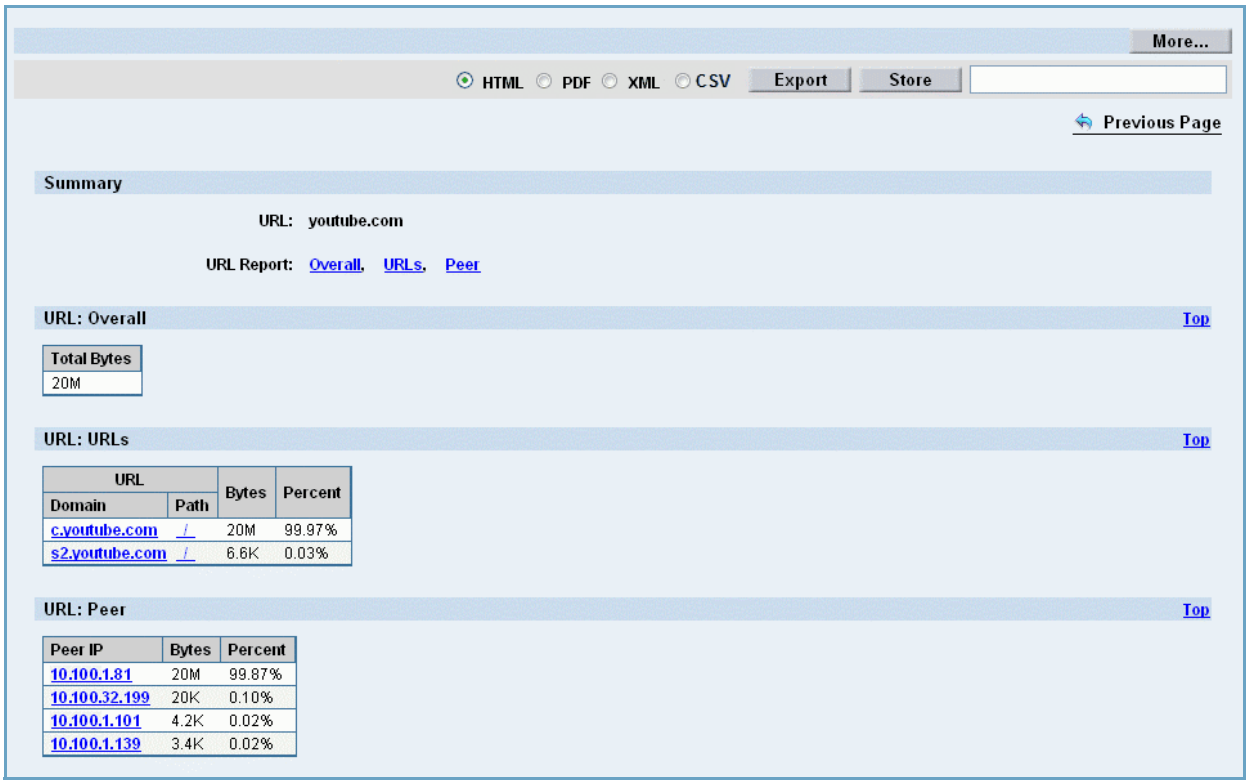
Figure 94 shows output using the default report settings.

FIGURE 94 Monitor > Report > Generate > URL - report output



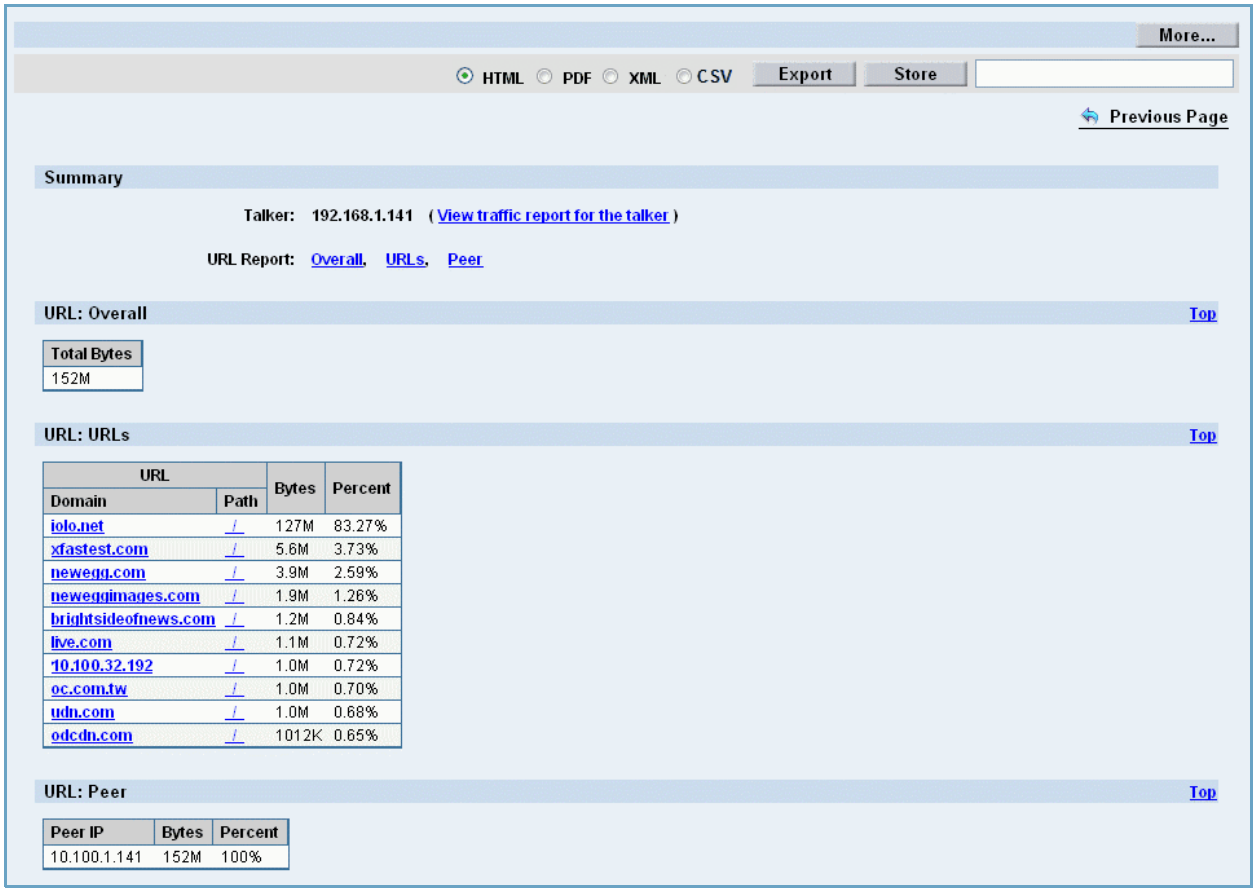
In the URLs table, you can click on a domain name to display a list of the hostnames accessed at that domain. Likewise, in the Peer table, you can click on an IP address to list the URLs accessed by that address. Figure 95 and Figure 96 show examples.

FIGURE 95 Monitor > Report > Generate > URL - URL details



Note: To return to the previous detail level of the report, click the Previous Page button, located in the upper right corner of the report page.

FIGURE 96 Monitor > Report > Generate > URL - Peer details



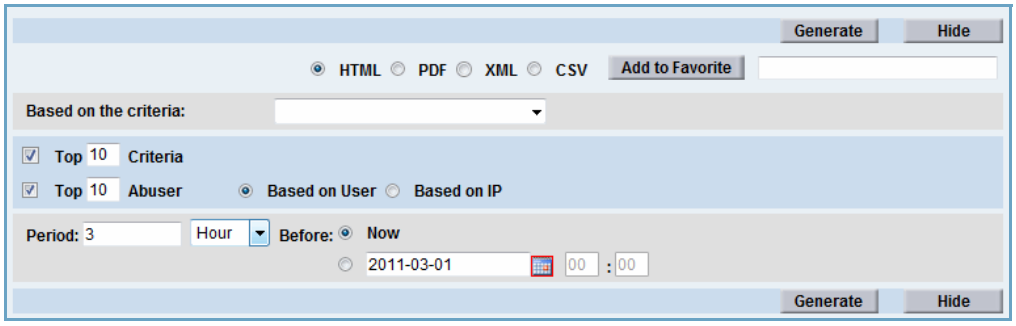
Abuser

Abuser reports show statistics for users who were in the abuser class during the report period. Users are placed in an abuser class when their network activity exceeds the thresholds specified by the configured abuser criteria. For details on configuring abuser criteria, see "Abuser Criteria" on page 133.

By default, the 10 most active abusers are listed, by username. You can change the number of abusers listed. You can also choose to list them by IP address, username, or abuser criteria.

Figure 97 shows the default Abuser report settings.

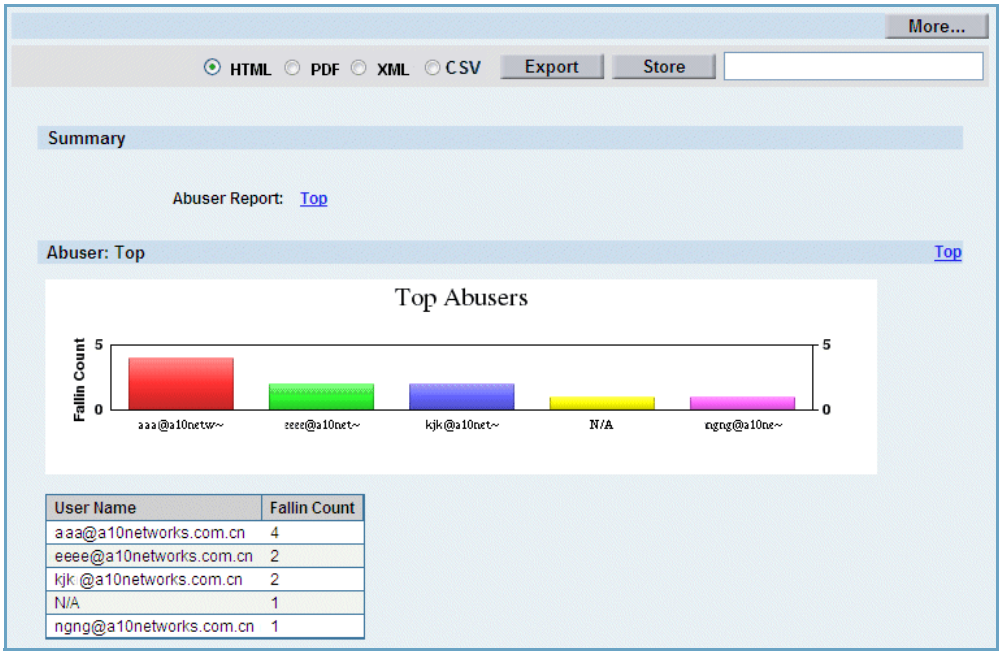
FIGURE 97 Monitor > Report > Generate > Abuser - default report configuration options



You can use the **Based on the criteria** drop-down menu to select an existing Abuser Criteria. This field is blank by default, in which case the generated report will be based on the global scope, or you can select "example_criteria" to generate an abuser report based on the associated Fall-in or Fall-out rules set up for that Abuser Criteria. The rules for Abuser Criteria can be configured by navigating to Config Mode > QoS > Class. Then, select Abuser Criteria from the menu bar.

Figure 98 shows abuser report output.

FIGURE 98 Monitor > Report > Generate > Abuser - report output



Others

Others reports show activity for the Others traffic class. By default, overall statistics are shown for all IP addresses and Layer 4 protocol ports, by source address.

You can narrow the scope of the report by entering a specific IP address or protocol port. You also can enable statistics for the following:

- Top services (listed by IP address and protocol port)
- Top IP addresses
- Top protocol ports

Figure 99 shows the default Others report settings.

FIGURE 99 Monitor > Report > Generate > Others - default report configuration options

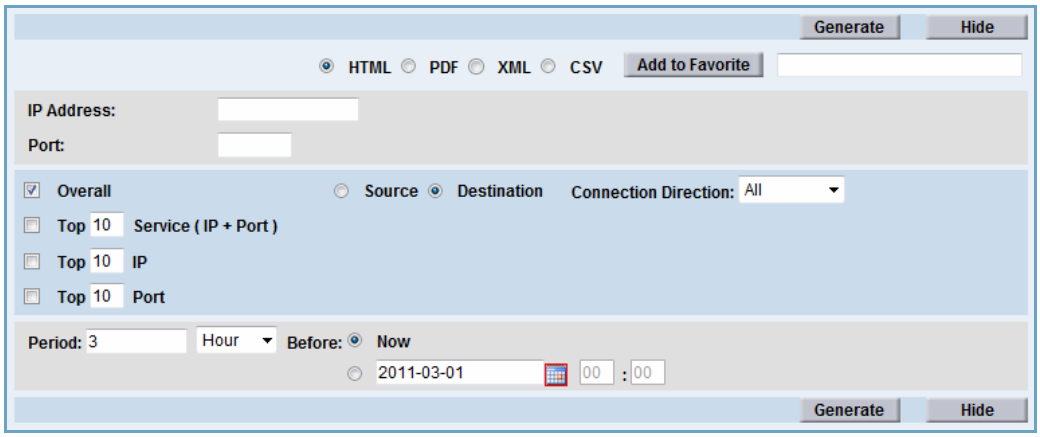
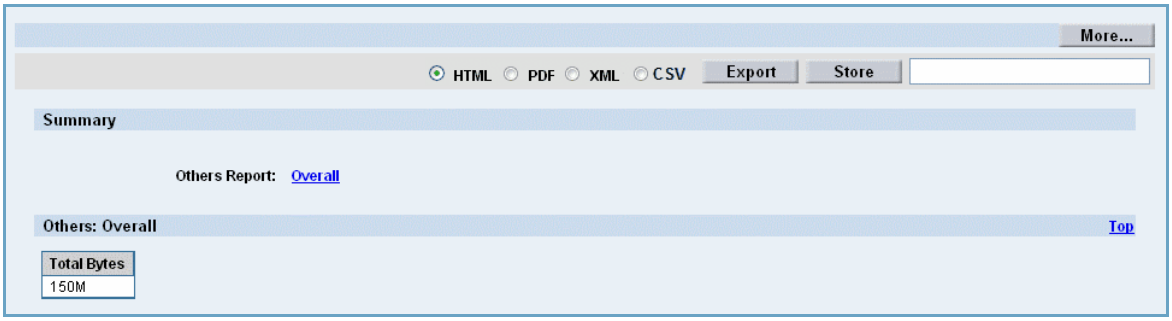


Figure 100 shows output using the default report settings.

FIGURE 100 Monitor > Report > Generate > Others - report output



Alert

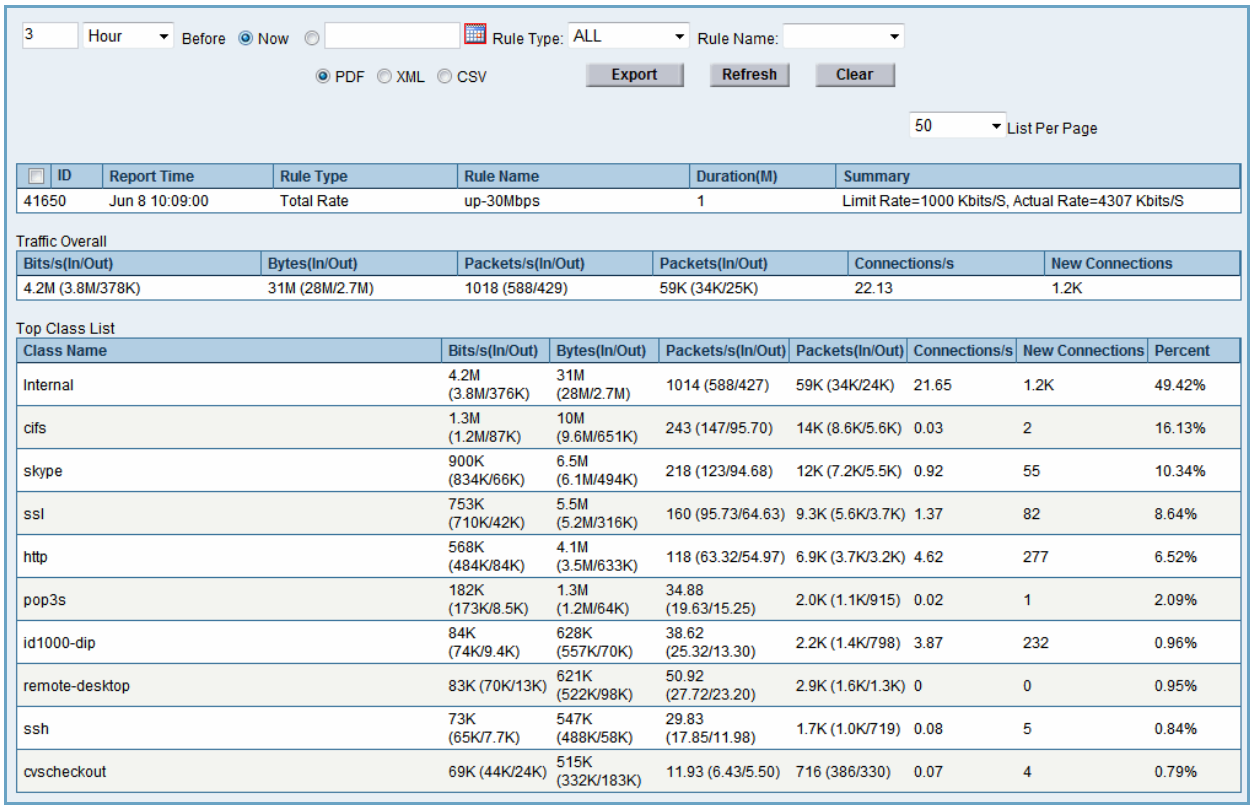
The Alert page shows the alerts generated by QoS. QoS alerts are generated when a traffic event matches a configured alert rule.

By default, all alerts generated during the most recent 3-hour period are listed. You can narrow the scope of the list by selecting one of the following alert types:

- Total rate
- User rate
- User connection

Figure 101 shows an example alert list using the type ALL report settings.

FIGURE 101 Monitor > Report > Generate > Alert - report output



ID	Report Time	Rule Type	Rule Name	Duration(M)	Summary
41650	Jun 8 10:09:00	Total Rate	up-30Mbps	1	Limit Rate=1000 Kbits/S, Actual Rate=4307 Kbits/S

Traffic Overall

Bits/s(In/Out)	Bytes(In/Out)	Packets/s(In/Out)	Packets(In/Out)	Connections/s	New Connections
4.2M (3.8M/378K)	31M (28M/2.7M)	1018 (588/429)	59K (34K/25K)	22.13	1.2K

Top Class List

Class Name	Bits/s(In/Out)	Bytes(In/Out)	Packets/s(In/Out)	Packets(In/Out)	Connections/s	New Connections	Percent
Internal	4.2M (3.8M/376K)	31M (28M/2.7M)	1014 (588/427)	59K (34K/24K)	21.65	1.2K	49.42%
cifs	1.3M (1.2M/87K)	10M (9.6M/651K)	243 (147/95.70)	14K (8.6K/5.6K)	0.03	2	16.13%
skype	900K (834K/66K)	6.5M (6.1M/494K)	218 (123/94.68)	12K (7.2K/5.5K)	0.92	55	10.34%
ssl	753K (710K/42K)	5.5M (5.2M/316K)	160 (95.73/64.63)	9.3K (5.6K/3.7K)	1.37	82	8.64%
http	568K (484K/84K)	4.1M (3.5M/633K)	118 (63.32/54.97)	6.9K (3.7K/3.2K)	4.62	277	6.52%
pop3s	182K (173K/8.5K)	1.3M (1.2M/64K)	34.88 (19.63/15.25)	2.0K (1.1K/915)	0.02	1	2.09%
id1000-dip	84K (74K/9.4K)	628K (557K/70K)	38.62 (25.32/13.30)	2.2K (1.4K/798)	3.87	232	0.96%
remote-desktop	83K (70K/13K)	621K (522K/98K)	50.92 (27.72/23.20)	2.9K (1.6K/1.3K)	0	0	0.95%
ssh	73K (65K/7.7K)	547K (488K/58K)	29.83 (17.85/11.98)	1.7K (1.0K/719)	0.08	5	0.84%
cvscheckout	69K (44K/24K)	515K (332K/183K)	11.93 (6.43/5.50)	716 (386/330)	0.07	4	0.79%

Configure and Generate Reports - Config Mode

The Config > Report > Report option enables you to do the following:

- View – Configure “views”, which are named sets of QoS categories that simplify report configuration by enabling you to include multiple classes in a report. When you select a view for a report, all the classes in the associated category are included in the report.
- Alert – Configure email alerts for notification when a network threshold has been breached.
- General – Configure email addresses for report and alert recipients, and access report history information.

Configure Views

To configure an alert:

1. Select Config > Report > Report.
2. On the menu bar, select the View tab.
3. Click the New button. The View tab appears.
4. Enter a name for the view in the Name field.
5. Click the drop-down menu and select the desired Category (e.g. P2P) from the list to add it to the view.
6. Click the Add button.
7. Repeat step 5 and step 6 to add more Categories to the view.
8. Click Apply to save the view and configure another one, or click OK to save the view and return to the Views table.

Configure Alerts

To configure an alert:

1. Select Config > Report > Report.
2. On the menu bar, select Alert.
3. Click New. The Alert Rule tab appears.

4. Enter a name for the rule in the Name field.

5. Select the alert type from the Type drop-down list:
   - Total Rate – Sets a limit for the total traffic rate. The alert will be raised if the total traffic rate exceeds the limit.
   - User Rate – Sets a limit for user traffic rate. The alert will be raised if any user's traffic rate exceeds the limit.
   - User Connection – Sets a limit for user connections. The alert will be raised if new user-sponsored connections within a certain time period exceed the limit.

6. Configure the alert parameters. (See Table 14.)

7. To enable emailing of alerts, select the Enabled radio button next to Email.

8. Enter one or more email addresses in the Email Address field to determine where alerts will be sent. Multiple addresses should be separated with a comma (,).

9. Click Apply to save the alert and configure another one, or click OK to save the alert and return to the alert table.

Table 14 lists the parameters you can configure for alert rules.

TABLE 14 Alert Rule Parameters

Alert Type	Parameter	Description
Total Rate	Rate	Maximum allowed traffic within the duration period, for all users. You can specify 1-8000000 kbits/s.
	Duration	Duration time for the rate limit. If the average rate exceeds the limit within the specified duration, the alert is generated. You can specify 0-2147483647 minutes.
	Notification Interval	Amount of time the EX appliance will wait between sending alerts generated by this alert rule. You can specify 0-2147483647 minutes.
User Rate	Rate	Maximum allowed traffic within the duration period, for a single user. You can specify 1-8000000 kbits/s.
	Duration	Duration time for the rate limit. If the average rate exceeds the limit within the specified duration, the alert is generated. You can specify 0-2147483647 minutes.
	Notification Interval	Amount of time the EX appliance will wait between sending alerts generated by this alert rule. You can specify 0-2147483647 minutes.
	Ignored IP List	Excludes the specified IP address from the alert.

TABLE 14 Alert Rule Parameters (Continued)

Alert Type	Parameter	Description
User Connection	Connection	Maximum number of connections allowed within the duration period, for a single user.
	Duration	Duration time for the connection limit. If the average number of new connections exceeds the limit within the specified duration, the alert is generated. You can specify 0-2147483647 minutes.
	Notification Interval	Amount of time the EX appliance will wait between sending alerts generated by this alert rule. You can specify 0-2147483647 minutes.
	Ignored IP List	Excludes the specified IP address from the alert.

Configure Export Settings for Alerts

To export alerts:

1. Select Monitor > Report > Generate.
2. On the menu bar, select Alert.
3. Optionally, change display settings to filter the list.
4. Select the output format: PDF, XML or CSV.
5. Click Export. The browser displays a file management dialog.
6. Click OK (Firefox) or Save (Internet Explorer), navigate to the save location, and click Save.

Configure General Report Settings

To configure General report settings:

1. Select Config > Report > Report.
2. On the menu bar, select the General tab.
3. To configure Email settings, click the Email tab and then:
   a. Enter one or more email addresses (separated by a comma) in the Email Address field.
   b. Click Apply to submit your changes.

4. To configure Export settings, click the Export tab and then:
   a. Select the desired file transfer protocol from the drop-down menu: FTP, TFTP, RCP, or SCP.
   b. If needed, change the protocol port number in the port field. By default, the default port number for the selected protocol is used.
   c. In the Host field, enter the IP address or Fully Qualified Domain Name (FQDN) of the server.
   d. In the Location field, enter the directory path and filename.
   e. In the User and Password fields, enter the username and password required for access to the remote server.
   f. Click Apply to submit your changes.
5. To view Report History, click the Report History tab and then:
   a. Enter the desired number of days for which you would like to view report history. Enter a number ranging from 7 days to 366 days. The default is 30 days.
   b. Click Apply to submit your changes.

Manage Report Configurations (Favorites)

The Monitor > Report > Favorite option provides access to saved report configurations. You can use the saved report configurations to generate new report output. On-demand and scheduled reports are also available.

To save a report to the Favorite page:

1. Navigate to the configuration page for the report (for example, Monitor > Report > Generate > Traffic).
2. Configure report settings.
3. Enter a name for the report configuration in the input field next to the Add to Favorite button.
4. Click Add to Favorite.

Generate On-Demand Reports

To generate an on-demand report:

1. Select Monitor > Report > Favorite.
2. Click on the report name in the Name column.

   The EX appliance generates the report and displays the output.
3. Optionally, to modify report settings:
   a. Click More to display the report configuration fields.
   b. Modify the settings.
   c. Click Generate.

Edit Reports

To edit a report configuration:

1. Select Monitor > Report > Favorite.
2. Click the  icon next to the report name. The report configuration fields appear.
3. Modify the settings.
4. To test the report configuration, click Generate.

5. To save the edited report configuration, click More to return to the report configuration fields.
6. Click Add to Favorite.

Schedule Reports

To schedule a report:

1. Select Monitor > Report > Favorite.
2. Select the checkbox next to the name of each report you want to schedule.
3. Click the Schedule button.
4. Specify the time period for the schedule:
   a. Click the calendar icon on the From field. A calendar is displayed.
   b. Select the start date for the schedule. The date appears in the field.
   c. To specify an end date for the schedule, select the To checkbox and use the calendar to select the end date. Otherwise, if you do not want to specify an end date, leave the To checkbox unselected.

Note: To use the current date as the start or end date, you must click on the date. The current date is not automatically entered in the From or To field.

5. Specify how often the report will be generated during the scheduled time period:
   a. From the drop-down list, select one of the following:
      - Days
      - Weeks
      - Months

      By default, the report is generated once per the selected interval; for example, 1 time per Day.
   b. To wait longer to generate the report, enter a higher number. For example, to generate a report only once every 3 days, select Days and enter 3.
6. Specify when within the specified period to generate the reports:
   - Days – Enter the time (*hh*:*mm*) at which to generate the reports. You can generate up to 4 reports per day.
   - Weeks – Enter the time(s) of day as described above, then select the days of the week.

- Months – Enter the time(s) of day as described above, then enter the days of the month. To enter a day of the month, select it from the drop-down list, then click <<.

7. Optionally, enter one or more email addresses to which to send the generated report. You can separate multiple email addresses with a comma (,) after each address.

8. Optionally, you can choose to export the generated report to a remote server as follows:
   a. Select the desired file transfer protocol from the drop-down menu: FTP, TFTP, RCP, or SCP.
   b. If needed, change the protocol port number in the port field. By default, the default port number for the selected protocol is used.
   c. In the Host field, enter the IP address or Fully Qualified Domain Name (FQDN) of the server.
   d. In the Location field, enter the directory path and filename.
   e. In the User and Password fields, enter the username and password required for access to the remote server.

9. Click OK to submit your changes.

The favorites list is redisplayed. The schedule information for the report is listed in the Next Run Time and Schedule columns.

When a scheduled report is generated, the output is stored on the EX appliance. If you specified an email address, the report is also emailed. If you configured a file transfer protocol, the report is exported to the specified server.

To view locally stored reports, see "Manage Locally Stored Reports" on page 200.

Manage Locally Stored Reports

The Monitor > Report > Stored option provides access to saved report output. To view a saved report, click on the report name in the Name column.

If the report output was generated by a scheduled favorite report, the report configuration name is listed in the Favorite column.

Search fields above the report list enable you to filter the list.

By default, saved reports are stored locally for the number of days specified for the report history. Reports that are older than the number of days allowed by the report history are deleted. If the EX appliance runs out of room for stored reports, the oldest reports are deleted to make room for new ones.

To export reports:

1. Select the checkbox next to the name of each report you want to export.
2. Click Export. The browser displays a file management dialog.
3. Click OK (Firefox) or Save (Internet Explorer), navigate to the save location, and click Save.

Network Settings

This chapter describes how to configure the EX Secure WAN Manager for internetworking with other devices. You can configure settings for Layer 2 switching, Layer 3 routing, and DNS caching.

Overview

The following sections describes the network features you can configure on the EX appliance.

IP Interfaces

The EX appliance has copper ethernet ports, and some models offer fiber ethernet port interfaces. You can configure up to 12 IP interfaces on each ethernet interface. The IP interfaces can be in different subnets, allowing the EX appliance to belong to multiple subnets.

(To configure IP interfaces, see "Interfaces" on page 205.)

VLANs

A Virtual LAN (VLAN) is a Layer 2 broadcast domain. Generally, traffic within a VLAN is in the same subnet and is forwarded at Layer 2. Traffic from one VLAN to another is forwarded at Layer 3 (routed).

You can add the EX appliance to a VLAN by configuring the VLAN on the device and adding one or more of the device's ethernet interfaces to the VLAN.

Each ethernet interface can belong to one or more VLANs (or none). To belong to more than one VLAN, an interface must be tagged. You can tag an interface when configuring a VLAN.

When you configure a VLAN, the EX appliance automatically adds a virtual ethernet (VE) interface for it. The VE number is the same as the VLAN number. The VE provides a router (Layer 3) interface for the VLAN. If you disable the VE, the VLAN also is disabled.

You can configure up to 64 VLANs on the EX appliance, allowing the device to belong to up to 64 Layer 2 broadcast domains.

(To configure VLANs, see "VLANs" on page 211.)

ARP Table

The Address Resolution Protocol (ARP) table maps MAC addresses to IP addresses. The EX Secure WAN Manager uses the ARP table to select an interface on which to forward traffic.

The ARP table can contain the following types of entries:

- Dynamic – Dynamic entries are added in the ARP table automatically when the EX appliance learns the MAC address-IP address mapping from traffic. Dynamic entries age out of the ARP table if they are unused. The aging time is 5 minutes and is not configurable.
- Static – Static entries are configured by an administrator and do not age out. A static entry can be removed only by an administrator.

(To display or configure ARP entries, see "ARP Table" on page 212.)

IP Routing

The EX Secure WAN Manager has an IP route table. You can add static routes to the table to provide basic routing through a default gateway. (To configure static routes, see "Static Routes" on page 214.)

The EX appliance also supports dynamic routing using the following popular interdomain routing protocols:

- Open Shortest Path First (OSPF)
- Routing Information Protocol (RIP)

The EX appliance supports OSPF as specified in RFCs 2328 and 3137. RIP version 2 is supported as described in RFCs 1058, 2082, and 2453.

(To configure OSPF, see "OSPF Routing" on page 216. To configure RIP, see "RIP Routing" on page 224.)

Reply Interface for Locally Received Requests

By default, the EX appliance may send the response to a locally received request (request addressed to the EX appliance's IP address) out a different interface than the one that receives the request. Optionally, you can configure the EX appliance to send replies out the same interface that receives the requests. (See "Configure Reply Interface Selection for Locally Received Requests" on page 229.)

DNS

The following DNS parameters are configurable:

- Primary and secondary DNS servers to use for resolving requests.
- Local domain names, hosts, and MX records.
- Domain-based DNS proxies

In addition, you can view the DNS cache. The DNS cache contains replies to queries sent to external DNS servers.

(To configure DNS, see "DNS" on page 230.)

Interfaces

This section shows how to configure and manage the EX appliance physical interfaces.

Configure an Interface

You can configure up to 16 IP addresses on each EX appliance physical interface.

To configure a physical interface:

1. Select Config Mode > Network > Interface.
2. On the menu bar, select Interface, if not already selected.
3. In the Interface column, click on the interface you want to configure. The Interface tab appears. (See Figure 102.)
4. In the Shape Interface field, specify the rate in Kbps at which traffic can pass through the interface.
5. To change the status of the interface, select the appropriate Enabled or Disabled radio button.
6. Select the Internal or External radio button to indicate whether the interface is connected to the internal network of the Internet:
   - Internal – The interface is connected to your internal network.
   - External – The interface is connected to an ISP link to the Internet.

7. To change the Maximum Transmission Unit (MTU), change the number in the MTU field. The MTU specifies the maximum size an IP datagram can be. You can specify from 100 to 1500. The default is 1500.

8. To change the interface speed, select the Manual radio button, then select one of the following options from the pull-down list:
   - 10Mb/s, Full-Duplex
   - 10Mb/s, Half-Duplex
   - 100Mb/s, Full-Duplex
   - 100Mb/s, Half-Duplex (see "Note" below)

Note: This does not effect the fiber interface. It is 1000Mb/s and Full-Duplex.

9. Select management access methods you want to allow on the interface:
   - SSH – Allows access using Secure Shell (SSH) version 1 or version 2.
   - Telnet – Allows access using Telnet.
   - HTTP – Allows access using the GUI described in this manual.

Caution: If you deselect HTTP, the EX appliance ends your Web management (GUI) session as soon as you click OK or Apply.
   - SNMP – Allows the interface to respond to SNMP GET and GET-NEXT SET requests.
   - Ping – Allows the interface to respond to ICMP echo requests.
   - Trust Host – Allows access only from trusted hosts configured for admin accounts. (See "Admin Accounts" on page 248.)

10. Select the Source NAT checkbox to to use the IP address of that interface (i.e. specify NAT without an IP Pool)

11. Click OK or Apply to submit your changes, and then click the flashing red Save button to save your changes to the startup-config file.

12. Click the IP Address tab to configure the EX appliance to receive an IP address from a DHCP server or to manually assign an IP address. (See Figure 103.)
    - **DHCP** – Select the DHCP radio button to receive an IP address from a DHCP server. Optionally, you can select the Retrieve Route and DNS Options checkbox to retrieve information about routers, static-routes, domain-name, and domain-name-servers when the IP address is assigned by DHCP.
    - **Manually** – Select the Manual radio button and enter the IP address and network mask of the interface in the IP Address and Mask

fields. Then, click the Add button. Repeat this process to manually add more IP addresses.

13. Click OK or Apply to submit your changes, and then click the flashing red Save button to save your changes to the startup-config file.
The interface table is updated with the new settings.

FIGURE 102 Interface Tab

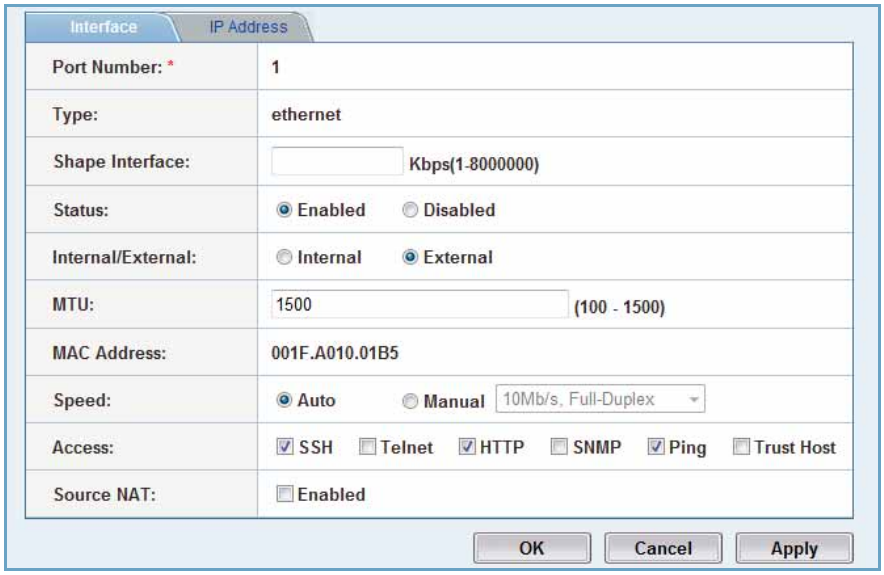
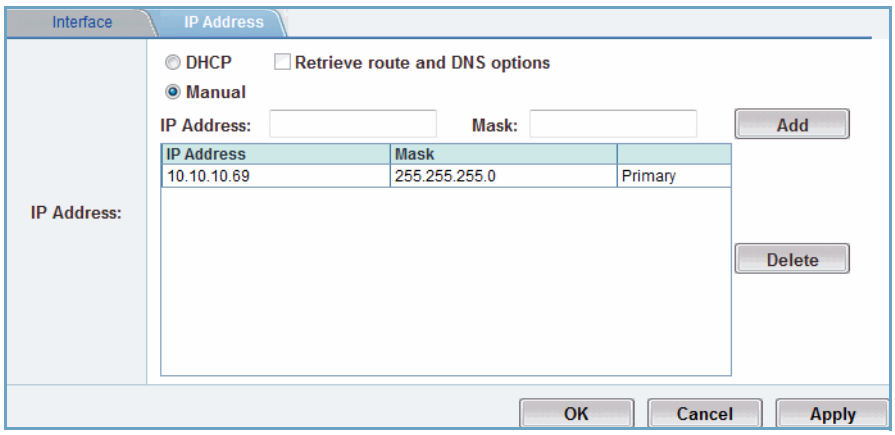


FIGURE 103 IP Address Tab



Display Ethernet Interfaces

To display the EX Secure WAN Manager ethernet interfaces, select Config Mode > Network > Interface.

FIGURE 104 Ethernet Interface Table

Interface	IP Address/Mask	MAC Address	Shape Interface	Internal/External	Speed	Status
ethernet1		0090.0B08.8511		Internal	Auto	
ethernet2		0090.0B08.8510		Internal	Auto	
ethernet3		0090.0B08.850F	1000	External	Auto	
ethernet4		0090.0B08.850E	100000	Internal	Auto	

Disable or Re-Enable an Interface

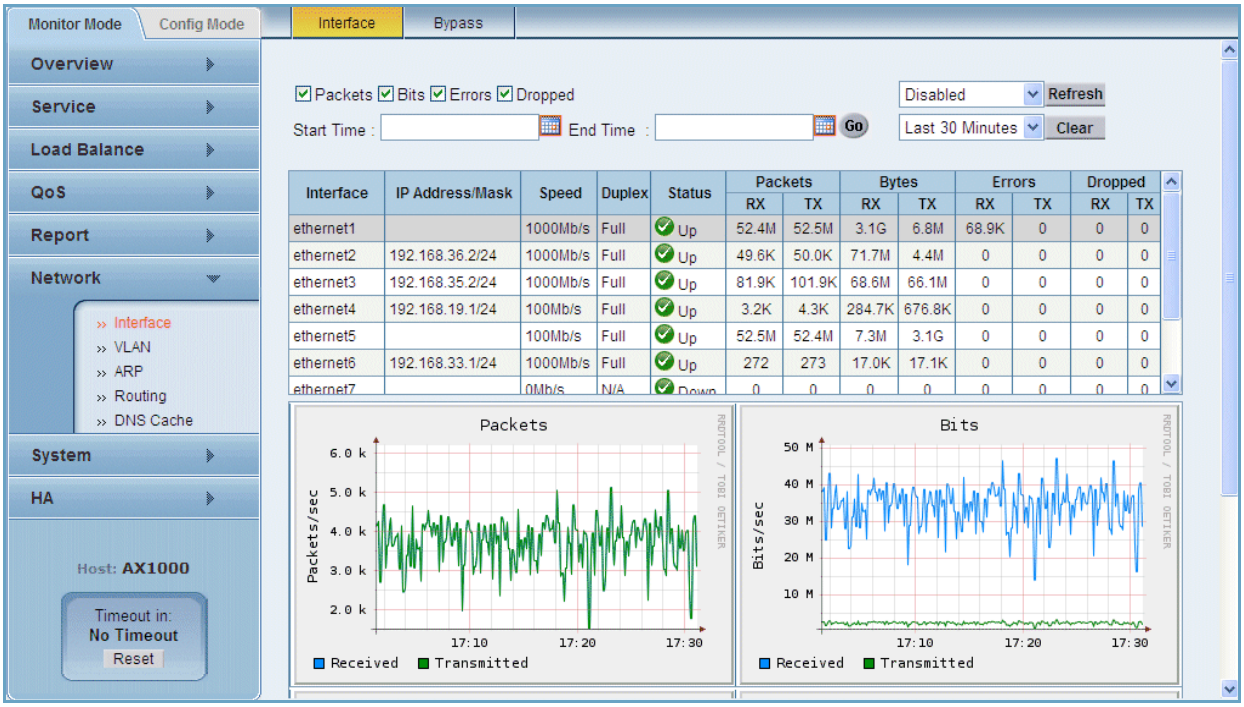
To disable or re-enable an interface:

1. Select Config Mode > Network > Interface.
2. Select the checkbox next to the interface name.
3. Click Disable to disable the interface or Enable to re-enable it.

Display Interface Statistics

To display interface statistics, select Monitor Mode > Network > Interface. Statistics are displayed in a table and in graphs. (See Figure 105.)

FIGURE 105 Interface Statistics



(For information about the display options for the graphs, see "Graph Display Options" on page 26.).

Port Bypass

Models EX 1100 and EX 2110 have a hardware feature that passes traffic between a pair of Ethernet interfaces at Layer 2 without processing the traffic. Hardware bypass is disabled when the EX appliance is powered on, and the feature engages automatically when the EX appliance is powered off, in order to avoid interrupting network traffic.

The EX 1100 and EX 2110 have the following bypass pairs:

- Pair 1 – Ethernet interfaces 1 and 2
- Pair 2 – Ethernet interfaces 3 and 4

To display the port bypass state:

1. Select Monitor > Network > Interface.
2. On the menu bar, select Bypass.

To enable port bypass:

1. Select Config > Network > Interface.
2. On the menu bar, select Bypass.
3. In the Bypass Interface Pair section of the window, select the Enabled checkbox for pair 1 (eth 1, eth 2) and for pair 2 (eth 3, eth 4). You can enable one or both pairs.
4. Click Apply.

To enable port Bypass on Shutdown:

Note: When the EX appliance is shutting down, the software stops processing packets. If the port bypass feature is enabled, the EX appliance will continue passing traffic between paired ports at Layer 2. However, traffic is dropped and TCP connections are terminated as control is passed from the software to the hardware. This hand-off period lasts approximately 12 seconds, but it can be reduced to only 4 seconds by enabling the Bypass on Shutdown feature.

1. Select Config > Network > Interface.
2. On the menu bar, select Bypass.
3. In the Bypass On Shutdown Interface Pair section of the window, select the Enabled checkbox for pair 1 (eth 1, eth 2) and for pair 2 (eth 3, eth 4). You can enable one or both pairs.
4. Click Apply.

VLANs

To add the EX Secure WAN Manager to a VLAN, configure the VLAN on the device and add one or more of the device's ethernet interfaces to the VLAN.

When you add interfaces to a VLAN, you can specify whether the interfaces are tagged or untagged:

- Untagged interfaces can be in only one VLAN.
- Tagged interfaces can be in multiple VLANs. The tag ID identifies the VLAN and is different for every VLAN. On the EX Secure WAN Manager, the tag ID is the same as the VLAN ID.

Configure a VLAN

By default, no VLANs are configured on the EX Secure WAN Manager. You can configure up to 64 VLANs. The EX appliance automatically creates a VE for a VLAN when you configure the VLAN.

To configure a VLAN:

1. Select Configure > Network > VLAN.

   The configured VLANs are displayed in a table.

2. Click New. The VLAN tab appears. (See Figure 106.)

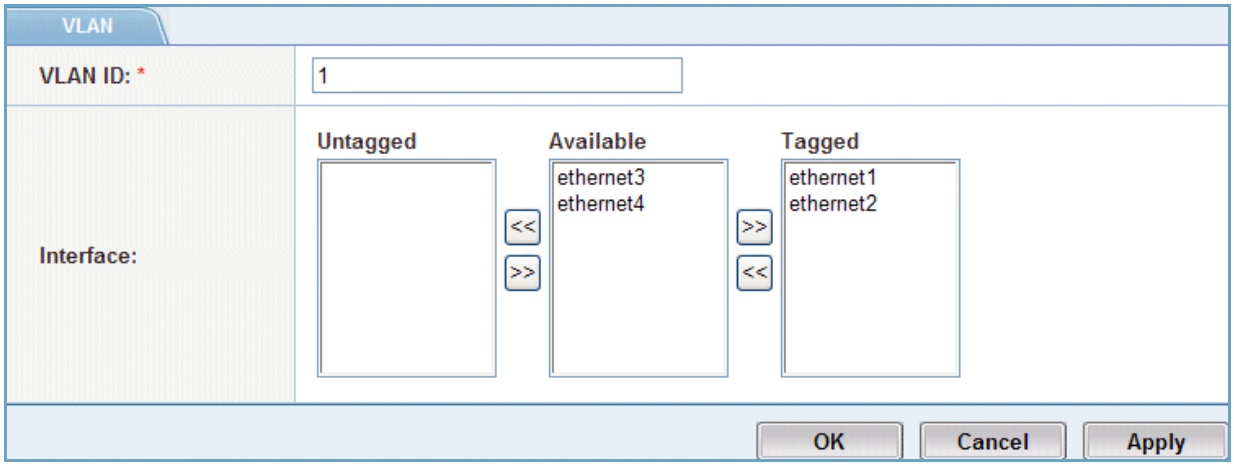
3. In the VLAN ID field, enter the VLAN number. You can use a value from 1 to 4094.

4. In the Available list, select the EX appliance interfaces you want to place in the VLAN.

5. Move them to the Untagged or Tagged list:
   - If the interfaces will be in this VLAN only, not members of any other VLAN, you can move them to the Untagged list. Click << .
   - If the interfaces will also be members of another VLAN, you must move them to the Tagged list. Click >> .

6. Click OK. The new VLAN appears in the VLAN table.

FIGURE 106 VLAN Tab



Display Forwarding Database Entries for a VLAN

Each VLAN has its own Forwarding Database (FDB). To display a VLAN's FDB:

1. Select Monitor Mode > Network > VLAN.
2. From the VLAN Forwarding Database pull-down list, select the VLAN ID.
3. Click Find.

ARP Table

Use the following sections to display and add static entries to the ARP table.

Display the ARP Table

To display the ARP table, select Monitor Mode > Network > ARP.

The ARP table lists the EX Secure WAN Manager interfaces through which the MAC addresses and IP addresses can be reached.

If the EX appliance is integrated with the A10 Networks IDsentrie, the Identity column indicates the users associated with the IP addresses.

Note: If a device is in another subnet, the MAC address listed for the device is the MAC address of the next-hop switch or router on the route to the device, not the MAC address belonging to the device itself. However, the IP address is always the IP address belonging to the device itself.

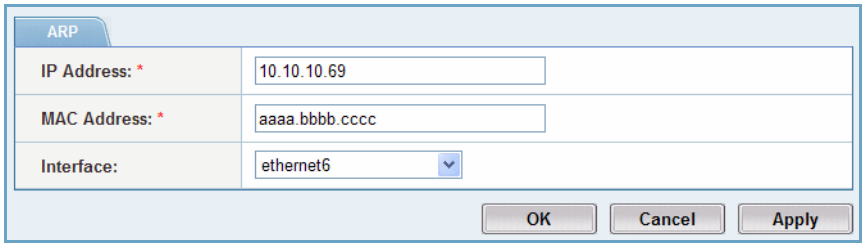
Note: The Identity column displays N/A unless the EX appliance is integrated with an IDsentrie to supply the identity information.

Add a Static ARP Entry

To add a static entry to the ARP table:

1. Select Config Mode > Network > ARP.
2. On the menu bar, select ARP, if not already selected.
3. Click New. The ARP tab appears. (See Figure 107.)
4. In the IP Address field, enter the IP address for the entry.
5. In the MAC Address field, enter the MAC address.
   - If the device is in the same subnet as the EX appliance, enter the MAC address of the device.
   - If the device is in another subnet, enter the MAC address of the next-hop interface to the device.
6. Select the Ethernet interface from the Interface drop-down list.
7. Click OK. The new entry appears in the table.

FIGURE 107 ARP Tab



IP Route Table

To display the IP route table, select Monitor Mode > Network > Routing.

By default, the IP route table displays all the IP routes on the EX Secure WAN Manager. This includes static routes configured by an administrator as well as "connected" routes, and routes the EX appliance has learned through RIP or OSPF. To filter the display based on route type, select the route type from the pull-down list above the table.

The Destination Address and Subnet Mask fields indicate the destination subnet that can be reached through the route. The Next Hop field indicates the router to which the EX appliance forward traffic is addressed to the destination network. The Interface column lists the EX appliance connected to the next-hop router. The Type field indicates how the route entered the table and can be one of the following:

- Connected – The route is to a subnet configured on the EX appliance itself. The EX appliance automatically creates the route when you configure an IP address on an EX appliance interface.
- Static – The route was configured by an administrator.
- RIP – The route was learned by the EX appliance through RIP.
- OSPF – The route was learned by the EX appliance through OSPF.

To configure IP routing, see the following sections:

- To configure a static route, see "Static Routes" on page 214.
- To configure an RIP route, see "OSPF Routing" on page 216.
- To configure a static route, see "RIP Routing" on page 224.

Static Routes

A static route is a route configured by an administrator. A static route specifies the destination subnet address and the gateway router used to reach that subnet. When the EX Secure WAN Manager needs to forward traffic to the subnet, the EX appliance sends the traffic to the gateway.

The subnet address is specified by an IP address prefix and a network mask (for example: 192.168.10.0 255.255.255.0). The gateway is specified only by its IP address.

Optionally, you can specify an Ethernet interface or Virtual Ethernet (VE) interface for the route. If you specify an interface, packets that use the route are sent only on the specified interface. If you specify both a physical inter-

face and a VE, only the Ethernet interface you specify within the VE is used.

Static routes have an administrative distance, which can be 1-255. The administrative distance is used as a tie breaker. If there are multiple routes to the same destination and all other costs associated with the routes are equal, the route with the lowest administrative distance is used.

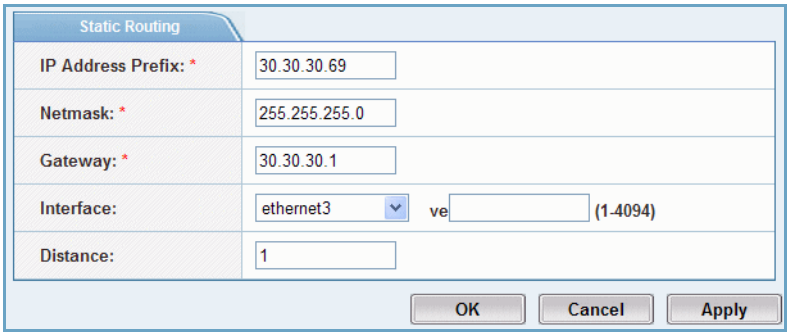
A common type of static route is a default route. A default route is the route used by a device to send traffic to another subnet, when the device does not have a route specifically to that subnet. The destination subnet address in default routes is all zeros (0.0.0.0 0.0.0.0).

Configure a Static Route

To configure a static route:

1. Select Config Mode > Network > Routing.
2. On the menu bar, select **Static**, if not already selected. The list of configured static routes is displayed.
3. Click New. The Static Routing tab is displayed. (See Figure 108.)
4. In the IP Address Prefix and Netmask fields, type the destination subnet address and network mask. For a default route, enter “0.0.0.0” in each field.
5. In the Gateway field, type the IP address of the next-hop router through which traffic forwarded by the EX appliance can reach the destination subnet.
6. To specify the interface through which traffic that uses the route must be sent, do one of the following:
   - From the Interface drop-down list, select the physical Ethernet interface.
   - In the ve field, enter the number of the VE interface. If you enter a VE number, you also can specify the physical interface within the VE, by selecting an Ethernet interface from the Interface drop-down list.
7. To change the administrative distance of the route, edit the number in the Distance field. The distance can be a value from 1 to 255.
8. Click OK. The new static route appears in the list of static routes.

FIGURE 108 Static Routing Tab



OSPF Routing

The following sections describe how to configure the EX Secure WAN Manager as an OSPF router.

Configure OSPF Routing

To configure OSPF:

1. Enable OSPF.

   You also can change other general settings from the same configuration tab. (The general settings are listed in Table 15 on page 217.)

2. Configure OSPF networks and normal areas.

3. Configure stub areas.

4. Change interface settings, if required. Generally, the only interface settings you need to change are for authentication. (The interface settings are listed in Table 16 on page 221.)

5. If your network uses authentication based on areas instead of interfaces, configure authentication settings for the areas.

You do not need to assign EX appliance ethernet interfaces to areas. When you configure an OSPF network and area, the EX appliance interface that is in the network is automatically assigned to the network's area.

You can configure the following types of OSPF areas:

- Normal – Normal areas can exchange External Link State Advertisements (LSAs) with other areas.
- Stub – Stub areas cannot send or receive External LSAs. OSPF routers in a stub area must use a default route to the area's Area Border Router (ABR) or Autonomous System Boundary Router (ASBR) to send traffic out of the area.

Enable OSPF

To enable OSPF:

1. Select Config Mode > Network > Routing.
2. On the menu bar, select OSPF > Route > General. The General Settings tab is displayed.
3. Select Enable next to Status.
4. To change other general settings:
   a. To enable redistribution of OSPF routes into other route types. select the other route types:
      - Connect (directly connected routes)
      - Static
      - RIP
   b. To change the default metric assigned to redistributed routes, enter the metric value in the Default Metric field.
   c. To set the router ID, enter an IP address in the Router ID field.
5. Click Apply.

Table 15 lists the general OSPF parameters you can configure.

TABLE 15 Configurable OSPF Parameters – General

Parameter	Description	Supported Values
Status	State of the OSPF protocol.	One of the following: • Enable • Disable
Redistribute	Other route types to which OSPF is allowed to redistribute routes. A redistributed route learned by OSPF can be used as a directly connected (Connected), static, or RIP route, if redistributed to these route types.	Any combination of the following: • Connect • Static • RIP

TABLE 15 Configurable OSPF Parameters – General (Continued)

Parameter	Description	Supported Values
Default Metric	Numeric cost assigned to an OSPF route. When the IP route table has more than one route to the same destination, the EX appliance selects the route with the lowest cost. The metric is added to routes when they are redistributed. **Note:** There is no default for this value.	1 to 16777214 1 is the lowest cost and 16777214 is the highest cost.
Router ID	Value used by the EX appliance to identify itself when exchanging route information with other OSPF routers. The EX appliance has only one router ID. The default router ID is the highest-numbered IP address configured on any of the EX appliance ethernet interfaces.	A valid IP address. The address does not need to match an address configured on the EX appliance; however, the address must be unique within the routing domain. New or changed router IDs require a restart of the EX appliance OSPF process.

Configure OSPF Networks and Normal Areas

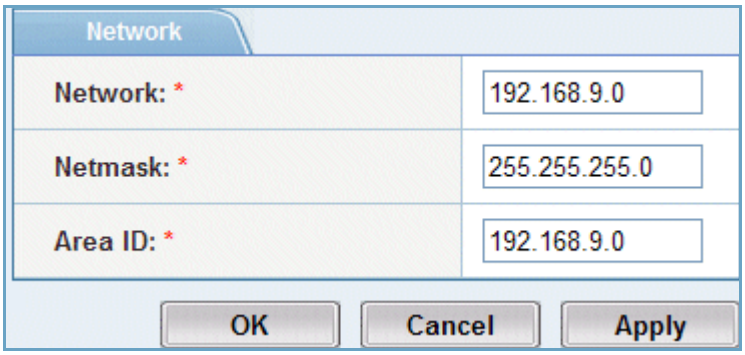
When you configure an OSPF network, the EX Secure WAN Manager automatically configures a normal area for the network. You do not need to configure the normal area separately.

To configure an OSPF network and normal area:

1. Select Config Mode > Network > Routing.
2. On the menu bar, select OSPF > Route > OSPF Network. The list of configured OSPF networks is displayed.
3. Click New. The Network tab is displayed. (See Figure 109.)
4. In the Network and Netmask fields, enter the interface address of the network.
5. In the Area ID field, enter an ID for the normal area. Area IDs must be in IP address format.

   If you intend to associate the area with a specific IP subnet, you can specify the subnet address as the Area ID.
6. Click OK. The new OSPF network appears in the list.

FIGURE 109 OSPF Network Tab

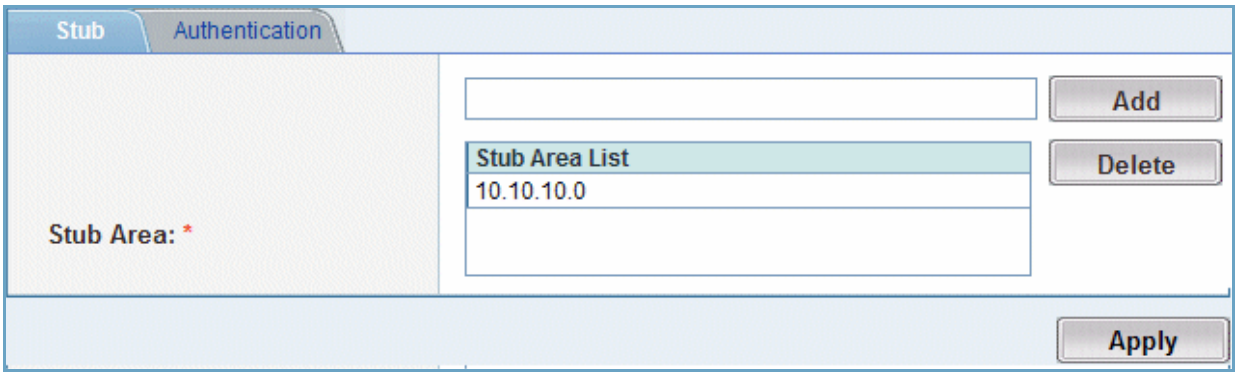


Configure Stub Areas

To configure a stub area:

1. Select Config Mode > Network > Routing.
2. On the menu bar, select OSPF > Route > Area. The Stub tab is displayed. (See Figure 110.)
3. Enter the stub area ID, in IP address format, in the entry field above the Stub Area list.
4. Click Add. The area appears in the Stub Area list.
5. Repeat step 3 and step 4 for each stub area.
6. Click Apply.
7. Go to "Change Interface Settings" on page 220.

FIGURE 110 Stub Tab



Change Interface Settings

To change OSPF settings on an individual EX Secure WAN Manager interface:

1. Select Config Mode > Network > Routing.
2. On the menu bar, select OSPF > Interface. A table listing the ethernet interfaces is displayed.
3. In the Name column, click on the interface you want to configure. The OSPF Interface tab is displayed. (See Figure 111.)
4. Edit the settings you want to change. (See Table 16 on page 221 below.)
5. Click OK.
6. Repeat step 3 through step 5 for each interface.

FIGURE 111 OSPF Interface Tab

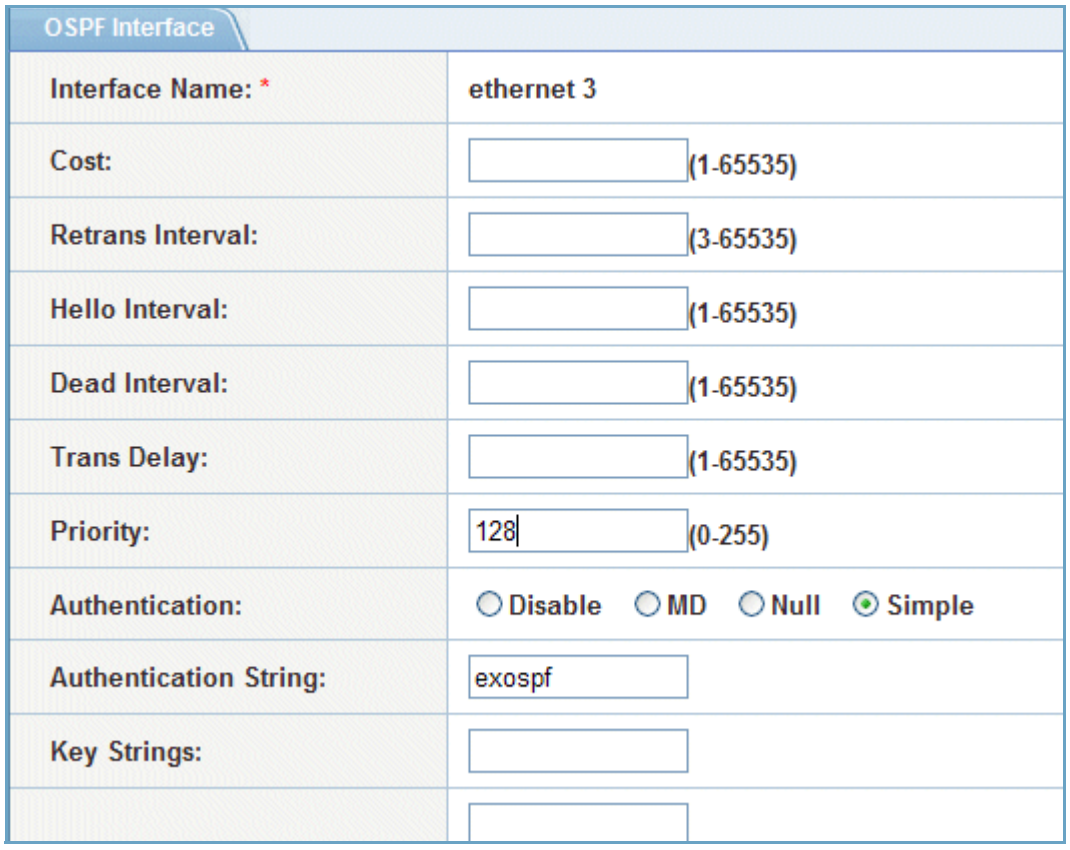


Table 16 lists the OSPF parameters used to configure individual interfaces.

TABLE 16 Configurable OSPF Parameters – Interface

Parameter	Description	Supported Values
Cost	Numeric cost for using the interface. This cost overrides the global default metric (either the system default or the value specified in the General settings).	1 to 65535 Default: Value is calculated by the interface bandwidth
Retrans Interval	Number of seconds between retransmissions of link-state advertisements (LSAs) to adjacent routers for this interface.	3 to 65535 seconds Default: 5 seconds
Hello Interval	Number of seconds between transmission of OSPF Hello packets on this interface.	1 to 65535 seconds Default: 10 seconds
Dead Interval	Number of seconds that neighbor OSPF routers will wait for a new OSPF Hello packet from the EX appliance before declaring this OSPF router (the EX Secure WAN Manager) to be down.	1 to 65535 seconds Default: 40 seconds
Trans Delay	Number of seconds it takes to transmit Link State Update packets (route updates) on this interface. This amount is added to the ages of LSAs sent in the updates. With the addition of the transit delay, when a neighbor OSPF router receives an Update, the ages of the LSAs are more accurate because the estimated travel time of the update is accounted for by the transit delay.	1 to 65535 seconds Default: 1 second
Priority	Eligibility of this OSPF router to be elected as the designated router (DR) or backup designated router (BDRs) for the routing domain. The OSPF router with the highest priority is elected as the DR and the router with the second highest priority is elected as the BDR. If more than one router has the highest priority, the router with the highest OSPF router ID is selected. Priority applies only to multi-access networks, not to point-to-point networks.	0 to 255 Default: 1 1 is the lowest priority and 255 is the highest priority. If you set the priority to 0, the EX Secure WAN Manager does not participate in DR and BDR election.
Authentication	Type of authentication used to validate OSPF route updates sent or received on this interface.	One of the following: • Disable: Authentication settings for the area are used instead of interface-specific authentication settings. • MD: Message Digest 5 (MD5) • Null: No authentication is used. This option is useful for overriding password or MD authentication. • Simple: Text password Default: Disable

TABLE 16 Configurable OSPF Parameters – Interface (Continued)

Parameter	Description	Supported Values
Authentication String	Password used by the interface to authenticate link-state messages exchanged with neighbor OSPF routers. The same authentication string value must be configured on the neighbor. Otherwise, the interface refuses (drops) the messages. This value applies only to simple authentication, not to MD authentication.	Any string of characters that can be entered from the keyboard, up to 8 characters long. The string cannot contain blanks.
Key Strings	Set of MD passwords used by the interface to authenticate link-state messages exchanged with neighbor OSPF routers. You can enter up to four key strings. Each neighbor must be configured with at least one of the strings. Otherwise, the interface refuses (drops) the messages. This value applies only to MD authentication, not to simple authentication.	Alphanumeric string up to 16 bytes long. The string cannot contain blanks.

Configure Authentication Type for an Area

Generally, OSPF authentication is configured on an interface basis rather than an area basis. However, for backward compatibility, the EX appliance does allow you to specify the authentication type for an area.

If authentication for an OSPF interface is set to Disable, the authentication type for the area will be used instead. However, if authentication for an OSPF interface is set to any other value but Disable, the authentication setting for the interface is used instead of the setting for the area.

You can set the authentication type for an area to one of the following:

- TEXT – The area uses simple passwords to authenticate link-state messages.
- MD5 – The area uses hash values derived from MD5 keys to authenticate link-state messages.

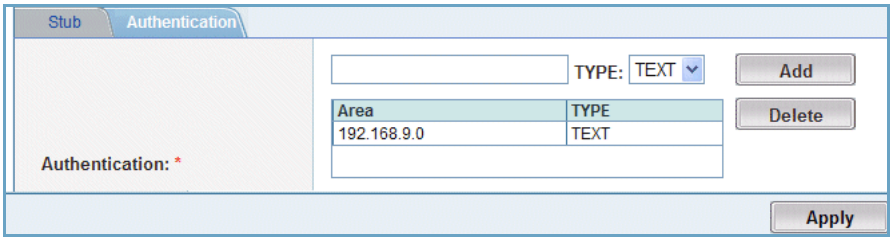
Each area can be set to use only one of these authentication types.

To configure authentication of link-state messages:

1. Select Config Mode > Network > Routing.
2. On the menu bar, select OSPF > Route > Area. The Stub tab is displayed.
3. Click on Authentication to display the tab. (See Figure 112.)
4. In the entry field above the Authentication list, type the area ID.

5. From the Type pull-down list, select the authentication type to use for the area:
   - TEXT
   - MD5
6. Click Add.
7. Repeat step 4 through step 6 for each area.
8. Click Apply.

FIGURE 112 OSPF Authentication Tab



Make an Interface Passive

By default, all OSPF interfaces on the EX Secure WAN Manager send OSPF link-state messages to neighbor OSPF routers. To prevent an interface from sending or accepting link-state messages, you can make the interface passive.

Note: Passive OSPF interfaces do not accept link-state messages from neighbors.

To make an OSPF interface passive:

1. Select Config Mode > Network > Routing.
2. On the menu bar, select OSPF > Route > Passive Interface. The Passive Interface tab is displayed.
3. In the Available Interface list, select the interface(s) you want to make passive.
4. Click << to move the selected interface(s) to the Passive Interfaces list.
5. Click Apply.

Restart OSPF

If you need to restart the OSPF protocol on the EX Secure WAN Manager, use the following procedure.

1. Select Config Mode > Network > Routing.
2. On the menu bar, select OSPF > Restart.

RIP Routing

The following sections describe how to configure the EX Secure WAN Manager as a RIP router.

Configure RIP Routing

To configure RIP:

1. Enable RIP.

   You also can enable route redistribution from the same configuration tab. (The general settings are listed in Table 15 on page 217.)
2. Configure the RIP networks the EX appliance will advertise and listen for updates on the router table.
3. Configure a key chain for authenticating route updates.
4. Change interface settings, if required. Generally, the only interface settings you need to change are for authentication. (The interface settings are listed in Table 16 on page 221.)

Enable RIP

To enable RIP:

1. Select Config Mode > Network > Routing.
2. On the menu bar, select RIP > Route > General. The General Settings tab is displayed. (See Figure 113.)
3. Select Enable next to Status.

4. To enable redistribution of RIP routes into other route types. select the other route types:
   - Connect (directly connected routes)
   - Static
   - OSPF
5. Click Apply.

FIGURE 113 RIP General Settings Tab

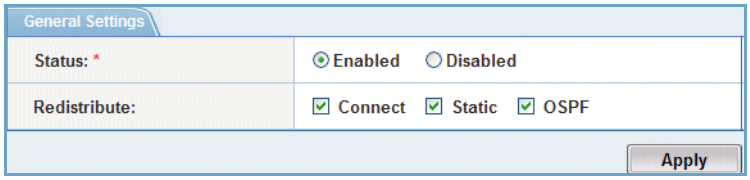


Table 17 lists the general RIP parameters you can configure.

TABLE 17 Configurable RIP Parameters – General

Parameter	Description	Supported Values
Status	State of the RIP protocol.	One of the following: • Enable • Disable
Redistribute	Other route types to which RIP is allowed to redistribute routes. A redistributed route learned by RIP can be used as a directly connected (Connected), static, or OSPF route, if redistributed to these route types.	Any combination of the following: • Connect • Static • OSPF

Configure RIP Networks

You must specify the networks that the EX Secure WAN Manager will advertise and listen for route updates on.

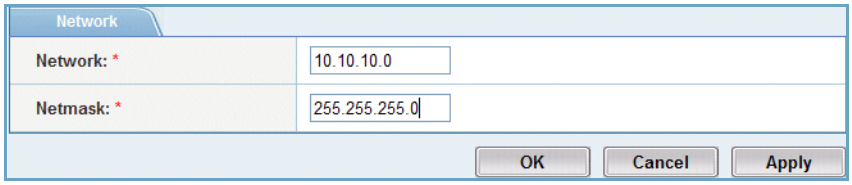
To configure an RIP network:

1. Select Config Mode > Network > Routing.
2. On the menu bar, select RIP > Route > Network. The list of configured RIP networks is displayed.
3. Click New. The RIP Network tab is displayed. (See Figure 114.)

4. In the Network and Netmask fields, enter the interface address of the network.

5. Click OK. The new RIP network appears in the list.

FIGURE 114 RIP Network Tab



Configure a Key Chain

RIP uses keys to authenticate route updates. You can configure multiple keys in a key chain.

To configure a key chain:

1. Select Config Mode > Network > Routing.

2. On the menu bar, select RIP > Key Chain. A table listing the configured key chains is displayed.

3. Enter the name of a new key chain in the entry field above the table.

   Key chain names can be up to 16 characters long.

4. Click New. The new key chain appears in the list.

5. Click on the key chain name. The Key Chain tab is displayed. (See Figure 115.)

6. In the Key ID field, enter a number to identify the key. The key ID can be a number from 1 to 255.

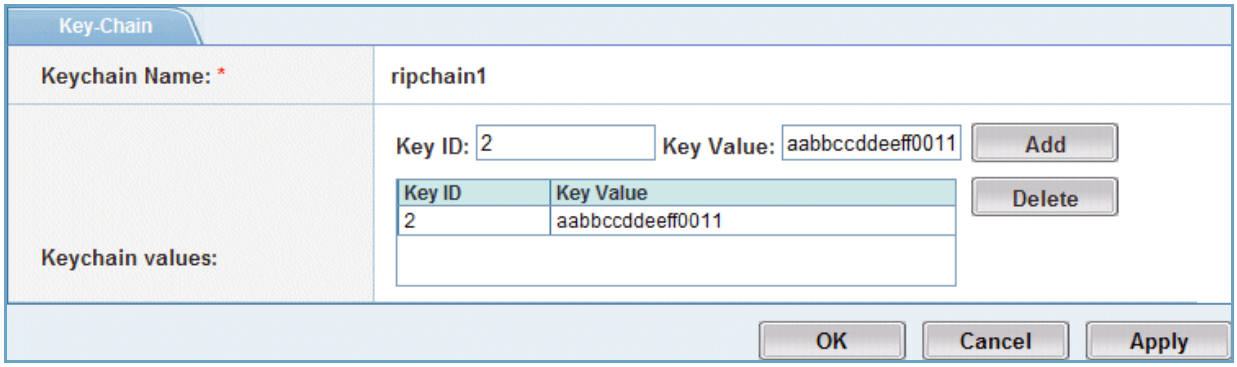
7. In the Key Value field, enter the key string. The key string can be 16 characters long.

8. Click Add. The new key appears in the list.

9. Repeat step 7 and step 8 for each key.

10. Click Apply.

FIGURE 115 RIP Key Chain Tab



Configure Interface Settings

To configure RIP interface settings:

1. Select Config Mode > Network > Routing.
2. On the menu bar, select RIP > Interface. A table listing the ethernet interfaces is displayed.
3. In the Name column, click on the interface you want to configure. The RIP Interface tab is displayed. (See Figure 116.)
4. Edit the settings you want to change. (See Table 18 on page 228 below.)
5. Click OK.
6. Repeat step 3 through step 5 for each interface.

FIGURE 116 RIP Interface Tab

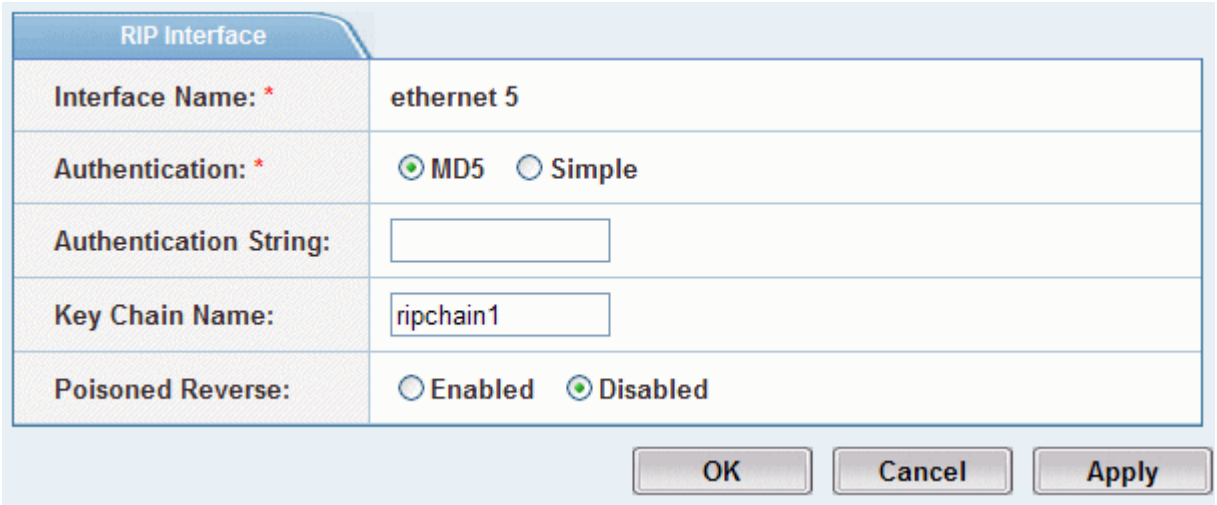


Table 18 lists the RIP parameters used to configure individual interfaces.

TABLE 18 Configurable RIP Parameters – Interface

Parameter	Description	Supported Values
Authentication	Type of authentication used to validate RIP route updates sent or received on this interface.	One of the following: • MD: Message Digest 5 (MD5) • Simple: Text password Default: Simple
Authentication String	Password used by the interface to authenticate route updates exchanged with other RIP routers. The same authentication string value must be configured on the other routers. Otherwise, the interface refuses (drops) the updates. This value applies only to simple authentication, not to MD5 authentication.	Any string of characters that can be entered from the keyboard, up to 8 characters long. The string cannot contain blanks.
Keychain Name	Name of a set of authentication keys.	Name of any key chain configured on the switch.
Poison Reverse	Specifies the method used to prevent routing loops. Each EX appliance interface can be configured to use one of the following methods: • Split horizon • Poison reverse By default, split horizon is enabled and poison reverse is disabled. If you enable poison reverse, split horizon is automatically disabled. Likewise, if you disable poison reverse again, split horizon is automatically re-enabled.	One of the following: • Enabled • Disabled

Make an Interface Passive

By default, all RIP interfaces on the EX Secure WAN Manager send and accept RIP route updates. To prevent an interface from sending route updates, you can make the interface passive.

Note: Passive RIP interfaces still accept route updates from other RIP routers.

To make an RIP interface passive:

1. Select Config Mode > Network > Routing.
2. On the menu bar, select RIP > Route > Passive Interface. The Passive Interface tab is displayed.
3. In the Available Interface list, select the interface(s) you want to make passive.
4. Click << to move the selected interface(s) to the Passive Interfaces list.
5. Click Apply.

Configure Reply Interface Selection for Locally Received Requests

By default, the EX Secure WAN Manager may send the response to a locally received request out a different interface than the one that received the request. This is because the EX appliance performs a route lookup on locally sent packets to determine the outgoing interface.

A locally received packet is a packet whose destination IP address is the address of the EX appliance itself. For example, HTTP, HTTPS, SSH, TELNET, SNMP, and DNS requests addressed to the EX appliance are locally received requests.

To specify how the EX appliance selects the interface for replies to locally received requests:

1. Select Config Mode > Network > Routing > Settings.
2. Select the option:
   - Default – Responses to a locally received packet may be sent out a different interface than the one the packet is received on by route.
   - Prefer reply to the same interface as the request (if route exists) – If a route to the reply destination exists and the next hop can be reached through the interface that received the request, the route is used. Otherwise, the same interface is used.

- Force reply to the same interface as the request – Forces the reply to a locally received request to be sent on the same interface that received the request.

3. Click Apply.

DNS

The EX Secure WAN Manager can be a DNS client, server, and/or proxy. You also can specify the EX Secure WAN Manager hostname and default domain name (DNS suffix).

DNS Client

The EX appliance can be used as a DNS client to resolve domain names into IP addresses or vice versa.

DNS Server

The EX appliance can also be a DNS server providing resolution for specific DNS zones or local DNS functionality. This is useful for inbound LLB as well as resolution of internal DNS requests for outbound traffic.

DNS Proxy

The EX appliance can act as a DNS proxy by accepting DNS requests from clients and proxying them to an external DNS server. This is useful for features such as inbound LLB, where the EX appliance requires DNS requests to pass through the EX appliance. In this case, the EX appliance becomes a virtual DNS server, where DNS requests from the Internet will be destined to the EX appliance and will be proxied to the real DNS server.

Configure DNS Servers

The following procedure configures the EX appliance as a DNS client to resolve IP addresses into host names.

1. Select Config Mode > Network > DNS.

2. On the System DNS Setting tab, in the Hostname field, enter a DNS name for the EX appliance.

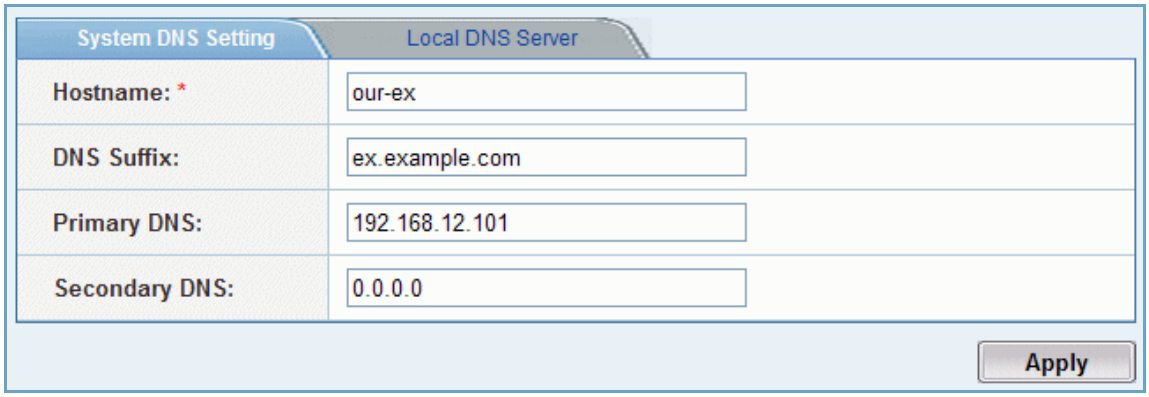
3. In the DNS Suffix field, enter the domain name to which the host (EX Secure WAN Manager) belongs.

4. In the Primary DNS field, enter the IP address of the external DNS server the EX appliance should use for resolving DNS queries.

5. In the Secondary DNS field, enter the IP address of an external backup DNS server the EX appliance should use if the primary DNS server is unavailable.

6. Click Apply.

FIGURE 117 Config Mode > Network > DNS



Enable DNS Server and Proxy Settings

To use the EX appliance as a DNS server or proxy, use the following procedure.

1. Select Config Mode > Network > DNS, if not already selected.

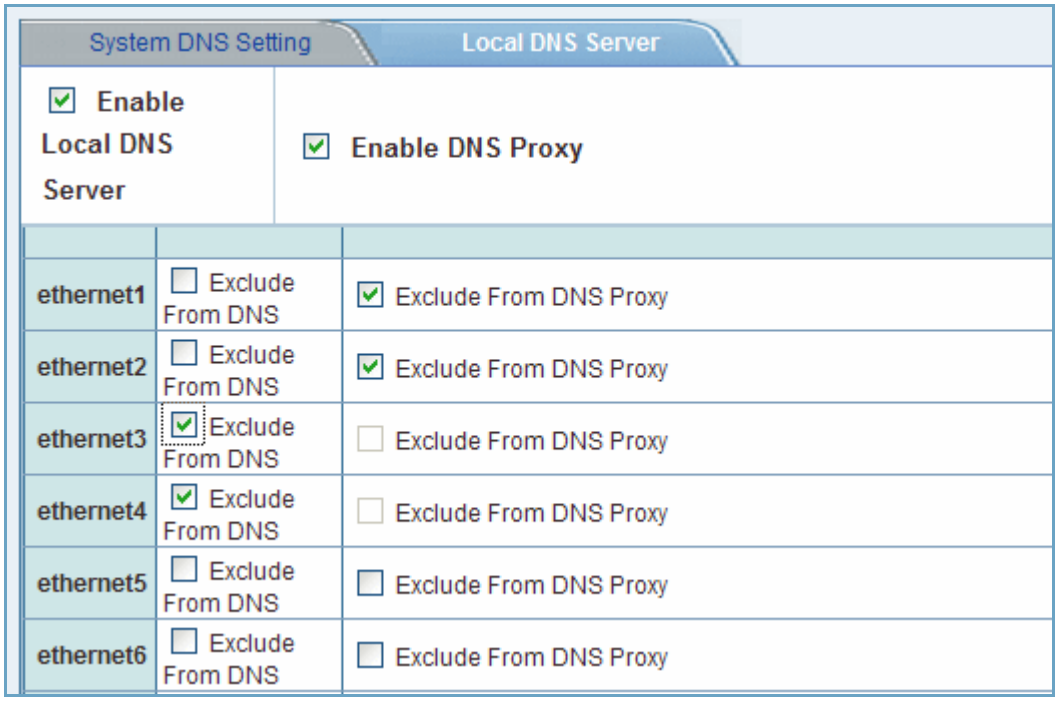
2. Click the Local DNS Server tab.

3. To use the EX appliance as a DNS server, click the Enable Local DNS Server checkbox.

4. To use the EX appliance as a DNS proxy, click the Enable DNS Proxy checkbox. (This checkbox is available only after you select the Enable Local DNS Server checkbox.)

5. Listening for DNS server and proxy traffic is enabled on all Ethernet data interfaces by default.
   - To disable listening for DNS server traffic on an interface, click the Exclude From DNS checkbox next to the interface name.
   - To disable listening for DNS proxy traffic on an interface, click the Exclude From DNS Proxy checkbox next to the interface name.
6. Click Apply.

FIGURE 118 Config Mode > Network > DNS - Local DNS Server



Configure Local Domains

1. Select Config Mode > Network > DNS, if not already selected.
2. On the menu bar, select Local Domains.
3. Click New.
4. On the Domain tab, enter the domain name in the Domain field.
5. To change the domain's status, click Enable or Disable.

6. To specify hosts in the domain:
   a. Click on the Hosts tab.
   b. Enter the host name in the Hostname field.

Note: To configure an Address (A) record for the base domain name, leave the Hostname field blank.

   c. Enter the IP address in the IP Address field.
   d. Enter the time-to-live (TTL) in the TTL field.
   e. Click Add. Repeat for each host.

7. To add a Canonical Name (CNAME) record:
   a. In the CNAME field, enter the domain name for which you are configuring the CNAME record.
   b. In the To field, enter the alias to insert into DNS replies.
   c. To configure aging for the CNAME (alias) sent in DNS replies, use the TTL field. You can specify 0-2592000 seconds. The default is 600 seconds. To disable aging, specify 0 seconds.

8. To add a Mail Exchange (MX) record:
   a. Click on the MX tab.
   b. Enter the domain name in the Domain field.
   c. If you are configuring more than one MX record, enter the priority in the Priority field. The MX record with the lowest priority value has the highest priority and is tried first. The priority can be 0-65535. There is no default.
   d. To configure aging, in the TTL field, specify the maximum number of seconds an MX reply remains valid. You can specify 0-2592000 seconds. The default is 600 seconds. To disable aging, specify 0 seconds.
   e. Click Apply.
   f. Repeat for up to 2 more MX records.

9. Click OK.

FIGURE 119 Config Mode > Network > DNS > Local Domains

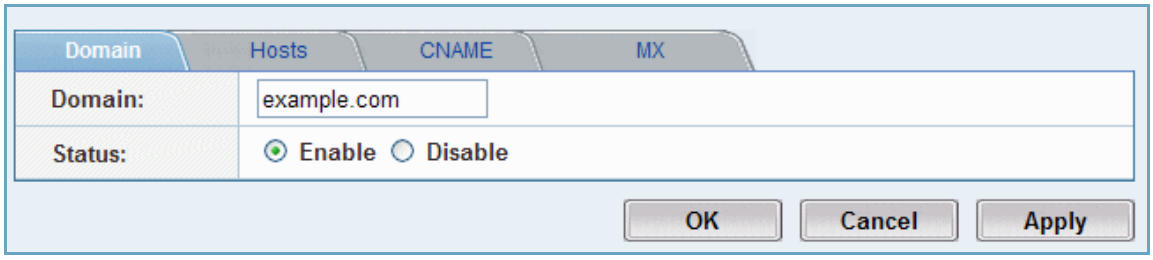


FIGURE 120 Config Mode > Network > DNS > Local Domains - Hosts

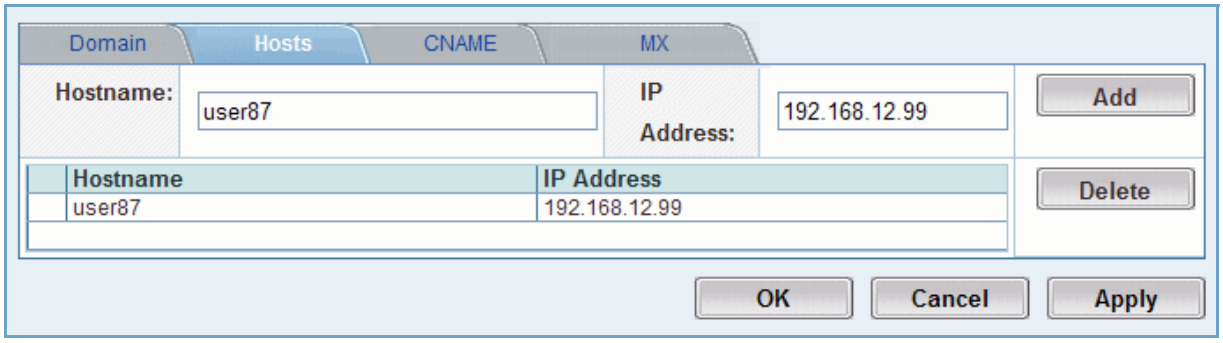
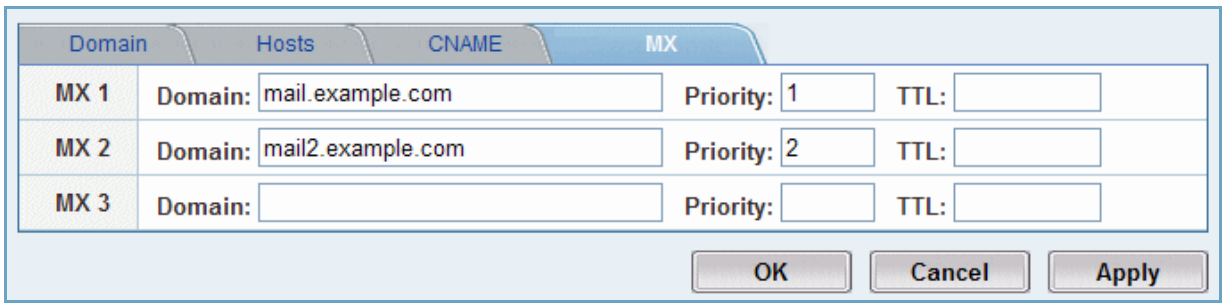


FIGURE 121 Config Mode > Network > DNS > Local Domains - CNAME

FIGURE 122 Config Mode > Network > DNS > Local Domains - MX

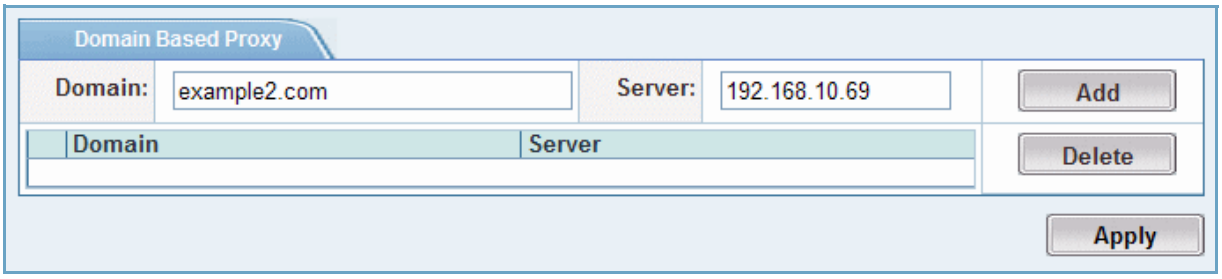


Configure Domain Based Proxies

Domain based proxies allow you to configure a different DNS server for each DNS zone. This configuration only applies when the DNS proxy is enabled. To proxy all DNS requests, enter a dot (**.**) in the domain field.

1. Select Config Mode > Network > DNS, if not already selected.
2. On the menu bar, select Domain Based Proxy.
3. In the Domain field, enter the domain for which the EX appliance will act as a DNS proxy.
4. In the Server field, enter the IP address of the DNS server.
5. Click Add.
6. Repeat for each DNS server for which to act as a DNS proxy.
7. Click Apply.

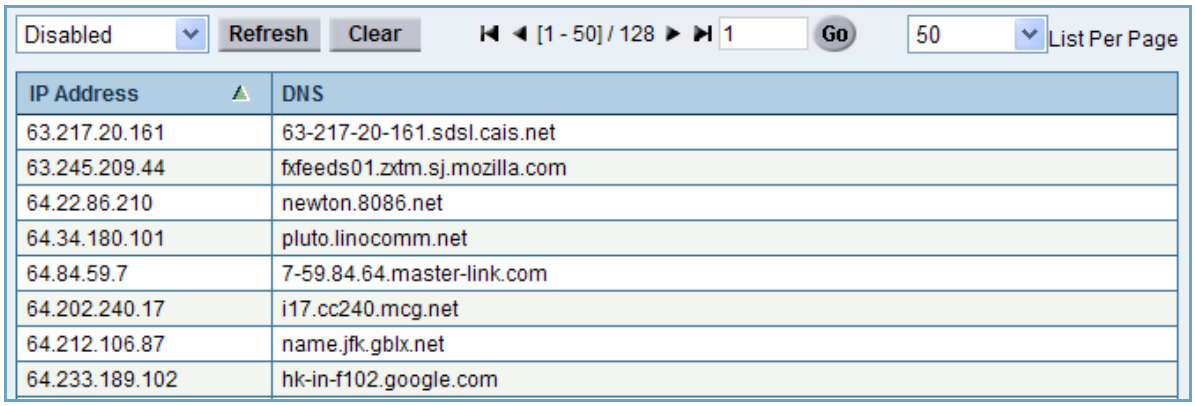
FIGURE 123 Config Mode > Network > DNS > Domain Based Proxy



Display DNS Cache Entries

To display the DNS cache, select Monitor Mode > Network > DNS Cache. The DNS name and corresponding IP address are listed for each entry.

FIGURE 124 Monitor Mode > Network > DNS Cache



IP Address	DNS
63.217.20.161	63-217-20-161.sdsl.cais.net
63.245.209.44	fxfeeds01.zxtm.sj.mozilla.com
64.22.86.210	newton.8086.net
64.34.180.101	pluto.linocomm.net
64.84.59.7	7-59.84.64.master-link.com
64.202.240.17	i17.cc240.mcg.net
64.212.106.87	name.jfk.gblx.net
64.233.189.102	hk-in-f102.google.com

System Settings

This chapter describes the system management options for the EX Secure WAN Manager.

System Actions

You can select menu bar options to perform the following system tasks:

- Shutdown – Powers down the EX appliance.
- Reboot – Restarts the EX appliance.
- Save – Syncs the configuration file (startup-config) with the running-config (running configuration), so that the startup-config includes all the current changes made to the running-config.
- Unsave – Reverts back to the previous version of the startup-config, before the latest changes were saved.
- Logout – Ends your admin session.

To select one of these options:

1. Select Config Mode > System > Settings.
2. On the menu bar, select Action. A pull-down menu containing the following actions appear:
   - Shutdown
   - Reboot
   - Save
   - Unsave
   - Logout
3. Select the action you want to perform.

General Settings

Web Access

To view or configure settings for Web management access to the EX Secure WAN Manager:

1. Select Config Mode > System > Settings.
2. On the menu bar, select Web, if not already selected. The Web tab appears.
3. To change the language used in the GUI, select one of the following from the pull-down list:
   - English
   - Simple Chinese
   - Japanese
   - Traditional Chinese
4. To change the number of minutes Web management sessions can remain idle before timing out, enter the number of minutes in the Web Timeout field.

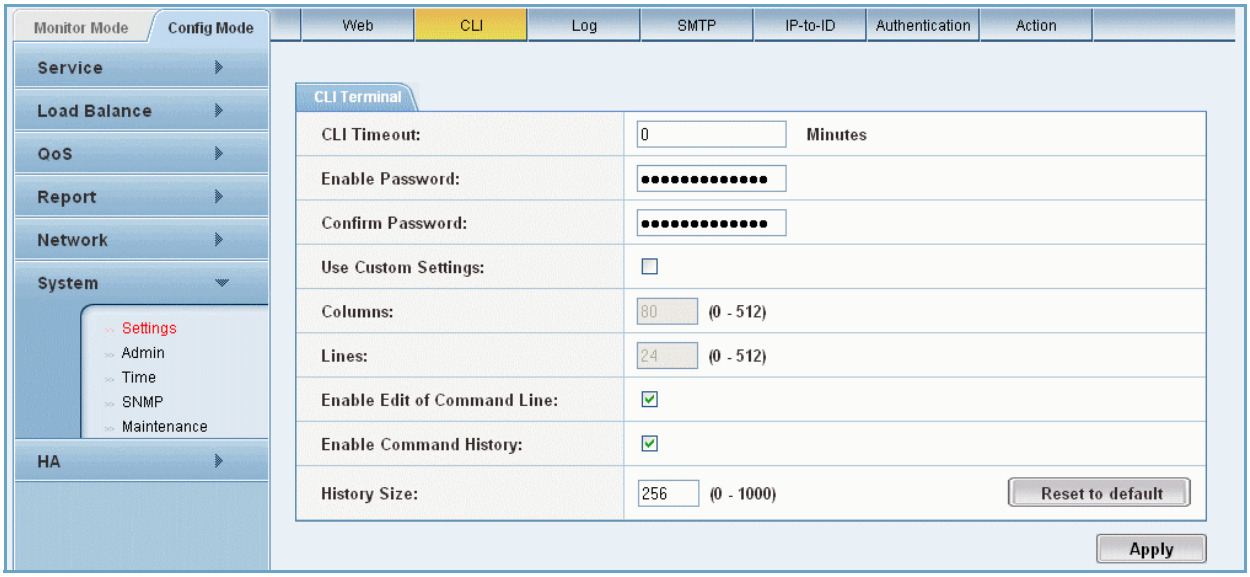
   When a Web management session times out, the EX appliance automatically ends the session and closes the Web page.

   You can specify from 0 to 60 minutes. To disable timeout, specify 0.
5. To change HTTP port settings:
   - To disable HTTP access, click to clear the checkbox next to HTTP.
   - To change the TCP port number on which the EX appliance accepts HTTP management connections, edit the number in the field.
6. To change HTTPS port settings:
   - To disable HTTPS access, click to clear the checkbox next to HTTPS.
   - To change the TCP port number on which the EX appliance accepts HTTPS management connections, edit the number in the field.
7. To redirect HTTP connection attempts to HTTPS, select the checkbox.
8. Click Apply.

CLI Terminal

To view or configure settings for CLI access to the EX Secure WAN Manager:

FIGURE 125 Config Mode > System > Settings - CLI



You can modify settings for CLI access or restore all settings to default values. To restore all CLI access settings to the default values, click the Reset To Default button.

Caution: The Reset To Default option also resets the enable password to its default value (*empty - no password*).

To view or configure settings for CLI management access to the EX appliance:

1. Select Config Mode > System > Settings.
2. On the menu bar, select CLI. The CLI terminal tab appears.
3. To set the number of minutes CLI management sessions can remain idle before timing out, enter the number of minutes in the CLI Timeout field.

   When a CLI management session times out, the EX appliance automatically ends the session. You can specify from 0 to 60 minutes. To disable timeout, specify 0.
4. To change the enable password, type the new password in the Enable Password and Confirm Password fields.

5. To set the management window display size, select the Use Custom Setting checkbox and edit the values in the Columns and Lines fields.
6. To disable or re-enable command-line editing, deselect or reselect the Enable Edit of Command Line checkbox.
7. To disable or re-enable the command history, deselect or reselect the Enable Command History checkbox.
8. To change the maximum number of commands that can be stored in the history, edit the value in the History Size field.
9. Click Apply.

Logging

To view or change system log settings:

1. Select Config Mode > System > Settings.
2. On the menu bar, select Log. The Log tab is displayed.
3. Change settings as needed. (For descriptions of the settings, see Table 19 on page 241.)
4. Click Apply.

Table 19 on page 241 lists the system log settings you can configure.

TABLE 19 Configurable Log Settings

Parameter	Description	Supported Values
Disposition	Output options for each message level. For each message level, you can select which of the following output options to enable: • Console – Messages are displayed in Console sessions. • Buffered – Messages are stored in the system log buffer. The GUI system log lists the messages in this buffer. (See "Display the System Log" on page 264.) • Email – Messages are sent to the email addresses in the Email To list. (See below.) • SNMP – SNMP traps are generated and sent to the SNMP receivers. (To specify the receivers, see "Configure SNMP Settings" on page 251.) • Syslog – Messages are sent to the external log servers specified in the Log Server fields. (See below.) • Monitor – Messages are displayed in Telnet and SSH sessions.	The following message levels can be individually selected for each output option: • Emergency • Alert • Critical • Error • Warning • Notification • Information • Debug Only Emergency, Alert, and Critical can be selected for SNMP. Only Emergency, Alert, Critical, and Notification can be selected for Email.
Facility	Standard Syslog facility to use.	Standard Syslog facilities listed in RFC 3164.
Log Buffer Entries	Maximum number of log entries the log buffer can store.	10000 to 50000 entries Default: 30000
Log Server	IP addresses or fully-qualified domain names of external log servers. Only the message levels for which Syslog is selected in the Disposition list are sent to log servers.	Any valid IP address or fully-qualified domain name. Default: None configured
Log Server Port	Protocol port to which log messages sent to external log servers are addressed.	Any valid protocol port number Default: 514

Email (SMTP)

The EX Secure WAN Manager has certain features that require access to a Simple Mail Transfer Protocol (SMTP) server for sending email. For example, you can configure the EX appliance to email QoS reports and alerts to you and to other admins.

To view or change Simple Mail Transfer Protocol (SMTP) settings:

1. Select Config Mode > System > Settings.
2. On the menu bar, select SMTP. The SMTP tab is displayed.
3. Enter or change settings as needed. (For descriptions of the settings, see Table 20.)
4. Click Apply.

Table 20 lists the SMTP settings you can configure.

TABLE 20 Configurable SMTP Settings

Parameter	Description	Supported Values
Authenticated SMTP	Indicates whether the SMTP server requires authentication (username and password). Selecting this checkbox activates the User Name and Password fields.	Enabled (selected) or disabled Default: disabled
User Name	User name required for access to the SMTP server.	Valid username Default: not set
Password	Password required for access to the SMTP server.	Valid password Default: not set
Email From	Email address the EX appliance will use as the From address in emails sent by the device.	Valid email address Default: <not set
Email To	Email addresses to which to send log messages. Only the message levels for which Email is selected in the Disposition list are sent to log servers.	List of up to 10 email addresses. Use commas to separate the addresses. Each email address can be a maximum of 31 characters long.
SMTP Server	IP address or fully-qualified domain name of an email server using Simple Message Transfer Protocol.	Any valid IP address or fully-qualified domain name. Default: None configured
SMTP Server Port	Protocol port to which email messages sent to the SMTP server are addressed. Click to the Test button to help test whether or not the currently configured SMTP settings works.	Any valid protocol port number Default: 25

Identity-Management Integration

Some displays have a column that lists user identity. The EX Secure WAN Manager can obtain the identity information dynamically or statically:

- Dynamically – You can integrate the EX appliance with an A10 Networks IDsentrie; so you can configure the EX appliance to obtain iden-

tity information from the IDsentrie. No special configuration is required on the IDsentrie. All integration is configured on the EX appliance.

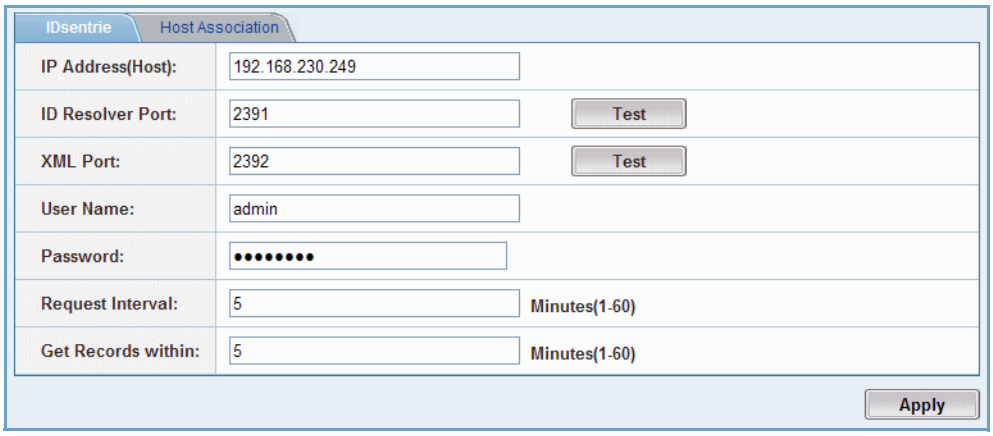
- Statically – You can add IP address-to-identity mappings to a table on the EX appliance.

Dynamic Identity-Management Integration

To integrate the EX Secure WAN Manager with an IDsentrie:

1. Select Config Mode > System > Settings.
2. On the menu bar, select IP-to-ID. The IDsentrie tab is displayed.

FIGURE 126 Config > System > Settings - IP-to-ID > IDsentrie



3. In the IP Address field, enter the IP address of the IDsentrie.
4. In the ID Resolver Port field, enter the protocol port number to use for connections with the IDsentrie.

   The port number you specify must match the port number configured on the IDsentrie.

5. In the XML Port field, enter the protocol port number to use for connections with the XML agent on the IDsentrie.
6. To specify the admin user name and password to use for authentication, enter them in the User Name and Password fields.

   The same admin user name and password must be configured on the IDsentrie.

7. The Request Interval parameter specifies the interval in minutes at which the IP-to-ID pairs are refreshed, from 1 to 60 minutes.

8. The Get Records within parameter specifies how far back to retrieve records. For example, if you use 5 minutes (the default), records that were active within the last 5 minutes are retrieved. This parameter ensures that records that were active after the previous request interval but that are no longer active, are retrieved. You can specify 1 to 60 minutes.

Note: To ensure that all records are retrieved, set this value to the same value as the "Process account activity logs every" parameter on the IDsentrie or IDaccess. (The "Process account activity logs every" parameter is set on the UIM General tab, accessed by selecting UIM > General.)

9. Click Apply.

Display Dynamic Identity Information

To display the IP address-to-username mappings learned from an IDsentrie, select Monitor Mode > System > IP-to-ID Cache.

The hostnames also appear in internal talker reports. The MAC addresses also appear in the drill-down reports for individual IP addresses in internal talker reports.

Host Association Identity Mappings

To statically map IP addresses to user identities:

1. Select Config Mode > System > Settings.

2. On the menu bar, select IP-to-ID. The IDsentrie tab is displayed.

3. Click Host Association to display the Host Association tab.

4. In the IP field, type the user's IP address.

5. In the ID field, type the user name.

6. Click Add. The identity is added to the Static IP-to-ID list.

7. Repeat step 4 through step 6 for each identity.

8. Click Apply.

Authentication

The EX Secure WAN Manager can use the following types of authentication to authenticate admin accounts during login. (These types can be viewed by going to Config Mode > System > Settings > Authentication and selecting the Type tab.)

- Local – The EX appliance checks its running configuration for the username and password provided during an admin login attempt.
- Local/RADIUS – The EX appliance checks an external RADIUS server for the username and password. The EX appliance checks its running configuration (i.e. Local). If this user cannot be found in the running configuration, the EX appliance will check the RADIUS server.
- Local/LDAP – The EX appliance checks an external LDAP server for the username and password. The EX appliance checks its running configuration (i.e. Local). If this user cannot be found in the running configuration, the EX appliance will check the LDAP server.

Local is the simplest way to configure authentication, because all configuration takes place on the EX appliance. However, Local/RADIUS or Local/LDAP have the advantage of providing centralized authentication, so these approaches may be preferred if your network already uses a RADIUS or LDAP server.

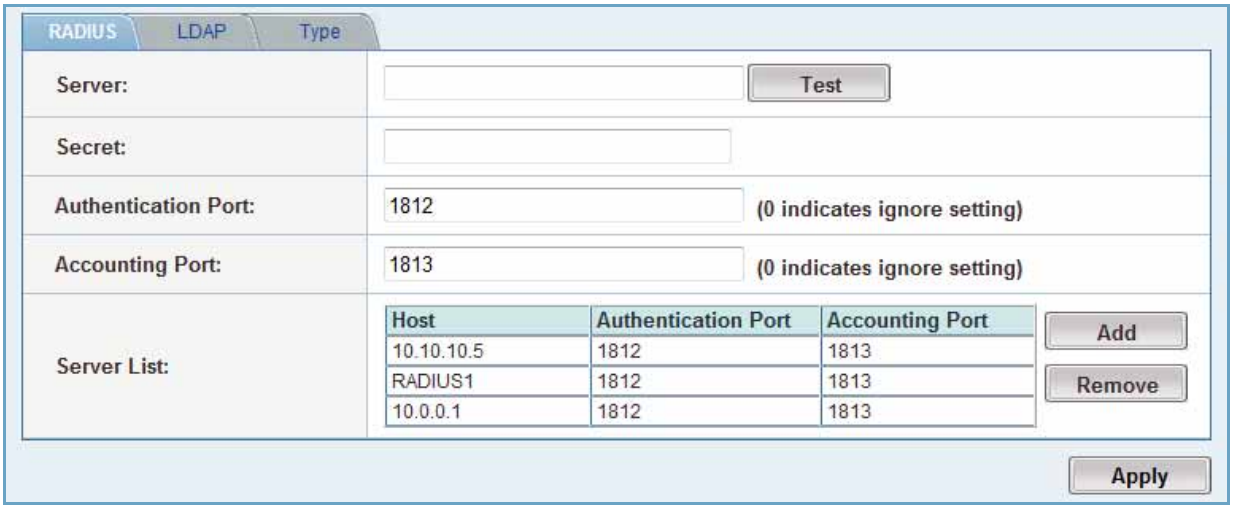
RADIUS or LDAP authentication types must be used in conjunction with Local – they cannot be used exclusively. This is true because the EX appliance always checks its running configuration before checking an external authentication server.

The *admin* username is in the configuration by default. Even if you do not add any local admins to the EX appliance configuration, you can still access the device by logging in with the *admin* account.

To configure admin authentication:

1. Select Config Mode > System > Settings.
2. On the menu bar, select Authentication. The RADIUS tab is displayed, as shown in Figure 127 on page 246:

FIGURE 127 Config > System > Settings > Authentication



3. If you plan to use Local authentication only, go to step 6. Otherwise, go to one of the following steps:
   - To configure RADIUS settings, go to step 4.
   - To configure LDAP settings, go to step 5.

4. Configure RADIUS settings:
   a. In the Server field, enter the IP address or hostname of the RADIUS server.
   b. In the Secret field, enter the shared secret configured on the RADIUS server. The shared secret is used to validate RADIUS requests and replies. The value entered here must match what is configured on the RADIUS server.
   c. If the server uses non-standard protocol port numbers, edit the numbers in the Authentication Port and Accounting Port fields.
   d. Click the Add button to add the RADIUS server to the Server List.
   e. Repeat this process to add more than one RADIUS server. The first Radius server on the Server List will be the primary, and the following one will be the secondary. If the primary does not work, the EX appliance will try to authenticate using the other servers in the sequence that they appear on the Server List.

Note: The "A10-Admin-Privilege" option determines administrative privileges, allowing two acceptable values: (1) Read only and (2) Read & Write. The EX appliance also recognizes the RADIUS protocol's "Service-Type" privilege definitions for the following values:

- **1 – Login** (the user should be connected to a host)
- **6 – Administrative** (allows privileged commands)
- **7 – NAS Prompt** (allows non-privileged commands)

If both the "A10-Admin-Privilege" and RADIUS "Service Type" administrative privileges are configured, then the priority is given to the "A10-Admin-Privilege".

f. Click Apply to submit your changes.

g. Go to step 6.

5. Configure LDAP settings:

   a. Click the LDAP tab to display it.

   b. In the Server field, enter the IP address or hostname of the LDAP server.

   c. In the Port field, enter the protocol port number on which the LDAP server listens for authentication requests.

   d. In the Common Name Identifier field, enter the identifier used by the LDAP server to identify the individual entered in the LDAP server.

   e. In the Distinguished Name field, enter the distinguished name (DN). For example:

   ```
   DC=My Networks,DC=com
   ```

   f. Click Apply.

   g. Go to step 6.

6. Specify the authentication type by clicking the Type tab.

7. From the drop-down menu, select one of the following:

   - Local
   - Local/RADIUS
   - Local/LDAP

8. Click Apply to submit your changes.

Admin Accounts

You can fine-tune management access to the EX Secure WAN Manager by configuring the following settings for each admin account:

- Privilege – Indicates whether the admin can make configuration changes to the EX appliance. The following privilege levels are supported:
  - Root – The admin has Read/Write privileges and can never be deleted. The Root privilege level is reserved for user *admin*, which is included in the EX appliance configuration by default. The admin account is the only one that can create or change settings for other admin accounts.
  - Read/Write – The admin can make configuration changes, including changes to the admin's own account.
  - Read Only – The admin can view monitoring and configuration information but cannot make configuration changes. The admin cannot modify any admin accounts, including the admin's own account.
- Trusted Host – IP address and network mask of the admin's management station. The admin is allowed to log on to the EX appliance only if the login request is from the trusted host.

You also can create new admin accounts, and disable or delete existing accounts.

Note: To configure settings for admin accounts other than the one you are logged in with, you must be logged in as *admin*, which has root privileges.

Display Admin Accounts

1. Select Config Mode > System > Admin.
2. On the menu bar, select Administrators, if not already selected. The list of EX appliance administrators is displayed.
3. To display additional configuration information for the admin account, click the admin name. The Admin tab is displayed.

Configure an Admin Account

To configure an admin account on the EX Secure WAN Manager:

1. Select Config Mode > System > Admin.
2. On the menu bar, select Administrator, if not already selected. The list of EX appliance administrators is displayed.
3. To create a new admin account, click New. Otherwise, to modify an existing account, click the admin name. The Admin tab is displayed.
4. In the Administrator Name field, enter the admin name.
5. In the Password and Confirm Password fields, type the admin's password.
6. To restrict the admin's access based on the IP address of the admin's management station, enter the management station's IP address and network mask in the Trusted Host IP Address and Netmask for Trusted Host fields.

   Address and network mask value 0.0.0.0 allows access from any address.
7. Select one of the following privilege levels:
   - Read Only
   - Read/Write
8. Select the state of the admin account:
   - Enabled
   - Disabled

Note: A disabled admin account is retained in the EX appliance configuration but cannot be used to log on.

9. Click OK. The admin appears in the list.

Configure the Lockout Policy

The lockout policy prevents access by an admin account if the admin has entered the incorrect password too many times in a row.

To configure the lockout policy, use the following procedure.

1. Select Config Mode > System > Admin.
2. On the menu bar, select Lockout Policy. The Lockout Policy tab is displayed.
3. To enable lockout, select the Enable Administrator Lockout Feature checkbox.
4. To change lockout settings:
   a. In the Login Attempts field, enter the maximum number of times the admin is allowed to enter an incorrect password before the EX appliance locks the admin out.
   b. In the Lockout time field, enter the number of minutes a locked out admin remains locked out.
   c. In the Reset Lockout field, enter the number of minutes the EX appliance retains the record of an admin lockout.
5. Click Apply.

Configure Time Settings

You can set the system time and date or configure the EX Secure WAN Manager to use a Network Time Protocol (NTP) server to obtain time and date information.

To configure time and date settings:

1. Select Config Mode > System > Time.
2. On the menu bar, select Time, if not already selected. The Time tab is displayed.
3. To configure the time and date manually:
   a. Enter the date in the Date field or select the date using the calendar.
   b. Enter the time in the Time field.

4. To set the time and date using NTP:
   a. Select the Automatically Synchronize with Internet Time Server checkbox.
   b. In the Server IP Address/Name field, enter the NTP server's IP address or fully-qualified domain name.
   c. In the Update System Clock Every field, enter the number of minutes you want the EX appliance to wait between synchronizations with the NTP server.
5. To select the timezone:
   a. Click Time Zone to display the tab.
   b. From the Time Zone Name pull-down list, select the time zone.
   c. Click Apply.
   d. Click Date/Time to re-display the tab, if not already displayed.
6. If you configured the EX appliance to use NTP, click Sync to synchronize with the NTP server. If enabled, the ntp Sync icon will disappear. The Sync function is synchronizing with PC time.
7. Click Apply.

Configure SNMP Settings

The EX Secure WAN Manager supports SNMP versions 1 and 2c. All communities configured on the EX appliance are read-only.

To configure SNMP:

1. Select Config Mode > System > SNMP. The General tab is displayed.
2. To enable SNMP, select Enabled next to System SNMP Service.
3. Configure general settings:
   a. To enable the EX appliance to send SNMP traps, select Enabled next to System SNMP Trap.
   b. In the System Location field, enter a description of the EX appliance location.
   c. In the System Contact field, enter the name or email address of the EX appliance administrator to contact for system issues.
   d. Click Apply.

4. Configure community strings:
   a. Click Community to display the tab.
   b. In the SNMP Community field, enter a community name.
   c. To restrict SNMP access to specific hosts, enter a hostname or an IP address and network mask in the Hostname (IP/Mask) field.

      By default, any host can access the SNMP agent on the EX appliance.
   d. In the Object Identifier field, enter the OID at which SNMP management applications can reach the EX appliance.
   e. Click Add.
   f. Repeat step b through step e for each combination of community string, management host, and OID.
   g. Click Apply.
5. Specify trap receivers:
   a. In the Community field, enter the name of the community sending the traps.
   b. In the IP Address (host) field, enter the IP address or fully-qualified hostname of the SNMP trap receiver.
   c. If the trap receiver does not use the standard protocol port to listen for traps, change the port number in the Port field.
   d. Select SNMP the version from the Version drop-down list:
      - V1
      - V2c
   e. Click Add to add the receiver.
   f. Repeat step a through step e for each trap receiver.
6. Click Apply.

System Maintenance

The following sections describe the maintenance options for the EX Secure WAN Manager system software and configuration files.

Note: System Reset - When performing an upgrade, allow up to five minutes for the reset procedure to complete, during which time the system performs a full reset and will be offline. The actual time may vary depending on system parameters.

Upgrade the Software

The EX Secure WAN Manager system software can be upgraded from a file located on either a local or a remote host.

To Upgrade the System Software (Local or Remote)

To upgrade the software from a remote host, follow these steps:

1. Select Config Mode > System > Maintenance.
2. On the menu bar, select Upgrade > System.
3. You can retrieve the software upgrade image either locally or from a remote server.

   To perform a local installation, select the Local radio button, and then following the sub-procedure below:

   a. In the Filename field, enter the path and file name of the upgrade file, or select the Browse button to navigate to the upgrade file.

   b. Click the Apply button.

   c. The system will reboot automatically after the upgrade completes. Please allow five minutes for the backup procedure to complete. During this time, the system performs a full reset and will be offline. The actual time may vary depending on system parameters.

   To perform a remote installation, select the Remote radio button, and then following the sub-procedure below:

   a. From the Protocol field, select the file transfer protocol to use for downloading the software from the file server:
      - FTP
      - TFTP
      - RCP
      - SCP

   b. In the Host field, enter the IP address or fully qualified name of the file server.

   c. In the Location field, enter the directory path to the system software file, if the file is not in the server's default file-transfer directory.

   d. In the User and Password fields, enter the username and password required by the file server to download files.

   e. Click Apply to begin the upgrade.

   f. The system will reboot automatically after the upgrade completes. Allow five minutes for the backup procedure to complete. During

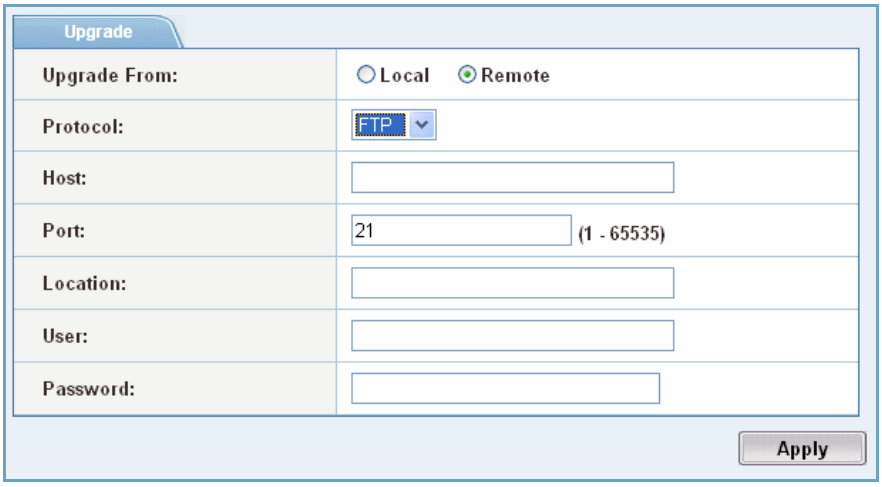
this time, the system performs a full reset and will be offline. The actual time may vary depending on system parameters.

To Upgrade the Application Protocol Library

To upgrade the Application Protocol Library, follow these steps:

1. Select Config Mode > System >Maintenance.
2. On the menu bar, select Upgrade > Application Protocol Library.

FIGURE 128 Config Mode > System > Maintenance > Remote



3. On the menu bar, select Upgrade, if not already selected.
4. Select the Remote radio button.
5. From the Protocol field, select the file transfer protocol to use for downloading the software from the file server:
   - FTP
   - TFTP
   - RCP
   - SCP
6. In the Host field, enter the IP address or fully qualified name of the file server.
7. In the Location field, enter the directory path to the system software file, if the file is not in the server's default file-transfer directory.
8. In the User and Password fields, enter the username and password required by the file server to download files.

9. Click Apply to begin the upgrade.

10. The system will reboot automatically after the upgrade completes.

Note: Please allow five minutes for the backup procedure to complete. During this time, the system performs a full reset and will be offline. The actual time may vary depending on system parameters.

Display the Upgrade History

To display the history of upgrades to the EX Secure WAN Manager:

1. Select Monitor > System > Maintenance.

2. On the menu bar, select Upgrade.

Back Up the Configuration (On Demand)

You can back up the running-config or the startup-config.

- To save the backup immediately, use the following procedure.
- To instead schedule regular backups, see "Schedule Periodic Configuration Backups" on page 260.

To Backup to a Local Host

1. Select Config Mode > System >Maintenance.

2. On the menu bar, select Backup. (See Figure 129.)

3. Select the Configuration to back up:
   - Startup-config - The configuration file is backed up.
   - Running-config - A file containing the currently running configuration is backed up.

4. Select Backup To: Local radio button.

5. To include the software version in the backup filename, leave Backup File Name With Version enabled.

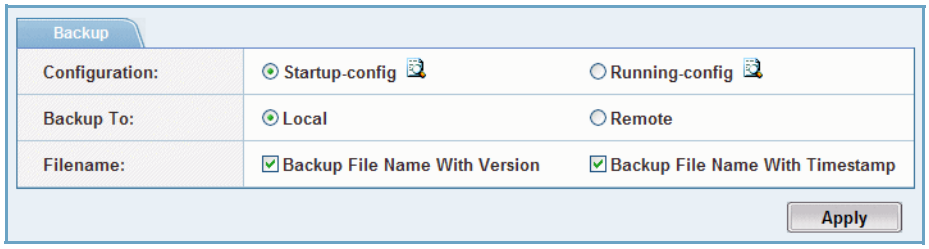
6. To include a timestamp in the backup filename, leave Backup File Name With Timestamp enabled.

7. Click Apply.

8. A File Download wind appears; click Save to navigate to the location you want to save the backup file to.

9. Click Save.

FIGURE 129 Config Mode > System > Maintenance - Backup > Local



To Back Up to a Remote Host

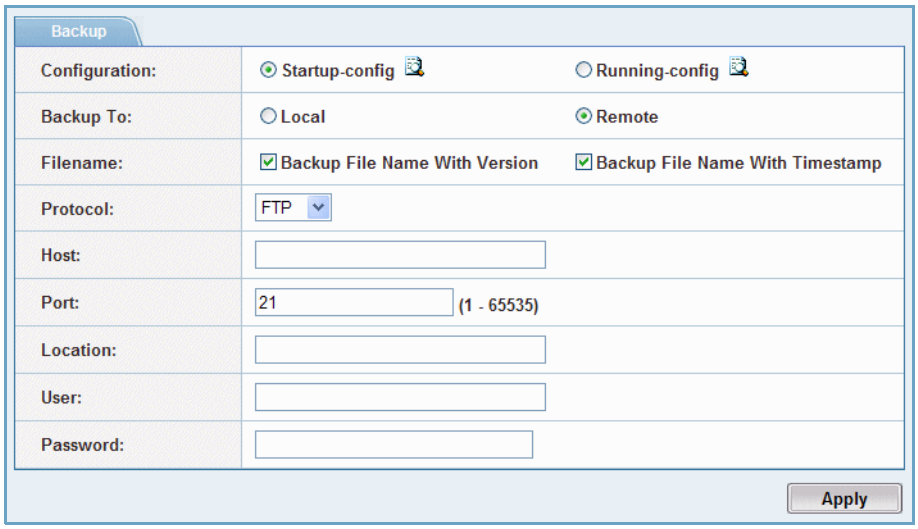
1. Select Config Mode > System >Maintenance.

2. On the menu bar, select Backup.

3. Select the configuration to back up:
   - Startup-config – The configuration file is backed up.
   - Running-config – A file containing the currently running configuration is backed up.

4. Select the Backup To: Remote radio button, if not already selected. Fields open in the display to specify the Protocol, Host IP address, Port, Location, User and Password for the backup file transfer.

FIGURE 130 Config Mode > System > Maintenance - Backup > Remote



5. To include the software version in the backup filename, leave Backup File Name With Version enabled.

6. To include a timestamp in the backup filename, leave Backup File Name With Timestamp enabled.

7. From the Protocol field, select the file transfer protocol to use for uploading the configuration to the file server:
   - FTP
   - TFTP
   - RCP
   - SCP

8. In the Host field, enter the IP address or fully qualified name of the file server.

9. In the Location field, enter the directory path to the backup directory on the file server, if it is not the server's default file-transfer directory.

   Optionally, you also can specify the file name to use for the backup.

10. In the User and Password fields, enter the username and password required by the file server to upload files.

11. Click Apply to begin the backup.

Restore a Configuration

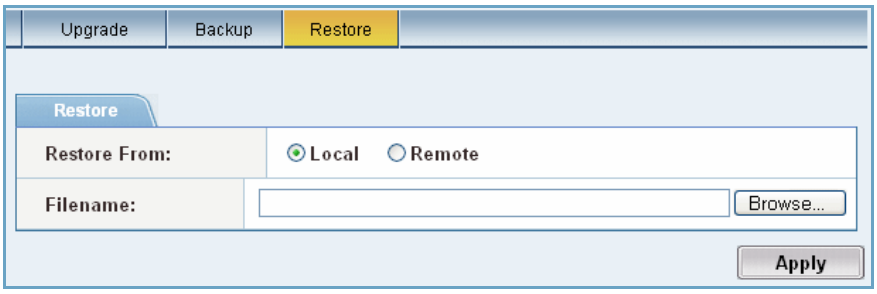
You can restore the EX Secure WAN Manager to a saved backup configuration from a previously saved backup file on either a local or a remote host.

Note: System Reboot - When performing a restore, allow five minutes for the backup procedure to complete, during which time the system performs a full reset and will be offline. The actual time may vary depending on system parameters.

To Restore from a Local Host

1. Select Config Mode > System >Maintenance.
2. On the menu bar, select Restore.
3. Select the Local radio button, if not already selected.
4. In the Filename field, enter the path and file name of the upgrade file, or select the Browse button to navigate to the backup file to be restored.
5. Click the Apply button.
6. The system will reboot automatically after restore (see note above).

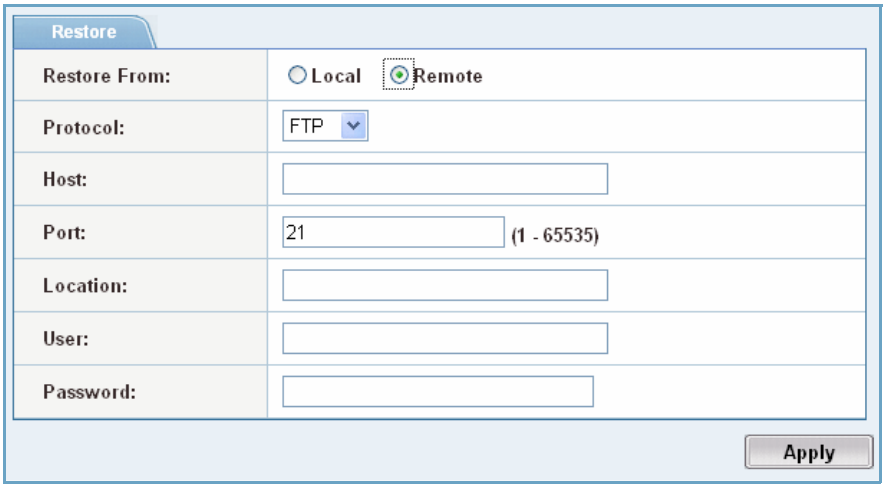
FIGURE 131 Config Mode > System >Maintenance - Restore > Local



To Restore from a Remote Host

1. Select Config Mode > System >Maintenance.
2. On the menu bar, select Restore.
3. Select Remote radio button, if not already selected.

FIGURE 132 Config Mode > System >Maintenance - Restore > Remote



4. From the Protocol field, select the file transfer protocol to use for downloading the configuration from the file server:
   - FTP
   - TFTP
   - RCP
   - SCP
5. In the Host field, enter the IP address or fully qualified name of the file server.
6. In the Port field, enter the port number to access on the remote host.
7. In the Location field, enter the directory path to the backup file, if the file is not in the server's default file-transfer directory.
8. In the User and Password fields, enter the username and password required by the file server to download files.
9. Click Apply.
10. The system will reboot automatically after restore (see note above).

Schedule Periodic Configuration Backups

To schedule regular backups of the running-config or startup-config, use the following procedure.

Note: To save a backup immediately, see "Back Up the Configuration (On Demand)" on page 255.

1. Select Config Mode > System >Maintenance.
2. On the menu bar, select Schedule.
3. Select Enable.
4. Select the configuration to back up:
   - Startup-config – The configuration file is backed up.
   - Running-config – A file containing the currently running configuration is backed up.
5. In the Repeat section, specify the backup schedule. You can configure one of the following types of schedules:
   - Daily backups – Select Daily, and enter the time of day (Hour and Minutes).
   - Weekly backups – Select Weekly, and select the Day and the time (Hour and Minutes).
   - Monthly backups – Select Monthly, and select the Day of the month and the time (Hour and Minutes).
6. To include the software version in the backup filename, leave Backup File Name With Version enabled.
7. To include a timestamp in the backup filename, leave Backup File Name With Timestamp enabled.
8. From the Protocol field, select the file transfer protocol to use for downloading the configuration from the file server:
   - FTP
   - TFTP
   - RCP
   - SCP
9. In the Host field, enter the IP address or fully qualified name of the file server.

10. In the Port field, enter the port number to access on the remote host.
11. In the Location field, enter the directory path to the backup file, if the file is not in the server's default file-transfer directory.
12. In the User and Password fields, enter the username and password required by the file server to download files.
13. Click Apply.

Export Techsupport Data

If you contact Technical Support for help with a system issue, they may request techsupport data for the EX Secure WAN Manager.

To generate and download techsupport data:

1. Select Config Mode > System >Maintenance.
2. On the menu bar, select Tech Support.
3. Click Apply. The browser displays a file management dialog.
4. Click OK (Firefox) or Save (Internet Explorer), navigate to the save location, and click Save.
5. Send the file to Technical Support.

Note: Generating techsupport data may take a while the first time. Generally, the process is faster the next time.

Display System Information

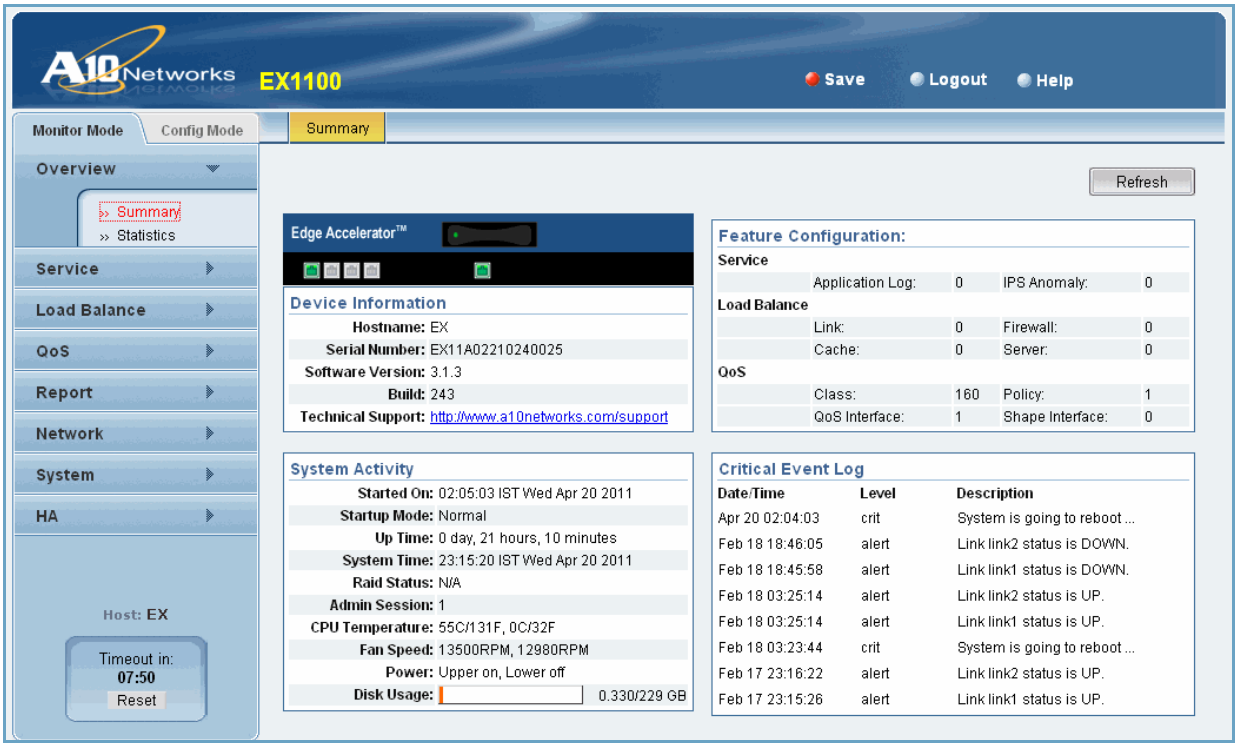
To display system information, use the procedures in the following sections.

Display the System Summary

The system summary provides a high-level view of the EX Secure WAN Manager configuration and status. (See Figure 133.)

The system summary is displayed by default when you log on to the EX appliance. To re-display the system summary, select Monitor Mode > Overview > Summary.

FIGURE 133 Monitor Mode > Overview > Summary



The Interface Status section shows the status of the EX appliance physical interfaces. Status is indicated by the following colors:

- – The interface is enabled and the link is up.
- – The interface is disabled, the link is down, or the link is not working properly.

The Device Information section shows the hardware and software versions and also has a link to the A10 Networks Technical Support Web page.

The System Activity section shows basic operating information. The RAID Status information indicates the device's status in a high-availability configuration between two alternate hard disks. Pause with the mouse over the black panels to view a popup with the status information.

FIGURE 134 View RAID Status

The Critical Event Log lists the critical system messages that have occurred since the last time the switch was powered on or rebooted. Only the messages at the Critical level are displayed. (To display system messages for all levels, see "Display the System Log" on page 264.)

Display Summary Statistics

To display summary statistics, select Monitor Mode > Overview > Statistics.

The following graphs are displayed:

- Throughput In Bits
- Throughput In Packets
- Connections

(For information about refreshing the data and changing the time period, see "Graph Display Options" on page 26.)

Display Active Admin Sessions

To display the admin sessions that are active on the EX Secure WAN Manager, select Monitor Mode > System > Session, then select Admin Session. A table listing the admin sessions is displayed.

The start time, user name, and IP address for each session are displayed.

If the EX appliance is integrated with an A10 Networks IDsentrie, the Identity column shows the admin's identity, which may be different from the EX appliance admin user name.

Note: The Identity column is blank unless the EX appliance is integrated with an IDsentrie to supply the identity information or the identity has been statically configured.

The Config Mode column indicates whether the admin session has configuration access. Only one admin session can have configuration access at any one time.

The Type column indicates the management interface the admin session is on. The Type can be one of the following:

- CLI
- Web

Clear Admin Sessions

If you need configuration access but another admin session already has it, you can clear the other admin session. To clear an admin session:

1. Display the admin session table, if not already displayed. (Select Monitor Mode > System > Session, then select Admin Session.)
2. Select the checkbox next to the row of information about the session. To clear the session that currently has configuration access, select the session that has “Yes” in the Config Mode column.
3. Click Delete.

After you clear the session that has configuration access, you can gain the access. You gain the access automatically when you click a button to send a configuration change to the EX appliance.

Display Active User Sessions

To display the currently active session flows transiting the EX Secure WAN Manager:

1. Select Monitor Mode > System > Session.
2. On the menu bar, select Flow Session.

Summary connection statistics are displayed, followed by a list of the currently active user sessions.

Filter fields allow you to filter display of the session list.

Display the System Log

The system log displays EX Secure WAN Manager system messages.

Note: The system log does not display messages for application usage or the Intrusion Prevention System (IPS) messages. To display these messages, use the application log. (See “Application Log” on page 39.)

To display the system log, select Monitor Mode > System > Logging.

Export Log Entries

You can export system log entries to a file. The entries are exported in Gzip format.

To export log entries:

1. Select Monitor Mode > System > Logging.
2. Click Export. The File Download dialog is displayed.
3. Click Save. The Save As dialog is displayed.
4. Navigate to the folder where you want to save the log and click Save.
5. When the download is complete, click Close in the Save As dialog if you have it configured to appear when downloads are completed.

High Availability

This chapter describes how to configure a pair of EX Secure WAN Managers for redundancy.

Overview

The High Availability (HA) feature provides failover support for the EX appliance. HA support is based on the Virtual Router Redundancy Protocol (VRRP).

You can configure a pair of EX appliance devices in a virtual group. One of the devices is the master and actively performs traffic management. The other device is a hot standby.

The hot standby does not perform traffic management. Instead, the hot standby listens for heartbeat messages from the master. If the master stops sending heartbeat messages, the hot standby takes over, resuming traffic management service for the network.

Supported HA Configurations

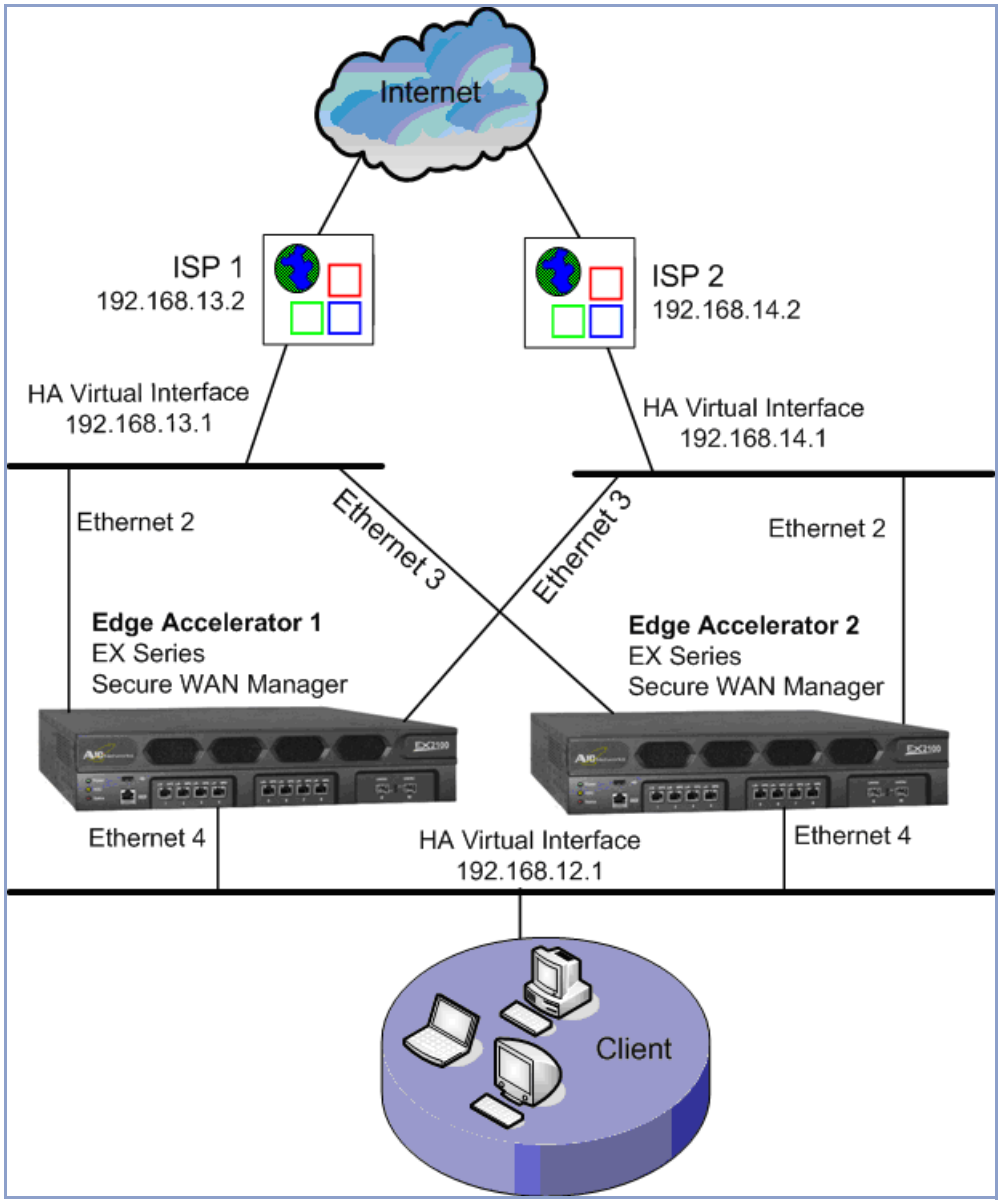
The EX Secure WAN Manager supports HA in the following modes:

- Gateway mode – Gateway mode provides redundancy for multinetted EX appliances. A separate virtual group with a separate HA virtual interface can be configured for each subnet. The virtual groups are grouped together using a tag to ensure that failure on any of the virtual groups triggers failover in all groups.
- Transparent mode – Transparent mode provides redundancy for an EX appliance that is deployed as a Layer 2 device. A single virtual group is configured.

Gateway Mode

The gateway mode of HA provides failover support for a multinetted (Layer 3) EX appliance. Figure 135 shows an example of a gateway HA deployment.

FIGURE 135 HA – Gateway Mode



In this example, three subnets are configured on each of a pair of EX Secure WAN Managers. A virtual group containing an HA virtual interface is configured for each of them.

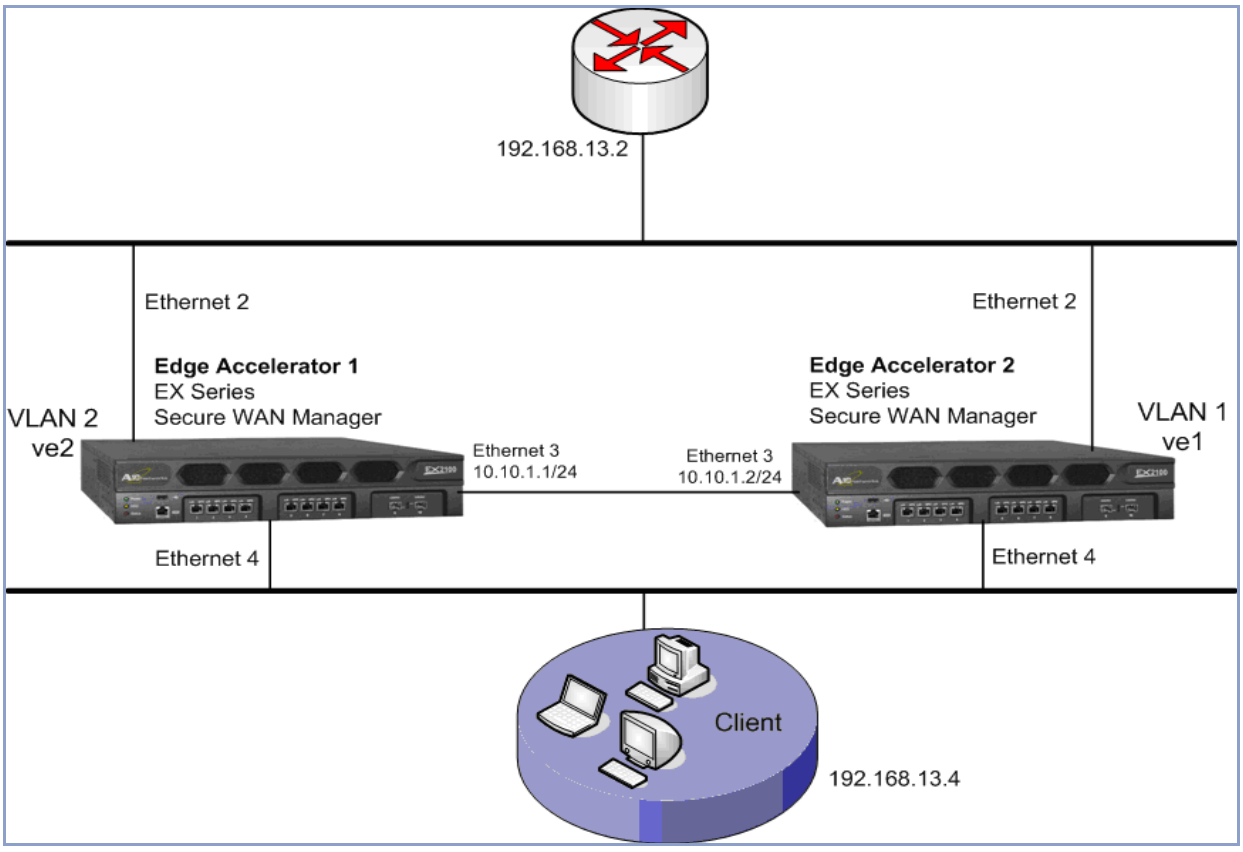
The virtual groups are tagged together to ensure that if any one of the virtual interfaces stops sending heartbeat messages, the virtual interfaces in all the virtual groups fail over. Tagging all the virtual groups together is required to ensure proper failover.

On the master EX appliance, a data interface in each of the virtual groups sends heartbeat messages to the backup. If the standby EX appliance stops receiving the heartbeat messages from any of the virtual groups, the standby initiates failover and becomes the active EX appliance. In gateway mode, use of a dedicated HA interface for heartbeat messages is optional. The EX appliance can use data interfaces instead, as in this example.

Transparent Mode

The transparent mode of HA provides failover support for a single-netted (Layer 2) EX Secure WAN Manager. Figure 136 shows an example of a transparent HA deployment.

FIGURE 136 HA – Transparent Mode



In this example, a single virtual group is configured on each EX appliance in the HA pair. The group is configured on a virtual ethernet (VE) configured on VLAN 1, which contains ethernet ports 2 and 4.

Ethernet port 3 is dedicated to HA heartbeat messages. In transparent mode, use of a dedicated HA port for heartbeat messages is required. In transparent mode, the EX appliance cannot use a data port for heartbeat messages. In this example, ethernet 3 on each EX appliance is used exclusively for HA heartbeat messages. The heartbeat interfaces in transparent mode cannot also be used for data and cannot belong to any VLANs.

HA Connection Requirements

Each pair of physical interfaces that has the same virtual interface (HA virtual interface in gateway mode or VE in transparent mode) must be linked by a Layer 2 switch. For example, in Figure 135 and Figure 136, each of the thick lines representing a virtual interface connection represents a Layer 2 switch.

If a dedicated heartbeat interface is used on each EX Secure WAN Manager, the heartbeat interfaces can be connected through a Layer 2 switch or directly attached.

In transparent mode, the Layer 2 switches must run the Spanning Tree Protocol (STP).

Master Election

The EX Secure WAN Manager with the higher HA priority becomes the master. The other EX appliance becomes a hot standby. The hot standby becomes the master only as a result of failover.

If the priority value is the same on both EX appliances, the primary IP addresses of the virtual groups are used as the tie breaker. The EX appliance that has the higher-numbered primary IP address in a virtual group or tagged group becomes the master.

For each virtual group (whether tagged or untagged), the group's primary IP address is one of the following:

- If the group has a real IP interface, the real interface is the primary IP address.
- If the real interface has no IP address, the primary IP address is the first heartbeat interface IP address.
- For virtual groups that are tagged together (have the same tag value), the primary IP address is the primary address on the group with the lowest group ID.

Configuration Synchronization

Configuration synchronization enables the EX Secure WAN Managers in an HA pair to keep their configurations in sync. This feature ensures that the configuration remains the same following a failover.

This option is disabled by default. To enable it and synchronize the configuration, see "Enable Configuration Synchronization" on page 280.

Session Synchronization

Session synchronization provides stateful failover for active sessions. If a failover occurs, active sessions that have been synchronized continue uninterrupted. Clients experience little or no service interruption.

Session synchronization applies to the following types of connections:

- Forwarded IP with session (TCP, UDP, ICMP, other IP)
- IP NAT and NAT ALG connections
- Connections to internal servers such as IPsec of PPTP VPN, SSL VPN, internal email, or web server

The following state information is synchronized:

- Link information (persistence info, session and link associatation, and so on)
- NAT info (source be source or destination NAT, or both)
- Layer 2 though Layer 7 Information

Session synchronization applies to the following features:

- Outbound LLB
- Inbound LLB in combination with DNAT or SLB
- Transparent bridge mode
- CLB
- FWLB
- QoS Policy

Note: Session synchronization requires the configurations on the EX appliances in the HA pair to be the same.

Auto-Port Restart Following Failover

Transparent mode supports an option to briefly flap (disable and re-enable) a virtual group's HA interfaces. This option forces the other devices connected to the EX Secure WAN Managers to more quickly relearn their MAC and ARP entries for the EX appliance. Until the other devices relearn the MAC and ARP entries, the entries will still refer to the EX appliance that is no longer Active.

You can set the duration of the disabled state to 100-10000 ms. The default is 2000 ms.

Note: This option applies only to Virtual Ethernet (VE) interfaces, and only in transparent mode.

HA Configuration Parameters

Table 21 lists the HA configuration parameters.

TABLE 21 HA Configuration Parameters

Parameter	Description	Supported Values
Global HA Parameters		
Configuration Synchronization	Synchronization of configuration changes made on the active EX appliance to the standby EX appliance. To enable the feature, specify the IP address of the HA heartbeat interface on the peer EX appliance. After the feature is enabled, you can synchronize the configuration on demand. **Note:** Before synchronizing the configuration, make sure HA is configured and is working properly.	IP address of the other EX appliance Default: Disabled
Session Synchronization	Stateful synchronization of active sessions to the standby EX appliance, to prevent service interruption following failover. **Note:** Session synchronization requires the configurations on the EX appliances in the HA pair to be the same.	Enabled or disabled Default: Disabled
HA Virtual Group Parameters		
Virtual Group ID	Number that identifies the virtual group. The EX Secure WAN Manager can be a member of up to 32 virtual groups.	1 to 255

TABLE 21 HA Configuration Parameters (Continued)

Parameter	Description	Supported Values
Interface	Data interface on which the HA virtual interface is configured. The interface can be a physical interface (ethernet port) or a virtual ethernet (VE) configured on one or more physical ports. • In gateway mode, you must select a physical interface. • In transparent mode, the interface must be a Virtual Ethernet (VE). The interface does not need an HA virtual interface.	One of the EX Secure WAN Manager ethernet interfaces or a VE Default: no interface is selected
Priority	Preference of this EX appliance to become the master. The EX appliance with the higher priority number becomes the master by default. The EX appliance with the lower priority becomes master only if the EX appliance with the higher priority stops sending heartbeat messages. If the priority values match, the EX appliance with the higher primary IP address number in a virtual group or tagged group becomes the master. (See "Master Election" on page 270.)	1 to 253 Default: 100
Weight	Weight of the virtual group. Total weight accumulates from all HA weight factors in until it reaches the priority value. If the priority value is reached, a failover occurs. The total of all weight values can not exceed the priority value.	1-255
Advertisement Interval	Number of seconds the EX appliance waits between sending heartbeat messages to the other EX Secure WAN Manager in the virtual group. If the standby EX appliance does not receive a heartbeat message from the master EX appliance for three consecutive advertisement intervals, failover to the standby EX appliance occurs.	1 to 255 seconds Default: 1 second
Tag	Number that allows the virtual group to be joined with other virtual groups on the same EX appliance. Tagging is required in gateway mode to ensure that all the virtual interfaces fail over to the standby. Tagging is not applicable to transparent mode since this mode uses only one virtual group.	0 to 255 Default: 0 When the tag value is 0, the virtual group is not joined with any other virtual groups.

TABLE 21 HA Configuration Parameters (Continued)

Parameter	Description	Supported Values
Heartbeat Interface	Ethernet interface this EX appliance uses to exchange heartbeat messages with the other EX appliance in the virtual group. If a heartbeat interface is specified, the interface cannot also be used for data and cannot be a member of any VLAN. • In gateway mode, use of a dedicated heartbeat interface is optional. If you do not specify one, the EX appliance uses the data interfaces for heartbeat messages. The heartbeat messages do not interfere with data traffic on the interfaces. • In transparent mode, a dedicated heartbeat interface is required and the interface cannot be used for data.	One of the EX appliance ethernet interfaces Default: no interface is selected
Preemptive Mode	Preemptive mode can be enabled on both master and standby. The unit that has this mode enabled can preempt to become master when its priority is higher than the other unit.	Enabled or disabled Default: Enabled
Enabled / Disabled	State of the virtual group.	Enabled or disabled Default: disabled
Disable Port Hold Time (Transparent mode only)	Number of milliseconds (ms) during which to flap (disable, then re-enable) the HA interface following HA failover. Flapping the interface forces the other devices connected to the EX appliances to more quickly relearn their MAC and ARP entries for the EX appliance. Until the other devices relearn the MAC and ARP entries, the entries will still refer to the EX appliance that is no longer Active. You can specify 100-10000 ms. **Note:** This option applies only to VE interfaces, in transparent mode.	100-10000 ms Default: 2000 ms
Virtual IP Address	HA virtual interface, which is the IP address used for an HA pair in gateway mode. The address must be unused. It cannot be an address that is assigned to interfaces on either EX appliance. The address must be in the same subnet as the physical interface in the virtual group. Transparent mode does not use virtual IP addresses. Instead, transparent mode uses VEs.	Any valid IP address

TABLE 21 HA Configuration Parameters (Continued)

Parameter	Description	Supported Values
Track Interface	Tracks other physical interfaces in the virtual group. If the tracked interface fails, the priority value of the current interface is reduced by the amount of the tracked interface's weight.	Ethernet interface The weight can be 1-255. Default: • Gateway mode – Not set • Transparent mode – all physical interfaces in the VLAN are tracked automatically.
Track Service Weight	Tracks background services in the virtual group. The *service* can be one of the following • Log (includes syslog and kernel log) • Health monitor • Web • SSH • Routing (includes routing manager, OSPF, and RIP) • System (includes health monitoring, IP2ID, DNS, system timer, and SNMP) • Report – Report service If a tracked service fails, the priority value will be reduced by the amount of the failed service's weight.	1-255 The sum of the weight value must be less than the priority value. Default: when you add tracking of a service, the default weight depends on the service: • Log – 10 • Health monitor – 5 • Web – 5 • SSH – 5 • Routing – 5 • System – 5 • Report – 5

Configure HA

To configure a virtual group, perform one of the following procedures. Perform the same procedure on both EX Secure WAN Managers in the HA pair.

Configure Gateway Mode

1. Select Config Mode > HA > Virtual Group. The list of configured virtual groups (if any) is displayed.
2. Click New. The General tab is displayed.
3. In the Virtual Group ID field, enter the group ID.

   If you are configuring multiple virtual groups, use a unique ID for each group.
4. From the Interface pull-down list, select the physical interface on which the HA virtual interface will be configured.
5. In the Priority field, change the priority value:
   - To configure this EX appliance as the master, leave the priority value at 100 or increase it. Set the priority on the other EX appliance to a lower value.
   - To configure this EX appliance as the standby, decrease the priority value. Make sure the priority on the other EX appliance is set to a higher value.
6. In the Weight field, set the group's weight value within the range 1 to 255. Total weight accumulates from all HA weight factors in until it reaches the priority value. If the priority value is reached, a failover occurs. The total of all weight values can not exceed the priority value.
7. To increase the advertisement interval, enter the number of seconds in the Advertisement Interval field. Otherwise, leave the interval set to 1.
8. In the Tag field, enter a value to group this virtual group with the other virtual groups configured on the same EX appliance.

   Use the same tag value for all virtual groups on this EX appliance.
9. To use a dedicated heartbeat interface, select the interface from the Heartbeat pull-down list. To use a data interface instead, do not select an interface here.
10. To change the preemptive mode setting, click on the checkbox.

11. To enable the virtual group, select Enable.

12. To change the number of milliseconds for which the HA interface is disabled following a failover, edit the value in the Disable hold port time field.

Note: This option applies only to VE interfaces, in transparent mode.

13. Configure the HA virtual interface:
    a. Click Virtual IP Address to display the tab.
    b. Enter an IP address in the entry field. The address cannot be configured on any other interfaces and must be in the same subnet as the interface's IP address.
    c. Click Add. The virtual interface appears in the list.
    d. Click OK. The new virtual group appears in the list.

14. Repeat step 2 through step 13 for each virtual group.

Figure 138 and Figure 139 show how to configure HA for ethernet interface 4 on the EX appliances as shown in Figure 137.

FIGURE 137 HA Virtual Group – General Tab (gateway example)

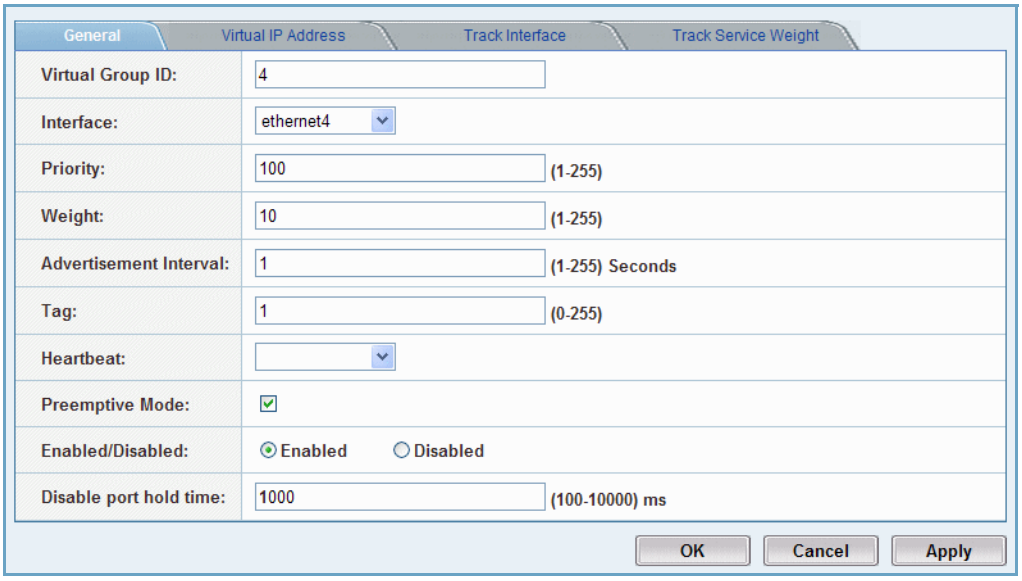
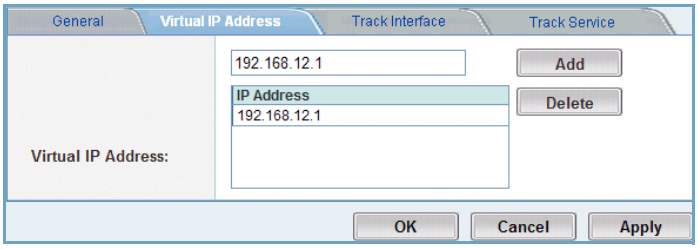


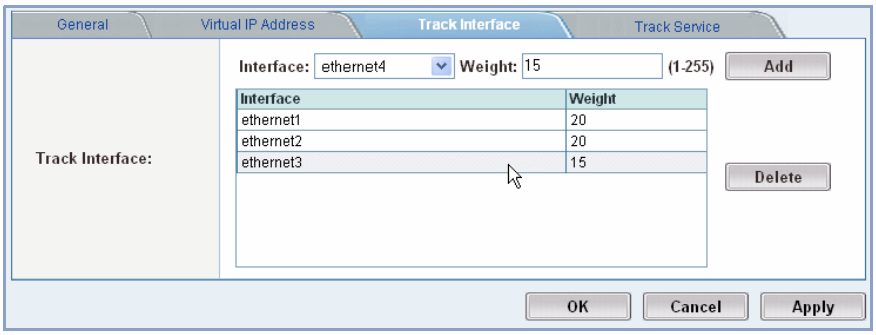
FIGURE 138 HA Virtual Group – Virtual IP Address Tab (gateway example)



Track Interface Tab

On the Track Interface tab, you can set the weight for the Unified Enterprise Management's ethernet interfaces. You can not exceed the total weight (the Priority field value) when setting weight values.

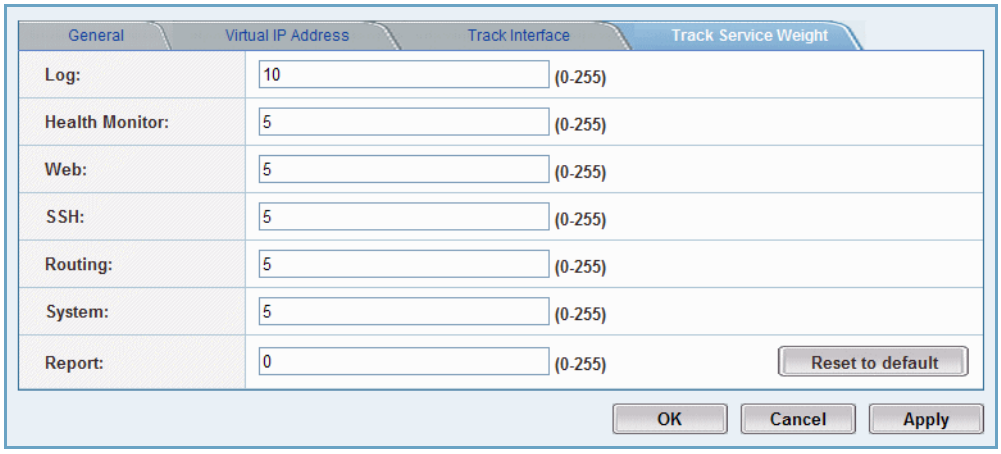
FIGURE 139 HA Virtual Group – Track Interface tab



Track Service Tab

On the Track Service tab, you can set the weight for the Unified Enterprise Management's monitored services. You can not exceed the total weight (the Priority field value) when setting weight values.

FIGURE 140 HA Virtual Group – Track Service tab



Configure Transparent Mode

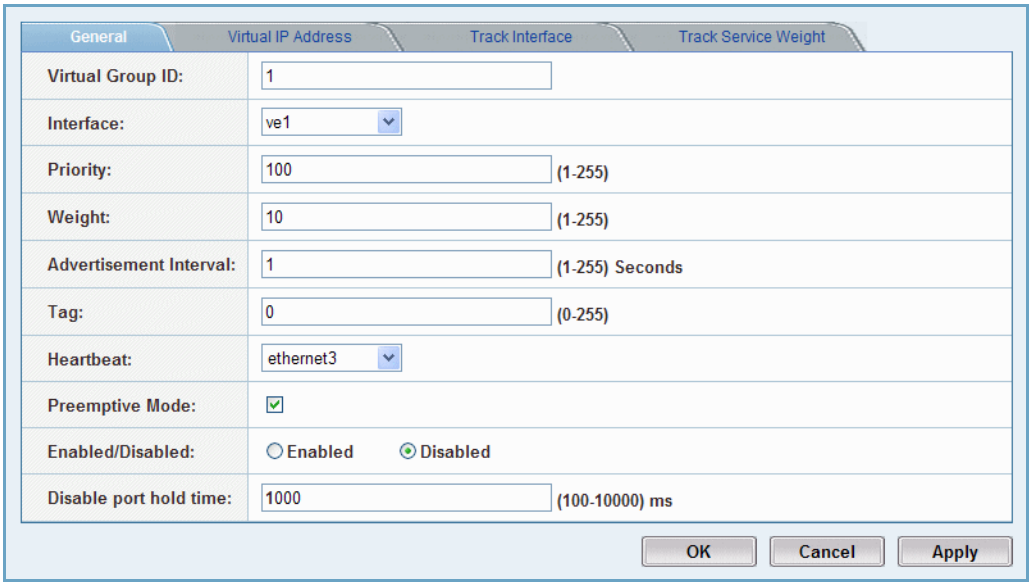
1. Select Config Mode > HA > Virtual Group. The list of configured virtual groups (if any) is displayed.
2. Click New. The General tab is displayed.
3. In the ID field, enter the group ID.
4. From the Interface pull-down list, select the VE interface.
5. In the Priority field, change the priority value:
   - To configure this EX appliance as master, leave the priority value at 100 or increase it. Set the priority on the other EX appliance to a lower value.
   - To configure this EX appliance as standby, decrease the priority value. Make sure the priority on the other EX appliance is set to a higher value.
6. To increase the advertisement interval, enter the number of seconds in the Advertisement Interval field. Otherwise, leave the interval set to 1.
7. From the Heartbeat pull-down list, select the ethernet interface to use for heartbeat messages.
8. To change the preemptive mode setting, click on the checkbox.

9. To enable the virtual group, select Enable.

10. Click OK. The new virtual group appears in the list.

Figure 141 shows how to configure HA on EX appliances in Transparent Mode.

FIGURE 141 HA Virtual Group – General Tab (transparent example)



Enable Configuration Synchronization

The Full Sync tab allows you to manually synchronize the HA Master's configuration with the configuration on an HA Backup. When you use this option, the EX Secure WAN Manager copies its running-config and startup-config to the specified Backup, to replace the running-config and startup-config on the Backup with those from the Master.

Manual synchronization can be performed only from the HA Master to an HA Backup. Configurations cannot be synchronized from a Backup to another Backup or to a Master.

Note: Before synchronizing the configuration, make sure HA is configured and is working properly.

To enable configuration synchronization:

1. Select Config Mode > HA > Virtual Group.

2. On the menu bar, select Full sync.

3. In the IP Address field, enter the IP address of the HA heartbeat interface on the peer EX appliance.

4. Click Apply.

The next time you need to synchronize configuration changes, navigate to the Sync Session tab again and click Apply.

Enable Automatic Session Synchronization

To enable automatic session synchronization:

1. Select Config Mode > HA > Virtual Group.

2. On the menu bar, select Sync Session.

3. Select Enabled.

4. Click Apply.

Display HA Information

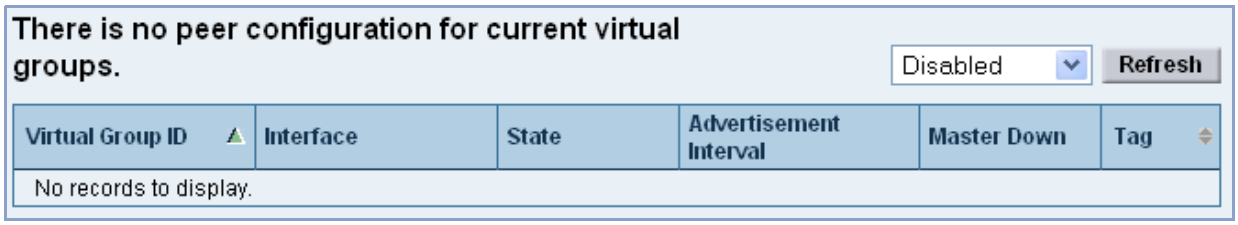
To display virtual group information, select Monitor Mode > HA > Virtual Group.

The following information is shown for each group:

- Virtual Group ID
- Interface
- State
- Advertisement Interval
- Master Down
- Tag

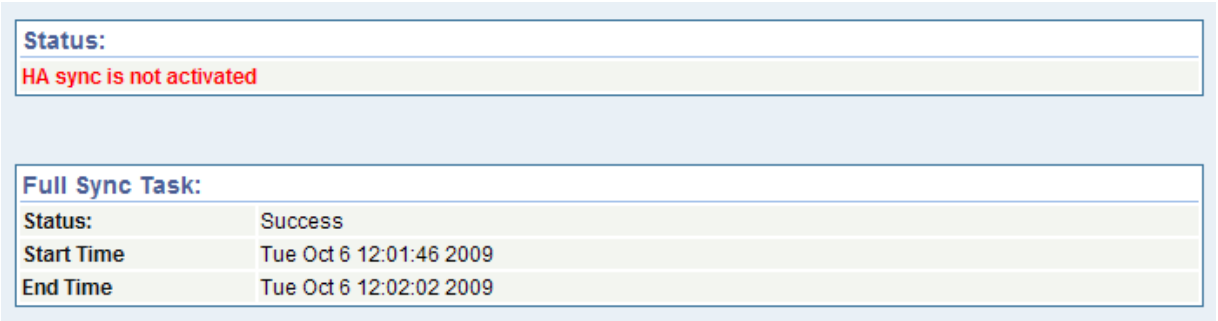
You can sort the list by either Virtual ID Group or Tag. Click on a column heading with the green up/down arrows to sort by that column.

FIGURE 142 Monitor Mode > HA



To display synchronization information, select Monitor Mode > HA > Virtual Group > Full Sync.

FIGURE 143 Monitor Mode > HA > Virtual Group > Full Sync



Corporate Headquarters

A10 Networks, Inc.
2309 Bering Dr.
San Jose, CA 95131-1125 USA

www.a10networks.com