



CHAPTER 1

Configuring Logging Policies on Firewall Devices

The Logging feature lets you enable and manage NetFlow “collectors,” and enable system logging, set up logging parameters, configure event lists (syslog filters), apply the filters to a destination, set up syslog messages, configure syslog servers, and specify e-mail notification parameters.

After you enable logging and set up the logging parameters using the Logging Setup page, the Event Lists page lets you configure filters (for a set of syslogs) which can be sent to a logging destination. The Logging Filters page lets you specify a logging destination for the syslogs to be sent. Finally, the Syslog and E-Mail pages configure syslog and e-mail setup.

This chapter contains the following topics:

- [NetFlow Page, page 1-1](#)
- [E-Mail Setup Page, page 1-2](#)
- [Event Lists Page, page 1-3](#)
- [Logging Filters Page, page 1-7](#)
- [Configuring Logging Setup, page 1-9](#)
- [Configuring Rate Limit Levels, page 1-11](#)
- [Configuring Syslog Server Setup, page 1-14](#)
- [Defining Syslog Servers, page 1-18](#)

NetFlow Page

A device configured for NetFlow data export captures flow-based traffic statistics on the device. This information is periodically transmitted from the device to a NetFlow collection server, in the form of User Datagram Protocol (UDP) datagrams.

The NetFlow page lets you enable NetFlow export on the selected device, and define and manage NetFlow “collectors” to which collected flow information is transmitted.

Navigation Path

- (Device view) Select **Platform > Logging > NetFlow** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > NetFlow** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- [Using Rules Tables, page 1-7](#)
- [Filtering Tables, page 1-37](#)
- [Table Columns and Column Heading Features, page 1-37](#)

Field Reference**Table 1-1** *NetFlow Page*

Element	Description
Enable Flow Export	If checked, NetFlow data export is enabled.
Template Export Interval	Interval (in minutes) between transmissions of flow information to the collectors. The value can be from one to 3600 minutes; the default is 30.
Collectors table	Lists the currently defined NetFlow collectors. Use the Add Row, Edit Row and Delete Row buttons below the table to manage these entries. The Add Row and Edit Row buttons open the Add and Edit Collector Dialog Boxes (NetFlow), page 1-2 .

Add and Edit Collector Dialog Boxes (NetFlow)

Use the Add Collector and Edit Collector dialog boxes to define and edit NetFlow “collectors.” Except for the title, the two dialog boxes are identical; the following information applies to both.

Navigation Path

You can open the Add and Edit Collector dialog boxes from the [NetFlow Page, page 1-1](#).

Field Reference**Table 1-2** *Add and Edit Collector Dialog Boxes*

Element	Description
Interface	Enter or Select the name of the device interface through which the collector is contacted.
Collector	Enter the IP address or the network name of the server to which NetFlow packets will be sent. You also can Select a Networks/Hosts object.
UDP Port	Specify the UDP port on the specified Collector to which NetFlow packets will be sent. Values can range from 1 to 65535; the default is 2055.

E-Mail Setup Page

The E-Mail Setup page (PIX 7.0/ASA Only) lets you set up a source e-mail address, as well as a list of recipients for specified syslog messages to be sent as e-mails. You can filter the syslog messages sent to a destination e-mail address by severity. The table shows which entries have been set up.

The syslog severity filter used for the destination e-mail address will be the higher of the severity selected in this section and the global filter set for all e-mail recipients in the Logging Filters page.

Navigation Path

- (Device view) Select **Platform > Logging > Syslog > E-Mail Setup** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > E-Mail Setup** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- [Chapter 1, “Configuring Logging Policies on Firewall Devices”](#)

Field Reference**Table 1-3 E-Mail Setup Page**

Element	Description
Source Email Address	Enter the email address to be used as the source address when syslogs are sent as emails.
Destination Address table	Lists the currently defined email recipients of syslog messages. Use the Add Row, Edit Row and Delete Row buttons below the table to manage this list; the Add Row and Edit Row buttons open the Add/Edit Email Recipient Dialog Box, page 1-3 .

Add/Edit Email Recipient Dialog Box

The Add/Edit Email Recipient dialog box lets you configure a destination address to be sent emails containing syslog messages; you can limit the messages sent according to severity.

The syslog severity filter used for the destination email address will be the higher of the severity selected in this section and the global filter set for all email recipients on the [Logging Filters Page, page 1-7](#).

Navigation Path

You can access the Add/Edit Email Recipient dialog box from the [E-Mail Setup Page, page 1-2](#).

Field Reference**Table 1-4 Add/Edit Email Recipient Dialog Box**

Element	Description
Destination Email Address	Enter the recipient email address for the chosen type of syslog messages.
Syslog Severity list	Choose the severity of the syslogs to be emailed to this recipient; messages of the chosen severity and higher are sent. Message severity levels are described in Logging Levels, page 1-17 .

Event Lists Page

The Event Lists page (PIX 7.0+/ASA only) lets you define a set of syslog message filters for logging. After you enable logging and set up global logging parameters on the Logging Setup page, use this page to configure event lists used to filter syslog messages sent to different logging destinations. (The

[Logging Filters Page, page 1-7](#) lets you specify logging destinations for event lists.)

Use the Add Row, Edit Row and Delete Row buttons below the Event Lists table to manage the entries. Add Row and Edit Row open the [Add/Edit Event List Dialog Box, page 1-5](#).

Navigation Path

- (Device view) Select **Platform > Logging > Syslog > Event Lists** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > Event Lists** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- [Logging Setup Page, page 1-10](#)
- [Chapter 1, “Configuring Logging Policies on Firewall Devices”](#)

Message Classes and Associated Message ID Numbers

The following table lists the message classes and the range of message IDs in each class.

Table 1-5 *Message Classes and Associated Message ID Numbers*

Class	Definition	Message ID Numbers
auth	User Authentication	109, 113
bridge	Transparent Firewall	110, 220
ca	PKI Certification Authority	717
config	Command interface	111, 112, 208, 308
e-mail	E-mail Proxy	719
ha	Failover (High Availability)	101, 102, 103, 104, 210, 311, 709
ids	Intrusion Detection System	400, 401, 415
ip	IP Stack	209, 215, 313, 317, 408
np	Network Processor	319
ospf	OSPF Routing	318, 409, 503, 613
rip	RIP Routing	107, 312
rm	Resource Manager	321
session	User Session	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
snmp	SNMP	212
sys	System	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615, 701, 711
vpdn	PPTP and L2TP Sessions	213, 403, 603
vpn	IKE and IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	VPN Client	611
vpnfo	VPN Failover	720
vpnlb	VPN Load Balancing	718

Table 1-5 Message Classes and Associated Message ID Numbers (Continued)

Class	Definition	Message ID Numbers
webvpn	Web-based VPN	716

Add/Edit Event List Dialog Box

The Add/Edit Event List dialog box lets you create or edit an event list, and specify which syslog messages to include in the event list filter.

You can use the following criteria to define an event list:

- Class and Severity
- Message ID

Class represents specific types of related syslog messages. For example, the class `auth` represents all syslog messages related to user authentication.

Severity classifies syslogs based on the relative importance of the event in the normal functioning of the network. The highest severity is Emergency, which means the resource is no longer available. The lowest severity is Debugging, which provides detailed information about every network event.

The message ID is a numeric value that uniquely identifies each individual message. You can specify a single message ID, or a range of IDs, in an event list.

Navigation Path

You can access the Add/Edit Event List dialog box from the [Event Lists Page, page 1-3](#).

Related Topics

- [Chapter 1, “Configuring Logging Policies on Firewall Devices”](#)

Field Reference

Table 1-6 Add/Edit Event List Dialog Box

Element	Description
Event List Name	Enter a name that uniquely identifies this event list.
Event Class/Severity Filters	This table lists the event class and severity level filters defined for this event list. Use the Add Row, Edit Row and Delete Row buttons below this table to manage the entries. Add Row and Edit Row open the Add/Edit Syslog Class Dialog Box, page 1-5 .
Message ID Filters	This table list the message ID filters defined for this event list. Use the Add Row, Edit Row and Delete Row buttons below this table to manage the entries. Add Row and Edit Row open the Add/Edit Syslog Message ID Filter Dialog Box, page 1-6 .

Add/Edit Syslog Class Dialog Box

The Add/Edit Syslog Class dialog box lets you specify an event class and a related severity level as an event list filter.

Class represents specific types of related syslog messages, so you do not have to select the syslogs individually. For example, the class `auth` represents all syslog messages related to user authentication.

Severity classifies syslogs based on the relative importance of the event in the normal functioning of the network. The highest severity is Emergency, which means the resource is no longer available. The lowest severity is Debugging, which provides detailed information about every network event.

Navigation Path

You access the Add/Edit Syslog Class dialog box from the [Add/Edit Event List Dialog Box](#), page 1-5.

Related Topics

- [Add/Edit Syslog Message ID Filter Dialog Box](#), page 1-6
- [Event Lists Page](#), page 1-3

Field Reference

Table 1-7 *Add/Edit Syslog Class Dialog Box*

Element	Description
Event Class	Choose the desired event class. Event classes are described in Table 1-5 on page 1-4 .
Severity	Choose the desired message severity level. Severity levels are described in Logging Levels , page 1-17.

Add/Edit Syslog Message ID Filter Dialog Box

The Add/Edit Syslog Message ID Filter dialog box lets you specify the a syslog message ID, or a range of IDs, as an the event list filter.

Navigation Path

You can access the Add/Edit Syslog Message ID Filter dialog box from the [Add/Edit Event List Dialog Box](#), page 1-5.

Related Topics

- [Add/Edit Syslog Class Dialog Box](#), page 1-5
- [Event Lists Page](#), page 1-3

Field Reference

Message IDs – Enter a syslog message ID, or a range of IDs. Use a hyphen to specify a range; for example, 101001-101010. Message IDs must be between 100000 and 999999.

Message IDs and their corresponding messages are listed in the System Log Message guides for the appropriate product. You can access these guides from cisco.com:

PIX Firewall

- http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_system_message_guides_list.html

ASA

- http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html

FWSM

- http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html

Logging Filters Page

The Logging Filters page lets you configure a logging destination for event lists (syslog filters) that have been configured using the Event Lists page, or for only the syslog messages that you specify using the Edit Logging Filters page. Syslog messages from specific or all event classes can be selected using the Edit Logging Filters page.

Navigation Path

- (Device view) Select **Platform > Logging > Syslog > Logging Filters** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > Logging Filters** from the Policy Type selector. Right-click **Logging Filters** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- [Chapter 1, “Configuring Logging Policies on Firewall Devices”](#)
- [Edit Logging Filters Dialog Box, page 1-8](#)

Field Reference

Table 1-8 *Logging Filters Page*

Element	Description
Logging Destination	<p>Lists the name of the logging destination to which messages matching this filter are sent. Logging destinations are as follows:</p> <ul style="list-style-type: none"> • Internal Buffer. Messages matching this filter are published to the internal buffer of the security appliance. • Console. Messages matching this filter are published to any console port connections. • Telnet Sessions. Messages matching this filter are published to any Telnet sessions connected to the security appliance. • Syslog Servers. Messages matching this filter are published to any syslog servers specified on the Platform > Logging > Syslog Servers page. • E-Mail. Messages matching this filter are published to any recipients specified on the Platform > Logging > E-mail Setup (PIX7.0/ASA Only) page. • SNMP Trap. Messages matching this filter are published to any SNMP management stations specified on the Platform > Device Admin > Device Access > SNMP page. • ASDM. Messages matching this filter are published to any ASDM sessions.

Table 1-8 Logging Filters Page (Continued)

Element	Description
Syslogs From All Event Classes	Lists the severity on which to filter, the event list to use, or whether logging is disabled from all event classes. Event classes are described in Message Classes and Associated Message ID Numbers , page 1-4.
Syslogs From Specific Event Classes	Lists event class and severity set up as the filter. Event classes are described in Message Classes and Associated Message ID Numbers , page 1-4. Severity levels are described in Logging Levels , page 1-17.

Edit Logging Filters Dialog Box

The Edit Logging Filters dialog box lets you edit filters for a logging destination. Syslogs can be configured from all or specific event classes, or disabled for a specific logging destination.

Navigation Path

You can access the Edit Logging Filters dialog box from the Logging Filters page. For more information about the Logging Filters page, see [Logging Filters Page](#), page 1-7.

Related Topics

- [Chapter 1, “Configuring Logging Policies on Firewall Devices”](#)
- [Logging Filters Page](#), page 1-7

Field Reference

Table 1-9 Edit Logging Filters Dialog Box

Element	Description
Logging Destination list	<p>Specifies the logging destination for this filter:</p> <ul style="list-style-type: none"> • Internal Buffer. Messages matching this filter are published to the internal buffer of the security appliance. • Console. Messages matching this filter are published to any console port connections. • Telnet Sessions. Messages matching this filter are published to any Telnet sessions connected to the security appliance. • Syslog Servers. Messages matching this filter are published to any syslog servers specified on the Platform > Logging > Syslog Servers page. • E-Mail. Messages matching this filter are published to any recipients specified on the Platform > Logging > E-mail Setup (PIX7.0/ASA Only) page. • SNMP Trap. Messages matching this filter are published to any SNMP management stations specified on the Platform > Device Admin > Device Access > SNMP page. • ASDM. Messages matching this filter are published to any ASDM sessions.

Table 1-9 *Edit Logging Filters Dialog Box (Continued)*

Element	Description
Syslog from All Event Classes	
Filter on severity option	Filters on the severity of the logging messages.
Filter on severity list	Specifies the level of logging messages on which to filter.
Use event list option	Specifies to use an event list.
Use event list	Specifies the event list to use. Event lists are defined on the Event Lists Page, page 1-3 .
Disable logging option	Disables all logging to the selected destination.
Syslog from Specific Event Classes (PIX7.0)	
Event Class	Specifies the event class and severity. Event classes include one or all available items. Event classes are described in Table 1-5 on page 1-4 .
Severity	Specifies the level of logging messages. Severity levels are described in Table 1-15 on page 1-17 .

Configuring Logging Setup

The Logging Setup page lets you enable system logging on the security appliance and configure other logging options. These options include enabling logging on the security appliance and failover unit, specifying the base log format and detail, and logging to longer-term storage devices, FTP server or Flash, before purging the internal buffer.

Related Topics

- [Logging Setup Page, page 1-10](#)

-
- Step 1** Select **Platform > Logging > Syslog > Logging Setup** to display the Logging Setup page.
- Step 2** Check **Enable Logging**.
- This option enables logging on the security appliance.
- Step 3** To enable logging on the failover unit paired with this security appliance, select the **Enable logging on the standby failover unit** check box.
- Step 4** To enable EMBLEM format, or to send debug messages as part of the syslog messages, select the corresponding check boxes.
- If you enable EMBLEM, you must use the UDP protocol to publish syslog messages. It is not compatible with TCP.
- Step 5** To write the internal buffer data to an FTP server for future processing prior to clearing the buffer, do the following:
- Check **FTP Server Buffer wrap**.
 - Enter the IP address of the FTP server in the **IP Address** field.
 - Enter the user name of the account used to log into the FTP server in the **User Name** field.
 - Enter the path in the **Path** field, relative to the FTP root, where the file should be stored.
 - Enter and confirm the password used to authenticate the user name.

- Step 6** To write the internal buffer data to Flash for future processing prior to clearing the buffer, do the following:
- Check **Flash**.
 - Specify the maximum amount of memory to allocate to the storage of internal buffer data.
 - Specify the minimum memory that should remain free on the Flash drive. If this minimum value cannot be retained while writing out the data from the internal buffer, the messages will be pruned to meet the space requirements.
- Step 7** To specify the maximum queue size maintained on the appliance for viewing by an ASDM client, enter that value in the **Message Queue Size (Messages)** field.

Logging Setup Page

The Logging Setup page lets you enable system logging on the security appliance and configure other logging options.

Navigation Path

- (Device view) Select **Platform > Logging > Syslog > Logging Setup** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > Logging Setup** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- [Chapter 1, “Configuring Logging Policies on Firewall Devices”](#)

Field Reference

Table 1-10 Logging Setup Page

Element	Description
Enable Logging	Turns on logging for the main security appliance.
Enable Logging on the Failover Standby Unit	Turns on logging for the standby security appliance, if available.
Send syslogs in EMBLEM format (PIX7.x+, ASA, FWSM 3.x+)	Enables EMBLEM format logging for every logging destination. If you enable EMBLEM, you must use the UDP protocol to publish syslog messages; EMBLEM is not compatible with TCP. Note This setting is not compatible with CS-MARS.
Send debug messages as syslogs (PIX7.x+, ASA, FWSM 3.x+)	Redirects all the debug trace output to the syslog. The syslog message does not appear in the console if this option is enabled. Therefore, to see debug messages, you must enable logging at the console and configure it as the destination for the debug syslog message number and logging level. The syslog message number used is <i>711011</i> . Default logging level for this syslog is <i>debug</i> .
Memory Size of Internal Buffer (bytes)	Specify the size of the internal buffer to which syslogs is saved if the logging buffer is enabled. When the buffer fills up, it is overwritten. The default is 4096 bytes. The range is 4096 to 1048576.

Table 1-10 Logging Setup Page (Continued)

Element	Description
Specify FTP Server Information (PIX7.x+, ASA, FWSM 3.x+)	
FTP Server Buffer Wrap	To save the buffer contents to the FTP server before it is overwritten, check this box and enter the necessary destination information in the following fields. To remove the FTP configuration, deselect this option.
IP Address	Enter the IP address of the FTP server.
User Name	Enter the user name to use when connecting to the FTP server.
Path	Enter the path, relative to the FTP root, where the buffer contents should be saved.
Password/Confirm	Enter and confirm the password used to authenticate the user name to the FTP server.
Specify flash size	
Flash	To save the buffer contents to the flash memory before it is overwritten, check this box. This option is only available in routed or transparent single mode.
Maximum flash to be used by logging (KB)	Specify the maximum space to be used in the flash memory for logging (in KB). This option is available only in routed or transparent single mode.
Minimum free space to be preserved (KB)	Specifies the minimum free space to be preserved in flash memory (in KB). This option is available only in routed or transparent single mode.
ASDM Logging (PIX7.x+, ASA, FWSM 3.x+)	
Message Queue Size	Specify the queue size for syslogs intended for viewing in ASDM.

Configuring Rate Limit Levels

The Rate Limit page lets you specify the maximum number of log messages of specific types (e.g., “alert” or “critical”), and messages with specific Syslog IDs, that can be generated within given periods of time. You can specify individual limits for each logging level, and each Syslog message ID. If the settings conflict, the Syslog message ID limits take precedence.

The [Add/Edit Rate Limited Syslog Message Dialog Box, page 1-14](#) is used to specify the maximum number of messages that can be generated for a particular Syslog message ID within a given period of time.

The [Add/Edit Rate Limit for Syslog Logging Levels Dialog Box, page 1-13](#) is used to specify the maximum number of messages that can be generated for a particular Syslog logging level within a given period of time.

Related Topics

- [Rate Limit Page, page 1-12](#)

Follow these steps to manage rate limits for message logging:

-
- Step 1** Access the Rate Limit page by doing one of the following:
- (Device view) Select **Platform > Logging > Syslog > Rate Limit** from the Device Policy selector.

- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > Rate Limit** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new policy.

Step 2 Add, edit and delete rate limits for Syslog logging levels:

- To specify the maximum number of messages that can be generated within a given period of time for particular logging level, click the **Add Row** button under the Rate Limits for Syslog Logging Levels table to open the [Add/Edit Rate Limit for Syslog Logging Levels Dialog Box, page 1-13](#). Choose a logging level and define a rate limit.
- To edit the rate limit for a particular logging level, select the appropriate entry in the Rate Limits for Syslog Logging Levels table, and then click the **Edit Row** button under the table to open the [Add/Edit Rate Limit for Syslog Logging Levels Dialog Box, page 1-13](#). Alter the rate limit as necessary.
- To delete a rate limit entry from the Rate Limits for Syslog Logging Levels table, select it and then click the **Delete Row** button under the table. A confirmation dialog box may be displayed; click OK to delete the entry.

Step 3 Add, edit and delete limits for log messages according to message IDs:

- To specify the maximum number of messages that can be generated within a given period of time for particular message ID, click the **Add Row** button under the Individually Rate Limited Syslog Messages table to open the [Add/Edit Rate Limited Syslog Message Dialog Box, page 1-14](#). Choose a Syslog message ID and define a rate limit.
- To edit the rate limit for a particular Syslog message ID, select the appropriate entry in the Individually Rate Limited Syslog Messages table, and then click the **Edit Row** button under the table to open the [Add/Edit Rate Limited Syslog Message Dialog Box, page 1-14](#). Alter the rate limit as necessary.
- To delete a message limit entry from the Individually Rate Limited Syslog Messages table, select it and then click the **Delete Row** button under the table. A confirmation dialog box may be displayed; click OK to delete the entry.

Rate Limit Page

The Rate Limit page allows you to specify the maximum number of log messages of a particular type (for example, alert or critical) that should be generated within a given period of time. You can specify a limit for each logging level and Syslog message ID. If the settings differ, Syslog message ID limits take precedence.

Navigation Path

- (Device view) Select **Platform > Logging > Syslog > Rate Limit** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > Rate Limit** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new policy.

Related Topics

- [Chapter 1, “Configuring Logging Policies on Firewall Devices”](#)
- [Add/Edit Rate Limit for Syslog Logging Levels Dialog Box, page 1-13](#)
- [Add/Edit Rate Limited Syslog Message Dialog Box, page 1-14](#)

Field Reference**Table 1-11** *Rate Limit Page*

Element	Description
Rate Limits for Syslog Logging Levels Table	
Logging Level	The Syslog logging level for which you are specifying a rate limit.
No. of Messages	Maximum number of messages of the specified type allowed in the specified time period.
Interval (seconds)	Number of seconds before the rate limit counter resets.
Individually Rate Limited Syslog Messages Table	
Syslog ID	Identification number of the Syslog message for which you are specifying a rate limit.
No. of Messages	Maximum number of messages with the specified ID allowed in the specified time period.
Interval (seconds)	Number of seconds before the rate limit counter resets.

Add/Edit Rate Limit for Syslog Logging Levels Dialog Box

Using the Add/Edit Rate Limit for Syslog Logging Levels dialog box, you can specify the maximum number of log messages for particular log level that should be generated within a given period of time. You can specify a limit for each logging level or syslog message ID (see [Add/Edit Rate Limited Syslog Message Dialog Box, page 1-14](#)). If the settings differ, the rate limited syslog message-level settings override rate limit logging level settings.

Navigation Path

You can access the Add/Edit Rate Limit for Syslog Logging Levels dialog box from the Rate Limit page. For more information, see [Rate Limit Page, page 1-12](#).

Related Topics

- [Chapter 1, “Configuring Logging Policies on Firewall Devices”](#)
- [Rate Limit Page, page 1-12](#)
- [Add/Edit Rate Limited Syslog Message Dialog Box, page 1-14](#)

Field Reference**Table 1-12** *Add/Edit Rate Limit for Syslog Logging Levels Dialog Box*

Element	Description
Logging Level	The syslog logging level for which you are specifying the rate limit.
Number of Messages	Maximum number of messages of the specified type allowed in the specified time period.
Interval (Seconds)	Number of seconds before the rate limit counter resets.

Add/Edit Rate Limited Syslog Message Dialog Box

Using the Add/Edit Rate Limited Syslog Message dialog box you can specify the maximum number of log messages of a particular Syslog ID that can be generated within a given period of time. You can specify a limit for each syslog message ID or logging level (see [Add/Edit Rate Limit for Syslog Logging Levels Dialog Box, page 1-13](#)). If the settings differ, the rate limited syslog message-level settings override rate limit logging level settings.

Navigation Path

You can access the Add/Edit Rate Limited Syslog Message dialog box from the Rate Limit page. For more information, see [Rate Limit Page, page 1-12](#).

Related Topics

- Chapter 1, “Configuring Logging Policies on Firewall Devices”
- Rate Limit Page, page 1-12
- Add/Edit Rate Limit for Syslog Logging Levels Dialog Box, page 1-13

Field Reference

Table 1-13 Add/Edit Rate Limited Syslog Message Dialog Box

Element	Description
Syslog ID	Identification number of the syslog message for which you are specifying a rate limit.
Number of Messages	Maximum number of messages with the specified ID allowed in the specified time period.
Interval (Seconds)	Number of seconds before the rate limit counter resets.

Configuring Syslog Server Setup

You can configure general syslog server settings to set the facility code to be included in syslog messages that are sent to syslog servers, specify whether a timestamp is included in each message, specify the device ID to include in messages, view and modify the severity levels for messages, and disable the generation of specific messages.

Related Topics

- [Defining Syslog Servers, page 1-18](#)

-
- Step 1** Do one of the following:
- (Device view) Select **Platform > Logging > Syslog > Server Setup** to open the [Server Setup Page, page 1-15](#).
 - (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > Server Setup** from the Policy Type selector. Select an existing policy or create a new one.
- Step 2** Change the basic message configuration as required:
- If your syslog server expects a different facility than the default, select the required facility in the **Facility** list.

- If you want to include the date and time a message was generated in the message, select **Enable Timestamp on Each Syslog Message**.
- If you want to add a device identifier to syslog messages (which is placed at the beginning of the message), select **Enable Syslog Device ID** and then select the type of ID:
 - **Interface**—To use the IP address of the specified interface, regardless of the interface through which the appliance sends the message. Click **Select** to select the interface or the interface role that identifies the interface. Interface roles must map to a single interface.
 - **User Defined ID**—To use a text string (up to 16 characters) of your choosing.
 - **Host Name**—To use the hostname of the device.

Step 3 Use the Syslog Message table to alter the default settings for specific syslog messages. You need to configure rules in this table only if you want to change the default settings. You can change the severity assigned to a message, or you can suppress (disable) the generation of a message.

- To add a rule, click the **Add Row** button and fill in the [Add/Edit Syslog Message Dialog Box](#), page 1-17.

You select the message number whose configuration you want to change, and then select the new severity level, or select **Suppressed** to disable the generation of the message. Typically, you would not change the severity level and disable the message, but you can make changes to both fields if desired. Click **OK** to add the rule to the table.

For a description of message severity levels, see [Logging Levels](#), page 1-17.

- To edit a rule, select it and click the **Edit Row** button, make the desired changes, and click **OK**.
- To delete a rule, select it and click the **Delete Row** button.
- If you are using NetFlow, you can easily disable the generation of syslog messages that have NetFlow equivalents by clicking the **Disable NetFlow Equivalent Syslogs** button. This adds the messages to the table as suppressed messages. Note that if any of these syslog equivalents are already in the table, your existing rules are not overwritten.

Server Setup Page

The Server Setup page allows you to set the facility code to be included in syslog messages that are sent to syslog servers, specify whether a timestamp is included in each message, specify the device ID to include in messages, view and modify the severity levels for messages, and disable the generation of specific messages.

Navigation Path

- (Device view) Select **Platform > Logging > Syslog > Server Setup** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > Server Setup** from the Policy Type selector. Select an existing policy or create a new one.

Related Topics

- [Configuring Syslog Server Setup](#), page 1-14
- [Defining Syslog Servers](#), page 1-18
- [Chapter 1, “Configuring Logging Policies on Firewall Devices”](#)
- [Logging Levels](#), page 1-17

Field Reference

Table 1-14 Server Setup Page

Element	Description
Facility	<p>The syslog facility code that the appliance includes in messages destined for syslog servers. The default is LOCAL4(20), which is what most UNIX systems expect. You can select a facility between LOCAL0(16) and LOCAL7(23).</p> <p>Syslog facility is useful when you have a central syslog monitoring system that needs to distinguish among the various network devices that generate syslog data streams. Because your network devices share the eight available facilities, you might need to change this value.</p>
Enable Timestamp on Each Syslog Message	Whether to include the date and time a message was generated in syslog messages. The default is to not include time stamps.
Enable Syslog Device ID	<p>Whether to configure a device ID in non-EMBLEM-format syslog messages. If you select this option, select one of the following to use as the device ID, which is placed at the start of all syslog messages:</p> <ul style="list-style-type: none"> Interface—The IP address of the selected interface. Enter the name of the interface or click Select to select it from a list (or to select an interface role that specifies the interface). Messages include the IP address of the interface specified, regardless of which interface the adaptive security appliance uses to send the log data to the external server. <p>If you select an interface role, that role must map to a single interface on the device.</p> <ul style="list-style-type: none"> User Defined ID—A text string you define as the device ID. This string can be up to 16 characters, but cannot contain any of the following special characters: & ' " < > ? Host Name—The hostname of the security appliance.
Syslog Message table	<p>Use this table to enable or disable the generation of specific syslog messages, or to change the severity level of a message. If you do not want to constrict which message types are generated, or change any message severity levels, you do not need to configure anything in this table. The table shows the messages you have configured with the message level and whether generation is suppressed (“true” in the table).</p> <ul style="list-style-type: none"> To add a rule, click the Add Row button and fill in the Add/Edit Syslog Message Dialog Box, page 1-17. To edit a rule, select it and click the Edit Row button. To delete a rule, select it and click the Delete Row button.

Table 1-14 Server Setup Page (Continued)

Element	Description
Disable/Enable NetFlow Equivalent Syslogs	<p>If you are using NetFlow logging, you might want to disable the generation of syslog messages that duplicate NetFlow messages. If you click the Disable button, these duplicate syslog messages are added to the Syslog Message table as suppressed messages, and the button is renamed Enable NetFlow Equivalent Syslogs.</p> <p>Clicking the Enable button removes the duplicate syslog messages from the table, meaning that they will no longer be suppressed, and the device will start sending them again. However, if you manually edited any message that was added to the list by the Disable button, the Enable button does not remove them.</p>

Logging Levels

The following table describes logging levels.

Table 1-15 Logging Levels

Logging Level	Type	Description
0	Emergency	System unusable. Generates messages that identify system instabilities.
1	Alerts	Immediate action needed. Generates messages that identify system integrity issues that require immediate administrative action.
2	Critical	Critical condition. Generates messages that identify critical system issues.
3	Errors	Error condition. Generates messages that identify system errors during operation.
4	Warnings	Warning condition. Generates messages that identify system warnings. For example, device might be configured incorrectly.
5	Notifications	Normal but significant condition. Generates messages that identify normal operations that are typically considered significant events.
6	Information	Informational only. Generates messages that identify system information that is typical of day-to-day activity, such as network session records.
7	Debugging	Generates syslog messages that assist you in debugging. Also generates logs that identify the commands issued during FTP sessions and the URLs requested during HTTP sessions. Includes all emergency, alert, critical, error, warning, notification, and information messages.
-	Disabled	No logging.

Add/Edit Syslog Message Dialog Box

The Add/Edit Syslog Message dialog box lets you modify the logging level or suppression setting for a syslog message.

Navigation Path

You can access the Add/Edit Syslog Message dialog box from the [Server Setup Page, page 1-15](#).

Related Topics

- [Chapter 1, “Configuring Logging Policies on Firewall Devices”](#)

Field Reference

Table 1-16 Add/Edit Syslog Message Dialog Box

Element	Description
Syslog ID list	<p>The message log ID of the message whose severity level or suppression setting you want to alter. These values and their corresponding messages are identified in the System Log Message guides for the appropriate product:</p> <p>PIX Firewall</p> <p>http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_system_message_guides_list.html</p> <p>ASA</p> <p>http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html</p> <p>FWSM</p> <p>http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html</p>
Logging Level list	<p>The logging level that you want to assign to the message. For logging levels and descriptions, see Logging Levels, page 1-17.</p> <p>Select (default) to use the default level assigned to the message.</p>
Suppressed	<p>Whether to suppress the generation of the syslog message. Suppressing a message disables its generation, so you will not see it in syslogs.</p>

Defining Syslog Servers

The Syslog Servers page lets you specify the syslog servers to which the security appliance will send syslog messages. To make use of the syslog servers you define, you must enable logging using the Logging Setup page and set up the appropriate filters for destinations using the Logging Filters page.

**Tip**

If you want to view events from an ASA device using Security Manager Event Viewer, ensure that you define the Security Manager server as a syslog server. Also, if you use CS-MARS or other applications to manage syslog events, include those servers in this policy.

By directing syslog records generated by a security appliance to a syslog server, you can process and study the records.

Before You Begin

Enable logging. See [Configuring Logging Setup, page 1-9](#).

Related Topics

- [Syslog Servers Page, page 1-19](#)
- [Add/Edit Syslog Server Dialog Box, page 1-20](#)

-
- Step 1** Select **Platform > Logging > Syslog > Syslog Servers** to display the Syslog Servers page.
- Step 2** Do one of the following:
- To add a new syslog target, click the **Add Row** button.
 - To edit an existing syslog target, select the check box for the row, then click the **Edit Row** button.
- Step 3** Enter or select the interface name in the **Interface** field.
The list displays all interfaces defined at the current scope.
- Step 4** Enter or select the IP address of the syslog server in the **IP Address** field.
- Step 5** Determine whether to use UDP or TCP, then click the appropriate radio button under Protocol.
- Step 6** Enter the port from which the security appliance sends either UDP or TCP syslog messages. The port must be the same port on which the syslog server listens.
- TCP—1470 (Default). TCP ports work only with a security appliance syslog server.
 - UDP—514 (Default).
- Step 7** To generate syslog messages using the EMBLEM format, select the **Log messages in Cisco EMBLEM format** check box.
To enable this option, you must select UDP protocol to publish messages to this syslog server.
- Step 8** Click **OK**.
The definition appears in the Syslog Servers table.
-

Syslog Servers Page

The Syslog Servers page lets you specify the syslog servers to which the security appliance sends syslog messages. To make use of the syslog servers you define, you must enable logging using the Logging Setup page and set up the appropriate filters for destinations using the Logging Filters page.

**Tip**

If you want to view events from an ASA device using Security Manager Event Viewer, ensure that you define the Security Manager server as a syslog server. Also, if you use CS-MARS or other applications to manage syslog events, include those servers in this policy.

Navigation Path

- (Device view) Select **Platform > Logging > Syslog > Syslog Servers** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > Syslog Servers** from the Policy Type selector. Select an existing policy or create a new one.

Related Topics

- [Defining Syslog Servers, page 1-18](#)

- Chapter 1, “Configuring Logging Policies on Firewall Devices”

Field Reference

Table 1-17 Syslog Servers Page

Element	Description
Syslog Servers table	<p>The syslog servers to which this device sends syslog messages. The table shows the device interface that publishes messages to the server, the server’s IP address, syslog protocol and port number, and whether the messages are in Cisco EMBLEM syslog format.</p> <p>There is a limit of four syslog servers that can be set up per context.</p> <ul style="list-style-type: none"> • To add a server, click the Add Row button and fill in the Add/Edit Syslog Server Dialog Box, page 1-20. • To edit a server, select it and click the Edit Row button. • To delete a server, select it and click the Delete Row button.
Queue Size	Specifies the size of the queue for storing syslog messages on the security appliance when syslog server is busy. Minimum is 1 message. Default is 512. Specify 0 to allow an unlimited number of messages to be queued (subject to available block memory).
Allow user traffic to pass when TCP syslog server is down	Whether to restrict all traffic if any syslog server that is using the TCP protocol is down.

Add/Edit Syslog Server Dialog Box

The Add/Edit Syslog Servers dialog box lets you add or edit the syslog servers to which the security appliance will send syslog messages. To make use of the syslog servers you define, you must enable logging using the Logging Setup page and set up the appropriate filters for destinations using the Logging Filters page.



Note

There is a limit of four syslog servers that can be set up per context.

Navigation Path

You can access the Add Syslog Servers dialog box from the Syslog Servers page. For more information about the Syslog Servers page, see [Syslog Servers Page](#), page 1-19.

Related Topics

- [Defining Syslog Servers](#), page 1-18
- Chapter 1, “Configuring Logging Policies on Firewall Devices”

Field Reference

Table 1-18 Add/Edit Syslog Server Dialog Box

Element	Description
Interface	The interface used to communicate with the syslog server. Enter the name of the interface or interface role object, or click Select to select it from a list or to create a new object.
IP Address	The IP address of syslog server. Enter the IP address or the name of the network/host policy object that defines the address, or click Select to select the network/host object.
Protocol	The protocol used by syslog server, either TCP or UDP. UDP is the default. TCP ports work only with a security appliance syslog server. Note You must select UDP if you intend to use the EMBLEM format.
Port	The TCP or UDP port from which the security appliance sends syslog messages and on which the syslog server receives them. The default ports for each protocol are: <ul style="list-style-type: none"> • TCP—1470. • UDP—514. Tip If you are defining the Security Manager server as a syslog server, you can find the port number on the Security Manager Administration Event Management Page , page 1-20. Note During the installation or upgrade of Security Manager, the Common Services syslog service port is changed from 514 to 49514. Later, if Security Manager is uninstalled, the port is not reverted to 514.
Log messages in Cisco EMBLEM format (UDP only)	Whether to log messages in Cisco EMBLEM format. The syslog server must use UDP. Note If the syslog server is a Cisco Security MARS appliance, do not select this option. Cisco Security MARS does not process the EMBLEM format.

