



CHAPTER 24

Monitoring the Firewall Services Module

This chapter describes how to configure logging and SNMP for the FWSM. It also describes the contents of syslog messages and the syslog message format.

This chapter does not provide comprehensive information about all monitoring, logging, and SNMP commands and options. For detailed descriptions and additional commands, see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*.

This chapter includes the following sections:

- [Configuring and Managing Syslog Messages, page 24-1](#)
- [Configuring SNMP, page 24-20](#)

Configuring and Managing Syslog Messages

This section describes the logging functionality and configuration. It also describes the syslog message format, options, and variables. This section includes the following topics:

- [Logging Overview, page 24-1](#)
- [Enabling and Disabling Logging, page 24-2](#)
- [Configuring Log Output Destinations, page 24-3](#)
- [Filtering Syslog Messages, page 24-11](#)
- [Customizing the Log Configuration, page 24-14](#)
- [Understanding Syslog Messages, page 24-19](#)

Logging Overview

The FWSM supports the generation of an audit trail of syslog messages that describe its activities (for example, what kinds of network traffic has been allowed and denied) and enables you to configure system logging.

All syslog messages have a default severity level. You can reassign a message to a new severity level, if necessary. When you choose a severity level, logging messages from that level and lower levels are generated. Messages from a higher level are not included. The higher the severity level, the more messages are included. For more information about logging and syslog messages, see *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module System Log Messages*.

The FWSM syslog messages provide you with information for monitoring and troubleshooting the FWSM. Using the logging feature, you can do the following:

- Specify which syslog messages should be logged.
- Disable or change the severity level of a syslog message.
- Specify the severity level of a syslog message by color.
- Display a brief description of the syslog message as a tooltip.
- Specify explanations and recommended actions for a syslog message.
- Specify one or more locations to which syslog messages should be sent, including an internal buffer, one or more syslog servers, an SNMP management station, specified e-mail addresses, or Telnet and SSH sessions.
- Configure and manage syslog messages in groups, such as by severity level or class of message.
- Specify what happens to the contents of the internal buffer when the buffer becomes full: overwrite the buffer, send the buffer contents to an FTP server, or save the contents to internal flash memory.
- Send all syslog messages, or subsets of syslog messages, to any or all output locations.
- Filter which syslog messages are sent to which locations by the severity of the syslog message, the class of the syslog message, or by creating a custom log message list.

Security Contexts and Logging

Each security context includes its own logging configuration and generates its own messages. If you log in to the system or admin context, and then change to another context, messages you view in your session are only those that are related to the current context.

Syslog messages that are generated in the system execution space, including failover messages, are viewed in the admin context along with messages generated in the admin context. You cannot configure logging or view any logging information in the system execution space.

You can configure the FWSM to include the context name with each message, which helps you differentiate context messages that are sent to a single syslog server. This feature also helps you to determine which messages are from the admin context and which are from the system; messages that originate in the system execution space use a device ID of **system**, and messages that originate in the admin context use the name of the admin context as the device ID. For more information about enabling logging device IDs, see the [“Including the Device ID in Syslog Messages”](#) section on page 24-15.

Enabling and Disabling Logging

This section describes how to enable and disable logging on the FWSM. It includes the following topics:

- [Enabling Logging to All Configured Output Destinations, page 24-2](#)
- [Disabling Logging to All Configured Output Destinations, page 24-3](#)
- [Viewing the Log Configuration, page 24-3](#)

Enabling Logging to All Configured Output Destinations

The following command enables logging; however, you must also specify at least one output destination so that you can view or save the logged messages. If you do not specify an output destination, the FWSM does not save syslog messages that are generated when events occur.

For more information about configuring log output destinations, see the “[Configuring Log Output Destinations](#)” section on page 24-3.

To enable logging, enter the following command:

```
hostname(config)# logging enable
```

Disabling Logging to All Configured Output Destinations

To disable all logging to all configured log output destinations, enter the following command:

```
hostname(config)# no logging enable
```

Viewing the Log Configuration

To view the running log configuration, enter the following command:

```
hostname(config)# show logging
```

The following is sample output of the **show logging** command:

```
Syslog logging: enabled
  Facility: 16
  Timestamp logging: disabled
  Standby logging: disabled
  Deny Conn when Queue Full: disabled
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: disabled
  Trap logging: level errors, facility 16, 3607 messages logged
    Logging to infrastructure 10.1.2.3
  History logging: disabled
  Device ID: 'inside' interface IP address "10.1.1.1"
  Mail logging: disabled
  ASDM logging: disabled
```

Configuring Log Output Destinations

This section describes how to specify where the FWSM should save or send the log messages it generates. To view syslog messages generated by the FWSM, you must specify a log output destination. If you enable logging without specifying a log output destination, the FWSM generates messages but does not save them to a location from which you can view them.

This section includes the following topics:

- [Sending Syslog Messages to a Syslog Server, page 24-4](#)
- [Sending Syslog Messages to an E-mail Address, page 24-5](#)
- [Sending Syslog Messages to ASDM, page 24-6](#)
- [Sending Syslog Messages to a Switch Session, Telnet Session, or SSH Session, page 24-7](#)
- [Sending Syslog Messages to the Log Buffer, page 24-8](#)

Sending Syslog Messages to a Syslog Server

This section describes how to configure the FWSM to send syslog messages to a syslog server.

Configuring the FWSM to send syslog messages to a syslog server enables you to archive syslog messages, limited only by the available disk space on the server, and it enables you to manipulate log data after it is saved. For example, you could specify actions to be executed when certain types of syslog messages are logged, extract data from the log and save the records to another file for reporting, or track statistics using a site-specific script.

The syslog server must run a program (known as a server) called `syslogd`. UNIX provides a syslog server as part of its operating system. For Windows 95 and Windows 98, obtain a `syslogd` server from another vendor.



Note

To start logging to a syslog server you define in this procedure, be sure to enable logging for all output locations. See the “[Enabling Logging to All Configured Output Destinations](#)” section on page 24-2. To disable logging, see the “[Disabling Logging to All Configured Output Destinations](#)” section on page 24-3.

To configure the FWSM to send syslog messages to a syslog server, perform the following steps:

Step 1 To designate a syslog server to receive the syslog messages, enter the following command:

```
hostname(config)# logging host interface_name ip_address [tcp[/port] | udp[/port]]
[format emblem]
```

Where the **format emblem** keyword enables EMBLEM format logging for the syslog server (UDP only).

The *interface_name* argument specifies the interface through which you access the syslog server.

The *ip_address* argument specifies the IP address of the syslog server.

The **tcp[/port]** or **udp[/port]** argument specifies that the FWSM should use TCP or UDP to send syslog messages to the syslog server. The default protocol is UDP. You can configure the FWSM to send data to a syslog server using either UDP or TCP, but not both. If you specify TCP, the FWSM discovers when the syslog server fails and discontinues sending syslog messages. If you specify UDP, the FWSM continues to send syslog messages regardless of whether the syslog server is operational. The *port* argument specifies the port that the syslog server listens to for syslog messages. Valid port values are 1025 through 65535, for either protocol. The default UDP port is 514. The default TCP port is 1470.

For example:

```
hostname(config)# logging host dmz1 192.168.1.5
```

If you want to designate more than one syslog server as an output destination, enter a new command for each syslog server.

Step 2 To specify which syslog messages should be sent to the syslog server, enter the following command:

```
hostname(config)# logging trap {severity_level | message_list}
```

Where the *severity_level* argument specifies the severity levels of messages to be sent to the syslog server. You can specify the severity level number (0 through 7) or name. For severity level names, see the “[Severity Levels](#)” section on page 24-19. For example, if you set the severity level to 3, then the FWSM sends syslog messages for severity levels 3, 2, 1, and 0.

The *message_list* argument specifies a customized message list that identifies the syslog messages to send to the syslog server. For information about creating custom message lists, see the “[Filtering Syslog Messages with Custom Message Lists](#)” section on page 24-13.

The following example specifies that the FWSM should send to the syslog server all syslog messages with a severity level of 3 (errors) and higher. The FWSM will send messages with the severity level of 3, 2, and 1.

```
hostname(config)# logging trap errors
```

- Step 3** (Optional) If needed, set the logging facility to a value other than its default of 20 by entering the following command:

```
hostname(config)# logging facility number
```

Most UNIX systems expect the syslog messages to arrive at facility 20.

```
hostname(config)# logging
```

- Step 4** (Optional) To continue to pass traffic when the TCP syslog server is down, enter the following command:

```
hostname(config)# logging permit-hostdown
```

Where the **permit-hostdown** keyword allows new network access sessions for a TCP-based syslog server.

Sending Syslog Messages to an E-mail Address

You can configure the FWSM to send some or all syslog messages to an e-mail address. When sent by e-mail, a syslog message appears in the subject line of the e-mail message. For this reason, we recommend configuring this option to notify administrators of syslog messages with high severity levels, such as critical, alert, and emergency.



Note

To start logging to an e-mail address you define in this procedure, be sure to enable logging for all output locations. See the [“Enabling Logging to All Configured Output Destinations”](#) section on page 24-2. To disable logging, see the [“Disabling Logging to All Configured Output Destinations”](#) section on page 24-3.

To designate an e-mail address as an output destination, perform the following steps:

- Step 1** To specify the syslog messages to be sent to one or more e-mail addresses, enter the following command:

```
hostname(config)# logging mail {severity_level | message_list}
```

Where the *severity_level* argument specifies the severity levels of messages to be sent to the e-mail address. You can specify the severity level number (0 through 7) or name. For severity level names, see the [“Severity Levels”](#) section on page 24-19. For example, if you set the severity level to 3, then the FWSM sends syslog messages for severity levels 3, 2, 1, and 0.

The *message_list* argument specifies a customized message list that identifies the syslog messages to send to the e-mail address. For information about creating custom message lists, see the [“Filtering Syslog Messages with Custom Message Lists”](#) section on page 24-13.

The following example uses a *message_list* with the name “high-priority,” previously set up with the **logging list** command:

```
hostname(config)# logging mail high-priority
```

- Step 2** To specify the source e-mail address to be used when sending syslog messages to an e-mail address, enter the following command:

```
hostname(config)# logging
from-address email_address
```

For example:

```
hostname(config)# logging from-address xxx-001@example.com
```

- Step 3** Specify the recipient e-mail address to be used when sending syslog messages to an e-mail destination. You can configure up to five recipient addresses. You must enter each recipient separately.

To specify a recipient address, enter the following command:

```
hostname(config)# logging recipient-address e-mail_address [severity_level]
```

If a severity level is not specified, the default severity level is used (error condition, severity level 3).

For example:

```
hostname(config)# logging recipient-address admin@example.com
```

- Step 4** To specify the SMTP server to be used when sending syslog messages to an e-mail destination, enter the following command:

```
hostname(config)# smtp-server ip_address
```

For example:

```
hostname(config)# smtp-server 10.1.1.1
```

Sending Syslog Messages to ASDM

You can configure the FWSM to send syslog messages to ASDM. The FWSM sets aside a buffer area for syslog messages waiting to be sent to ASDM and saves messages in the buffer as they occur. The ASDM log buffer is a different buffer than the internal log buffer. For information about the internal log buffer, see the [“Sending Syslog Messages to the Log Buffer”](#) section on page 24-8.

When the ASDM log buffer is full, the FWSM deletes the oldest syslog message to make room in the buffer for new syslog messages. To control the number of syslog messages retained in the ASDM log buffer, you can change the size of the buffer.

This section includes the following topics:

- [Configuring Logging for ASDM, page 24-6](#)
- [Clearing the ASDM Log Buffer, page 24-7](#)

Configuring Logging for ASDM



Note

To start logging to ASDM as defined in this procedure, be sure to enable logging for all output locations. See the [“Enabling Logging to All Configured Output Destinations”](#) section on page 24-2. To disable logging, see the [“Disabling Logging to All Configured Output Destinations”](#) section on page 24-3.

To specify ASDM as an output destination, perform the following steps:

- Step 1** To specify which syslog messages should go to ASDM, enter the following command:

```
hostname(config)# logging asdm {severity_level | message_list}
```

where the *severity_level* argument specifies the severity levels of messages to be sent to ASDM. You can specify the severity level number (0 through 7) or name. For severity level names, see the “[Severity Levels](#)” section on page 24-19. For example, if you set the level to 3, then the FWSM sends syslog messages for severity levels 3, 2, 1, and 0.

The *message_list* argument specifies a customized message list that identifies the syslog messages to send to ASDM. For information about creating custom message lists, see the “[Filtering Syslog Messages with Custom Message Lists](#)” section on page 24-13.

The following example shows how to enable logging and send syslog messages of severity levels 0, 1, and 2 to the ASDM log buffer:

```
hostname(config)# logging asdm 2
```

- Step 2** To specify the number of syslog messages retained in the ASDM log buffer, enter the following command:

```
hostname(config)# logging asdm-buffer-size num_of_msgs
```

where *num_of_msgs* specifies the number of syslog messages that the FWSM retains in the ASDM log buffer.

The following example shows how to set the ASDM log buffer size to 200 syslog messages:

```
hostname(config)# logging asdm-buffer-size 200
```

Clearing the ASDM Log Buffer

To erase the current contents of the ASDM log buffer, enter the following command:

```
hostname(config)# clear logging asdm
```

Sending Syslog Messages to a Switch Session, Telnet Session, or SSH Session

When you log in to the FWSM from the switch, you are connected using a Telnet session. Therefore, you configure logging to a switch session the same way as you configure logging to a Telnet or SSH session.

Viewing syslog messages in a Telnet or SSH session requires two steps:

1. Specify which messages should be sent to a Telnet or SSH session.
2. View syslog messages in the current session.

This section includes the following topics:

- [Configuring Logging for Telnet and SSH Sessions, page 24-8](#)
- [Viewing Syslog Messages in the Current Session, page 24-8](#)

Configuring Logging for Telnet and SSH Sessions



Note

To start logging to a Telnet or SSH session as defined in this procedure, be sure to enable logging for all output locations. See the “[Enabling Logging to All Configured Output Destinations](#)” section on page 24-2. To disable logging, see the “[Disabling Logging to All Configured Output Destinations](#)” section on page 24-3.

To specify which messages should be sent to a Telnet or SSH session, enter the following command:

```
hostname(config)# logging monitor {severity_level | message_list}
```

Where the *severity_level* argument specifies the severity levels of messages to be sent to the session. You can specify the severity level number (0 through 7) or name. For severity level names, see the “[Severity Levels](#)” section on page 24-19. For example, if you set the severity level to 3, then the FWSM sends syslog messages for severity levels 3, 2, 1, and 0.

The *message_list* argument specifies a customized message list that identifies the syslog messages to send to the session. For information about creating custom message lists, see the “[Filtering Syslog Messages with Custom Message Lists](#)” section on page 24-13.

Viewing Syslog Messages in the Current Session

To enable logging in the current session, perform the following steps:

-
- Step 1** After you log in to the FWSM, enable logging for the current session by entering the following command:

```
hostname# terminal monitor
```

This command enables logging only for the current session. If you log out, and then log in again, you need to reenter this command.

- Step 2** To disable logging for the current session, enter the following command:

```
hostname(config)# terminal no monitor
```

Sending Syslog Messages to the Log Buffer

If configured as an output destination, the log buffer serves as a temporary storage location for syslog messages. New messages are appended to the end of the listing. When the buffer is full, (that is, when the buffer wraps), old messages are overwritten as new messages are generated, unless you configure the FWSM to save the full buffer to another location.

This section includes the following topics:

- [Enabling the Log Buffer as an Output Destination, page 24-9](#)
- [Viewing the Log Buffer, page 24-9](#)
- [Automatically Saving the Full Log Buffer to Flash Memory, page 24-10](#)
- [Automatically Saving the Full Log Buffer to an FTP Server, page 24-10](#)
- [Saving the Current Contents of the Log Buffer to Internal Flash Memory, page 24-10](#)
- [Clearing the Contents of the Log Buffer, page 24-11](#)

Enabling the Log Buffer as an Output Destination



Note

To start logging to the buffer as defined in this procedure, be sure to enable logging for all output locations. See the “[Enabling Logging to All Configured Output Destinations](#)” section on page 24-2. To disable logging, see the “[Disabling Logging to All Configured Output Destinations](#)” section on page 24-3.

To enable the log buffer as a log output destination, enter the following command:

```
hostname(config)# logging buffered {severity_level | message_list}
```

Where the *severity_level* argument specifies the severity levels of messages to be sent to the buffer. You can specify the severity level number (0 through 7) or name. For severity level names, see the “[Severity Levels](#)” section on page 24-19. For example, if you set the severity level to 3, then the FWSM sends syslog messages for severity levels 3, 2, 1, and 0.

The *message_list* argument specifies a customized message list that identifies the syslog messages to send to the buffer. For information about creating custom message lists, see the “[Filtering Syslog Messages with Custom Message Lists](#)” section on page 24-13.

For example, to specify that messages with severity levels 1 and 2 should be saved in the log buffer, enter one of the following commands:

```
hostname(config)# logging buffered critical
```

or

```
hostname(config)# logging buffered level 2
```

For the *message_list* option, specify the name of a message list containing criteria for selecting messages to be saved in the log buffer.

```
hostname(config)# logging buffered notif-list
```

Viewing the Log Buffer

To view the log buffer, enter the following command:

```
hostname(config)# show logging
```

Changing the Log Buffer Size

By default, the log buffer size is 4 KB. To change the size of the log buffer, enter the following command:

```
hostname(config)# logging buffer-size bytes
```

Where the *bytes* argument sets the amount of memory used for the log buffer, in bytes. For example, if you specify 8192, the FWSM uses 8 KB of memory for the log buffer.

The following example specifies that the FWSM uses 16 KB of memory for the log buffer:

```
hostname(config)# logging buffer-size 16384
```

Automatically Saving the Full Log Buffer to Flash Memory

Unless configured otherwise, the FWSM sends messages to the log buffer on a continuing basis, overwriting old messages when the buffer is full. If you want to keep a history of syslog messages, you can configure the FWSM to send the buffer contents to another output location each time the buffer fills. Buffer contents can be saved either to internal flash memory or to an FTP server.

When saving the buffer content to another location, the FWSM creates log files with names that use a default time-stamp format, as follows:

```
LOG-YYYY-MM-DD-HHMMSS.TXT
```

Where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

While the FWSM writes the log buffer contents to internal flash memory or an FTP server, it continues saving new messages to the log buffer.

To specify that messages in the log buffer should be saved to internal flash memory each time the buffer wraps, enter the following command:

```
hostname(config)# logging flash-bufferwrap
```

Automatically Saving the Full Log Buffer to an FTP Server

For more information about saving the buffer, see the [“Saving the Current Contents of the Log Buffer to Internal Flash Memory”](#) section.

To specify that messages in the log buffer should be saved to an FTP server each time the buffer wraps, perform the following steps:

Step 1 To enable the FWSM to send the log buffer contents to an FTP server each time the buffer wraps, enter the following command:

```
hostname(config)# logging ftp-bufferwrap
```

Step 2 To identify the FTP server, enter the following command:

```
hostname(config)# logging ftp-server server path username password
```

where the *server* argument specifies the IP address of the external FTP server.

The *path* argument specifies the directory path on the FTP server where the log buffer data is to be saved. This path is relative to the FTP root directory.

The *username* argument specifies a username that is valid for logging in to the FTP server.

The *password* argument specifies the password for the username specified.

For example:

```
hostname(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs
```

Saving the Current Contents of the Log Buffer to Internal Flash Memory

At any time, you can save the contents of the buffer to internal flash memory. To save the current contents of the log buffer to internal flash memory, enter the following command:

```
hostname(config)# logging savefile [savefile]
```

For example, the following command saves the contents of the log buffer to internal flash memory using the filename, latest-logfile.txt:

```
hostname(config)# logging savefile latest-logfile.txt
```

Clearing the Contents of the Log Buffer

To delete the contents of the log buffer, enter the following command:

```
hostname(config)# clear logging buffer
```

Filtering Syslog Messages

This section describes how to specify which syslog messages should go to output destinations, and includes the following topics:

- [Message Filtering Overview, page 24-11](#)
- [Filtering Syslog Messages by Class, page 24-11](#)
- [Filtering Syslog Messages with Custom Message Lists, page 24-13](#)

Message Filtering Overview

You can filter generated syslog messages so that only certain syslog messages are sent to a particular output destination. For example, you could configure the FWSM to send all syslog messages to one output destination and also to send a subset of those syslog messages to a different output destination.

Specifically, you can configure the FWSM so that syslog messages are directed to an output destination according to the following criteria:

- Syslog message ID number
- Syslog message severity level
- Syslog message class (equivalent to a functional area of the FWSM)

You customize these criteria by creating a message list that you can specify when you set the output destination in the [“Configuring Log Output Destinations” section on page 24-3](#).

Alternatively, you can configure the FWSM to send a particular message class to each type of output destination independently of the message list.

For example, you could configure the FWSM to send to the internal log buffer all syslog messages with severity levels of 1, 2 and 3, send all syslog messages in the “ha” class to a particular syslog server, or create a list of messages that you name “high-priority” that are sent to an e-mail address to notify system administrators of a possible problem.

Filtering Syslog Messages by Class

The syslog message class provides a method of categorizing syslog messages by type, equivalent to a feature or function of the FWSM. For example, the “auth” class denotes user authentication.

This section includes the following topics:

- [Message Class Overview, page 24-12](#)
- [Sending All Messages in a Class to a Specified Output Destination, page 24-12](#)

Message Class Overview

With logging classes, you can specify an output location for an entire category of syslog messages with a single command.

You can use syslog message classes in two ways:

- Issue the **logging class** command to specify an output location for an entire category of syslog messages.
- Create a message list using the **logging list** command that specifies the message class. For instructions, see the [“Filtering Syslog Messages with Custom Message Lists” section on page 24-13](#).

All syslog messages in a particular class share the same initial three digits in their syslog message ID numbers. For example, all syslog message IDs that begin with the digits 400 are associated with the `ids` class. Syslog messages associated with the IDS feature range from 400400 to 400415.

Sending All Messages in a Class to a Specified Output Destination

When you configure all messages in a class to go to a type of output destination, this configuration overrides the configuration in the specific output destination command. For example, if you specify that messages at severity level 7 should go to the log buffer, and you also specify that a class messages at severity level 3 should go to the buffer, then the latter configuration takes precedence.

To configure the FWSM to send an entire syslog message class to a configured output destination, enter the following command:

```
hostname(config)# logging class message_class {buffered | history | mail | monitor | trap}
[severity_level]
```

Where the `message_class` argument specifies a class of syslog messages to be sent to the specified output destination. See [Table 24-1](#) for a list of syslog message classes.

The **buffered**, **history**, **mail**, **monitor**, and **trap** keywords specify the output destination to which syslog messages in this class should be sent. The **history** keyword enables SNMP logging. The **monitor** keyword enables Telnet and SSH logging. The **trap** keyword enables syslog server logging. Select one destination per command-line entry. If you want to specify that a class should go to more than one destination, enter a new command for each output destination.

The `severity_level` argument further restricts the syslog messages to be sent to the output destination by specifying a severity level. For more information about message severity levels, see the [“Severity Levels”](#) section on page 24-19.

The following example specifies that all syslog messages related to the class `ha` (high availability, also known as failover) with a severity level of 1 (alerts) should be sent to the internal logging buffer.

```
hostname(config)# logging class ha buffered alerts
```

[Table 24-1](#) lists the syslog message classes and the ranges of syslog message IDs associated with each class.

Table 24-1 Syslog Message Classes and Associated Message ID Numbers

Class	Definition	Syslog 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
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

Table 24-1 Syslog Message Classes and Associated Message ID Numbers (continued)

Class	Definition	Syslog Message ID Numbers
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

Filtering Syslog Messages with Custom Message Lists

Creating a custom message list is a flexible way to exercise fine control over which syslog messages are sent to which output destination. In a custom syslog message list, you specify groups of syslog messages using any or all of the following criteria: severity level, message IDs, ranges of syslog message IDs, or message class.

For example, you can use message lists to:

- Select syslog messages with severity levels of 1 and 2 and send them to one or more e-mail addresses.
- Select all syslog messages associated with a message class (such as “ha”) and save them to the internal buffer.

A message list can include multiple criteria for selecting messages. However, you must add each message selection criterion with a new command entry. You can create a message list containing overlapping message selection criteria. If two criteria in a message list select the same message, the message is logged only once.

To create a customized list that the FWSM can use to select messages to be saved in the log buffer, perform the following steps:

Step 1 Create a message list containing criteria for selecting messages by entering the following command:

```
hostname(config)# logging list name {level level [class message_class] |
message start_id[-end_id]}
```

Where the *name* argument specifies the name of the list. Do not use the names of severity levels as the name of a syslog message list. Prohibited names include “emergency,” “alert,” “critical,” “error,” “warning,” “notification,” “informational,” and “debugging.” Similarly, do not use the first three characters of these words at the beginning of a filename. For example, do not use a filename that starts with the characters “err.”

The **level** *level* argument specifies the severity level. You can specify the severity level number (0 through 7) or name. For severity level names, see the “Severity Levels” section on page 24-19. For example, if you set the severity level to 3, then the FWSM sends syslog messages for severity levels 3, 2, 1, and 0.

The **class** *message_class* argument specifies a particular message class. For a list of class names, see Table 24-1 on page 24-12.

The **message** *start_id[-end_id]* argument specifies an individual syslog message ID number or a range of numbers.

The following example creates a message list named `notif-list` that specifies messages with a severity level of 3 or higher should be saved in the log buffer:

```
hostname(config)# logging list notif-list level 3
```

Step 2 (Optional) If you want to add more criteria for message selection to the list, enter the same command as in the previous step specifying the name of the existing message list and the additional criterion. Enter a new command for each criterion you want to add to the list.

The following example adds criteria to the message list: a range of message ID numbers, and the message class ha (high availability or failover).

```
hostname(config)# logging list notif-list 104024-105999
hostname(config)# logging list notif-list level critical
hostname(config)# logging list notif-list level warning class ha
```

The preceding example states that syslog messages that match the criteria specified will be sent to the output destination. The specified criteria for syslog messages to be included in the list are:

- Syslog message IDs that fall in the range of 104024 to 105999
- All syslog messages with the level of critical or higher (emergency, alert, or critical)
- All ha class syslog messages with a severity level of warning or higher (emergency, alert, critical, error, or warning)

A syslog message is logged if it satisfies any of these conditions. If a syslog message satisfies more than one of the conditions, the message is logged only once.

Customizing the Log Configuration

This section describes other options for fine tuning the logging configuration. It includes the following topics:

- [Configuring the Logging Queue, page 24-15](#)
- [Including the Date and Time in Syslog Messages, page 24-15](#)
- [Including the Device ID in Syslog Messages, page 24-15](#)
- [Generating Syslog Messages in EMBLEM Format, page 24-16](#)
- [Disabling a Syslog Message, page 24-16](#)
- [Changing the Severity Level of a Syslog Message, page 24-17](#)
- [Changing the Amount of Internal Flash Memory Available for Syslog Messages, page 24-18](#)

Configuring the Logging Queue

The FWSM has a fixed number of blocks in memory that can be allocated for buffering syslog messages while they are waiting to be sent to the configured output destination. The number of blocks required depends on the length of the syslog message queue and the number of syslog servers specified.

To specify the number of syslog messages the FWSM can hold in its queue before sending them to the configured output destination, enter the following command:

```
hostname(config)# logging queue message_count
```

where the *message_count* variable specifies the number of syslog messages that can remain in the syslog message queue while awaiting processing. The default is 512 syslog messages. A setting of 0 (zero) indicates unlimited syslog messages, that is, the queue size is limited only by block memory availability.

To view the queue and queue statistics, enter the following command:

```
hostname(config)# show logging queue
```

Including the Date and Time in Syslog Messages

To specify that syslog messages should include the date and time that the syslog messages was generated, enter the following command:

```
hostname(config)# logging timestamp
```

Including the Device ID in Syslog Messages

To configure the FWSM to include a device ID in non-EMBLEM-format syslog messages, enter the following command:

```
hostname(config)# logging device-id {context-name | hostname | ipaddress interface_name | string text}
```

You can specify only one type of device ID for the syslog messages.

The **context-name** keyword indicates that the name of the current context should be used as the device ID (applies to multiple context mode only). If you enable the logging device ID for the admin context in multiple context mode, messages that originate in the system execution space use a device ID of **system**, and messages that originate in the admin context use the name of the admin context as the device ID.

The **hostname** keyword specifies that the hostname of the FWSM should be used as the device ID.

The **ipaddress interface_name** argument specifies that the IP address of the interface specified as *interface_name* should be used as the device ID. If you use the **ipaddress** keyword, the device ID becomes the specified FWSM interface IP address, regardless of the interface from which the syslog message is sent. This keyword provides a single, consistent device ID for all syslog messages that are sent from the device.

The **string text** argument specifies that the text string should be used as the device ID. The string can contain up to 16 characters. You cannot use blank spaces or any of the following characters:

- & (ampersand)
- ' (single quote)
- " (double quote)
- < (less than)
- > (greater than)
- ? (question mark)



Note

If enabled, the device ID does not appear in EMBLEM-formatted syslog messages or SNMP traps.

The following example enables the logging device ID for the security appliance:

```
hostname(config)# logging device-id hostname
```

The following example enables the logging device ID for a security context on the security appliance:

```
hostname(config)# logging device-id context-name
```

Generating Syslog Messages in EMBLEM Format

To use the EMBLEM format for syslog messages sent to a syslog server over UDP, specify the **format emblem** option when you configure the syslog server as an output destination by entering the following command:

```
hostname(config)# logging host interface_name ip_address {tcp[/port] | udp[/port]}
[format emblem]
```

Where the *interface_name* and *IP_address* specify the syslog server to receive the syslog messages, **tcp[/port]** and **udp[/port]** indicate the protocol and port that should be used, and **format emblem** enables EMBLEM formatting for messages sent to the syslog server.

The security appliance can send syslog messages using either the UDP or TCP protocol; however, you can enable the EMBLEM format only for messages sent over UDP. The default protocol and port are UDP and 514.

For example:

```
hostname(config)# logging host interface_1 122.243.006.123 udp format emblem
```

To use the EMBLEM format for syslog messages sent to destinations other than a syslog server, enter the following command:

```
hostname(config)# logging emblem
```

For more information about syslog servers, see the [“Sending Syslog Messages to a Syslog Server” section on page 24-4](#).

Disabling a Syslog Message

To prevent the security appliance from generating a particular syslog message, enter the following command:

```
hostname(config)# no logging message message_number
```

For example:

```
hostname(config)# no logging message 113019
```

To reenabling a disabled syslog message, enter the following command:

```
hostname(config)# logging message message_number
```

For example:

```
hostname(config)# logging message 113019
```

To see a list of disabled syslog messages, enter the following command:

```
hostname(config)# show logging message
```

To reenabling logging of all disabled syslog messages, enter the following command:

```
hostname(config)# clear config logging disabled
```

Changing the Severity Level of a Syslog Message

To specify the logging level of a syslog message, enter the following command:

```
hostname(config)# logging message message_ID level severity_level
```

The following example modifies the severity level of syslog message 113019 from 4 (warnings) to 5 (notifications):

```
hostname(config)# logging message 113019 level 5
```

To reset the logging level of a syslog message to its default level, enter the following command:

```
hostname(config)# no logging message message_ID level current_severity_level
```

The following example modifies the severity level of syslog message 113019 to its default value of 4 (warnings):

```
hostname(config)# no logging message 113019 level 5
```

To see the severity level of a specific message, enter the following command:

```
hostname(config)# show logging message message_ID
```

To see a list of syslog messages with modified severity levels, enter the following command:

```
hostname(config)# show logging message
```

To reset the severity level of all modified syslog messages back to their defaults, enter the following command:

```
hostname(config)# clear configure logging level
```

The series of commands in the following example illustrate the use of the **logging message** command to control both whether a syslog message is enabled and the severity level of the syslog message:

```
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)

hostname(config)# logging message 403503 level 1
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)

hostname(config)# logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503 level 3
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

Changing the Amount of Internal Flash Memory Available for Syslog Messages

You can have the FWSM save the contents of the log buffer to internal flash memory in two ways:

- Configure logging so that the contents of the log buffer are saved to internal flash memory each time the buffer wraps
- Enter a command instructing the FWSM to save the current contents of the log buffer to internal flash memory immediately

By default, the FWSM can use up to 1 MB of internal flash memory for log data. The default minimum amount of internal flash memory that must be free for the FWSM to save log data is 3 MB.

If a log file being saved to internal flash memory would cause the amount of free internal flash memory to fall below the configured minimum limit, the FWSM deletes the oldest log files to ensure that the minimum amount of memory remains free after saving the new log file. If there are no files to delete or if, after all old files are deleted, free memory would still be below the limit, the FWSM fails to save the new log file.

To modify the settings for the amount of internal flash memory available for syslog messages, perform the following steps:

-
- Step 1** To specify the maximum amount of internal flash memory available for saving log files, enter the following command:

```
hostname(config)# logging flash-maximum-allocation kbytes
```

Where *kbytes* specifies the maximum amount of internal flash memory, in kilobytes, that can be used for saving log files.

The following example sets the maximum amount of internal flash memory that can be used for log files to approximately 1.2 MB:

```
hostname(config)# logging flash-maximum-allocation 1200
```

- Step 2** To specify the minimum amount of internal flash memory that must be free for the FWSM to save a log file, enter the following command:

```
hostname(config)# logging flash-minimum-free kbytes
```

Where *kbytes* specifies the minimum amount of internal flash memory, in kilobytes, that must be available before the FWSM saves a new log file.

The following example specifies that the minimum amount of free internal flash memory must be 4000 KB before the FWSM can save a new log file:

```
hostname(config)# logging flash-minimum-free 4000
```

Understanding Syslog Messages

This section describes the contents of syslog messages generated by the security appliance. It includes the following topics:

- [Syslog Message Format, page 24-19](#)
- [Severity Levels, page 24-19](#)

Syslog Message Format

Syslog messages begin with a percent sign (%) and are structured as follows:

```
%FWSM Level Message_number: Message_text
```

Field descriptions are as follows:

FWSM	Identifies the syslog message facility code for messages generated by the security appliance. This value is always FWSM.
Level	Specifies 1 through 7. The level reflects the severity of the condition described by the syslog message. The lower the number, the more severe the condition. For more information, see Table 24-2 .
Message_number	A unique six-digit number that identifies the syslog message.
Message_text	A text string describing the condition. This portion of the syslog message sometimes includes IP addresses, port numbers, or usernames. For a list of variable fields and their descriptions, see <i>Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module System Log Messages</i> .

Severity Levels

[Table 24-2](#) lists the syslog message severity levels.

Table 24-2 Syslog Message Severity Levels

Level Number	Level Keyword	Description
0	emergency	System unusable.
1	alert	Immediate action needed.
2	critical	Critical condition.
3	error	Error condition.
4	warning	Warning condition.
5	notification	Normal but significant condition.
6	informational	Informational message only.
7	debugging	Appears during debugging only.



Note

The security appliance does not generate syslog messages with a severity level of 0 (emergency). This level is provided in the **logging** command for compatibility with the UNIX system log feature, but is not used by the security appliance.

Configuring SNMP

This section describes how to configure SNMP, but does not provide comprehensive information about all SNMP MIBs and traps. For detailed MIB and event notification information, see [Appendix D, “Mapping MIBs to CLI Commands.”](#)

It includes the following topics:

- [SNMP Overview, page 24-20](#)
- [Enabling SNMP, page 24-32](#)

SNMP Overview

The FWSM provides support for network monitoring using SNMP V1 and V2c. The FWSM supports traps and SNMP read access, but does not support SNMP write access.

You can configure the FWSM to send traps (event notifications) to a network management station (NMS), or you can use the NMS to browse the MIBs on the FWSM. MIBs are a collection of definitions, and the FWSM maintains a database of values for each definition. Browsing a MIB entails issuing an SNMP get request from the NMS. Use CiscoWorks for Windows or any other SNMP V1 or V2C, MIB-II-compliant browser to receive SNMP traps and browse a MIB.

Table 24-3 lists supported MIBs and traps for the FWSM and, in multiple mode, for each context. You can download Cisco MIBs from the following website.

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

After you download the MIBs, compile them for your NMS.



Note

Limit the frequency of using SNMP to obtain data, because it might degrade performance. In addition, to collect resource usage data efficiently, schedule polling on a per-context basis.

Table 24-3 SNMP MIB and Trap Support

MIB and Trap	Description
CISCO-CRYPTO-ACCELERATOR-MIB	The FWSM supports browsing of the MIB.
<ul style="list-style-type: none"> • CISCO-ENTITY-MIB • CISCO-ENTITY-ALARM-MIB • CISCO-ENTITY-FRU-CONTROL-MIB • CISCO-ENTITY-REDUNDANCY-MIB 	<p>The FWSM supports browsing of the following groups and tables:</p> <ul style="list-style-type: none"> • entLogicalTable • entPhysicalTable <p>The FWSM sends the following traps:</p> <ul style="list-style-type: none"> • alarm-asserted • alarm-cleared • config-change • fru-insert • fru-remove • redun-switchover

Table 24-3 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
CISCO-IP-PROTOCOL-FILTER-MIB	<p>The FWSM supports browsing of the following tables:</p> <ul style="list-style-type: none"> • cippfIpProfileTable • cippfIpFilterExtTable • cippfIpFilterStatsTable • cippfIpFilterTable <p>The following example shows how to retrieve entries displayed from the show access-list command through SNMP operations on the cippfIpfilterTable and cippfIpfilterStatsTable objects.</p> <pre> ! interface Vlan50 nameif inside security-level 100 ip address 50.0.0.2 255.0.0.0 ! interface Vlan60 nameif outside security-level 0 ip address 60.0.0.2 255.0.0.0 ! snmp-server host outside 60.0.0.1 community public version 2c udp-port 161 ! hostname# show access-list access-list aaa line 1 extended permit tcp any any eq www (hitcnt=0) 0xe0998155 snmpwalk 60.0.0.2 -c public -v 2c 1.3.6.1.4.1.9.9.278 returns as SNMPv2-SMI::enterprises.9.9.278.1.1.1.1.2.3.97.97.97 = INTEGER: 2 <<<< 2 means extended access-list SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.2.1.1 = STRING: "aaa" SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.2.2.1 = STRING: "aaa" SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.3.1.1 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.3.2.1 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.3.3.97.97.97.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.4.3.97.97.97.1 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.5.3.97.97.97.1 = Hex-STRING: 00 00 00 00 <-- denotes src network SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.6.3.97.97.97.1 = Hex-STRING: 00 00 00 00 <-- denotes src network mask SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.7.3.97.97.97.1 = Hex-STRING: 00 00 00 00 <-- denotes dest network SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.8.3.97.97.97.1 = Hex-STRING: 00 00 00 00 <-- denotes dest network mask SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.9.3.97.97.97.1 = INTEGER: 6 <-- 6 stands for tcp protocol number SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.10.3.97.97.97.1 = Gauge32: 0 <-0 means any port SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.11.3.97.97.97.1 = Gauge32: 0 <-0 means any port. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.12.3.97.97.97.1 = Gauge32: 80 <- www translates to 80 </pre>

Table 24-3 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
CISCO-IP-PROTOCOL-FILTER-MIB (Continued)	<pre> SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.13.3.97.97.97.1 = Gauge32: 0 <- 0 means any port. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.16.3.97.97.97.1 = INTEGER: 2 <- 2 means log for ACL is disabled. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.17.3.97.97.97.1 = INTEGER: 1 <- 1 means ACL log enabled. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.22.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.23.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.24.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.25.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.26.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.27.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.2.3.97.97.97.1 = INTEGER: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.3.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.2.1.1.1.3.97.97.97.1 = Counter64: 0 <<<< 0 is current ACL hit counter for ACL 'aaa' where "3.97.97.97" denotes the access-list name in ASCII characters. The access-list name "aaa" translates to 97.97.97, where "97" is the ASCII equivalent of the character "a." The "3" denotes the number of characters in the ASCII list name. The following example shows an unexpanded access-list with a network object-group, which can be retrieved through SNMP operations. The hit counter for individual access-lists is aggregated and displayed in the SNMP OID "cippfIpFilterHits." ! interface Vlan50 nameif inside security-level 100 ip address 50.0.0.2 255.0.0.0 ! interface Vlan60 nameif outside security-level 0 ip address 60.0.0.2 255.0.0.0 ! object-group network src-network network-object 50.1.1.1 255.255.255.255 network-object 50.1.1.2 255.255.255.255 network-object 50.1.1.3 255.255.255.255 object-group network dest-network network-object 60.1.1.1 255.255.255.255 network-object 60.1.1.2 255.255.255.255 network-object 60.1.1.3 255.255.255.255 access-list aaa extended permit tcp object-group src-network object-group dest-network ! snmp-server host outside 60.0.0.1 community public version 2c udp-port 161 ! hostname(config)# show access-list </pre>

Table 24-3 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
CISCO-IP-PROTOCOL-FILTER-MIB (Continued)	<pre> access-list mode auto-commit access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300 access-list aaa; 9 elements access-list aaa line 1 extended permit tcp object-group src-network object-group dest-network 0x705bc913 <---- only exposed access-list aaa line 1 extended permit tcp host 50.1.1.1 host 60.1.1.1 (hitcnt=0) 0xcb224dc0 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.1 host 60.1.1.2 (hitcnt=0) 0x324aa638 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.1 host 60.1.1.3 (hitcnt=0) 0xca52e993 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.2 host 60.1.1.1 (hitcnt=0) 0xa45db454 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.2 host 60.1.1.2 (hitcnt=0) 0xd69df47f <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.2 host 60.1.1.3 (hitcnt=0) 0xb06956a6 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.3 host 60.1.1.1 (hitcnt=0) 0xcd7aeba4 <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.3 host 60.1.1.2 (hitcnt=0) 0x3210272d <---- not exposed access-list aaa line 1 extended permit tcp host 50.1.1.3 host 60.1.1.3 (hitcnt=0) 0xa2b03187 <---- not exposed snmpwalk 60.0.0.2 -c public -v 2c 1.3.6.1.4.1.9.9.278 SNMPv2-SMI::enterprises.9.9.278.1.1.1.2.3.97.97.97 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.3.3.97.97.97.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.4.3.97.97.97.1 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.5.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.6.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.7.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.8.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.9.3.97.97.97.1 = INTEGER: 6 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.10.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.11.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.12.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.13.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.16.3.97.97.97.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.17.3.97.97.97.1 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.22.3.97.97.97.1 = STRING: "src-network" <--- source network object group name SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.23.3.97.97.97.1 = STRING: "dest-network" <-- destination network object-group name.. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.24.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.25.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.26.3.97.97.97.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.27.3.97.97.97.1 = "" </pre>

Table 24-3 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
CISCO-IP-PROTOCOL-FILTER-MIB (Continued)	<pre> SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.2.3.97.97.97.1 = INTEGER: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.3.3.97.97.97.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.2.1.1.1.3.97.97.97.1 = Counter64: 0 <-- aggregated ACL hit counter The following example shows access-list entries displayed in the show ipv6 access-list command can be retrieved and displayed through SNMP operations. interface Vlan50 nameif inside security-level 100 ip address 50.0.0.2 255.0.0.0 ipv6 address 2000:400:3:1::100/64 ! interface Vlan60 nameif outside security-level 0 ip address 60.0.0.2 255.0.0.0 ipv6 address 2001:400:3:1::100/64 ! ! ipv6 access-list allow_ipv6 permit tcp any any eq www ! access-group allow_ipv6 in interface inside access-group allow_ipv6 in interface outside ! snmp-server host outside 60.0.0.1 community public version 2c udp-port 161 ! FWSM# show ipv6 access-list ipv6 access-list allow_ipv6; 1 elements ipv6 access-list allow_ipv6 line 1 permit tcp any any eq www (hitcnt=0) 0xfabbda56 snmpwalk 60.0.0.2 -c public -v 2c 1.3.6.1.4.1.9.9.278 returns as SNMPv2-SMI::enterprises.9.9.278.1.1.1.1.2.10.97.108.108.111.119.9 5.105.112.118.54 = INTEGER: 3 SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.2.1.3 = STRING: "allow_ipv6" SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.2.2.3 = STRING: "allow_ipv6" SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.3.1.3 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.2.1.3.2.3 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.3.10.97.108.108.111.119.9 5.105.112.118.54.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.4.10.97.108.108.111.119.9 5.105.112.118.54.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.5.10.97.108.108.111.119.9 5.105.112.118.54.1 = Hex-STRING: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.6.10.97.108.108.111.119.9 5.105.112.118.54.1 = Hex-STRING: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 95.105.112.118.54.1 = Gauge32: 0 </pre>

Table 24-3 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
CISCO-IP-PROTOCOL-FILTER-MIB (Continued)	<pre> SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.7.10.97.108.108.111.119.9 5.105.112.118.54.1 = Hex-STRING: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.8.10.97.108.108.111.119.9 5.105.112.118.54.1 = Hex-STRING: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.9.10.97.108.108.111.119.9 5.105.112.118.54.1 = INTEGER: 6 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.10.10.97.108.108.111.119. SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.11.10.97.108.108.111.119. 95.105.112.118.54.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.12.10.97.108.108.111.119. 95.105.112.118.54.1 = Gauge32: 80 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.13.10.97.108.108.111.119. 95.105.112.118.54.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.16.10.97.108.108.111.119. 95.105.112.118.54.1 = INTEGER: 2 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.17.10.97.108.108.111.119. 95.105.112.118.54.1 = INTEGER: 1 SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.22.10.97.108.108.111.119. 95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.23.10.97.108.108.111.119. 95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.24.10.97.108.108.111.119. 95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.25.10.97.108.108.111.119. 95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.26.10.97.108.108.111.119. 95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.3.1.27.10.97.108.108.111.119. 95.105.112.118.54.1 = "" SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.2.10.97.108.108.111.119.9 5.105.112.118.54.1 = INTEGER: 0 SNMPv2-SMI::enterprises.9.9.278.1.1.4.1.3.10.97.108.108.111.119.9 5.105.112.118.54.1 = Gauge32: 0 SNMPv2-SMI::enterprises.9.9.278.1.2.1.1.1.10.97.108.108.111.119.9 5.105.112.118.54.1 = Counter64: 0 </pre>
	<p>Note You cannot perform an SNMP query for either type of access-list.</p> <p>You cannot perform an SNMP query for access-list entries expanded because of the use of an object-group. You can only perform an SNMP query for unexpanded access-lists using an object-group. You can only perform an SNMP query for an aggregated access-list hit counter for an access-list using an object-group. You cannot perform an SNMP query for the hit counter for access-list entries expanded because of an object-group in an access-list.</p> <p>You cannot perform an SNMP query for access-list names configured with more than 112 characters.</p>

Table 24-3 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
CISCO-FIREWALL-MIB	<p>The FWSM supports browsing of the MIB.</p> <p>The FWSM supports browsing of the following group:</p> <ul style="list-style-type: none"> • cfwSystem <p>The information in cfwSystem.cfwStatus, which relates to failover status, pertains to the entire device and not just a single context.</p> <p>The FWSM supports browsing of the following table:</p> <ul style="list-style-type: none"> • cfwConnectionStatTable
CISCO-IPSEC-FLOW-MONITOR-MIB	<p>The FWSM supports browsing of the MIB.</p> <p>The FWSM sends the following traps:</p> <ul style="list-style-type: none"> • start • stop
CISCO-L4L7-RESOURCE-LIMIT-MIB	<p>The FWSM supports browsing of the MIB.</p> <p>The FWSM supports browsing of the following traps:</p> <ul style="list-style-type: none"> • limit-reached • rate-limit-reached <p>The FWSM supports browsing of the following tables:</p> <ul style="list-style-type: none"> • ciscoL4L7ResourceLimitTable • ciscoL4L7ResourceRateLimitTable
CISCO-MEMORY-POOL-MIB	<p>The FWSM supports browsing of the following table:</p> <ul style="list-style-type: none"> • ciscoMemoryPoolTable—The memory usage described in this table applies only to the security appliance general-purpose processor, and not to the network processors.
CISCO-NAT-EXT-MIB	<p>The FWSM supports browsing of the MIB.</p>
CISCO-PROCESS-MIB	<p>The FWSM supports browsing of the MIB.</p> <p>The FWSM supports browsing of the following table:</p> <ul style="list-style-type: none"> • cpmCPUTotalTable <p>The FWSM sends the following trap:</p> <ul style="list-style-type: none"> • rising threshold
CISCO-REMOTE-ACCESS-MONITOR-MIB	<p>The FWSM supports browsing of the MIB.</p> <p>The FWSM sends the following trap:</p> <ul style="list-style-type: none"> • session-threshold-exceeded
CISCO-SYSLOG-MIB	<p>The FWSM sends the following trap:</p> <ul style="list-style-type: none"> • clogMessageGenerated <p>You cannot browse this MIB.</p>

Table 24-3 *SNMP MIB and Trap Support (continued)*

MIB and Trap	Description
CISCO-UNIFIED-FIREWALL-MIB	The FWSM supports browsing of the MIB. The FWSM supports browsing of the following group: <ul style="list-style-type: none">• <code>cufwUrlFilterGlobals</code>—This group provides global URL filtering statistics.
IF-MIB	The FWSM supports browsing of the following tables: <ul style="list-style-type: none">• <code>ifTable</code>• <code>ifXTable</code>

Table 24-3 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
IP-FORWARD-MIB	<p>The FWSM supports browsing of the following table: inetCidrRouteTable.</p> <p>The following example shows how entries displayed from the show route command can be retrieved through SNMP operations.</p> <pre> ! interface Vlan50 nameif inside security-level 100 ip address 50.0.0.2 255.0.0.0 ! interface Vlan60 nameif outside security-level 0 ip address 60.0.0.2 255.0.0.0 ! snmp-server host outside 60.0.0.1 community public version 2c udp-port 161 ! hostname# show route 50.0.0.0 255.0.0.0 is directly connected, inside 60.0.0.0 255.0.0.0 is directly connected, outside </pre> <p>An SNMP request from the inetCidrRouteTable returns:</p> <pre> snmpwalk 60.0.0.2 -c public -v 2c 1.3.6.1.2.1.4.24.7 returns IP-MIB::ip.24.7.1.7.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 1 <---- ifindex IP-MIB::ip.24.7.1.7.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 2 <---- Inindex IP-MIB::ip.24.7.1.8.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 3 <---- refer local IP-MIB::ip.24.7.1.8.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 3 <---- refer local IP-MIB::ip.24.7.1.9.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 2 <---- 2 means local or connected route IP-MIB::ip.24.7.1.9.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 2 <---- 2 means local or connected route IP-MIB::ip.24.7.1.10.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = Gauge32: 0 IP-MIB::ip.24.7.1.10.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = Gauge32: 0 IP-MIB::ip.24.7.1.11.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = Gauge32: 0 IP-MIB::ip.24.7.1.11.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = Gauge32: 0 IP-MIB::ip.24.7.1.12.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 0 <--- primary metric 0 for connected route IP-MIB::ip.24.7.1.12.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 0 <--- primary metric 0 for connected route IP-MIB::ip.24.7.1.13.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1 IP-MIB::ip.24.7.1.13.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1 IP-MIB::ip.24.7.1.14.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1 IP-MIB::ip.24.7.1.14.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1 IP-MIB::ip.24.7.1.15.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1 IP-MIB::ip.24.7.1.15.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1 IP-MIB::ip.24.7.1.16.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1 IP-MIB::ip.24.7.1.16.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: -1 IP-MIB::ip.24.7.1.17.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 1 <----- 1 means route is active IP-MIB::ip.24.7.1.17.1.4.60.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 1 <----- 1 means route is active </pre>

Table 24-3 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
IP-FORWARD-MIB (Continued)	<p>For an SNMP request to retrieve the SNMP OID "inetCidrRouteIfIndex" from the inetCidrRouteTable, enter the following:</p> <pre>snmpget 60.0.0.2 -c public -v 2c ip.24.7.1.7.1.4.50.0.0.0.8.0.1.4.0.0.0.0 returns as IP-MIB::ip.24.7.1.7.1.4.50.0.0.0.8.0.1.4.0.0.0.0 = INTEGER: 1</pre> <p>Note You cannot perform an SNMP query for IPv6 route entries.</p> <p>Up to a three-minute delay may occur between route entries displayed in the show route command, and you can perform an SNMP query for this entry.</p>

Table 24-3 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
IP-MIB	<p>The FWSM supports browsing of the following table: ipNetToPhysicalTable</p> <p>The following examples show how entries displayed through the show arp command can be retrieved through SNMP operations.</p> <pre>interface Vlan50 nameif inside security-level 100 ip address 50.0.0.2 255.0.0.0 ! interface Vlan60 nameif outside security-level 0 ip address 60.0.0.2 255.0.0.0 ! snmp-server host outside 60.0.0.1 community public version 2c udp-port 161 !</pre> <pre>hostname# show arp inside 50.0.0.1 0004.23b3.9dea outside 60.0.0.1 000e.0c4e.f6cc</pre> <p>For an SNMP request from the ipNetToPhysicalTable, enter the following:</p> <pre>snmpwalk 60.0.0.2 -c public -v 2c IP-MIB::ip.35 returns</pre> <pre>IP-MIB::ip.35.1.4.1.1.4.50.0.0.1 = Hex-STRING: 00 04 23 B3 9D EA IP-MIB::ip.35.1.4.2.1.4.60.0.0.1 = Hex-STRING: 00 0E 0C 4E F6 CC</pre> <p>For an SNMP request for a specific IP address from the ipNetToPhysicalTable, enter the following:</p> <pre>snmpwalk 60.0.0.2 -c public -v 2c IP-MIB::ip.35.1.4.1.1.4.50.0.0.1 returns</pre> <pre>IP-MIB::ip.35.1.4.1.1.4.50.0.0.1 = Hex-STRING: 00 04 23 B3 9D EA</pre> <p>The ipNetToPhysicalTable object is indexed by ipNetToPhysicalIfIndex, ipNetToPhysicalNetAddressType, and ipNetToPhysicalNetAddress, in which ipNetToPhysicalIfIndex will be the VLAN interface number. The ipNetToPhysicalNetAddress object is the IP address for which the MAC entry is to be retrieved. Only the ipNetToPhysicalPhysAddress object is populated from ipNetToPhysicalTable to retrieve the MAC address for the indexed IP address.</p> <p>Note Up to a three-minute delay may occur between ARP entries displayed in the show arp command, and you can perform an SNMP query for this entry.</p>
MIB-II	<p>The FWSM supports browsing of the following group and table:</p> <ul style="list-style-type: none"> • system

Table 24-3 SNMP MIB and Trap Support (continued)

MIB and Trap	Description
NAT-MIB	<p>The FWSM supports browsing of the MIB.</p> <p>The FWSM sends the following trap:</p> <ul style="list-style-type: none"> packet-discard <p>The FWSM supports browsing of the following tables:</p> <ul style="list-style-type: none"> natAddrBindTable natAddrPortBindTable
RFC1213-MIB	<p>The FWSM supports browsing of the following table:</p> <ul style="list-style-type: none"> ip.ipAddrTable
SNMP core traps	<p>The FWSM sends the following SNMP core traps:</p> <ul style="list-style-type: none"> authentication—An SNMP request fails because the NMS did not authenticate with the correct community string. linkup—An interface has transitioned to the “up” state. linkdown—An interface is down, for example, if you removed the nameif command. coldstart—The FWSM is running after a reload.
SNMPv2-MIB	<p>The FWSM supports browsing of the following:</p> <ul style="list-style-type: none"> snmp
TCP-MIB	<p>The FWSM supports browsing of the following table:</p> <ul style="list-style-type: none"> tcpConnectionTable
UDP-MIB	<p>The FWSM supports browsing of the following table:</p> <ul style="list-style-type: none"> udpEndpointTable

Enabling SNMP

This section describes how to enable SNMP on the FWSM. The SNMP agent that runs on the FWSM performs two functions:

- Replies to SNMP requests from NMSs.
- Sends traps (event notifications) to NMSs.

To enable the SNMP agent and identify an NMS that can connect to the FWSM, perform the following steps:

Step 1 To ensure that the SNMP server on the FWSM is enabled, enter the following command:

```
hostname(config)# snmp-server enable
```

The SNMP server is enabled by default.

Step 2 To identify the IP address of the NMS that can connect to the FWSM, enter the following command:

```
hostname(config)# snmp-server host interface_name ip_address [trap | poll]
[community text] [version {1 | 2c}] [udp-port port]
```

Where the *interface_name* argument specifies the interface through which you access the NMS.

The *ip_address* argument specifies the IP address of the NMS.

Specify **trap** or **poll** if you want to limit the NMS to receiving traps only or browsing (polling) only. By default, the NMS can use both functions.

To change the port number, use the **udp-port** keyword.

Step 3 To specify the community string, enter the following command:

```
hostname(config)# snmp-server community key
```

The SNMP community string is a shared secret between the FWSM and the NMS. The key is a case-sensitive value up to 32 characters in length. Spaces are not permitted.

Step 4 (Optional) To set the SNMP server location or contact information, enter the following command:

```
hostname(config)# snmp-server {contact | location} text
```

Where *text* defines the SNMP server location or contact information.

Step 5 To enable the FWSM to send traps to the NMS, enter the following command:

```
hostname(config)# snmp-server enable traps [all | syslog | snmp [trap] [...] |
cpu threshold [trap] | entity [trap] [...] | ipsec [trap] [...] | nat [trap] |
remote-access [trap] | resource [trap]]
```

Enter this command for each feature type to enable individual traps or sets of traps, or enter the **all** keyword to enable all traps.

The default configuration has all SNMP traps enabled (**snmp-server enable traps snmp authentication linkup linkdown coldstart**). You can disable these traps using the **no** form of this command with the **snmp** keyword. However, the **clear configure snmp-server** command restores the default enabling of SNMP traps.

If you enter this command and do not specify a trap type, then the default is **syslog**. (The default **snmp** traps continue to be enabled along with the **syslog** trap.)

Traps for **snmp** include:

- **authentication**
- **linkup**
- **linkdown**
- **coldstart**

Traps for **entity** include:

- **config-change**
- **fru-insert**
- **fru-remove**
- **redun-switchover**
- **alarm-asserted**
- **alarm-cleared**

Traps for **ipsec** include:

- **start**
- **stop**

Traps for **nat** include:

- **packet-discard**

Traps for **remote-access** include:

- **session-threshold-exceeded**

Traps for **resource** include:

- **limit-reached**
- **rate-limit-reached**

Traps for **cpu threshold** include:

- **rising**

To receive cpu threshold rising traps, the cpu threshold rising and monitoring values must be specified by entering the following command:

```
hostname(config)# cpu threshold rising threshold_value monitoring level
```

Step 6 To enable syslog messages to be sent as traps to the NMS, enter the following command:

```
hostname(config)# logging history level
```

You must also enable **syslog** traps using the preceding **snmp-server enable traps** command.

Step 7 To enable logging and generate syslog messages, which can then be sent to an NMS, enter the following command:

```
hostname(config)# logging enable
```

The following example sets the FWSM to receive requests from host 192.168.3.2 on the inside interface.

```
hostname(config)# snmp-server host inside 192.168.3.2  
hostname(config)# snmp-server location building 42  
hostname(config)# snmp-server contact Pat lee  
hostname(config)# snmp-server community ohwhatakeyisthee
```

