Logging Commands on the Virtual Firewall

This module describes the commands required to configure logging in Cisco IOS XR software.

Note The commands described in this module are SanOS (Linux) commands used on the VFW application. Before you can access any of these commands, you must attach from the route processor to the VFW application using the **service firewall attach location** command. For more information, see the "Attaching to the VFW Application" section in *Cisco IOS XR Virtual Firewall Configuration Guide*.

clear logging

To clear information stored in the logging buffer, use the **clear logging** command in EXEC mode.

clear logging [**disabled** | **rate-limit**]

Syntax Description

disabled	(Optional) Clears the logging buffer of "disabled" messages.
rate-limit	(Optional) Clears the logging buffer of "rate-limit configuration" messages.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

To clear all the information stored in the logging buffer, execute the **clear logging** command without using either of the optional keywords.

Examples

The following example shows how to clear all the information stored in the logging buffer:

```
firewall/Admin# clear logging
```

Related Commands

Command	Description
logging buffered	Enables system logging to a local buffer and limits the messages sent to the buffer based on severity.
show logging	Displays the current severity level and state of all syslog messages stored in the logging buffer.

logging buffered

To enable system logging to a local buffer and to limit the messages sent to the buffer based on severity, use the **logging buffered** command in configuration mode. To disable message logging, use the **no** form of this command.

logging buffered *severity_level*

no logging buffered

Syntax Description

severity_level	Maximum level for system log messages sent to the buffer. The severity level that you specify indicates that you want syslog messages at that level and below. Allowable entries include: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)

Defaults

Logging to the local buffer on the VFW application is disabled.

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **logging buffered** command to enable system logging to a local buffer and to limit the messages sent to the buffer based on severity. By default, logging to the local buffer on the VFW application is disabled. New messages append to the end of the buffer. The first message displayed is the oldest message in the buffer. When the log buffer fills, the VFW application deletes the oldest message to make space for new messages.

Examples

The following example shows how to set the logging buffer level to 3 for logging error messages:

```
firewall/Admin(config)# logging buffered 3
```

Related Commands

Command	Description
logging enable	Enables message logging.

logging device-id

To specify that the device ID of the VFW application is included in the syslog message, use the **logging device-id** command in configuration mode. To disable device ID logging for the VFW application in the syslog message, use the **no** form of this command.

logging device-id {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}

no logging device-id

Syntax Description

context-name	Specifies the name of the current context as the device ID to uniquely identify the syslog messages sent from the VFW application.
hostname	Specifies the hostname of the VFW application as the device ID to uniquely identify the syslog messages sent from the VFW application.
ipaddress *interface_name*	Specifies the IP address of the interface as the device ID to uniquely identify the syslog messages sent from the VFW application. If you use the **ipaddress** keyword, syslog messages sent to an external server contain the IP address of the interface specified, regardless of which interface the VFW application uses to send the log data to the external server. The maximum *interface_name* length is 64 characters.
string *text*	Specifies a text string to uniquely identify the syslog messages sent from the VFW application. The maximum **string** length is 64 characters without spaces. You cannot use the following characters: & (ampersand), ‘ (single quote), “ (double quote), < (less than), > (greater than), or ? (question mark).

Defaults

By default, the device ID of the VFW application is not included in the syslog message.

Command Modes

Configuration

Admin and user contexts

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **logging device-id** command to specify that the device ID of the VFW application is included in the syslog message. If enabled, the VFW application displays the device ID in all non-EMBLEM-formatted syslog messages.

The device ID part of the syslog message is viewed through the syslog server only and not directly on the VFW application. The device ID does not appear in EMBLEM-formatted messages, SNMP traps, management session, or buffer.

Examples

The following example shows how to instruct the VFW application to use the hostname of the VFW application to uniquely identify the syslog messages:

```
firewall/Admin(config)# logging device-id hostname
```

Related Commands

Command	Description
logging enable	Enables message logging.

logging enable

To enable message logging, use the **logging enable** command in configuration mode. To stop message logging to all output locations, use the **no** form of this command.

logging enable

no logging enable

Syntax Description

This command has no arguments or keywords.

Defaults

Message logging is disabled by default.

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Message logging is disabled by default. When enabled, log messages are sent to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages. You must set a logging output location to view any logs.

Examples

The following example shows how to enable message logging to all output locations:

```
firewall/Admin(config)# logging enable
```

Related Commands

This command has no related commands.

logging facility

To change the logging facility to a value other than the default of 20 (LOCAL4), use the **logging facility** command in configuration mode. To set the syslog facility to its default of 20, use the **no** form of this command.

logging facility *number*

no logging facility *number*

Syntax Description

number	Syslog facility. Enter an integer from 16 (LOCAL0) to 23 (LOCAL7).

Defaults

The default logging facility is 20 (LOCAL4).

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **logging facility** command to change the logging facility to a value other than the default of 20 (LOCAL4). Most UNIX systems expect the messages to use facility 20. The VFW application allows you to change the syslog facility type to identify the behavior of the syslog daemon (syslogd) on the host.

The syslog daemon uses the specified syslog facility to determine how to process messages. Each logging facility configures how the syslog daemon on the host handles a message. Syslog servers file messages based on the facility number in the message. For more information on the syslog daemon and facility levels, see your syslog daemon documentation.

Examples

The following example shows how to set the syslog facility as 16(LOCAL0) in syslog messages:

```
firewall/Admin(config)# logging facility 16
```

Related Commands

Command	Description
logging enable	Enables message logging.

logging fastpath

To enable the logging of connection setup and teardown messages, use the **logging fastpath** command in configuration mode. To disable the logging of connection setup and teardown syslog messages, use the **no** form of this command.

logging fastpath

no logging fastpath

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the VFW application does not log connection setup and teardown syslog messages.

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Examples

The following example shows how to configure the VFW application to log connection setup and teardown syslog messages:

```
firewall/Admin(config)# logging fastpath
```

Related Commands

Command	Description
logging enable	Enables message logging.

logging history

To set the Simple Network Management Protocol (SNMP) message severity level when sending log messages to an Network Management System (NMS), use the **logging history** command in configuration mode. To disable logging of informational system messages to an NMS, use the **no** form of this command.

logging history *severity_level*

no logging history

Syntax Description

severity_level	Maximum level system log messages sent as traps to the NMS. The severity level that you specify indicates that you want to log messages at that level and below. Allowable entries include: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)

Defaults

No default behavior or values

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

To enable or disable all SNMP syslog message logging, use the **logging history** command without the *severity_level* argument.

We recommend that you use the debugging (7) level during initial setup and during testing. After setup, set the level from debugging (7) to a lower value for use in your network.

Examples

The following example shows how to send informational system message logs to an SNMP NMS:

```
firewall/Admin(config)# logging history 6
```

Related Commands

Command	Description
logging enable	Enables message logging.

logging host

To specify a host (the syslog server) that receives the syslog messages sent by the VFW application, use the **logging host** command in configuration mode. To disable logging to a syslog server, use the **no** form of this command.

logging host *ip_address* [**tcp** | **udp** [*/port#*] | [**default-udp**] | [**format emblem**] | **level** *severity_level*]

no logging host *ip_address* [**level** *severity_level*]

Syntax Description

ip_address	IP address of the host to be used as the syslog server.
tcp	(Optional) Specifies to use TCP to send messages to the syslog server. A server can be specified to receive either UDP or TCP, not both.
udp	(Optional) Specifies to use UDP to send messages to the syslog server. A server can be specified to receive either UDP or TCP, not both.
/port#	(Optional) Port that the syslog server listens to for syslog messages. Enter an integer from 1025 to 65535. The default protocol and port are UDP/514. The default TCP port, if specified, is 1470.
default-udp	(Optional) Instructs the VFW application to default to UDP if the TCP transport fails to communicate with the syslog server.
format emblem	(Optional) Enables EMBLEM-format logging for each syslog server. The Cisco Resource Management Environment (RME) is a network management application that collects syslogs. RME can process syslog messages only if they are in EMBLEM format.
level *severity_level*	(Optional) Specifies the level for system log messages to be sent as traps to the NMS. The severity level that you specify indicates that you want to log messages at that level only. Allowable entries include: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)

Defaults

By default, logging to a syslog server on a host is disabled on the VFW application.

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	The **level** keyword was added.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **logging host** command to specify a host (the syslog server) that receives the syslog messages sent by the VFW application. You can use multiple **logging host** commands to specify additional servers to receive the syslog messages.

If you choose to send log messages to a host, the VFW application sends those messages using either UDP or TCP. The host must run a program (known as a server) called syslogd, a daemon that accepts messages from other applications and the network, and writes them out to system wide log files. UNIX provides the syslog server as part of its operating system. For Microsoft Windows, you must obtain a syslog server for the Windows operating system.

If you use TCP as the logging transport protocol, the VFW application denies new network access sessions as a security measure in the following instances:

- The VFW application is unable to reach the syslog server.
- The syslog server is misconfigured.
- The TCP queue is full.
- The disk is full.

The **format emblem** keywords allows you to enable EMBLEM-format logging for each syslog server. EMBLEM-format logging is available for either TCP or UDP syslog messages. If you enable EMBLEM-format logging for a particular syslog host, then the messages are sent to that host. If you also enable the **logging timestamp** command, the messages are sent to the syslog server with a time stamp.

For example, the EMBLEM format for a message with a time stamp appears as follows:

```
ipadress or dns name [Dummy Value/Counter]: [mmm dd hh:mm:ss TimeZone]:
%FACILITY-[SUBFACILITY-]SEVERITY-MNEMONIC: [vtl-ctx: context id] Message-text
```

If the **logging host** command is configured without the **level** keyword, the server receives messages from level 0 up to the level defined by the **logging trap** command. Use the **level** keyword to specify that the server receive messages with the defined level only. If you configure the **logging host** command without the **level** keyword, and subsequently configure it with the **level** keyword, the server receives all the defined messages from both commands. In other words, the server is sent messages from level 0 up to the level defined by the **logging trap** command, as well as messages defined with the **level** keyword.

Examples

The following example shows how to send log messages to a syslog server:

```
firewall/Admin(config)# logging host 192.168.10.1 tcp/1025 format-emblem default-udp
```

The following example shows how to send level 4 messages only to the syslog server 192.168.10.2:

```
firewall/Admin(config)# logging host 192.168.10.2 level 4
```

In the following example, syslog messages up to level 6 are set to the host 192.168.10.3:

```
firewall/Admin(config)# logging trap 6
firewall/Admin(config)# logging host 192.168.10.3
```

In the following example, messages up to level 3, in addition to messages from level 7 are set to host 192.168.10.4, while only level 1 messages are sent to host 192.168.10.5:

```
firewall/Admin(config)# logging trap 3
firewall/Admin(config)# logging host 192.168.10.4
firewall/Admin(config)# logging host 192.168.10.5 level 1
firewall/Admin(config)# logging host 192.168.10.4 level 7
```

Related Commands

Command	Description
logging enable	Enables message logging.
logging timestamp	Specifies that syslog messages should include the date and time that the message was generated.

logging message

To control the display of a specific system logging message or to change the severity level associated with the specified system logging message, use the **logging message** command in configuration mode. To disable logging of the specified syslog message, use the **no** form of this command.

logging message *syslog_id* [**level** *severity_level*]

no logging message *syslog_id*

Syntax Description

syslog_id	Specific message you want to disable or to enable.
level *severity_level*	(Optional) Changes the severity level associated with a specific system log message. For example, the %<ACE>-4-411001 message listed in the syslog has the default assigned severity level of 4 (warning message). You can change the assigned default severity level to a different level. Allowable entries include: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)

Defaults

No default behavior or values

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

You can use the **show logging** command to determine the level currently assigned to a message and whether the message is enabled.

Examples

The following example shows how to disable the %<ACE>-6-615004 syslog message:

```
firewall/Admin(config)# no logging message 615004
```

The following example shows how to resume logging of the disabled syslog message:

```
firewall/Admin(config)# logging message 615004 level 6
```

The following example shows how to change the severity level of the 615004 syslog message from the default of 6 (informational) to a severity level of 5 (notification):

```
(config)# logging message 615004 level 5
```

Related Commands

Command	Description
logging enable	Enables message logging.

logging monitor

To display syslog messages as they occur when accessing the VFW application through a Secure Shell (SSH) or a Telnet session, use the **logging monitor** command in configuration mode. To disable system message logging to the current Telnet or SSH session, use the **no** form of this command.

logging monitor *severity_level*

no logging monitor

Syntax Description

severity_level	Maximum level for system log messages displayed during the current SSH or Telnet session. The severity level that you specify indicates that you want to log messages at that level and below. Allowable entries include: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)

Defaults

By default, logging to a remote connection using the Secure Shell (SSH) or Telnet is disabled on the VFW application.

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **logging monitor** command to display syslog messages as they occur when accessing the VFW application through an SSH or a Telnet session. You can limit the display of messages based on severity.

Before using this command, enable remote access on the VFW application and establish a remote connection using the Secure Shell (SSH) or Telnet protocols from a PC.

To display logs during the SSH or Telnet session, use the **terminal monitor** command in EXEC mode. This command enables syslog messages for all sessions in the current context. The **logging monitor** command sets the logging preferences for all SSH and Telnet sessions, while the **terminal monitor** command controls logging for each individual Telnet session. However, in each session, the **terminal monitor** command controls whether syslog messages appear on the terminal during the session.

Examples

The following example shows how to send informational system message logs to the current Telnet or SSH session:

```
firewall/Admin# terminal monitor
firewall/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
firewall/Admin(config)# logging monitor 6
```

Related Commands

Command	Description
logging enable	Enables message logging.
terminal	Configures the terminal display settings.

logging persistent

To send specific log messages to compact flash on the VFW application, use the **logging persistent** command in configuration mode. To disable logging to compact flash, use the **no** form of this command.

logging persistent *severity_level*

no logging persistent

Syntax Description

severity_level	Maximum level for system log messages sent to compact flash. The severity level that you specify indicates that you want to log messages at that level and below. Allowable entries include: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)

Defaults

By default, logging to compact flash is disabled on the VFW application.

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **logging persistent** command to send specific log messages to compact flash on the VFW application. The VFW application allows you to specify the system message logs that you want to keep after a system reboot by saving them to compact flash.

We recommend that you use a lower severity level, such as 3, because logging at a high rate to flash memory on the VFW application may impact performance.

Examples

The following example shows how to send informational system message logs to flash memory on the VFW application:

```
firewall/Admin(config)# logging persistent 6
```

Related Commands

Command	Description
logging enable	Enables message logging.

logging queue

To change the number of syslog messages that can appear in the message queue, use the **logging queue** command in configuration mode. To reset the logging queue size to the default of 100 messages, use the **no** form of this command.

logging queue *queue_size*

no logging queue *queue_size*

Syntax Description

queue_size	The size of the queue for storing syslog messages. Enter an integer from 1 to 8192. The default is 100 messages.

Defaults

By default, the VFW application can hold 100 syslog messages in the message queue while awaiting processing.

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Set the queue size before the VFW application processes syslog messages. When traffic is heavy, messages may be discarded.

Examples

The following example shows how to set the size of the syslog message queue to 1000:

```
firewall/Admin(config)# logging queue 1000
```

Related Commands

Command	Description
logging enable	Enables message logging.

logging rate-limit

To limit the rate at which the VFW application generates messages in the syslog, use the **logging rate-limit** command in configuration mode. To disable rate-limiting for message logging in the syslog, use the **no** form of this command.

logging rate-limit {*num* {*interval* | **level** *severity_level* | **message** *syslog_id*} | **unlimited** {**level** *severity_level* | **message** *syslog_id*}}

no logging rate-limit {*num* {*interval* | **level** *severity_level* | **message** *syslog_id*} | **unlimited** {**level** *severity_level* | **message** *syslog_id*}}

Syntax Description

num	Number at which the syslog is to be rate limited.
interval	Time interval in seconds over which the system message logs should be limited. The default time interval is one second.
level *severity_level*	Sets the maximum level for system log messages. The severity level that you specify indicates that you want to log messages at that level and below. Allowable entries include: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)
message *syslog_id*	Identifies the ID of the specific message you want to suppress reporting.
unlimited	Disables rate limiting for messages in the syslog.

Defaults

No default behavior or values

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **logging rate-limit** command to limit the rate at which the VFW application generates messages in the syslog. You can limit the number of syslog messages generated by the VFW application for specific messages.

Examples

The following example shows how to limit the syslog rate for a 60-second time interval:

```
firewall/Admin(config)# logging rate-limit 42 60
```

Related Commands

Command	Description
logging enable	Enables message logging.

logging reject-newconn

To define if the VFW application prohibits new connections from passing through the device if a specified condition has been met, use the **logging-reject-newconn** command in configuration mode. To prevent the VFW application from rejecting new connections, use the **no** form of this command.

logging reject-newconn {**cp-buffer-full** | **rate-limit-reached** | **tcp-queue-full**}

no logging reject-newconn {**cp-buffer-full** | **rate-limit-reached** | **tcp-queue-full**}

Syntax Description

cp-buffer-full	Specifies that the VFW application reject new connections when the syslog daemon internal buffer is full. Disabled by default.
rate-limit-reached	Specifies that the VFW application reject new connections if the syslog message rate specified through the **logging rate-limit** command has been reached. See the **logging rate-limit** command. Disabled by default.
tcp-queue-full	Specifies that the VFW application reject new connections when syslogs can no longer reach the TCP syslog server. Enabled by default.

Defaults

No default behavior or values

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Examples

The following example shows how to configure the VFW application to reject new connections if the specified syslog message rate has been reached:

```
firewall/Admin(config)# logging reject-newconn rate-limit-reached
```

Related Commands

Command	Description
logging enable	Enables message logging.
logging rate-limit	Limits the rate at which the VFW application generates messages in the syslog.

logging rp

To enable syslog messages to be logged and sent to the route processor, use the **logging rp** command in configuration mode. To prevent the VFW application from sending syslog messages to the route processor, use the **no** form of this command.

logging rp *severity_level*

no logging rp

Syntax Description

severity_level	Severity level of messages that you want sent to the route processor. Allowable entries include: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)

Defaults

No default behavior or values

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Examples

The following example shows how to configure the VFW application to send notification level (severity level 5) syslog messages to the router processor:

```
firewall/Admin(config)# logging rp 5
```

Related Commands

Command	Description
logging enable	Enables message logging.

logging standby

To enable logging on the failover standby VFW application, use the **logging standby** command in configuration mode. To disable logging on the standby VFW application, use the **no** form of this command.

logging standby

no logging standby

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **logging standby** command to enable logging on the failover standby VFW application. When enabled, the standby VFW application syslog messages remain synchronized should failover occur. When enabled, this command causes twice the message traffic on the syslog server.

Examples

The following example shows how to enable logging on the failover standby VFW application:

```
firewall/Admin(config)# logging standby
```

Related Commands

Command	Description
logging enable	Enables message logging.

logging timestamp

To specify that syslog messages should include the date and time that the message was generated, use the **logging timestamp** command in configuration mode. To specify that the VFW application not include the date and time when logging syslog messages, use the **no** form of this command.

logging timestamp

no logging timestamp

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the VFW application does not include the date and time in syslog messages.

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

This command is disabled by default.

Examples

The following example shows how to enable the time-stamp display on system logging messages:

```
firewall/Admin(config)# logging timestamp
```

Related Commands

Command	Description
logging enable	Enables message logging.

logging trap

To identify which messages are sent to a syslog server, use the **logging trap** command in configuration mode. To return the trap level to the default (information messages), use the **no** form of this command.

logging trap *severity_level*

no logging trap

Syntax Description

severity_level	Maximum level for system log messages. The severity level that you specify indicates that you want to log messages at that level and below. Allowable entries include: • **0**—emergencies (system unusable messages) • **1**—alerts (take immediate action) • **2**—critical (critical condition) • **3**—errors (error message) • **4**—warnings (warning message) • **5**—notifications (normal but significant condition) • **6**—informational (information message) • **7**—debugging (debug messages)

Defaults

No default behavior or values

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **logging trap** command to identify which messages are sent to a syslog server. This command limits the logging messages sent to a syslog server based on severity.

To send logging messages to a syslog server, use the **logging host** command to specify the name or IP address of the host to be used as the syslog server.

Examples

The following example shows how to send informational system message logs to the syslog server:

```
firewall/Admin(config)# logging trap 6
```

Related Commands

Command	Description
logging enable	Enables message logging.
logging host	Specifies a host (the syslog server) that receives the syslog messages sent by the VFW application.

show logging

To display the current severity level and state of all syslog messages stored in the logging buffer, or to display information related to specific syslog messages, use the **show logging** command in EXEC mode.

show logging [**history** | **internal** {**event-history dbg** | **facility**} | **message** [*syslog_id* | **all** | **disabled**] | **persistent** | **queue** | **rate-limit** | **statistics**]

Syntax Description

history	(Optional) Displays the logging history file.
internal	(Optional) Displays syslog internal messages.
event-history dbg	Displays the debug history for the syslog server.
message	(Optional) Displays a list of syslog messages that have been modified from the default settings. These are messages that have been assigned a different severity level or messages that have been disabled.
syslog_id	(Optional) Identifier of a specific system log message to display, specified by message ID, and whether the message is enabled or disabled.
all	(Optional) Displays all system log message IDs and identifies whether they are enabled or disabled.
disabled	(Optional) Displays a complete list of suppressed syslog messages.
persistent	(Optional) Displays statistics for the log messages sent to flash memory on the VFW application.
queue	(Optional) Displays statistics for the internal syslog queue.
rate-limit	(Optional) Displays the current syslog rate-limit configuration.
statistics	(Optional) Displays syslog statistics.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.5.0	This command was introduced on the Multi-Service Blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.

Usage Guidelines

This command requires the syslog feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Configuring Virtualization on the Virtual Firewall* module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

To use the **show logging** command, you must have the VFW application buffer enabled as a logging output location. By default, logging to the local buffer on the VFW application is disabled. To enable system logging to a local buffer and to limit the messages sent to the buffer based on severity, use the **logging buffered** command in configuration mode from the desired context.

The **show logging** command lists the current syslog messages and identifies which logging command options are enabled.

To clear the VFW application buffer of the logging information currently stored there, use the **clear logging** command.

Examples

The following example shows how to display the contents of the logging history buffer:

```
firewall/Admin# show logging history
```

The following example shows how to display the contents of the internal facility messages buffer:

```
firewall/Admin# show logging internal facility
```

The following example shows how to display statistics for the log messages sent to flash memory on the VFW application:

```
firewall/Admin# show logging persistent
```

The following example shows how to display statistics for the internal syslog queue:

```
firewall/Admin# show logging queue
```

The following example shows how to display the current syslog rate-limit configuration:

```
firewall/Admin# show logging rate-limit
```

The following example shows how to display the current syslog statistics:

```
firewall/Admin# show logging statistics
```

Related Commands

Command	Description
clear logging	Clears information stored in the logging buffer.
logging buffered	Enables system logging to a local buffer and limits the messages sent to the buffer based on severity.