System and File Management Commands on the Virtual Firewall

This module describes a variety of commands that are used to view system status and configurations, as well as to manipulate system files and directories.

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*.

banner motd

To specify a message to display as the message-of-the-day banner when a user connects to the VFW application command-line interface (CLI), use the **banner motd** command in configuration mode. To delete or replace a banner or a line in a multiline banner, use the **no** form of this command.

banner motd *text*

no banner motd *text*

Syntax Description

motd	Configures the system to display as the message-of-the-day banner when a user connects to the VFW application.
text	Line of message text to be displayed as the message-of-the-day banner. The *text* string consists of all characters following the first space until the end of the line (carriage return or line feed). The # character functions as the delimiting character for each line. For the banner text, spaces are allowed but tabs cannot be entered at the CLI. Multiple lines in a message-of-the-day banner are handled by entering a new **banner motd** command for each line that you wish to add. The banner message is a maximum of 80 characters per line, up to a maximum of 3000 characters (3000 bytes) total for a message-of-the-day banner. This maximum value includes all line feeds and the last delimiting character in the message.

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 AAA 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 replace a banner or a line in a multiline banner, use the **no banner motd** command before adding the new lines.

To add multiple lines in a message-of-the-day banner, precede each line by the **banner motd** command. The VFW application appends each line to the end of the existing banner. If the text is empty, the VFW application adds a carriage return (CR) to the banner.

You can include tokens in the form $(token) in the message text. Tokens are replaced with the corresponding configuration variable. For example:

- $(hostname)—Displays the hostname for the VFW application during run time.
- $(line)—Displays the tty (teletypewriter) line or name (for example, “/dev/console”, “/dev/pts/0”, or “1”).

To use the $(hostname) in single line banner motd input, ensure that you include double quotes (“) around the $(hostname) so that the $ is interpreted as a special character for the beginning of a variable in the single line. For example:

```
switch/Admin(config)# banner motd #Welcome to “$(hostname)”...#
```

Do not use the double quote character (“) or the percent sign character (%) as a delimiting character in a single-line message string. Do not use the delimiting-character in the message string.

For multiline input, double quotes (“) are not required for the token, because the input mode is different from single-line mode. The VFW application treats the double quote character (“) as is when you operate in multiline mode.

Examples

The following example shows how to add a message-of-the-day banner:

```
firewall/Admin(config)# banner motd #Welcome to the “$(hostname)”.
firewall/Admin(config)# banner motd Contact me at admin@admin.com for any
firewall/Admin(config)# banner motd issues.#
```

Related Commands

Command	Description
show banner motd	Displays the configured banner message of the day.

capture

To enable the context packet capture function for packet sniffing and network fault isolation, use the **capture** command in EXEC mode. As part of the packet capture process, you specify whether to capture packets from all interfaces or from an individual interface.

capture *buffer_name* {{**all** | **interface** *interface_name*} **access-list** *name* [**bufsize** *buf_size* [**circular-buffer**]] | **remove** | **start** | **stop**}

Syntax Description

buffer_name	Name of the packet capture buffer. The *buffer_name* argument associates the packet capture with a name. Specify a text string from 1 to 80 alphanumeric characters in length.
all	Specifies that packets from all input interfaces are captured.
interface	Specifies a particular input interface from which to capture packets.
access-list *name*	Selects packets to capture based on a specific access list. A packet must pass the access list filters before the packet is stored in the capture buffer. Specify a previously created access list identifier. Enter an unquoted text string with a maximum of 64 characters. **Note** Ensure that the access list is for an input interface; input is considered with regards to the direction of the session you want to capture. If you configure the packet capture on the output interface, the VFW application fails to match any packets.
bufsize *buf_size*	(Optional) Specifies the buffer size, in kilobytes, used to store the packet capture. The range is from 1 to 2147483647 kilobytes.
circular-buffer	(Optional) Enables the packet capture buffer to overwrite itself, starting from the beginning, when the buffer is full.
remove	Clears the packet capture configuration.
start	Starts the packet capture function. The packet capture function automatically stops when the buffer is full unless you enable the circular buffer function.
stop	Stops the packet capture function.

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 has no user role feature restrictions. 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*.

The packet capture function enables access control lists (ACLs) to control what packets are captured by the VFW application on the input interface. If the ACLs are selecting an excessive amount of traffic for the packet capture operation, the VFW application sees a heavy load, which can cause a degradation in performance. We recommend that you avoid using the packet capture function when high network performance is critical.

The capture packet function works on an individual context basis. The VFW application traces only the packets that belong to the context where you execute the **capture** command. The context ID is passed along with the packet, which can be used to isolate packets that belong to a specific context. To trace the packets for a single, specific context, use the **changeto** command and enter the **capture** command for the new context.

The VFW application does not automatically save the packet capture in a configuration file. To copy the capture buffer information as a file in flash memory, use the **copy capture** command.

Examples

The following example shows how to start the packet capture function for CAPTURE1:

```
firewall/Admin# access-list ACL1 line 10 extended permit ip any any
firewall/Admin# capture CAPTURE1 interface xyz access-list ACL1
firewall/Admin# capture CAPTURE1 start
```

The following example shows how to stop the packet capture function for CAPTURE1:

```
firewall/Admin# capture CAPTURE1 stop
```

Related Commands

Command	Description
changeto	Moves from one context on the VFW application to another.
clear icmp statistics	Clears the Internet Control Message Protocol (ICMP) statistics.
copy capture	Copies an existing context packet capture buffer as the source file in the VFW application compact flash to another file system.
show capture	Displays the packet information that the VFW application traces as part of the packet capture function.

checkpoint

To create or modify a checkpoint (snapshot) of the running configuration, use the **checkpoint** command in EXEC mode.

checkpoint {**create** | **delete** | **rollback**} *name*

Syntax Description

create	Creates a new checkpoint with the value of *name*.
delete	Deletes the existing checkpoint with the value of *name*.
rollback	Reverts back to the checkpoint with the value of *name*.
name	Name of a new or existing checkpoint. Specify a text string from 1 to 64 alphanumeric characters (no spaces) in length.

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 Admin 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 create the checkpoint CP102305:

```
firewall/Admin# checkpoint create CP102305
```

Related Commands

Command	Description
show checkpoint	Displays information relating to the configured checkpoints.

clear buffer stats

To clear the control plane buffer statistics, use the **clear buffer stats** command in EXEC mode.

clear buffer stats

Syntax Description

This command has no arguments or keywords.

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 has no user role feature restrictions. 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*.

The **clear buffer stats** command is intended for use by trained Cisco personnel for troubleshooting purposes only.

Examples

The following example shows how to clear the control plane buffer statistics:

```
firewall/Admin# clear buffer stats
```

Related Commands

Command	Description
show buffer	Displays the buffer manager module messages.

clear capture

To clear an existing capture buffer, use the **clear capture** command in EXEC mode.

clear capture *name*

Syntax Description

name	Name of an existing capture buffer.

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 has no user role feature restrictions. 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 **dir** command to view the capture files you copied to the disk0: file system using the **copy capture** command.

Examples

The following example shows how to clear the capture buffer CAPTURE1:

```
firewall/Admin# clear capture CAPTURE1
```

Related Commands

Command	Description
capture	Enables the context packet capture function for packet sniffing and network fault isolation.
copy capture	Copies an existing context packet capture buffer as the source file in the VFW application compact flash to another file system.
dir	Displays the contents of a specified VFW application file system.
show capture	Displays the packet information that the VFW application traces as part of the packet capture function.

clear cores

To clear all the core dumps stored in the core: file system, use the **clear cores** command in EXEC mode.

clear cores

Syntax Description

This command has no arguments or keywords.

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 Admin 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*.

The VFW application creates a core dump when it experiences a fatal error. Core dump information is for Cisco Technical Support use only. We recommend contacting Cisco Technical Support for assistance in interpreting the information in the core dump.

To view the list of core files in the core: file system, use the **dir core:** command.

To save a copy of a core dump to a remote server before clearing it, use the **copy capture** command.

To delete a specific core dump file from the core: file system, use the **delete core:** command.

Examples

The following example shows how to clear all core dumps:

```
firewall/Admin# clear cores
```

Related Commands

Command	Description
copy capture	Copies an existing context packet capture buffer as the source file in the VFW application compact flash to another file system.
delete	Deletes a specified file in a VFW application file system.
dir	Displays the contents of a specified VFW application file system.

clear debug-logfile

To remove a debug log file, use the **clear debug-logfile** command in EXEC mode.

clear debug-logfile *filename*

Syntax Description

filename	Name of an existing debug log file.

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 has no user role feature restrictions. 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*.

The VFW application **debug** commands are intended for use by trained Cisco Technical Support personnel only. Entering these commands may cause unexpected results. Do not attempt to use these commands without guidance from Cisco Technical Support personnel.

Examples

The following example shows how to clear the debug log file DEBUG1:

```
firewall/Admin# clear debug-logfile DEBUG1
```

Related Commands

Command	Description
debug	Enables the VFW application debugging functions.
show debug	Displays the debug flags.

clear fifo stats

To clear the control plane packet first in, first out (FIFO) statistics, use the **clear fifo stats** command in EXEC mode.

clear fifo stats

Syntax Description

This command has no arguments or keywords.

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 has no user role feature restrictions. 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*.

The **clear fifo stats** command is intended for use by trained Cisco Technical Support personnel for troubleshooting purposes only.

Examples

The following example shows how to clear the control plane FIFO statistics:

```
firewall/Admin# clear fifo stats
```

Related Commands

Command	Description
show fifo	Displays the packet first in, first out (FIFO) statistics for the Pkt-Fifo module.

clear netio stats

To clear the control plane network I/O statistics, use the **clear netio stats** command in EXEC mode.

clear netio stats

Syntax Description

This command has no arguments or keywords.

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 has no user role feature restrictions. 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*.

The **clear netio stats** command is intended for use by trained Cisco Technical Support personnel for troubleshooting purposes only.

Examples

The following example shows how to clear the control plane network I/O statistics:

```
firewall/Admin# clear netio stats
```

Related Commands

Command	Description
show netio	Displays the control plane network I/O information.

clear processes log

To clear processes log statistics, use the **clear processes** command in EXEC mode.

clear processes log {**all** | **pid** *id*}

Syntax Description

all	Clears all processes logs.
pid *id*	Specifies the processes log to clear.

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 has no user role feature restrictions. 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 display the list of process identifiers assigned to each of the processes running on the VFW application, use the **show processes** command.

Examples

The following example shows how to clear all the processes log statistics:

```
firewall/Admin# clear processes all
```

Related Commands

Command	Description
show processes	Displays the general information about all the processes running on the VFW application.

clear screen

To clear the display screen, use the **clear screen** command in EXEC mode.

clear screen

Syntax Description

This command has no arguments or keywords.

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 has no user role feature restrictions. 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 clear the display screen:

```
firewall/Admin# clear screen
```

Related Commands

This command has no related commands.

clear startup-config

To clear the startup configuration of the current context, use the **clear startup config** command in EXEC mode.

clear startup-config

Syntax Description

This command has no arguments or keywords.

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 Admin 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*.

Clearing the startup configuration does not affect the context running-configuration.

To clear the startup configuration, you can also use the **write erase** command.

Before you clear a startup configuration, we recommend that you back up your current startup configuration to a file on a remote server using the **copy startup-config** command. When you clear the startup configuration, you can perform one of the following processes to recover a copy of an existing configuration:

- Use the **copy running-config startup-config** command to copy the contents of the running configuration to the startup configuration.
- Upload a backup of a previously saved startup-configuration file from a remote server using the **copy startup-config** command.

Examples

The following example shows how to clear the startup configuration:

```
firewall/Admin# clear startup-config
```

Related Commands

Command	Description
copy capture	Copies an existing context packet capture buffer as the source file in the VFW application compact flash to another file system.
show startup-config	Displays the startup-configuration information associated with the current context.
write	Manages persistent and nonpersistent configuration information.

clear vnet stats

To control plane virtual network (VNET) device statistics, use the **clear vnet stats** command in EXEC mode.

clear vnet stats

Syntax Description

This command has no arguments or keywords.

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 has no user role feature restrictions. 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*.

The **clear vnet stats** command is intended for use by trained Cisco Technical Support personnel for troubleshooting purposes only.

Examples

The following example shows how to clear the VNET statistics:

```
firewall/Admin# clear vnet stats
```

Related Commands

Command	Description
show vnet	Displays the virtual network (VNET) device information.

configure

To access configuration mode and configure the VFW, use the **configure** command in EXEC mode.

configure [**terminal**]

Syntax Description

terminal	(Optional) Enables you to configure the system from the terminal.

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 one or more features assigned to your user role that allow configuration, such as AAA, interface, or fault-tolerant. 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 return to the EXEC mode from the configuration mode, use the **exit** command.

To execute a command in EXEC mode from any of the configuration modes, use the **do** version of the command.

Examples

The following example shows how to access configuration mode:

```
firewall/Admin# configure
firewall/Admin(config)#
```

Related Commands

Command	Description
exit	Exits out of EXEC mode and logs out of the CLI session.

copy capture

To copy an existing context packet capture buffer as the source file in the VFW application compact flash to another file system, use the **copy capture** command in EXEC mode.

copy capture *capture_name* **disk0:** [*path/*]*destination_name*

Syntax Description

capture_name	Name of the packet capture buffer on the disk0: file system. Specify a text string from 1 to 80 alphanumeric characters.
disk0:	Specifies that the buffer is copied to the disk0: file system.
[*path/*] *destination_name*	Destination path (optional) and name for the packet capture buffer. Specify a text string from 1 to 80 alphanumeric characters. If you do not provide the optional path, the VFW application copies the file to the root directory on the disk0: file system.

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 config-copy 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*.

After you copy a capture file to a remote server, you can use the **delete disk0:***filename* command to delete the file from the VFW application and free up memory.

Examples

The following example shows how to copy the packet capture buffer to a file in disk0: called MYCAPTURE1:

```
firewall/Admin# copy capture CAPTURE1 disk0:MYCAPTURE1
```

Related Commands

Command	Description
clear capture	Clears an existing capture buffer.
show capture	Displays the packet information that the VFW application traces as part of the packet capture function.

copy core:

To copy and save a core file to a remote server, use the **copy core:** command in EXEC mode.

copy core:*filename* **disk0:**[*path/*\]*filename* | {**ftp://***server*/*path*[*/filename*] | **sftp://**[*username*@]*server*/*path*[*/filename*] | **tftp://***server*[**:***port*]*/path*[*/filename*]}

Syntax Description

filename1	Core dump residing on the VFW application in flash memory. Use the **dir core:** command to view the core dump files available in the core: file system.
disk0:[*path/*\]*filename*	Specifies that the file destination is the disk0: directory of the current context and the filename for the core. If you do not provide the optional path, the VFW application copies the file to the root directory on the disk0: file system.
ftp://*server*/*path*[*/filename*]	Specifies the File Transfer Protocol (FTP) network server and, optionally, the renamed core dump.
sftp://[*username*@]*server*/*path*[*/filename*]	Specifies the Secure File Transfer Protocol (SFTP) network server and, optionally, the renamed core dump.
tftp://*server*[**:***port*]*/path*[*/filename*]	Specifies the Trivial File Transfer Protocol (TFTP) network server and, optionally, the renamed core dump.

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 config-copy 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 display the list of available core files, use the **dir core:** command. Copy the complete filename (for example, 0x401_vsh_log.25256.tar.gz) into the **copy core:** command.

When you select a destination file system using **ftp:**, **sftp:**, or **tftp:**, the VFW application:

- Prompts you for your username and password if the destination file system requires user authentication.
- Prompts you for the server information if you do not provide the information with the command.

- Copies the file to the root directory of the destination file system if you do not provide path information.

Examples

The following example shows how to copy a core file from the VFW application to a remote FTP server:

```
firewall/Admin# copy core:ixp0_crash.txt ftp://192.168.1.2
Enter the destination filename[]? [ixp0_crash.txt]
Enter username[]? user1
Enter the file transfer mode[bin/ascii]: [bin]
Password:
Passive mode on.
Hash mark printing on (1024 bytes/hash mark).
```

Note The bin (binary) file transfer mode is intended for transferring compiled files (executables). The ASCII file transfer mode is intended for transferring text files, such as configuration files. The default selection of bin should be sufficient in all cases when copying files to a remote FTP server.

Related Commands

Command	Description
dir	Displays the contents of a specified VFW application file system.

copy disk0:

To copy a file from one directory in the disk0: file system of flash memory to another directory in disk0: or a network server, use the **copy disk0:** command in EXEC mode.

copy disk0:[*path/*\]*filename1* {**disk0:**[*path/*\]*filename2* | **ftp://***server*/*path*[*/filename*] | **sftp://**[*username*@]*server*/*path*[*/filename*] | **tftp://***server*[**:***port*]*/path*[*/filename*] | **running-config** | **startup-config**}

Syntax Description

disk0:[*path/*\]*filename1*	Specifies the name of the file to copy in the disk0: file system. Use the **dir disk0:** command to view the files available in disk0:. If you do not provide the optional path, the VFW application copies the file from the root directory on the disk0: file system.
disk0:[*path/*\]*filename2*	Specifies that the file destination is the disk0: directory of the current context and the filename for the core. If you do not provide the optional path, the VFW application copies the file to the root directory on the disk0: file system.
ftp://*server*/*path*[*/filename*]	Specifies the File Transfer Protocol (FTP) network server and, optionally, the renamed file.
sftp://[*username*@]*server*/*path*[*/filename*]	Specifies the Secure File Transfer Protocol (SFTP) network server and, optionally, the renamed file.
ftp://*server*[**:***port*]*/path*[*/file name*]	Specifies the Trivial File Transfer Protocol (TFTP) network server and, optionally, the renamed file.
running-config	Specifies to replace the running-configuration file currently residing on the VFW application in volatile memory.
startup-config	Specifies to replace the startup-configuration file currently residing on the VFW application in flash memory.

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 config-copy 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*.

When you select a destination file system using **ftp:**, **sftp:**, or **tftp:**, the VFW application:

- Prompts you for your username and password if the destination file system requires user authentication.
- Prompts you for the server information if you do not provide the information with the command.
- Copies the file to the root directory of the destination file system if you do not provide path information.

Examples

The following example shows how to copy the file called SAMPLEFILE to the MYSTORAGE directory in flash memory:

```
firewall/Admin# copy disk0:samplefile disk0:MYSTORAGE/SAMPLEFILE
```

Related Commands

Command	Description
dir	Displays the contents of a specified VFW application file system.

copy ftp:

To copy a file, software image, running-configuration file, or startup-configuration file from a remote FTP server to a location on the VFW application, use the **copy ftp:** command in EXEC mode.

copy ftp://*server***/***path*[**/***filename*] {**disk0:**[*path/*]*filename* | **image:**[*image_name*] | **running-config** | **startup-config**}

Syntax Description

ftp://*server***/***path*[**/***filename*]	Specifies the File Transfer Protocol (FTP) network server and, optionally, the file to copy.
disk0:[*path/*]*filename*	Specifies that the file destination is the disk0: directory of the current context and the filename. If you do not provide the optional path, the VFW application copies the file to the root directory on the disk0: file system.
image: [*image_name*]	Specifies to copy a system software image to flash memory. Use the **boot system** command in configuration mode to specify the BOOT environment variable. The BOOT environment variable specifies a list of image files on various devices from which the VFW application can boot at startup. The **image:** keyword is available only in the Admin context. The *image_name* argument is optional. If you do not enter a name, the VFW application uses the source filename.
running-config	Specifies to replace the running-configuration file currently residing on the VFW application in RAM (volatile memory).
startup-config	Specifies to replace the startup-configuration file currently residing on the VFW application in flash memory (nonvolatile memory).

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 config-copy 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 copy a startup-configuration file from a remote FTP server to the VFW application:

```
firewall/Admin# copy ftp://192.168.1.2/startup_config_Adminctx startup-config
```

Related Commands

Command	Description
show running-config	Displays the running-configuration information associated with the current context.
show startup-config	Displays the startup-configuration information associated with the current context.

copy image:

To copy a VFW application software system image from flash memory to a remote server using FTP, SFTP, or TFTP, use the **copy image:** command in EXEC mode.

copy image:*image_filename* {**ftp://***server*/*path*[/*filename*] |
sftp://[*username*@]*server*/*path*[/*filename*] | **tftp://***server*[**:***port*]/*path*[/*filename*]}

Syntax Description

image_filename	Name of the VFW application system software image. Use the **dir image:** command or the **show version** command to view the software system images available in flash memory.
ftp://*server*/*path*[/*filename*]	Specifies the File Transfer Protocol (FTP) network server and, optionally, the renamed image.
sftp://[*username*@]*server*/*path*[/*filename*]	Specifies the Secure File Transfer Protocol (SFTP) network server and, optionally, the renamed image.
tftp://*server*[**:***port*]/*path*[/*filename*]	Specifies the Trivial File Transfer Protocol (TFTP) network server and, optionally, the renamed image.

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 config-copy 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*.

When you select a destination file system using **ftp:**, **sftp:**, or **tftp:**, the VFW application:

- Prompts you for your username and password if the destination file system requires user authentication.
- Prompts you for the server information if you do not provide the information with the command.
- Copies the file to the root directory of the destination file system if you do not provide path information.

Examples

The following example shows how to save a software system image to a remote FTP server:

```
firewall/Admin# copy image:sb-ace.NOV_11 ftp://192.168.1.2
```

Related Commands

Command	Description
dir	Displays the contents of a specified VFW application file system.

copy running-config

To copy the contents of the running-configuration file in RAM (volatile memory) to the startup-configuration file in flash memory (nonvolatile memory) or a network server, use the **copy running-config** command in EXEC mode.

copy running-config {**disk0:**[*path/*]*filename* | **startup-config** | **ftp://***server/path*[*/filename*] | **sftp://**[*username*@]*server/path*[*/filename*] | **tftp://***server*[**:***port*]*/path*[*/filename*]}

Syntax Description

disk0:[*path/*]*filename*	Specifies that the running configuration is copied to a file on the disk0: file system. If you do not provide the optional path, the VFW application copies the file to the root directory on the disk0: file system.
startup-config	Copies the running-configuration file to the startup-configuration file.
ftp://*server/path*[*/filename*]	Specifies the File Transfer Protocol (FTP) network server and, optionally, the renamed file.
sftp://[*username*@]*server/path*[*/filename*]	Specifies the Secure File Transfer Protocol (SFTP) network server and, optionally, the renamed file.
tftp://*server*[**:***port*]*/path*[*/filename*]	Specifies the Trivial File Transfer Protocol (TFTP) network server and, optionally, the renamed file.

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 config-copy 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*.

When you select a destination file system using **ftp:**, **sftp:**, or **tftp:**, the VFW application:

- Prompts you for your username and password if the destination file system requires user authentication.
- Prompts you for the server information if you do not provide the information with the command.
- Copies the file to the root directory of the destination file system if you do not provide path information.

To copy the running configuration to the startup configuration, you can also use the **write memory** command.

Examples

The following example shows how to save the running-configuration file to the startup-configuration file in flash memory on the VFW application:

```
firewall/Admin# copy running-config startup-config
```

Related Commands

Command	Description
show running-config	Displays the running- configuration information associated with the current context.
show startup-config	Displays the startup-configuration information associated with the current context.
write	Manages persistent and nonpersistent configuration information.

copy sftp:

To copy a file, software image, running-configuration file, or startup-configuration file from a remote SFTP server to a location on the VFW application, use the **copy sftp:** command in EXEC mode.

copy sftp://[*username*@]*server*/*path*[/*filename*] {**disk0:**[*path*/]*filename*| **image:**[*image_name*]| **running-config** | **startup-config**}

Syntax Description

sftp://[*username*@]*server*/*path*[/*filename*]	Specifies the Secure File Transfer Protocol (SFTP) network server and, optionally, the renamed file.
disk0:[*path*/]*filename*	Specifies that the file destination is the disk0: directory of the current context and the filename. If you do not provide the optional path, the VFW application copies the file to the root directory on the disk0: file system.
image: [*image_name*]	Specifies to copy a system software image to flash memory. Use the **boot system** command in configuration mode to specify the BOOT environment variable. The BOOT environment variable specifies a list of image files on various devices from which the VFW application can boot at startup.The **image:** keyword is available only in the Admin context. The *image_name* argument is optional. If you do not enter a name, the VFW application uses the source filename.
running-config	Specifies to replace the running-configuration file currently residing on the VFW application in RAM (volatile memory).
startup-config	Specifies to replace the startup-configuration file currently residing on the VFW application in flash memory (nonvolatile memory).

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 config-copy 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 copy a startup-configuration file from a remote SFTP server to the VFW application:

```
firewall/Admin# copy sftp://192.168.1.2/startup_config_Adminctx startup-config
```

Related Commands

Command	Description
show running-config	Displays the running-configuration information associated with the current context.
show startup-config	Displays the startup-configuration information associated with the current context.

copy startup-config

To merge the contents of the startup-configuration file into the running-configuration file or copy the startup-configuration file to a network server, use the **copy startup-config** command in EXEC mode.

copy startup-config {**disk0:**[*path/*]*filename* | **running-config** | **ftp://***server*/*path*[/*filename*] | **sftp://**[*username*@]*server*/*path*[/*filename*] | **tftp://***server*[**:***port*]/*path*[/*filename*]}

Syntax Description

disk0:[*path/*]*filename*	Specifies that the startup configuration is copied to a file on the disk0: file system. If you do not provide the optional path, the VFW application copies the file to the root directory on the disk0: file system.
running-config	Merges contents of the startup-configuration file into the running-configuration file.
ftp://*server*/*pat*[/*filename*]	Specifies the File Transfer Protocol (FTP) network server and, optionally, the renamed file.
sftp://[*username*@]*server*/*path*[/*filename*]	Specifies the Secure File Transfer Protocol (SFTP) network server and, optionally, the renamed file.
tftp://*server*[**:***port*]/*path*[/*filename*]	Specifies the Trivial File Transfer Protocol (TFTP) network server and, optionally, the renamed file.

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 config-copy 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*.

When you select a destination file system using **ftp:**, **sftp:**, or **tftp:**, the VFW application:

- Prompts you for your username and password if the destination file system requires user authentication.
- Prompts you for the server information if you do not provide the information with the command.
- Copies the file to the root directory of the destination file system if you do not provide path information.

Examples

The following example shows how to merge the contents of the startup-configuration file into the running-configuration file in flash memory:

```
firewall/Admin# copy startup-config running-config
```

Related Commands

Command	Description
show startup-config	Displays the startup-configuration information associated with the current context.

copy tftp:

To copy a file, software image, running-configuration file, or startup-configuration file from a remote TFTP server to a location on the VFW application, use the **copy tftp:** command in EXEC mode.

copy tftp://*server*[**:***port*]**/***path*[**/***filename*] {**disk0:**[*path/*]*filename* | **image:**[*image_name*]| **running-config** | **startup-config**}

Syntax Description

tftp://*server*[**:***port*]**/***path* [**/***filename*]	Specifies the Trivial File Transfer Protocol (TFTP) network server and, optionally, the renamed file.
disk0:[*path/*]*filename*	Specifies that the file destination is the disk0: directory of the current context and the filename. If you do not provide the optional path, the VFW application copies the file to the root directory on the disk0: file system.
image: [*image_name*]	Specifies to copy a system software image to flash memory. Use the **boot system** command in configuration mode to specify the BOOT environment variable. The BOOT environment variable specifies a list of image files on various devices from which the VFW application can boot at startup.The **image:** keyword is available only in the Admin context. The *image_name* argument is optional. If you do not enter an name, the VFW application uses the source filename.
running-config	Specifies to replace the running-configuration file currently residing on the VFW application in RAM (volatile memory).
startup-config	Specifies to replace the startup-configuration file currently residing on the VFW application in flash memory (nonvolatile memory).

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 config-copy 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 copy a startup-configuration file from a remote TFTP server to the VFW application:

```
firewall/Admin# copy tftp://192.168.1.2/startup_config_Adminctx startup-config
```

Related Commands

Command	Description
show running-config	Displays the running-configuration information associated with the current context.
show startup-config	Displays the startup-configuration information associated with the current context.

debug

To enable the VFW application debugging functions, use the **debug** command in EXEC mode.

debug {**aaa** | **access-list** | **buffer** | **cfg_cntlr** | **cfgmgr** | **clock** | **fifo** | **fm** | **fwc** | **ha_dp_mgr** | **ha_mgr** | **hm** | **ifmgr** | **ipcp** | **ldap** | **logfile** | **nat-download** | **netio** | **pfmgr** | **pktcap** | **radius** | **security** | **sme** | **snmp** | **syslogd** | **system** | **tacacs+** | **tl** | **virtualization** | **vnet**}

Syntax Description

aaa	Enables debugging for aaa.
access-list	Enables access-list debugging.
buffer	Configures debugging of CP buffer manager.
cfg_cntlr	Enables configuration controller debugging.
cfgmgr	Enables configuration manager debugging.
clock	Enables clock module debugging.
fifo	Configures debugging of the Packet FIFO Driver.
fm	Enables VFW application Feature Manager debugging.
fwc	Enables FWC debugging.
ha_dp_mgr	Enables HA-DP debugging.
ha_mgr	Enables HA debugging.
hm	Enables HM debugging.
ifmgr	Enables interface manager debugging.
ipcp	Enables debugging of kernel IPCP components.
ldap	Configures debugging for LDAP.
logfile	Directs the debug output to a log file.
nat-download	Enables NAT download debugging.
netio	Enables debugging of CP network I/O.
pfmgr	Enables platfrom manager debugging.
pktcap	Enables packet capture debugging.
radius	Configures debugging for the RADIUS daemon.
routemgr	Enables route manager debugging.
security	Configures debugging for security and accounting.
sme	Enables System Manager Extension debugging.
snmp	Configures SNMP-server debugging.
syslogd	Enables syslogd debugging.
system	Enables debugging of the system components.
tacacs+	Configures debugging for TACACS+.
tl	Configures debugging of the TL driver.
virtualization	Enables virtualization debugging.
vnet	Configures debugging of the virtual net-device driver.

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	The **all** and **hardware** keywords were removed.

Usage Guidelines

This command is available to roles that allow debugging and available to network monitor or technician users. 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*.

The VFW application **debug** commands are intended for use by trained Cisco Technical Support personnel only. Entering these commands may cause unexpected results. Do not attempt to use these commands without guidance from Cisco Technical Support personnel.

Examples

The following example shows how to enable all AAA debugging options:

```
firewall/Admin# debug aaa all
```

Related Commands

Command	Description
clear debug-logfile	Removes a debug log file.
show debug	Displays the debug flags.

delete

To delete a specified file in a VFW application file system, use the **delete** command in EXEC mode.

delete {**core:***filename* | **disk0:**[*path/*]*filename* | **image:***filename* | **volatile:***filename*}

Syntax Description

core:*filename*	Deletes the specified file from the core: file system.
disk0:[*path/*]*filename*	Deletes the specified file from the disk0: file system. If you do not specify the optional path, the VFW application looks for the file in the root directory of the disk0: file system.
image:*filename*	Deletes the specified file from the image: file system.
volatile:*filename*	Deletes the specified file from the volatile: file system.

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 has no user role feature restrictions. 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*.

If you do not specify a filename with the specified file system, the VFW application prompts you for a file name.

To display the list of files that reside in a file system, use the **dir** command.

Examples

The following example shows how to delete the file 0x401_VSH_LOG.25256.TAR.GZ from the core: file system:

```
firewall/Admin# delete core:0x401_VSH_LOG.25256.TAR.GZ
```

Related Commands

Command	Description
dir	Displays the contents of a specified VFW application file system.

dir

To display the contents of a specified VFW application file system, use the **dir** command in EXEC mode.

dir {**core:** | **disk0:**[*path/*][*filename*] | **image:**[*filename*] | **volatile:**[*filename*]}

Syntax Description

core:	Displays the contents of the core: file system.
disk0:[*path/*]	Displays the contents of the disk0: file system. Specify the optional path to display the contents of a specific directory on the disk0: file system.
image:	Displays the contents of the image: file system.
volatile:	Displays the contents of the volatile: file system.
filename	(Optional) Specified file to display. Displays information, such as file size and the date the file was created. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

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 has no user role feature restrictions. 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 delete a file from a file system, use the **delete** command.

To delete all core dumps, use the **clear cores** command.

Examples

The following example shows how to display the contents of the drive0: file system:

```
firewall/Admin# dir disk0:
```

Related Commands

Command	Description
clear cores	Clears all the core dumps stored in the core: file system.
delete	Deletes a specified file in a VFW application file system.
show file	Displays the contents of a specified file in a directory in persistent memory (flash memory) or volatile memory (RAM).

end

To exit from configuration mode and return to EXEC mode, use the **end** command in configuration mode.

end

Syntax Description

This command has no arguments or keywords.

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 has no user role restrictions. 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 also press **Ctrl-Z** or enter the **exit** command to exit configuration mode.

Examples

The following example shows how to exit from configuration mode and return to EXEC mode:

```
firewall/Admin(config)# end
firewall/Admin#
```

Related Commands

Command	Description
exit	Exits out of EXEC mode and logs out of the CLI session.
exit (config)	Exits from the current configuration mode and returns to the previous mode.

exit

To exit EXEC mode and log out of the CLI session, use the **exit** command in EXEC mode.

exit

Syntax Description

This command has no arguments or keywords.

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 has no user role feature restrictions. 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 log out of an active CLI session:

```
firewall/Admin# exit
```

Related Commands

Command	Description
end	Exits from configuration mode and returns to EXEC mode.
exit (config)	Exits from the current configuration mode and returns to the previous mode.

exit (config)

To exit from the current configuration mode and return to the previous mode, use the **exit** command in the appropriate configuration mode.

exit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

All configuration modes

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 has no user role restrictions. 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*.

In configuration mode, the **exit** command transitions to the EXEC mode.

In all other configuration modes, the **exit** command transitions to the previous configuration mode.

You can also press **Ctrl-Z**, enter the **end** command, or enter the **exit** command to exit configuration mode.

Examples

The following example shows how to exit from configuration mode and return to EXEC mode:

```
firewall/Admin(config)# exit
firewall/Admin#
```

The following example shows how to exit from interface configuration mode and return to configuration mode:

```
firewall/Admin(config-if)# exit
firewall/Admin(config)#
```

Related Commands

Command	Description
end	Exits from configuration mode and returns to EXEC mode.
exit	Exits out of EXEC mode and logs out of the CLI session.

format disk0:

To erase all data stored on the flash memory and reformat it with the FAT16 version of the file allocation table, use the **format disk0:** command in EXEC mode. All user-defined configuration information is erased and the VFW application returns to the factory default settings.

format disk0:

Syntax Description

This command has no arguments or keywords.

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 Admin 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*.

Before you reformat the flash memory, consider saving a copy of the following VFW application operation and configuration attributes to a remote server:

- VFW application software image (use the **copy image:** command)
- Startup configuration of each context (use the **copy startup-config** command)
- Running configuration of each context (use the **copy running-config** command)
- Core dump files of each context (use the **copy core:** command)
- Packet capture buffers of each context (use the **copy capture** command)

After you reformat the flash memory, perform the following actions:

- Copy the VFW application software image to the image: file system using the **copy ftp:**, **copy tftp:**, or **copy sftp:** command
- Import the following configuration files into the associated context using the **copy disk0:** command:
  - Startup-configuration file
  - Running-configuration file

Examples

The following example shows how to reformat flash memory:

```
firewall/Admin# format disk0:
```

Related Commands

Command	Description
copy capture	Copies an existing context packet capture buffer as the source file in the VFW application compact flash to another file system.
copy ftp:	Copies a file, software image, running-configuration file, or startup-configuration file from a remote FTP server to a location on the VFW application.
copy sftp:	Copies a file, software image, running-configuration file, or startup-configuration file from a remote SFTP server to a location on the VFW application.
copy tftp:	Copies a file, software image, running-configuration file, or startup-configuration file from a remote TFTP server to a location on the VFW application.
dir	Displays the contents of a specified VFW application file system.

gunzip

To uncompress (unzip) LZ77 coded files residing in the disk0: file system, use the **gunzip** command in EXEC mode.

gunzip disk0:[*path/*]*filename*.gz

Syntax Description

disk0:[*path/*]*filename***.gz**	Specifies the name of the compressed file on the disk0: file system. The filename must end with a .gz extension. If you do not specify the optional path, the VFW application looks for the file in the root directory.

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 has no user role feature restrictions. 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 useful in uncompressing large files. The filename must end with a .gz extension for the file to be uncompressed using the **gunzip** command. The .gz extension indicates a file zipped by the gzip (GNU zip) compression utility.

To display a list of available zipped files on disk0:, use the **dir** command.

Examples

The following example shows how to unzip a series of compressed files from the file FILES_NEW in the disk0: file system:

```
firewall/Admin# gunzip disk0:FILES_NEW.gz
```

Related Commands

Command	Description
dir	Displays the contents of a specified VFW application file system.

hostname

To specify a hostname for the VFW application, use the **hostname** command in configuration mode. To reset the hostname to the default of switch, use the **no** form of this command.

hostname *name*

no hostname *name*

Syntax Description

name	New host name for the VFW application. Enter a case-sensitive text string that contains from 1 to 32 alphanumeric characters.

Defaults

No default behavior or values

Command Modes

Configuration

Admin context only

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 Admin user role. For details about role-based access control (RBAC) and user roles, see *Cisco Virtual Firewall Configuration Guide*.

The **hostname** command can be used in the Admin context only.

The hostname is used for the command-line prompts and default configuration filenames. If you establish sessions to multiple devices, the hostname helps you keep track of where you enter commands.

By default, the hostname for the VFW application is *firewall*.

Examples

The following example shows how to change the hostname of the VFW application from switch to VFW_1:

```
switch/Admin(config)# hostname VFW_1
VFW_1/Admin(config)#
```

Related Commands

This command has no related commands.

mkdir disk0:

To create a new directory in disk0:, use the **mkdir disk0:** command in EXEC mode.

mkdir disk0:[*path/*]*directory_name*

Syntax Description

[*path/*]*directory_name*	Name you assign the new directory. Specify the optional path if you want to create a directory within an existing directory.

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 has no user role feature restrictions. 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*.

If a directory with the same name already exists, the VFW application does not create the new directory and the "Directory already exists" message appears.

Examples

The following example shows how to create a directory in disk0: called TEST_DIRECTORY:

```
firewall/Admin# mkdir disk0:TEST_DIRECTORY
```

Related Commands

Command	Description
dir	Displays the contents of a specified VFW application file system.
rmdir disk0:	Removes a directory from the disk0: file system.

move disk0:

To move a file between directories in the disk0: file system, use the **move disk0:** command in EXEC mode.

move disk0:[*source_path/*]*filename* disk0:[*destination_path/*]*filename*

Syntax Description

source_path/	Path of the source directory
destination_path/	Path of the destination directory
filename	Name of the file to move in the disk0: file system

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 has no user role feature restrictions. 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*.

If a file with the same name already exists in the destination directory, that file is overwritten by the file you move.

Examples

The following example shows how to move the file called SAMPLEFILE in the root directory of disk0: to the MYSTORAGE directory in disk0:

```
firewall/Admin# move disk0:SAMPLEFILE disk0:MYSTORAGE/SAMPLEFILE
```

Related Commands

Command	Description
dir	Displays the contents of a specified VFW application file system.

ping

To verify the connectivity of a remote host or server by sending echo messages from the VFW application, use the **ping** (packet internet groper) command in EXEC mode.

ping *target_ip*

Syntax Description]

target_ip	IP address of the remote host to ping. Enter an IP address in dotted-decimal notation.

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 has no user role feature restrictions. 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*.

The ping program sends an echo request packet to an address from the current context on the VFW application, and then awaits a reply. The ping output can help you evaluate path-to-host reliability, delays over displaying the name of the current directory and path, and whether the host can be reached or is functioning.

To terminate a ping session before reaches its timeout value, type the Ctrl-C escape sequence.

Examples

The following example shows how to ping the FTP server with an IP address of 196.168.1.2, using the default ping session values:

```
firewall/Admin# ping 196.168.1.2
```

Related Commands

Command	Description
traceroute	Traces the route an IP packet takes to a network host from the VFW application.

rmdir disk0:

To remove a directory from the disk0: file system, use the **rmdir disk0:** command in EXEC mode.

rmdir disk0:*directory*

Syntax Description

directory	Name of the directory to remove

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 has no user role feature restrictions. 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 remove a directory from disk0:, the directory must be empty. To view the contents of a directory, use the **dir** command. To delete files from a directory, use the **delete** command.

Examples

The following example shows how to remove the directory TEST_DIRECTORY from disk0:

```
firewall/Admin# rmdir disk0:TEST-DIRECTORY
```

Related Commands

Command	Description
delete	Deletes a specified file in a VFW application file system.
dir	Displays the contents of a specified VFW application file system.
mkdir disk0:	Creates a new directory in disk0:.

show banner motd

To display the configured banner message of the day, use the **show banner motd** command in EXEC mode.

show banner motd

Syntax Description

This command has no arguments or keywords.

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 AAA 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 configure the banner message, use the **banner** command in configuration mode.

Examples

The following example shows how to display the message of the day:

```
firewall/Admin# show banner motd
```

Related Commands

Command	Description
banner motd	Specifies a message to display as the message-of-the-day banner when a user connects to the VFW application CLI.

show buffer

To display the buffer manager module messages, use the **show buffer** command in EXEC mode.

show buffer {**events-history** | **stats** | **usage**}

Syntax Description

events-history	Displays a historic log of the most recent messages generated by the buffer manager event history.
stats	Displays detailed counters for various buffer manager event occurrences.
usage	Displays the number of buffers currently being held (allocated but not freed) by each buffer module. The **usage** keyword also shows an estimate of the number of times a particular buffer module has freed the same buffer more than once (this indicates a software error condition).

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 has no user role feature restrictions. 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*.

The **show buffer** command is intended for use by trained Cisco Technical Support personnel for troubleshooting purposes only.

Examples

The following example shows how to display the control plane buffer event history:

```
firewall/Admin# show buffer events-history

1) Event:E_DEBUG, length:72, at 477729 usecs after Sat Jan 1 00:01:29 2000
[102] headers=0xd2369000, ctrl_blocks=0xd280a040, data_blocks=0xd5403aa0
2) Event:E_DEBUG, length:50, at 477707 usecs after Sat Jan 1 00:01:29 2000
[102] total blocks=151682 (ctrl=75841, data=75841)
```

Related Commands

Command	Description
clear buffer stats	Clears the control plane buffer statistics.

show capture

To display the packet information that the VFW application traces as part of the packet capture function, use the **show capture** command in EXEC mode.

show capture *buffer_name* [**detail** [**connid** *connection_id* | **range** *packet_start packet_end*] | **status**]

Syntax Description

buffer_name	Name of the packet capture buffer. Specify a text string from 1 to 80 alphanumeric characters.
detail	(Optional) Displays additional protocol information for each packet.
connid *connection_id*	(Optional) Displays protocol information for a specified connection identifier.
range *packet_start packet_end*	(Optional) Displays protocol information for range of captured packets.
status	(Optional) Displays capture status information for each packet.

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 has no user role feature restrictions. 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*.

For all types of received packets, the console display is in tcpdump format.

To copy the capture buffer information as a file in flash memory, use the **copy capture** command.

Examples

The following example shows how to display the captured packet information contained in packet capture buffer CAPTURE1:

```
switch/Admin# show capture CAPTURE1
```

Related Commands

Command	Description
copy capture	Copies an existing context packet capture buffer as the source file in the VFW application compact flash to another file system.

show checkpoint

To display information relating to the configured checkpoints, use the **show checkpoint** command in EXEC mode.

show checkpoint {**all** | **detail** *name*}

Syntax Description

all	Displays a list of all existing checkpoints.
detail *name*	Displays the running configuration of the specified checkpoint.

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 has no user role feature restrictions. 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 display the running configuration for the checkpoint MYCHECKPOINT:

```
firewall/Admin# show checkpoint detail MYCHECKPOINT
```

Related Commands

Command	Description
checkpoint	Creates or modifies a checkpoint (snapshot) of the running configuration.

show clock

To display the current date and time settings of the system clock, use the **show clock** command in EXEC mode.

show clock

Syntax Description

This command has no arguments or keywords.

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 has no user role feature restrictions. 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 configure the system clock setting, use the **clock** command in the configuration mode.

Examples

The following example shows how to display the current clock settings:

```
firewall/Admin# show clock
Fri Feb 24 20:08:14 UTC 2006
```

Related Commands

This command has no related commands.

show copyright

To display the software copyright information for the VFW application, use the **show copyright** command in EXEC mode.

show copyright

Syntax Description

This command has no arguments or keywords.

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 has no user role feature restrictions. 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 display the VFW application software copyright information:

```
firewall/Admin# show copyright
```

Related Commands

This command has no related commands.

show debug

To display the debug flags, use the **show debug** command in EXEC mode.

show debug {**aaa** | **access-list** | **ascii-cfg** | **buffer** | **cfg_cntlr** | **cfgmgr** | **clock** | **fifo** | **fm** | **fs-daemon** | **fwc** | **ha_dp_mgr** | **ha_mgr** | **hm** | **ifmgr** | **ipcp** | **ldap** | **logfile** | **nat-download** | **netio** | **pfmgr** | **pktcap** | **radius** | **security** | **sme** | **snmp** | **syslogd** | **system** | **tacacs+** | **tl** | **ttyd** | **virtualization** | **vnet** | **vshd**}

Syntax Description

aaa	Displays the 301 debugging flags.
access-list	Displays the access-list debug flags.
ascii-cfg	Displays the ASCII-cfg debugging flags.
buffer	Displays the CP buffer debugging flags.
cfg_cntlr	Displays the configuration controller debug flags.
cfgmgr	Displays the configuration manager debug flags.
clock	Displays the state of clock debug settings.
fifo	Displays the show packet FIFO debugging flags.
fm	Displays the feature manager debug flags.
fs-daemon	Displays the fs daemon debugging flags.
fwc	Displays the FWC debugging flags.
ha_dp_mgr	Displays the HA-DP manager debug flags.
ha_mgr	Displays the HA manager debug flags.
hm	Displays the HM debug flags.
ifmgr	Displays the interface manager debug flags.
ipcp	Displays the kernel IPCP debugging flags.
ldap	Displays the LDAP debugging flags.
logfile	Displays the contents of the log file.
nat-download	Displays the NAT download debug flags.
netio	Displays the CP net I/O debugging flags.
pfmgr	Displays the platform manager debug flags.
pktcap	Displays the packet capture debug flags.
radius	Displays the RADIUS debugging flags.
security	Displays the security/accounting debugging flags.
sme	Displays the System Manager Extension debug flags.
snmp	Displays the SNMP server debugging flags.
syslogd	Displays the syslogd debug flags.
system	Displays the system debugging flags.
tacacs+	Displays the TACACS+ debugging flags.
tl	Displays the CP buffer debugging flags.
ttyd	Displays the TTYD debugging flags.
virtualization	Displays the virtualization debug flags.

vnet	Displays the VNet driver debugging flags.
vshd	Displays the VSHD debugging flags.

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 debug 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*.

The VFW application **debug** commands are intended for use by trained Cisco Technical Support personnel only. Entering these commands may cause unexpected results. Do not attempt to use these commands without guidance from Cisco Technical Support personnel.

Examples

The following example shows how to display the VSHD debugging flags:

```
firewall/Admin# show debug vshd
```

Related Commands

Command	Description
debug	Enables the VFW application debugging functions.
clear debug-logfile	Removes a debug log file.

show fifo

To display the packet first in, first out (FIFO) statistics for the Pkt-Fifo module, use the **show fifo** command in EXEC mode.

show fifo {**event-history** | **registers** | **stats**}

Syntax Description

event-history	Displays a historic log of the most recent debug messages generated by the Pkt-Fifo module
registers	Displays the state of all the registers associated with the transmit and receive hardware engines.
stats	Displays detailed counters for the various Pkt-Fifo module event occurrences.

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 has no user role feature restrictions. 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*.

The **show fifo** command is intended for use by trained Cisco Technical Support personnel for troubleshooting purposes only.

Examples

The following example shows how to display the control plane packet FIFO registers:

```
firewall/Admin# show fifo registers
```

Related Commands

Command	Description
clear fifo stats	Clears the control plane packet first in, first out (FIFO) statistics.

show file

To display the contents of a specified file in a directory in persistent memory (flash memory) or volatile memory (RAM), use the **show file** command in EXEC mode.

show file {**disk0: | volatile:**[*directory/*]*filename*} [**cksum | md5sum**]

Syntax Description

disk0:	Specifies the disk0 file system in persistent memory.
volatile:	Specifies the file system in volatile memory.
[*directory/*]*filename*	Path and name of the specified file.
cksum	(Optional) Displays the CRC checksum for the file. The checksum values compute a cyclic redundancy check (CRC) for each named file. Use this command to verify that the files are not corrupted. You compare the checksum output for the received file against the checksum output for the original file.
md5sum	(Optional) Displays the MD5 checksum for the file. MD5 is an electronic fingerprint for the file. MD5 is the latest implementation of the Internet standards described in RFC 1321 and is useful for data security as well as integrity.

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 has no user role feature restrictions. 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 display the contents of file FILE1 stored in the directory MYFILES in disk0:

```
firewall/Admin# show file disk0:MYFILES/FILE1
```

Related Commands

Command	Description
clear cores	Clears all the core dumps stored in the core: file system.
delete	Deletes a specified file in a VFW application file system.
dir	Displays the contents of a specified VFW application file system.

show ip

To display the IP statistics, use the **show ip** command in EXEC mode.

show ip traffic

Syntax Description

traffic	Displays the IP protocol 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 has no user role feature restrictions. 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 display all IP route entries:

```
firewall/Admin# show ip traffic
```

Related Commands

No related commands.

show netio

To display the control plane network I/O information, use the **show netio** command in EXEC mode.

show netio {**clients** | **event-history** | **stats**}

Syntax Description

clients	Displays basic statistics for the applications that are transmitting and receiving packets through the Netio module.
event-history	Displays a historic log of the most recent debug network I/O messages.
stats	Displays detailed counters for various Netio event occurrences.

Defaults

No default behavior or values

Command Modes

EXEC

Admin context only

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 has no user role feature restrictions. 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*.

The **show netio** command is intended for use by trained Cisco Technical Support personnel for troubleshooting purposes only.

Examples

The following example shows how to display control plane network I/O client information:

```
firewall/Admin# show netio event-history

1) Event:E_DEBUG, length:73, at 921762 usecs after Sat Jan 1 00:04:55 2000
[105] ed_request_encap: Sending ARP_RESOLUTION for 75.0.0.6, in context 0
2) Event:E_DEBUG, length:78, at 921752 usecs after Sat Jan 1 00:04:55 2000
[105] ed_egress_route_lookup: Route lookup failure -96 for 75.0.0.6, context 0
```

Related Commands

Command	Description
clear netio stats	Clears the control plane network I/O statistics.

show np

To display the hardware information stored on the three network processors, use the **show np** command in EXEC mode.

show np *np_number* {**access-list** {**node interface** *interface_name* {**in** | **out**} *node_address* | **resource** | **root interface** *interface_name* {**in** | **out**} | **syslog** {**lineno-table** | **name-table**} | **trace interface** *interface_name* {**in** | **out**} **protocol** *prot_number* **source** *source_ip source_port* **destination** *dest_ip dest_port*} | **cpu** | **interface** {**icmlookup** [**all**] | **iflookup** [**all**]} | **me-stats** *ucdump_option* | **memory** | **nat** {**bitmap** *map_id* | **dest_nat** *policy_id* | **implicit-pat** | **policies** | **src-nat** *policy_id interface_id*}}

Syntax Description

np_number	Network processor number. Enter one of the following processor identifier numbers: • **0**—SiByte processor • **1**—IXP 0 processor • **2**—IXP 1 processor
access-list	Displays information related to the access control list (ACL).
node	Displays the contents of the hardware ACL node, identified by *interface*.
interface *interface_name*	Specifes the interface for which to display information.
in	Specifies the inbound traffic flow.
out	Specifies the outbound traffic flow.
node_address	Address of the node.
resource	Displays the access-list resource consumption statistics.
root	Displays the hardware address of the root of the downloaded, aggregated ACL, identified by *interface*.
trace	Traces a packet through a specific access-list.
protocol *prot_number*	Specifies a protocol number.
source	Specifies the source of the flow.
source_ip	Source IP address.
source_port	Source port number.
destination	Specifies the destination of a flow.
dest_ip	Destination IP address.
dest_port	Destination port number.
cpu	Displays processes CPU information.
interface	Displays information related to the interface tables.
icmlookup	Displays the ICM/OCM interface table from the CP (0) or the specified NP.
iflookup	Displays the fast path interface lookup table from the CP (0) or the specified NP.
me-stats	Displays Micro Engine statistics for IXP2800 Network Processor.

ucdump_option	Options for the ucdump utility. The ucdump utility is a binary on Xscale that returns information about Micro Engine statistics. Specify **--help** as the *ucdump_option* argument to list all the supported ucdump utility options. The maximum UCDUMP utility is up to 80 alphanumeric characters. **Note** The following ucdump utility options are disabled from **show np me-stats**: -C, -f, and -i.
memory	Displays processes memory information.
nat	Displays information related to the network processor Network Address Translation (NAT) tables.
bitmap *map_id*	Specifies the NAT-pool bitmap table in the network processor.
dest_nat *policy_id*	Specifies the destination NAT policy.
implicit-pat	Specifies the implicit Port Address Translation (PAT) policy table.
policies	Specifies the full NAT policy table.
src-nat	Specifies the source NAT policy.
policy_id	Policy identifier number. Enter a value from 0 to 65535.
interface_id	Mapped interface identifier. Enter a value from 0 to 65535.

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 ACL or interface 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*.

The **show np** command is intended for use by trained Cisco Technical Support personnel for troubleshooting purposes only.

Examples

The following example shows how to display the access-list information from the hardware, using network processor 0:

```
firewall/Admin# show np 0 access-list
```

The following example shows how to display Micro Engine statistics for a ucdump utility (-b, which instructs the VFW application to dump fastpath buffer memory):

```
firewall/Admin# show np me-stats -b

Fastpath thread buffers
================================

ME:1 thread:0 addr:0x0010 particle:0x00000000 len:78 rx_seq=7
0018  0x8500004e  0x00608034  0x0000001e  0x00101e07    ...N .`.4 .... ....
001c  0x0000ffff  0xffffffff  0x00059a3b  0x9a390800    .... .... ...; .9..
0020  0x4500002c  0xa4540000  0xff11fd64  0x0c010105    E.., .T.. ...d ....
0024  0x0c010101  0xc350c352  0x00185db6  0x000100f0    .... .P.R ..]. ....
0028  0x00000008  0x00000000  0x00000064  0x00000000    .... .... ...d ....
```

Related Commands

Command	Description
show processes	Displays the general information about all the processes running on the VFW application.

show processes

To display the general information about all the processes running on the VFW application, use the **show processes** command in EXEC mode. The **show processes** command displays summary CPU information for the SiByte 1250 Processor.

show processes [**cpu** | **log** [**details** | **pid** *process_id*] | **memory**]

Syntax Description

cpu	(Optional) Displays CPU information for processes running on the SiByte 1250 Processor.
log	(Optional) Displays information about process logs for the SiByte 1250 Processor.
details	(Optional) Displays detailed process log information for all process identifiers.
pid *process_id*	(Optional) Displays process information about a specific process identifier. The value of the *process_id* argument can be from 0 to 2147483647.
memory	(Optional) Displays processes memory information for the SiByte 1250 Processor.

Defaults

No default behavior or values

Command Modes

EXEC

Admin users (users with an Admin role), across all 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 Admin 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*.

The **show processes** command is available only to Admin users (users with an Admin role) across all contexts. The displayed system processes information is at the CPU system level (the total CPU usage) and is not on a per-context level.

Examples

The following example shows how to display processes memory information for the SiByte 1250 Processor:

```
firewall/Admin# show processes mem
```

Related Commands

Command	Description
clear processes log	Clears processes log statistics.
show np	Displays the hardware information stored on the three network processors.
show tech-support	Displays information that is useful to technical support when reporting a problem with your VFW application.

show running-config

To display the running-configuration information associated with the current context, use the **show running-config** command in EXEC mode.

show running-config [**aaa** | **access-list** | **class-map** | **context** | **domain** | **ft** | **interface** | **object-group** | **parameter-map** | **policy-map** | **resource-class** | **role**]

Syntax Description

aaa	(Optional) Displays AAA information.
access-list	(Optional) Displays access list (ACL) information.
class-map	(Optional) Displays the list of all class-maps configured for the current context. The VFW application also displays configuration information for each class map listed.
context	(Optional) Displays the list of contexts configured on the VFW application. The VFW application also displays the resource class (member) assigned to each context. The **context** keyword works only from within the Admin context.
domain	(Optional) Displays the list of domains configured for the current context. The VFW application also displays configuration information for each domain listed.
ft	(Optional) Displays the list of redundancy or fault-tolerant (FT) configurations configured for the current context. The VFW application also displays configuration information for each FT configuration listed.
interface	(Optional) Displays interface information.
object-group	(Optional) Displays object group information.
parameter-map	(Optional) Displays parameter map information.
policy-map	(Optional) Displays policy map information.
resource-class	(Optional) Displays resource class information.
role	(Optional) Displays the list of roles configured for the current context. The VFW application also displays configuration information for each role on the list.

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	The **object-group** keyword was added.

Usage Guidelines

This command has no user role feature restrictions. 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*.

The **show running-config** command is a context-sensitive command. The VFW application creates a running configuration for each context you create; therefore, to display the running-config of a specific context, you must execute the **show running-config** command from within the desired context. If you need to change to another context before executing the **show running-config** command, use the **changeto** command or log directly in to the desired context.

Use the **copy capture** command to:

- Save a copy of the running configuration to a file on one or more destination locations.
- Save the running configuration as the startup configuration.
- Save the startup configuration as the running configuration.

Examples

The following example shows how to display the entire running configuration:

```
firewall/Admin# show running-config
```

Related Commands

Command	Description
copy capture	Copies an existing context packet capture buffer as the source file in the VFW application compact flash to another file system.
show startup-config	Displays the startup configuration information associated with the current context.
show tech-support	Displays information that is useful to technical support when reporting a problem with your VFW application.
write	Manages persistent and nonpersistent configuration information.

show security internal event-history

To display the security event history information, use the **show security internal event-history** command in EXEC mode.

show security internal event-history {**errors** | **msgs**}

Syntax Description

errors	Displays the debug error logs of the security manager.
msgs	Displays the message logs of the security manager.

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 Admin 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*.

The **show security internal event-history** command is intended for use by trained Cisco Technical Support personnel for troubleshooting purposes only.

Examples

The following example shows how to display the error logs of the security manager:

```
firewall/Admin# show security internal event-history errors
```

Related Commands

This command has no related commands.

show startup-config

To display the startup-configuration information associated with the current context, use the **show startup-config** command in EXEC mode.

show startup-config

Syntax Description

This command has no arguments or keywords.

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 has no user role feature restrictions. 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 the startup configuration, use the **clear startup-config** command.

To copy the running configuration to the startup configuration, or to copy the startup configuration to the running configuration, use the **copy running-config** command.

Examples

The following example shows how to display the startup-configuration information:

```
firewall/Admin# show startup-config
```

Related Commands

Command	Description
clear startup-config	Clears the startup configuration of the current context.
copy capture	Copies an existing context packet capture buffer as the source file in the VFW application compact flash to another file system.
show running-config	Displays the running-configuration information associated with the current context.

show system

To display the VFW application system information, use the **show system** command in EXEC mode.

show system {**cpuhog** | **error-id** {*hex_id* | **list**} | **internal** | **kmemtrack** | **resources** | **skbtrack** | **uptime**}

Syntax Description

cpuhog	Displays system CPU hogs.
error-id	Displays description about errors.
hex_id	Error ID in hexadecimal format. The range is 0x0 to 0xffffffff.
list	Specifies all error IDs.
internal	Displays Cisco internal system-related functions. The **internal** keywords and related keywords, options, and arguments are intended for use by trained Cisco Technical Support personnel for troubleshooting purposes only.
kmemtrack	Displays system kernel memory track.
resources	Displays system-related CPU and memory statistics.
uptime	Displays how long the VFW application has been up and running.

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 has no user role feature restrictions. 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 display system resource information:

```
firewall/Admin# show system resources
```

Related Commands

This command has no related commands.

show tech-support

To display information that is useful to technical support when reporting a problem with your VFW application, use the **show tech-support** command in EXEC command.

show tech-support [**details**]

Syntax Description

details	(Optional) Provides detailed information for each of the **show** commands described below in the "Usage Guidelines" section.

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 has no user role feature restrictions. 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*.

The **show tech-support** command is useful when collecting a large amount of information about your VFW application for troubleshooting purposes with Cisco Technical Support. The output of this command can be provided to technical support representatives when reporting a problem.

The **show tech-support** command displays the output of several **show** commands at once. The output from this command varies, depending on your configuration. The default output of the **show tech-support** command includes the output of the following commands:

- **show interface—**See the **show interface** command
- **show process—**See the **show processes** command
- **show running-config—**See the **show running-config** command

Explicitly set the terminal length command to 0 (zero) to disable auto-scrolling and enable manual scrolling.

Use the **tac-pac** command in EXEC mode to redirect the output of the **show tech-support** command to a file that you can then send to the disk0: file system on the VFW application or to a remote server using File Transfer Protocol (FTP), Secure Copy Protocol (SCP), Secure Transfer Protocol (SFTP), or Trivial Transfer Protocol (TFTP).

Examples

The following example shows how to display the summary version of the technical support report:

```
firewall/Admin# show tech-support

`show clock`
Thu Mar  6 11:59:22 PST 2008

`show system uptime`
System start time:          Fri Feb 22 02:06:57 2008
System uptime:              13 days, 9 hours, 52 minutes, 25 seconds
Kernel uptime:              13 days, 9 hours, 51 minutes, 13 seconds

`show running-config`

Generating configuration....
version 3.7.0.13I
access-list a1 line 8 extended permit tcp host 2.2.2.2 eq www host 3.3.3.3 eq www
interface i1
interface management m1
domain d2
domain d3
username ciscoSupport password 5 $1$ADSJELHX$5ueYedT9N.yZdE2gr/Mc71  role Admin domain
default-domain
username admin password 5 $1$faXJEFBj$TJR1Nx7sLPTi5BZ97v08c/  role Admin domain
default-domain
username www password 5 $1$UZIiwUk7$QMVYN1JASaycabrHkhGcS/  role Admin domain
default-domain
username user1 password 5 $1$3cAJlyK1$IwgNI6mibD1tiVRwsbI7X0  role Network-Monitor domain
default-domain

`show interface`

i1 is administratively down
  FT status is non-redundant
  Description:not set
  Last cleared: never
  Active IP address not set
     0 unicast packets input, 0 bytes
     0 broadcast
     0 input errors, 0 unknown, 0 ignored
     0 unicast packets output, 0 bytes
     0 broadcast
     0 output errors, 0 ignored

m1 is administratively down
  FT status is non-redundant
  Description:not set
  Last cleared: never
  Active IP address not set
  Active IP address not set
  Peer IP address not set
     0 unicast packets input, 0 bytes
     0 broadcast
     0 input errors, 0 unknown, 0 ignored
     0 unicast packets output, 0 bytes
     0 broadcast
     0 output errors, 0 ignored

`dir core:`

           Usage for core: filesystem
                    1068032 bytes total used
                  202029056 bytes free
                  203097088 total bytes
```

.
.

Related Commands

Command	Description
show interface	Displays the interface information.
show processes	Displays the general information about all the processes running on the VFW application.
show running-config	Displays the running-configuration information associated with the current context.

show vnet

To display the virtual network (VNET) device information, use the **show vnet** command in EXEC mode.

show vnet {**event-history** | **stats**}

Syntax Description

event-history	Displays a historic log of the most recent debug VNET messages.
stats	Displays detailed counters for various VNET event occurrences.

Defaults

No default behavior or values

Command Modes

EXEC

Admin context only

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 has no user role feature restrictions. 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*.

The **show vnet** command can be used in the Admin context only.

The **show vnet** command is intended for use by trained Cisco Technical Support personnel for troubleshooting purposes only.

Examples

The following example shows how to display control plane VNET device statistics:

```
firewall/Admin# show vnet stats
```

Related Commands

Command	Description
clear vnet stats	Controls plane virtual network (VNET) device statistics.

system internal snapshot service

To generate a debug snapshot of a service, use the **system internal snapshot service** command in EXEC mode.

system internal snapshot service {*name*}

Syntax Description

name	Name of a system service for which you want to take a snapshot. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

Defaults

No default behavior or values

Command Modes

EXEC

Admin context only

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 Admin role in the Admin context. 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*.

The **system internal snapshot service** command can be used in the Admin context only.

This command is intended for use by trained Cisco Technical Support personnel for troubleshooting purposes only.

Examples

The following example shows how to take a snapshot of a service:

```
firewall/Admin# system internal snapshot service
```

Related Commands

This command has no related commands.

tac-pac

To save Cisco Technical Support information to a local or remote location, use the **tac-pac** command in EXEC mode.

tac-pac [**ftp://***server*/*path*[/*filename*] | **scp://***server*/*path*[/*filename*] | **sftp://**[*username*@]*server*/*path*[/*filename*] | **tftp://***server*[**:***port*]/*path*[/*filename*] | **disk0:**[*path*/]*filename*]

Syntax Description

ftp://*server*/*path*[/*filename*	Specifies the File Transfer Protocol network server as the destination.
scp://*server*/*path*[/*filename*	Specifies the Secure Copy network server as the destination.
sftp://[*username*@]*server*/*path*[/*filename*]	Specifies the Secure File Transfer Protocol network server as the destination.
tftp://*server*[**:***port*]/*path*[/*filename*]	Specifies the Trivial File Transfer Protocol network server as the destination.
disk0:[*path*/]*filename*]	Specifies the disk0: file system in flash memory on the VFW application as the destination.

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 has no user role feature restrictions. 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*.

The Cisco Technical Support information that the VFW application saves when using the **tac-pac** command is the same information that you can display using the **show tech-support** command.

If you do not specify a directory on a file system, the default is the root directory.

Examples

The following example shows how to save Cisco Technical Support information to SFTP server 196.168.1.2:

```
firewall/Admin# tac-pac sftp:196.168.1.2/TACFILES/
```

Related Commands

Command	Description
show tech-support	Displays information that is useful to technical support when reporting a problem with your VFW application.

traceroute

To trace the route an IP packet takes to a network host from the VFW application, use the **traceroute** command in EXEC mode.

traceroute [*ip_address* [**size** *packet*]]

Syntax Description

ip_address	(Optional) IP address of the network host. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).
size *packet*	(Optional) Specifies the packet size. Enter a number from 40 to 452. The default is 40.

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 has no user role feature restrictions. 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*.

The **traceroute** command traces the route an IP packet follows to an Internet host by launching User Datagram Protocol (UDP) probe packets with a small time to live (TTL), then listening for an Internet Control Message Protocol (ICMP) “time exceeded” reply from a gateway.

Examples

The following example shows how to display the route a packet takes from the VFW application to a network host with the IP address 196.126.1.2:

```
firewall/Admin# traceroute 196.126.1.2
```

Related Commands

Command	Description
ping	Verifies the connectivity of a remote host or server by sending echo messages from the VFW application.

undebug all

To disable all debugging, use the **undebug all** command in EXEC mode.

undebug all

Syntax Description

This command has no arguments or keywords.

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 is available to all user roles that allow debugging and is not available to network monitor or technician users. 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*.

The VFW application **debug** commands are intended for use by trained Cisco Technical Support personnel only. Entering these commands may cause unexpected results. Do not attempt to use these commands without guidance from Cisco Technical Support personnel.

Examples

The following example shows how to disable all debugging:

```
firewall/Admin# undebug all
```

Related Commands

Command	Description
debug	Enables the VFW application debugging functions.

untar disk0:

To untar a single file with a .tar extension in the disk0: file system, use the **untar disk0:** command in EXEC mode.

untar disk0:[*path*/]*filename*

Syntax Description

[*path*/]*filename*	Name of the .tar file on the disk0: file system. The filename must end with a .tar extension.

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 has no user role feature restrictions. 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 untar the mytarfile.tar file on disk0:

```
firewall/Admin# untar disk0:mytarfile.tar
```

Related Commands

Command	Description
gunzip	Uncompresses (unzips) LZ77 coded files residing in the disk0: file system.

write

To manage persistent and nonpersistent configuration information, use the **write** command in EXEC mode.

write {**erase** | **memory** [**all**] | **terminal**}

Syntax Description

erase	Erases the entire startup configuration with the exception of any configuration that affects the loader functionality. The startup configuration then reverts back to the factory default values. The running configuration is not affected.
memory	Writes the running configuration to the startup configuration.
all	(Optional) Writes configurations for all existing contexts. This keyword is available only in the Admin context.
terminal	Writes the running configuration to the terminal.

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

The different versions of this command require the following user role or feature in your user role:

- **write erase**—Admin user
- **write mem**—config-copy feature
- **write all**—Admin user

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*.

If you intend to use the **write memory** command to save the contents of the running-configuration file for the current context to the startup-configuration file, be sure to also specify this command in the Admin context. This step is important to save changes to the Admin context startup-configuration file; the Admin context startup-configuration file contains all configurations used to create each user context.

To write the running configuration to the startup configuration, you can also use the **copy running-config startup-config** command. To erase the startup configuration, you can also use the **clear startup-config** command. To display the running configuration, you can also use the **show running-config** command.

Examples

The following example shows how to write the running configuration to the startup configuration:

```
firewall/Admin# write memory
```

Related Commands

Command	Description
clear startup-config	Clears the startup configuration of the current context.
show running-config	Displays the running-configuration information associated with the current context.

xml-show

To enable the display of raw XML request **show** command output in XML format, use the **xml-show** command in EXEC mode.

xml-show {**off** | **on** | **status**}

Syntax Description

off	Displays CLI **show** command output in regular CLI display output, not in XML format.
on	Displays CLI **show** command output in XML format unless a specific **show** command is not implemented to display its output in XML format.
status	Displays the current setting of the **xml-show** command (on or off).

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 has no user role feature restrictions. 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*.

By default, XML responses automatically appear in XML format if the corresponding CLI **show** command output supports the XML format. However, if you are running commands on the CLI console or you are running raw XML responses from NMS, the XML responses appear in regular CLI display format.

You can enable the display of raw XML request **show** command output in XML format by performing one of the following actions:

- Specifying the **xml-show on** command in EXEC mode from the CLI, or
- Including the **xml-show on** command in the raw XML request itself (CLI commands included in an XML wrapper).

Specification of the **xml-show on** command is not required if you are running true XML.

For details on the **show** command output supported in XML format, consult the VFW application DTD file, cisco_ace.dtd, that is included as part of the software image. The VFW application DTD File contains the information on the XML attributes for those **show** commands that support XML format.

The **off** and **on** keywords affect only the current CLI session in use; they are session-based functions.

Examples

The following example shows how to enable the display of raw XML request **show** command output in XML format from the CLI:

```
firewall/Admin# xml-show on
```

Related Commands

This command has no related commands.