



Interface Commands on the Virtual Firewall

This module describes the Cisco IOS XR software commands used to configure and view Virtual Firewall (VFW) management interfaces.



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*.

alias

To configure an IP address that is shared between active and standby modules for a VFW interface, use the **alias** command in management interface configuration mode. To instruct the VFW application to ignore the command, use the **no** form of this command.

alias *ip_address mask*

no alias

Syntax Description

<i>ip_address</i>	IP address in dotted-decimal notation.
<i>mask</i>	Network mask in dotted decimal notation.

Defaults

No default behavior or values

Command Modes

Management interface configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

This command requires the 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*.

You must configure redundancy (fault tolerance) on the virtual firewall application for the alias IP address to work. For more information on redundancy, see the [“Configuring High Availability on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*. An IP alias can be configured only on management interfaces.

Examples

The following example shows how to configure an alias:

```
firewall/Admin(config-if-mgmt) # alias 192.168.12.15 255.255.255.0
```

clear interface

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

clear interface

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines This command requires the 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 following example shows how to clear all the interface statistics:

```
firewall/Admin# clear interface
```

Command	Description
show interface	Displays the interface information.

description (interface)

To provide a description for an interface, use the **description** command in the appropriate interface configuration mode. To delete the description, use the **no** form of this command.

description *text*

no description

Syntax Description

<i>text</i>	Description for the interface. Enter an unquoted text string containing a maximum of 240 characters including spaces.
-------------	---

Defaults

No default behavior or values

Command Modes

Interface configuration
Management interface configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

This command requires the 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*.

Use the **description** command to add a description to an interface configuration. The maximum number of characters is 240.

Examples

The following example shows how to configure a description for an interface:

```
firewall/admin(config-if)# description Management Ethernet Interface
```

Related Commands

Command	Description
show interface	Displays the interface information.

follow-active

To configure an active IP address on a management interface, use the **follow-active** command in management interface configuration mode. To instruct the VFW application to ignore the command, use the **no** form of this command.

follow-active *ip_address mask*

no follow-active

Syntax Description

<i>ip_address</i>	IP address in dotted-decimal notation.
<i>mask</i>	Network mask in dotted decimal notation.

Defaults

No default behavior or values

Command Modes

Management interface configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

This command requires the 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 **follow-active** command is applicable to management interfaces only. The **follow-active** command specifies that the location of the VFW management interface follows the location of the active firewall context.

Examples

The following example shows how to configure an active IP address:

```
firewall/Admin(config-if-mgmt)# follow-active 192.168.12.15 255.255.255.0
```

interface

To configure a VFW interface and enter interface configuration mode, use the **interface** command in configuration mode. To delete the interface, use the **no** form of this command.

interface [**management**] *interface_name*

no interface [**management**] *interface_name*

Syntax Description

management	Specifies to configure a management interface.
<i>interface_name</i>	Name of the interface to configure. Enter an unquoted text string with no spaces and a maximum of 30 alphanumeric characters.

Defaults

No default behavior or values

Command Modes

Configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

This command requires the 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*.

When you create an interface, the interface is in the shutdown state until you enable it. Use the **no shutdown** command to enable an interface.

Usage Guidelines

The following example shows how to configure a VFW interface:

```
firewall/Admin(config)# interface vfw1
```

The following example shows how to configure a management interface:

```
firewall/Admin(config)# configure  
firewall/Admin(config-if)# interface management MGMT_ACCESS
```

Related Commands

Command	Description
no shutdown	Enables an interface.

ip address

To assign an IP address on a VFW management or fault-tolerant (FT) interface, use the **ip address** command in the appropriate interface configuration mode. To delete the IP address, use the **no** form of this command.

ip address *ip_address mask*

no interface *ip_address mask*

Syntax Description		
<i>ip_address</i>		IP address for the interface. Enter an IPv4 address in dotted-decimal notation.
<i>mask</i>		Mask for the associated IP subnet. The network mask is a four-part dotted decimal address. For example, 255.0.0.0 indicates that each bit equal to 1 means that the corresponding address bit belongs to the network address.

Defaults No default behavior or values

Command Modes Management interface configuration
FT interface configuration

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

Usage Guidelines This command requires the 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*.

IP addresses can be configured on management interfaces only.

Usage Guidelines The following example shows how to configure an IP address on a management interface:

```
firewall/Admin(config)# interface management MGMT_ACCESS
firewall/Admin(config-if)# ip address 192.168.1.1 255.255.255.0
```

Related Commands	Command	Description
	no shutdown	Enables an interface.

nat-pool

To create a pool of IP addresses for dynamic NAT for an interface, use the **nat-pool** command in interface configuration mode. To remove a NAT pool from the configuration, use the **no** form of this command.

```
nat-pool nat_id ip_address1 [ip_address2] netmask mask [pat]
```

```
no nat-pool nat_id ip_address1 [ip_address2] netmask mask [pat]
```

Syntax Description

<i>nat_id</i>	Identifier of the NAT pool of global IP addresses. Enter an integer from 1 to 2147483647.
<i>ip_address1</i>	Single IP address, or if also using the <i>ip_address2</i> argument, the first IP address in a range of global addresses used for NAT. Enter an IP address in dotted-decimal notation.
<i>ip_address2</i>	(Optional) Highest IP address in a range of global IP addresses used for NAT. Enter an IP address in dotted-decimal notation.
netmask <i>mask</i>	Specifies the subnet mask for the IP address pool. Enter a mask in dotted-decimal notation. If you do not specify a network mask for the global IP addresses in the pool, the VFW application, by default, uses the network mask of the interface to which the pool is attached.
pat	(Optional) Specifies that the VFW application perform port address translation (PAT) in addition to NAT.

Defaults

No default behavior or values

Command Modes

Interface configuration
Management interface configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

This command requires the 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*.

Dynamic NAT uses a pool of global IP addresses that you specify. You can define either a single global IP address for a group of servers with PAT to differentiate between them, or a range of global IP addresses when using dynamic NAT only. To use a single IP address or a range of addresses, you assign an identifier to the address pool. You then associate the NAT pool with a global interface that is different from the interface you use to filter and receive NAT traffic.

If a packet egresses an interface that you have not configured for NAT, the VFW application transmits the packet untranslated.

If the VFW application runs out of IP addresses in a NAT pool, it can switch over to a PAT rule, if configured. For example, you can configure the following:

```
nat-pool 1 10.1.100.10 10.1.100.99 netmask 255.255.255.255
nat-pool 1 10.1.100.100 10.1.100.100 netmask 255.255.255.255 pat
```

Examples

The following example shows how to configure a NAT pool consisting of a range of 100 global IP addresses with PAT:

```
firewall/C1(config-if)# nat-pool 1 172.27.16.10 172.27.16.109 netmask 255.255.255.0 pat
```

Related Commands

Command	Description
nat dynamic	Configures dynamic NAT and PAT as an action in a policy map.
nat static	Configures static NAT and static port redirection in a policy map.
show xlate	Displays the IP and port translation (XLATE) information.

show interface

To display the interface information, use the **show interface** command in EXEC mode.

show interface *interface_name*

Syntax Description	<i>interface_name</i> Name of the interface for which to display information. Enter an unquoted text string with no spaces and a maximum of 30 alphanumeric characters.
---------------------------	---

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	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 <i>Cisco IOS XR Virtual Firewall Configuration Guide</i> .
-------------------------	--

Use the **show interface** command to display all the interface statistical information.

Examples	The following example shows how to display all the interface statistical information:
-----------------	---

```
firewall/Admin# show interface
```

Related Commands	Command	Description
	clear interface	Clears the interface statistics.

show nat-fabric

To display the NAT (Network Address Translation) policy and pool information for the current context, use the **show nat-fabric** command in EXEC mode.

```
show nat-fabric { policies | src-nat policy_id mapped_if | dst-nat policy_id | nat-pools | implicit-pat }
```

Syntax	Description
policies	Displays the NAT policies.
src-nat <i>policy_id mapped_if</i>	Displays the specified source NAT policy information. To obtain the values for the <i>policy_id</i> and <i>mapped_if</i> arguments, view the <i>policy_id</i> and <i>mapped_if</i> fields displayed by the show nat-fabric policies command.
dst-nat <i>static_xlate_id</i>	Displays the static address translation for the specified static XLATE ID. To obtain the value for the <i>static_xlate_id</i> argument, view the <i>static_xlate_id</i> field displayed by the show nat-fabric policies command.
nat-pools	Displays NAT pool information for a dynamic NAT policy.
implicit-pat	Displays the implicit PAT policies.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

Usage Guidelines This command requires the NAT 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 nat-fabric** command is intended for use by trained Cisco personnel for troubleshooting purposes only.

To obtain the values for the *policy_id*, *mapped_if*, and *static_xlate_id* arguments, view their respective fields displayed by the **show nat-fabric policies** command.

Examples The following example shows how to display the implicit PAT policies:

```
firewall/Admin# show nat-fabric implicit-pat
```

■ `show nat-fabric`

Related Commands This command has no related commands.

show xlate

To display the IP and port translation (XLATE) information, use the **show xlate** command in EXEC mode.

```
show xlate [[global | local] {ip_address} [ip_address2 [netmask mask]] | [gport | lport] {port}
[port2]]
```

Syntax Description

global	Displays information for a global IP address or range of global IP addresses to which the VFW application translates source addresses for static and dynamic NAT, respectively.
local	Displays information for a local IP address or range of local IP addresses.
<i>p_address ip_address2</i>	IP address, or range of IP addresses, for which to display XLATE information. For a single global IP address, enter one address in dotted-decimal notation. To specify a range of IP addresses, enter a second IP address.
netmask mask	Specifies a subnet mask for the specified IP addresses.
gport	Displays information for a global port or a range of global ports to which the VFW application translates source ports for static port redirection and dynamic PAT, respectively.
lport	Displays information for a local port or a range of local ports.
<i>port port2</i>	Port number, or range of port numbers, for which to display XLATE information. Enter a port number as an integer from 0 to 65535. To specify a range of port numbers, enter a second port number.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

This command requires the NAT 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 display IP and XLATE information:

```
firewall/Admin# show xlate global 172.27.16.3 172.27.16.10 netmask 255.255.255.0 gport 100
200
```

■ show xlate

Related Commands	Command	Description
	clear xlate	Clears global address to local address mapping information based on global address, global port, local address, local port, interface address as global address, and NAT type.

shutdown

To disable a VFW interface, use the **shutdown** command in the appropriate interface configuration mode. To enable the interface, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Interface configuration
Management interface configuration
FT interface configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

This command requires the system 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 create an interface, the interface is in the shutdown state until you enable it. If you disable or reenble the interface within a context, only that context interface is affected.

Examples

The following example shows how to disable an interface:

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

The following example shows how to enable an interface:

```
firewall/Admin (config-if)# no shutdown
```

Related Commands

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

■ shutdown