



Access Control List Commands on the Virtual Firewall

This module describes the commands necessary to configure access control lists (ACLs) on the VFW application.



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*.

access-group

To apply an access control list (ACL) to the inbound or outbound direction of an interface and make the ACL active, use the **access-group** command in the appropriate interface configuration mode. To remove an ACL from an interface, use the **no** form of this command.

```
access-group {input | output} acl_name
```

```
no access-group {input | output} acl_name
```

Syntax Description	Parameter	Description
	input	Specifies the inbound direction of the interface to which you want to apply the ACL.
	output	Specifies the outbound direction of the interface to which you want to apply the ACL.
	<i>acl_name</i>	Identifier of an existing ACL that you want to apply to an interface.

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 You must apply ACLs to an interface to allow the passing of traffic on an interface. You can apply one ACL of each type (extended and EtherType) to both directions of the interface. For connectionless protocols, you need to apply the ACL to the source and destination interfaces if you want traffic to pass in both directions. For example, you can allow BGP in an ACL in transparent mode, but you must apply the ACL to both interfaces.

A bridge group interface supports extended ACLs for IP traffic, and EtherType ACLs for non-IP traffic. For non-IP traffic, configure an EtherType ACL. EtherType ACLs support Ethernet V2 frames. You can configure the VFW application to pass one or any of the following non-IP EtherTypes: Multiprotocol Label Switching (MPLS), Internet Protocol version 6 (IPv6), and bridge protocol data units (BDPUs).

The **output** option is not allowed for EtherType ACLs.

To apply an ACL globally to all interfaces in a context, use the **access-group (global)** command.

Examples

The following example shows how to apply an ACL named INBOUND to the inbound direction of an interface:

```
firewall/Admin(config)# interface xy  
firewall/Admin(config-if)# access-group input INBOUND
```

The following example shows how to remove an ACL from an interface:

```
firewall/Admin(config-if)# no access-group input INBOUND
```

Related Commands

Command	Description
access-group (global)	Applies an ACL to the inbound direction on all interfaces in a context and makes the ACL active.
access-list extended	Creates an extended ACL.
show access-list	Displays statistics associated with a specific ACL.

access-group (global)

To apply an access control list (ACL) to the inbound direction on all interfaces in a context and make the ACL active, use the **access-group** command in configuration mode. To remove an ACL from all interfaces in a context, use the **no** form of this command.

access-group input *acl_name*

no access-group input *acl_name*

Syntax Description

input	Specifies the inbound direction of all interfaces in a context on which you want to apply the ACL
<i>acl_name</i>	Identifier of an existing ACL that you want to apply to an interface

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 access-list 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 apply an ACL to an interface to allow the passing of traffic on that interface. This command enables you to apply an ACL to all interfaces in a context in the inbound direction only and to allow traffic on all interfaces simultaneously. The following considerations apply:

- You can use the **access-group** command in configuration mode only if there are no interfaces in the context to which you have applied an ACL previously using the **access-group** command in interface configuration mode.
- Similarly, if you have applied an ACL globally to all interfaces in a context, you cannot apply an ACL to an individual interface using the **access-group** command in interface configuration mode.
- You can apply one Layer 2 ACL and one Layer 3 ACL globally to all interfaces in a context.
- To all Layer 2 bridge-group virtual interfaces (BVI) in a context, you can apply both a Layer 3 and a Layer 2 ACL.
- To all Layer 3 interfaces in a context, you can apply only a Layer 3 ACL.

Examples

The following example shows how to apply an ACL named INBOUND to the inbound direction of all interfaces in the Admin context:

```
firewall/Admin(config)# access-group input INBOUND
```

Related Commands

Command	Description
access-group	Applies an access control list (ACL) to the inbound or outbound direction of an interface and makes the ACL active.
access-list extended	Creates an extended ACL.
show access-list	Displays statistics associated with a specific ACL.

access-list extended

To create an extended access control list (ACL), use the **access-list extended** command in configuration mode. To delete the ACL, use the **no** form of this command.

IP extended ACL

```
access-list name [line number] extended {deny | permit} protocol {src_ip_address netmask | any | host src_ip_address} {dest_ip_address netmask | any | host dest_ip_address}
```

```
no access-list name [line number] extended {deny | permit} protocol {src_ip_address netmask | any | host src_ip_address} {dest_ip_address netmask | any | host dest_ip_address}
```

TCP or a UDP extended ACL

```
access-list name [line number] extended {deny | permit} {tcp | udp} {src_ip_address netmask | any | host src_ip_address} [operator port [port2]] {dest_ip_address netmask | any | host dest_ip_address} [operator port3 [port4]]
```

```
no access-list name [line number] extended {deny | permit} {tcp | udp} {src_ip_address netmask | any | host src_ip_address} [operator port] {dest_ip_address netmask | any | host dest_ip_address} [operator port2]
```

ICMP extended ACL:

```
access-list name [line number] extended {deny | permit} icmp {src_ip_address netmask | any | host src_ip_address} {dest_ip_address netmask | any | host dest_ip_address} [icmp_type code operator code]
```

```
no access-list name [line number] extended {deny | permit} icmp {src_ip_address netmask | any | host src_ip_address} {dest_ip_address netmask | any | host dest_ip_address} [icmp_type] [code operator code]
```

Syntax Description

<i>name</i>	Unique identifier of the ACL. Enter an unquoted text string with a maximum of 64 characters.
<i>line number</i>	(Optional) Specifies the line number position where you want the entry you are configuring to appear in the ACL. The position of an entry affects the lookup order of the entries in an ACL. If you do not configure the line number of an entry, the VFW application applies a default increment and a line number to the entry and appends it at the end of the ACL.
extended	Specifies an extended ACL. Extended ACLs allow you to specify the destination IP address and subnet mask and other parameters not available with a standard ACL.
deny	Blocks connections on the assigned interface.
permit	Allows connections on the assigned interface.
<i>protocol</i>	Name or number of an IP protocol. Enter a protocol name or an integer from 0 to 255 that represents an IP protocol number. Valid protocol choices are provided in Table 1 .

<i>src_ip_address netmask</i>	Traffic from a source defined by the IP address and the network mask. Use these arguments to specify network traffic from a range of source IP addresses.
host <i>src_ip_address</i>	Specifies the IP address of the host from which network traffic originates. Use this keyword and argument to specify network traffic from a single IP address.
any	Specifies network traffic from any source.
<i>port</i> [<i>port2</i>]	TCP or UDP source port name or number from which you permit or deny services access. To enter an inclusive range of ports, enter two port numbers. <i>Port2</i> must be greater than or equal to <i>port1</i> . See Table 3 for a list of well-known port names and numbers.
<i>dest_ip_address netmask</i>	Specifies the IP address of the network or host to which the packet is being sent and the network mask bits to be applied to the destination IP address. Use these arguments to specify a range of destination IP addresses.
host <i>destination_address</i>	IP address and subnet mask of the destination of the packets in a flow. Use this keyword and argument to specify network traffic destined to a single IP address.
<i>port3</i> [<i>port4</i>]	TCP or UDP destination port name or number to which you permit or deny services access. To enter an optional inclusive range of ports, enter two port numbers. <i>Port4</i> must be greater than or equal to <i>port3</i> . See Table 3 for a list of well-known ports.
<i>icmp_type</i>	(Optional) Type of ICMP messaging. Enter either an integer corresponding to the ICMP code number or one of the ICMP types as described in Table 2 .
<i>icmp_operator</i>	An operator that the VFW application applies to the ICMP code number that follows. Enter one of the following operators: <ul style="list-style-type: none"> • lt—Less than. • gt—Greater than. • eq—Equal to. • neq—Not equal to. • range—An inclusive range of ICMP code values. When you use this operator, specify two code numbers to define the range.
<i>code</i>	ICMP code number that corresponds to an ICMP type. See Table 3 . If you entered the range operator, enter a second ICMP code value to define the upper limit of the range.

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	Modification
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Usage Guidelines

This command requires the access-list 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 does not explicitly support standard ACLs. To configure a standard ACL, specify the ports and destination addresses as “any” in an extended ACL.

There are three major types of extended ACLs:

- IP
- TCP or UDP
- ICMP

For TCP and UDP connections, you do not need to also apply an ACL on the destination interface to allow returning traffic, because the VFW application allows all returning traffic for established connections.

You can apply only one ACL of each type (extended and EtherType) to each direction of an interface. You can also apply the same ACLs on multiple interfaces.

Valid protocol choices for an IP extended ACL are provided in [Valid IP Protocols for access-list extended Command Table 1](#).

Table 1 Valid IP Protocols for access-list extended Command

Protocol	Code Number	Description
ah	51	Authentication Header
eigrp	88	Enhanced IGRP
esp	50	Encapsulated Security Payload
gre	47	Generic Routing Encapsulation
icmp	1	Internet Control Message Protocol (See Table 2 for optional ICMP messaging types)
igmp	2	Internet Group Management Protocol
ip	0	Internet Protocol
ip-in-ip	4	IP-in-IP Layer 3 Tunneling protocol
ospf	89	Open Shortest Path First
pim	103	Protocol Independent Multicast
tcp	6	Transmission Control Protocol
udp	17	User Datagram Protocol

If you selected **icmp** as the IP protocol type, you can optionally specify the type of ICMP messaging. Enter either an integer corresponding to the ICMP code number or one of the ICMP messaging types as described in [Table 2](#).

Table 2 ICMP Types

ICMP Code Number	ICMP Type
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
30	traceroute
31	conversion-error
32	mobile-redirect

Table 3 Well-Known Port Numbers and Keywords

Key Word	Port Number	Description
aol	5190	America-Online
bgp	179	Border Gateway Protocol
chargen	19	Character Generator
citrix-ica	1494	Citrix Independent Computing Architecture protocol
cmd	514	Same as exec , with automatic authentication
ctiqbe	2748	Computer Telephony Interface Quick Buffer Encoding
daytime	13	Daytime
discard	9	Discard
domain	53	Domain Name System
echo	7	Echo
exec	512	Exec (RSH)
finger	79	Finger
ftp	21	File Transfer Protocol

Table 3 Well-Known Port Numbers and Keywords (continued)

Key Word	Port Number	Description
ftp-data	20	FTP data connections
gopher	70	Gopher
h323	1720	H.323 call signaling
hostname	101	NIC hostname server
http	80	Hyper Text Transfer Protocol
https	443	HTTP over TLS/SSL
ident	113	Ident Protocol
imap4	143	Internet Message Access Protocol, version 4
irc	194	Internet Relay Chat
kerberos	88	Kerberos
klogin	543	Kerberos Login
kshell	544	Kerberos Shell
ldap	389	Lightweight Directory Access Protocol
ldaps	636	LDAP over TLS/SSL
login	513	Login (rlogin)
lotusnotes	1352	IBM Lotus Notes
lpd	515	Printer Service
matip-a	350	Mapping of Airline Traffic over Internet Protocol (MATIP) Type A
netbios-ssn	139	NetBios Session Service
nntp	119	Network News Transport Protocol
pcanywhere-data	5631	PC Anywhere data
pim-auto-rp	496	PIM Auto-RP
pop2	109	Post Office Protocol v2
pop3	110	Post Office Protocol v3
pptp	1723	Point-to-Point Tunneling Protocol, RFC 2637
rpc	71	Remote Procedure Call
rtsp	554	Real-time Stream Control Protocol
sip	5060	Session Initiation Protocol
smtp	25	Simple Mail Transfer Protocol
sqlnet	1521	Structured Query Language Network
ssh	22	Secure Shell
sunrpc	111	Sun Remote Procedure Call
tacacs	49	Terminal Access Controller Access Control System
talk	517	Talk
telnet	23	Telnet
time	37	Time

Table 3 Well-Known Port Numbers and Keywords (continued)

Key Word	Port Number	Description
uucp	540	UNIX-to-UNIX Copy Program
whois	43	Nickname
www	80	World Wide Web (HTTP)

Examples

The following example shows how to configure a TCP extended ACL:

```
firewall/Admin(config)# access-list INBOUND line 10 extended permit tcp 192.168.12.0
255.255.255.0 gt 1024 172.27.16.0 255.255.255.0 lt 4000
```

The following example shows how to remove an entry from an extended ACL:

```
firewall/Admin(config)# no access-list INBOUND line 10
```

The following example shows how to allow an external host with IP address 192.168.12.5 to be able to ping a host behind the VFW application with an IP address of 10.0.0.5:

```
firewall/Admin(config)# access-list INBOUND permit icmp host 192.168.12.5 host 10.0.0.5
```

Related Commands

Command	Description
clear access-list	Clears access control list (ACL) statistics.
show access-list	Displays statistics associated with a specific ACL.

access-list remark

To add a comment to an access control list (ACL), use the **access-list remark** command in configuration mode. To remove an ACL remark, use the **no** form of this command.

access-list *name* **remark** *text*

no access-list *name* **remark** *text*

Syntax Description

<i>name</i>	Unique identifier of the ACL. Enter an unquoted text string with a maximum of 64 characters.
remark <i>text</i>	Specifies any comments you want to include about the nature of the ACL. Comments appear at the top of the ACL. Enter an unquoted text string with a maximum of 100 alphanumeric characters. You can enter leading spaces at the beginning of the text. Trailing spaces are ignored.

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 access-list 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 **access-list remark** command to add comments about an ACL to clarify the function of the ACL. You can enter only one comment per ACL; the comment appears at the top of the ACL.

If you delete an ACL using the **no access-list** *name* command, then the remarks are also removed.

Examples

The following example shows how to add a comment to an ACL:

```
firewall/Admin(config)# access-list INBOUND remark This is a remark
```

The following example shows how to remove comments from an ACL:

```
firewall/Admin(config)# no access-list INBOUND line 200 remark
```

Related Commands	Command	Description
	clear access-list	Clears access control list (ACL) statistics.
	show access-list	Displays statistics associated with a specific ACL.

access-list resequence

To resequence the access control list (ACL) entries in an ACL with a specific starting number and interval, use the **access-list resequence** command in configuration mode. To reset the number assigned to an ACL entry to the default of 10, use the **no** form of this command.

access-list *name* **resequence** *number1* *number2*

no access-list *name* **resequence** *number1* *number2*

Syntax Description

<i>name</i>	Unique identifier of the ACL. Enter an unquoted text string with a maximum of 64 characters.
resequence	Specifies the renumbering of the entries in an ACL.
<i>number1</i>	Number assigned to the first entry in the ACL. Enter any integer.
<i>number2</i>	Number added to each entry in the ACL after the first entry. Enter any integer.

Defaults

The default resequence value is 10.

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 access-list 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 resequence the ACL entries by multiples of 15, starting with 5:

```
firewall/Admin(config)# access-list INBOUND resequence 5 15
```

Related Commands

Command	Description
clear access-list	Clears access control list (ACL) statistics.
show access-list	Displays statistics associated with a specific ACL.

clear access-list

To clear access control list (ACL) statistics, use the **clear access-list** command in EXEC mode.

clear access-list *name*

Syntax Description	<i>name</i> <i>Name of an existing ACL</i>
---------------------------	--

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 access-list 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 clear the statistics for access control list ACL1:

```
firewall/Admin# clear access-list ACL1
```

Related Commands	Command	Description
	access-list extended	Creates an extended ACL.
	show access-list	Displays statistics associated with a specific ACL.

show access-list

To display statistics associated with a specific access control list (ACL), use the **show access-list** command in EXEC mode.

show access-list *name*

Syntax Description	<i>name</i>	Name of an existing ACL. Enter the name as an unquoted text string.
---------------------------	-------------	---

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 access-list 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 ACL information the VFW application displays when you execute the **show access-list** command includes the ACL name, number of elements in the ACL, operating status of the ACL (ACTIVE or NOT ACTIVE), any configured remarks, the ACL entry, and the ACL hit count.

Examples The following example shows how to display statistical and configuration information for the ACL ACL1:

```
firewall/Admin# show access-list ACL1
```

Related Commands	Command	Description
	access-list extended	Creates an extended ACL.
	access-list remark	Adds a comment to an ACL.
	access-list resequence	Resequences the ACL entries in an ACL with a specific starting number and interval.
	clear access-list	Clears access control list (ACL) statistics.
	show running-config	Displays the running configuration information associated with the current context.

show acl-merge

To display statistics related to merged access control lists (ACLs), use the **show acl-merge** command in EXEC mode.

```
show acl-merge {acls interface {in | out} [summary] | match interface {in | out} ip_address1
ip_address2 protocol src_port dest_port | merged-list interface {in | out} [non-redundant |
summary]}
```

Syntax Description		
acls		Displays various feature ACLs and their entries before the merge.
interface		Specifies the interface on which the ACL was applied.
in out		Specifies the direction in which the ACL was applied to network traffic: incoming or outgoing.
summary		(Optional) Displays summary information before or after the merge.
match		Displays the ACL entry that matches the specified tuple.
<i>ip_address1</i>		Source IP address. Enter an IP address in dotted-decimal notation.
<i>ip_address2</i>		Destination IP address. Enter an IP address in dotted-decimal notation.
<i>protocol</i>		Protocol specified in the ACL.
<i>src_port</i>		Source port specified in the ACL.
<i>dest_port</i>		Destination port specified in the ACL.
merged-list		(Optional) Displays the merged ACL.
non-redundant		(Optional) Displays only those ACL entries that have been downloaded to a network processor.

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 access-list 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 acl-merge** command is intended for use by trained Cisco personnel for troubleshooting purposes only.

The ACL merge list number (instance ID) is locally generated (not synchronized) on each VFW application in a redundant configuration. The number assigned depends on the order in which the ACLs are applied to the interfaces. This number can be different on the two modules. Even the ACL merged list could be different on the two modules depending on when redundancy is enabled.

Examples

The following example shows how to display the ACL merge information for interface abc:

```
firewall/Admin# show acl-merge acls interface abc in summary
```

Related Commands

This command has no related commands.