ACL Commands

deny

To set conditions in a named IP access list or object group access control list (OGACL) that will deny packets, use the **deny** configuration command in the appropriate configuration mode. To remove a deny condition from an IP access list or OGACL, use the **no** form of this command.

TCP or UDP

sequence-number **deny** { *tcp* | *udp* } { *src-addr* *src-wildcard* | **any** | **host** *addr* | **object-group** *src-network-group* } [**eq** *port* | **range** *min-port* *max-port*] { *dest-addr* *dest-wildcard* | **any** | **host** *addr* | **object-group** *dest-network-group* } [**eq** *port* | **range** *min-port* *max-port*] [**log**]
no *sequence-number* [**deny**] [| { *tcp* | *udp* } | { *src-addr* *src-wildcard* | **any** | **host** *addr* | **object-group** *src-network-group* } | [**eq** *port* | **range** *min-port* *max-port*] | { *dest-addr* *dest-wildcard* | **any** | **host** *addr* | **object-group** *dest-network-group* } | [**eq** *port* | **range** *min-port* *max-port*]] [**log**]

All other protocols

sequence-number **deny** { *protocol* | **object-group** *service-group* } { *src-addr* *src-wildcard* | **any** | **host** *addr* | **object-group** *src-network-group* } { *dest-addr* *dest-wildcard* | **any** | **host** *addr* | **object-group** *dest-network-group* } [**log**]

no *sequence-number* [**deny**] [{ *protocol* | **object-group** *service-group* } | { *src-addr* *src-wildcard* | **any** | **host** *addr* | **object-group** *src-network-group* } | { *dest-addr* *dest-wildcard* | **any** | **host** *addr* | **object-group** *dest-network-group* | **range** *port* } | [**log**]]

Syntax Description

sequence-number	Specify a sequence number to **permit** or **deny** statements to order the statement in the list . You also can use sequence numbers to reorder, add, or remove statements in a list.

protocol	Name or number of a protocol; valid values are **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword **ip**. See the "Usage Guidelines" section for additional qualifiers.
object-group*service-group*	Specify an object group of type **service**.
src-addr	Number of the source network or host from which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
src-wildcard	Wildcard bits to be applied to source network in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
any	Specifies any source or any destination host as an abbreviation for the *source-addr*or *destination-addr value*and the *source-wildcard* or *destination-wildcard* value of 0.0.0.0 255.255.255.255.
host *addr*	Specifies the source or destination address of a single host.
tcp	Specifies the TCP protocol.
udp	Specifies the UDP protocol.
object-group *source-addr-group-name*	Specifies the name of the object-group that contains the group of source addresses. The source and destination object groups must be **network** object groups. You cannot use empty object groups in access control lists.
destination-addr	Number of the network or host to which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
destination-wildcard	Wildcard bits to be applied to the destination in a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
object-group *dest-addr-group-name*	Specifies the name of the object-group that contains the group of destination addresses. The source and destination object groups must be **network** object groups. You cannot use empty object groups in access control lists.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message for an extended list includes the access list number; whether the packet was permitted or denied; the protocol; whether the protocol was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. For both standard and extended lists, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from reloading because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

Command Default

There is no specific condition under which a packet is denied passing the access list.

Command Modes

Standard access-list configuration (config-std-nacl)
Extended access-list configuration (config-ext-nacl)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Additional parameters qualified: `udp`, `tcp`, `icmp`, and `range`

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `deny` command.

Examples

```
ip access-list standard 10
 10 deny 10.1.1.1

ip access-list standard 15
 10 deny any

ip access-list extended 105
 10 deny ip any any

ip access-list extended 105
 10 deny ip host 10.1.1.1 any
 20 deny object-group OBJ_PROTO object-group OBJ_SRC object-group OBJ_DEST

ip access-list extended EXTACL
 10 deny ip any any log
```

ip access-list

To define an IP access list or object-group access control list (ACL) by name or number or to enable filtering for packets with IP helper-address destinations, use the **ip access-list** command in global configuration mode. To remove the IP access list or object-group ACL or to disable filtering for packets with IP helper-address destinations, use the **no** form of this command.

ip access-list { { **standard** | **extended** } { *access-list-name access-list-number* } }
no ip access-list { { **standard** | **extended** } { *access-list-name access-list-number* } }

Syntax Description

standard	Specifies a standard IP access list. You can only filter based on the source with standard IP access lists.
extended	Specifies an extended IP access list. Required for object-group ACLs.
access-list-name	Name of the IP access list or object-group ACL. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
access-list-number	Number of the access list. • A standard IP access list is in the ranges 1-99 or 1300-1999. • An extended IP access list is in the ranges 100-199 or 2000-2699.

Command Default

No IP access list or object-group ACL is defined, and outbound ACLs do not match and filter IP helper relayed traffic.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	`ip access-list extended` command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Additional parameter qualified: `ip access-list standard`

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip access-list` command.

Examples

```
ip access-list standard 10
 10 deny 10.1.1.1
```

```
ip access-list standard 15
 10 deny any
```

```
ip access-list standard 15
 10 deny ip-address
```

```
ip access-list extended 105
 10 deny ip 10.1.1.1 any
 20 deny ip object-group1 any
```

In the following example, the source IP address is 10.1.1.1 and the destination IP address is 10.1.1.2

```
ip access-list extended 105
  10 permit host 10.1.1.1 10.1.1.2
```

```
ip access-list extended 105
 10 deny ip any any
```

```
ip access-list extended EXTACL
 10 deny ip any any log
```

ipv6 access-list

To define an IPv6 access list and to place the device in IPv6 access list configuration mode, use the **ipv6 access-list**command in global configuration mode. To remove the access list, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 access-list command.

Examples

```
Device# config-transaction
Device(config)# ipv6 access-list test300_v6
Device(config-ip-acl)# sequence 100 permit ipv6 any 2001:DB8::/32
Device(config-ip-acl)#
```

permit

To set conditions in named IP access list that will permit packets, use the **permit** command in the appropriate configuration mode. To remove a condition from an IP access list, use the **no** form of this command.

Syntax Description

sequence-number	Specify a sequence number to **permit** or **deny** statements to position the statement in the list. You can also use sequence numbers to reorder, add, or remove statements in a list.
protocol	Name or number of a protocol; valid values are; valid values are **ahp**, **eigrp**, **esp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, , **tcp**, **pcp**, **pim**, **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword **ip**. See the “Usage Guidelines” section for additional qualifiers.
object-group*service-group*	Specify an object group of type **service**.

source-addr	(Optional) Number of the network or host from which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
source-wildcard	(Optional) Wildcard bits to be applied to the source in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
any	Specifies any source or any destination host as an abbreviation for the *source-addr*or *destination-addr value*and the *source-wildcard* or *destination-wildcard* value of 0.0.0.0 255.255.255.255.
host *address name*	Specifies the source or destination address and name of a single host.
object-group *source-addr-group-name*	Specifies the name of the object group that contains the group of source addresses. The source and destination object groups must be **network** object groups. You cannot use empty object groups in access control lists.
destination-addr	Number of the network or host to which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
destination-wildcard	Wildcard bits to be applied to the destination in a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
object-group *dest-addr-group-name*	Specifies the name of the object-group that contains the group of destination addresses. The source and destination object groups must be **network** object groups. You cannot use empty object groups in access control lists.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message for an extended list includes the access list number; whether the packet was permitted or denied; the protocol; whether the protocol was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and port numbers and the user-defined cookie or router-generated hash value. For both standard and extended lists, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from reloading because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list. After you specify the **log** keyword (and the associated *word* argument), you cannot specify any other keywords or settings for this command.
tcp	Specifies the TCP protocol.
udp	Specifies the UDP protocol.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	Additional parameters qualified: `udp`, `tcp`, `icmp`, and `range`
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Additional parameters qualified: `geo-group`

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `permit` command.

Note You can configure a fully qualified domain name (FQDN) or a GEO as a source object group or as a destination object group using an Access Control List (ACL). Do not configure both a GEO and an FQDN as a source or destination object group.

```
object-group fqdn asdfa-Rule_2-fqdn-src_
pattern "www\.cisco\.com"
!
object-group fqdn asdfa-Rule_4-fqdn-dstn_
pattern "www\.cnn\.com"
!
object-group geo asdfa-Rule_1-geo-src_
country AGO
!
object-group geo asdfa-Rule_3-geo-dstn_
country CMR
!
object-group service asdfa-Rule_1-svc_
ip
!
object-group service asdfa-Rule_2-svc_
ip
!
object-group service asdfa-Rule_3-svc_
ip
!
object-group service asdfa-Rule_4-svc_
ip

ip access-list extended asdfa-seq-Rule_1-acl_
19 permit object-group asdfa-Rule_1-svc_ geo-group asdfa-Rule_1-geo-src_ any
!
ip access-list extended asdfa-seq-Rule_2-acl_
14 permit object-group asdfa-Rule_2-svc_ fqdn-group asdfa-Rule_2-fqdn-src_ any
!
ip access-list extended asdfa-seq-Rule_3-acl_
15 permit object-group asdfa-Rule_3-svc_ any geo-group asdfa-Rule_3-geo-dstn_
!
ip access-list extended asdfa-seq-Rule_4-acl_
12 permit object-group asdfa-Rule_4-svc_ any fqdn-group asdfa-Rule_4-fqdn-dstn_
```

sequence

To specify a sequence number for the permit condition in the IP access list, use the **sequence** command in the appropriate configuration mode. To remove a sequence number from an IP access list, use the **no** form of this command.

sequence *sequence-number* { **permit** } { **ipv6** } { **any** *ipv6-address* }

Syntax Description

sequence-number	Permits statements to position the statement in the list.
permit	Sets permit conditions for an IPv6 access list.
ipv6	Sets the IPv6 address to set permit conditions.
any *ipv6-address*	Specifies any source or any destination host as an abbreviation for the *source-addr* or *destination-addr value* and the *source-wildcard* or *destination-wildcard* value of 0.0.0. 255.255.255.255.

Command Default

There are no specific conditions under which a packet passes the access list.

Command Modes

IPv6 access-list configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Examples

```
Device(config)# ipv6 access-list test300_v6
Device(config-ipv6-acl)# sequence 100 permit ipv6 any 2001:DB8::/32
```