Configuring IP ACLs

This chapter describes how to configure IP access control lists (ACLs) on Cisco NX-OS devices.

Unless otherwise specified, the term IP ACL refers to IPv4 and IPv6 ACLs.

Information About ACLs

An ACL is an ordered set of rules that you can use to filter traffic. Each rule specifies a set of conditions that a packet must satisfy to match the rule. When the device determines that an ACL applies to a packet, it tests the packet against the conditions of all rules. The rule determines whether the packet is to be permitted or denied. If there is no match to any of the specified rules, the device applies the applicable implicit rule. The device continues processing packets that are permitted and drops packets that are denied.

You can use ACLs to protect networks and specific hosts from unnecessary or unwanted traffic. For example, you can use ACLs to disallow HTTP traffic from a high-security network to the Internet. You can also use ACLs to allow HTTP traffic to a specific site using the IP address of the site to identify it in an IP ACL.

ACL Types and Applications

In Cisco Nexus 1000V InterCloud, ACL can be only applied on port profiles .In Cisco Nexus 1000V InterCloud application of ACL on vEthernet Interfaces is not supported.

In Cisco Nexus 1000V InterCloud, IP ACL is supported for traffic filtering. In IP ACL, the device applies IPv4 ACLs only to IP traffic.

Note In this release, MAC ACL is not supported on Cisco Nexus 1000V InterCloud.

Order of ACL Application

When the device processes a packet, it determines the forwarding path of the packet. The device applies the ACLs in the following order:

1. Ingress port ACL
2. Egress port ACL

Rules

Rules are what you create, modify, and remove when you configure how an ACL filters network traffic. Rules appear in the running configuration. When you apply an ACL to an interface or change a rule within an ACL that is already applied to an interface, the supervisor module creates ACL entries from the rules in the running configuration and sends those ACL entries to the applicable InterCloud Switch.

You can create rules in ACLs in access-list configuration mode by using the **permit** or **deny** command. The device allows traffic that matches the criteria in a permit rule and blocks traffic that matches the criteria in a deny rule. You have many options for configuring the criteria that traffic must meet in order to match the rule.

Source and Destination

In each rule, you specify the source and the destination of the traffic that matches the rule. You can specify both the source and destination as a specific host, a network or group of hosts, or any host.

For information about specifying the source and destination, see the applicable permit and deny commands in the *Cisco Nexus 1000V Command Reference*.

Protocols

ACLs allow you to identify traffic by protocol. You can specify some protocols by name. For example, in an IP ACL, you can specify ICMP by name.

In IP ACLs, you can specify protocols by the integer that represents the Internet protocol number. For example, you can use 115 to specify Layer 2 Tunneling Protocol (L2TP) traffic.

Implicit Rules

ACLs have implicit rules, which means that although these rules do not appear in the running configuration, the device applies them to traffic when no other rules in an ACL match. When you configure the device to maintain per-rule statistics for an ACL, the device does not maintain statistics for implicit rules.

All IP ACLs include the following implicit rule that denies unmatched IP traffic:

```
deny ip any any
```

This implicit rule ensures that unmatched traffic is denied, regardless of the protocol specified in the Layer 2 header of the traffic.

Additional Filtering Options

You can identify traffic by using additional options. These options differ by ACL type. The following list includes most but not all additional filtering options:

- IP ACLs support the following additional filtering options:
  - Layer 4 protocol
  - TCP and UDP ports
  - ICMP types and codes
  - IGMP typesVersion1 only
  - Precedence level
  - Differentiated Services Code Point (DSCP) value
  - TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set

Sequence Numbers

The device supports sequence numbers for rules. Every rule that you enter receives a sequence number, either assigned by you or assigned automatically by the device. Sequence numbers simplify the following ACL tasks:

- Adding new rules between existing rules—By specifying the sequence number, you specify where in the ACL a new rule should be positioned. For example, if you need to insert a rule between rules numbered 100 and 110, you could assign a sequence number of 105 to the new rule.
- Removing a rule—Without using a sequence number, removing a rule requires that you enter the whole rule, as follows:

  ```
  switch(config-acl)# no permit tcp 10.0.0.0/8 any
  ```

  However, if the same rule had a sequence number of 101, removing the rule requires only the following command:

  ```
  switch(config-acl)# no 101
  ```

- Moving a rule—With sequence numbers, if you need to move a rule to a different position within an ACL, you can add a second instance of the rule by using the sequence number that positions it correctly, and then you can remove the original instance of the rule. This action allows you to move the rule without disrupting traffic.

If you enter a rule without a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule to the rule. For example, if the last rule in an ACL has a sequence number of 225 and you add a rule without a sequence number, the device assigns the sequence number 235 to the new rule.

In addition, you can reassign sequence numbers to rules in an ACL. Resequencing is useful when an ACL has rules numbered contiguously, such as 100 and 101, and you need to insert one or more rules between those rules.

Statistics

The device can maintain global statistics for each rule that you configure in IPv4 ACLs. If an ACL is applied to multiple interfaces, the maintained rule statistics are the sum of packet matches (hits) on all the interfaces on which that ACL is applied.

Note The device does not support interface-level ACL statistics.

For each ACL that you configure, you can specify whether the device maintains statistics for that ACL, which allows you to turn ACL statistics on or off as needed to monitor traffic filtered by an ACL or to help troubleshoot the configuration of an ACL.

The device does not maintain statistics for implicit rules in an ACL. For example, the device does not maintain a count of packets that match the implicit deny ip any any rule at the end of all IPv4 ACLs. If you want to maintain statistics for implicit rules, you must explicitly configure the ACL with rules that are identical to the implicit rules.

Prerequisites for IP ACLs

- You must be familiar with IP addressing and protocols to configure IP ACLs.
- You must be familiar with the port profile interface types that you want to configure with ACLs.

Guidelines and Limitations for IP ACLs

- In most cases, ACL processing for IP packets are processed on the I/O modules. Management interface traffic is always processed on the supervisor module, which is slower.
- IP ACLs can be applied only on port profiles and not on the Interfaces.
- IP ACLs should not be applied on port profiles allowing system vlans.
- If a non-existing ACL is applied on a port profile, a new ACL with the specified name is created and all traffic in the applied port profile is blocked due to the implicit deny.

Default Settings for IP ACLs

Parameters	Default
IP ACLs	No IP ACLs exist by default.
ACL rules	Implicit rules apply to all ACLs

Configuring IP ACLs

Creating an IP ACL

You can create an IPv4 ACL on the device and add rules to it.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# [**no**] **ip access-list** {*name* | **match-local-traffic**}
3. switch(config-acl)# [*sequence-number*] { **permit** | **deny**} *protocol source destination*
4. (Optional) switch# **statistics per-entry**
5. (Optional) switch(config-acl)# **show ip access-lists** *name*
6. (Optional) switch(config-acl)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Places you into global configuration mode.
Step 2	switch(config)# [**no**] **ip access-list** {*name* | **match-local-traffic**}	Creates the named IP ACL (up to 64 characters in length) and enters IP ACL configuration mode. The match-local-traffic option enables matching for locally-generated traffic. The no option removes the specified access list.
Step 3	switch(config-acl)# [*sequence-number*] { **permit** | **deny**} *protocol source destination*	Creates a rule in the IP ACL. You can create many rules. The sequence-number argument can be a whole number from 1 to 4294967295. The **permit** and **deny** keywords support many ways of identifying traffic
Step 4	switch# **statistics per-entry**	(Optional) Specifies that the device maintains global statistics for packets that match the rules in the ACL.
Step 5	switch(config-acl)# **show ip access-lists** *name*	(Optional) Displays the IP ACL configuration.
Step 6	switch(config-acl)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

```
switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
switch(config-acl)# statistics per-entry
switch(config-acl)# show ip access-lists acl-01
IPV4 ACL acl-01
        statistics per-entry
        10 permit ip 192.18.2.0/24 any
switch(config-acl)# copy running-config startup-config
```

Changing an IP ACL

You can add and remove rules in an existing IPv4 ACL. You cannot change existing rules. Instead, to change a rule, you can remove it and create it again with the desired changes.

If you need to add more rules between existing rules than the current sequence numbering allows, you can use the **resequence** command to reassign sequence numbers.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **ip access-list** *name*
3. (Optional) switch(config-acl)# [*sequence-number*] { **permit** | **deny**} *protocol source destination*
4. (Optional) switch(config-acl)# **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination}*
5. switch(config-acl)# **[no] statistics per-entry**
6. (Optional) switch(config-acl)# **show ip access-lists** *name*
7. (Optional) switch(config-acl)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Places you into global configuration mode.
Step 2	switch(config)# **ip access-list** *name*	Places you in IP ACL configuration mode for the specified ACL.
Step 3	switch(config-acl)# [*sequence-number*] { **permit** | **deny**} *protocol source destination*	(Optional) Creates a rule in the IP ACL. Using a sequence number allows you to specify a position for the rule in the ACL. Without a sequence number, the rule is added to the end of the rules. The sequence-number argument can be a whole number from 1 to 4294967295. The **permit** and **deny** keywords support many ways of identifying traffic.

	Command or Action	Purpose
Step 4	switch(config-acl)# **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination}*	(Optional) Removes the rule that you specified from the IP ACL. The **permit** and **deny** keywords support many ways of identifying traffic.
Step 5	switch(config-acl)# **[no] statistics per-entry**	Specifies that the device maintains global statistics for packets that match the rules in the ACL. The **no** option stops the device from maintaining global statistics for the ACL.
Step 6	switch(config-acl)# **show ip access-lists** *name*	(Optional) Displays the IP ACL configuration.
Step 7	switch(config-acl)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration

```
switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
switch(config-acl)# statistics per-entry
switch(config-acl)# show ip access-lists acl-01
IPV4 ACL acl-01
        statistics per-entry
        10 permit ip 192.168.2.0/24 any
switch(config-acl)# ip access-list acl-01
switch(config-acl)# no 10
switch(config-acl)# no statistics per-entry
switch(config-acl)# show ip access-lists acl-01

IPV4 ACL acl-01
switch(config-acl)# copy running-config startup-config
```

Removing an IP ACL

Removing an ACL does not affect the configuration of the interfaces where applied. Instead, the device considers the removed ACL to be empty and denies all traffic due to the implicit deny rule.

Before You Begin

Before beginning this procedure, be sure that you have done the following:

- Logged in to the CLI in EXEC mode
- Know whether the ACL is applied to an interface.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no ip access-list** *name*
3. (Optional) switch(config)# **show ip access-list** *name* **summary**
4. switch(config)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Places you into global configuration mode.
Step 2	switch(config)# **no ip access-list** *name*	Removes the IP ACL that you specified by name from the running configuration.
Step 3	switch(config)# **show ip access-list** *name* **summary**	(Optional) Displays the IP ACL configuration. If the ACL remains applied to an interface, the command lists the interfaces.
Step 4	switch(config)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

```
switch# configure terminal
switch(config)# no ip access-list acl-01
switch(config)# show ip access-lists acl-01 summary
switch(config)# copy running-config startup-config
```

Changing Sequence Numbers in an IP ACL

You can change all the sequence numbers assigned to the rules in an IP ACL.

Before You Begin

Before beginning this procedure, you must be logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **resequence ip access-list** *name starting-sequence-number increment*
3. switch(config)# **show ip access-lists** *name*
4. (Optional) switch(config)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Places you into global configuration mode.
Step 2	switch(config)# **resequence ip access-list** *name starting-sequence-number increment*	Assigns sequence numbers to the rules contained in the ACL, where the first rule receives the starting sequence number that you specify. Each subsequent rule receives a number larger than the preceding rule. The difference in numbers is determined by the increment that you specify. The starting-sequence-number argument and the increment argument can be a whole number from 1 to 4294967295.

	Command or Action	Purpose
Step 3	switch(config)# **show ip access-lists** *name*	Displays the IP ACL configuration.
Step 4	switch(config)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

```
switch# configure terminal
switch(config)# resequence access-list ip acl-01 100 10
switch(config)# show ip access-lists acl-01
switch(config)# copy running-config startup-config
```

Adding an IP ACL to a Port Profile

You can use this procedure to add an IP ACL to a port profile.

You must know the following information:

- If you want to create a new port profile, you must know the name you want to give the profile.
- The name of the IP access control list that you want to configure for this port profile.
- The direction of the packet flow for the access list.

Before You Begin

Before beginning this procedure, be sure you have done the following:

- Logged in to the CLI in EXEC mode.
- Created the IP ACL to add to this port profile and you know its name.
- If you are using an existing port profile, you have created it and you know its name.

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-profile** [**type vethernet**] *name*
3. switch(config-port-prof)# **ip port access-group** *name* { **in** | **out** }
4. (Optional) switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
5. (Optional) switch(config-port-prof)# **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Places you into global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **port-profile** [**type vethernet**] *name*	Enters port profile configuration mode for the named port profile.
Step 3	switch(config-port-prof)# **ip port access-group** *name* { **in** | **out** }	Adds the named ACL to the port profile for either inbound or outbound traffic.
Step 4	switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]	(Optional) Displays the configuration for verification.
Step 5	switch(config-port-prof)# **copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

```
switch# configure terminal
switch(config)# port-profile AccessProf
switch(config-port-prof)# ip port access-group allaccess4 out
switch(config-port-prof)# show port-profile name AccessProf
switch(config-port-prof)# copy running-config startup-config
```

Verifying the IP ACL Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show running-config aclmgr	Displays the ACL configuration, including the IP ACL configuration and interfaces that IP ACLs are applied to.
show ip access-lists [*name*]	Displays all IPv4 access control lists (ACLs) or a named IPv4 ACL.
show ip access-list [*name*] su**mmary**	Displays a summary of all configured IPv4 ACLs or a named IPv4 ACL.
show running-config port profile	Displays the configuration of a port profile to which you have applied an ACL.

Monitoring IP ACLs

Use one of the following commands for IP ACL monitoring:

Command	Purpose
show ip access-lists	Displays IPv4 ACL configuration.

Command	Purpose
show ip access-lists summary	Displays details about the interfaces that have access lists configured on them.

Feature History for IP ACLs

This table only includes updates for those releases that have resulted in additions to the feature

Feature History	Releases	Feature Information
IP ACLs Statistics	Release 5.2(1)IC1(1.2)	This feature was introduced.
IP ACLs	Release 5.2(1)IC1(1.1)	This feature was introduced.