CHAPTER 9

Configuring an IP ACL

This chapter describes how to configure IP access control lists (ACLs).

This chapter includes the following sections:

Information About ACLs

An ACL is an ordered set of rules for filtering traffic. When the device determines that an ACL applies to a packet, it tests the packet against the rules. The first matching rule determines whether the packet is permitted or denied. If there is no match, the device applies a default rule. The device processes packets that are permitted and drops packets that are denied. For more information, see the "Implicit Rules" section on page 9-3.

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

This section includes the following topics:

ACL Types and Applications

When a port ACL is applied to a trunk port, the ACL filters traffic on all VLANs on the trunk port.

The following types of port ACLs are supported for filtering Layer 2 traffic:

- IP ACLs—The device applies IPv4 ACLs only to IP traffic.
- MAC ACLs—The device applies MAC ACLs only to non-IP traffic.

Order of ACL Application

ACLs are applied in the following order:

1. Incoming Port ACL
2. Outgoing Port ACL

About 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 I/O module.

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.

This section describes some of the options that you can use when you configure a rule. For information about every option, see the applicable **permit** and **deny** commands in the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*.

This section includes the following topics:

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. How you specify the source and destination depends on whether you are configuring IP or MAC ACLs. For information about specifying source and destination, see the applicable **permit** and **deny** commands in the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*.

Protocols

IP and MAC ACLs let 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.

You can specify any protocol by number. In MAC ACLs, you can specify protocols by the Ethertype number of the protocol, which is a hexadecimal number. For example, you can use 0x0800 to specify IP traffic in a MAC ACL rule.

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.

For a list of the protocols that each type of ACL supports by name, see the applicable **permit** and **deny** commands in the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1).*

Implicit Rules

IP and MAC 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
```

All MAC ACLs include the following implicit rule:

```
deny 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 types
  - Precedence level
  - Differentiated Services Code Point (DSCP) value
  - TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set
- MAC ACLs support the following additional filtering options:
  - Layer 3 protocol
  - VLAN ID
  - Class of Service (CoS)

For information about all filtering options available in rules, see the applicable **permit** and **deny** commands in the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1).*

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:

  ```
  n1000v(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:

  ```
  n1000v(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 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 and MAC 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. For more information, see the "Implicit Rules" section on page 9-3.

ACL Logging

You can use access control list (ACL) logging to monitor flows that affect specific ACLs. The ACLs can be configured with the optional **log** keyword in each of the access control entries (ACEs). When you configure an option, statistics for each flow that match the ACL permit or deny conditions that you enter are logged in the software.

You can apply the log option to any ACL by entering the following commands:

```
(config)# ip access-list [name]
(config-acl)# permit tcp any 156.10.3.44/24 log
```

An implicit deny rule is the default action for ACLs. To log any packets that match the implicit deny rule, you must to create an explicit deny rule and add the **log** keyword.

ACL logging is only applicable to ACLs that are configured with the **ip access-list** command. Other traffic such as the Virtual Supervisor Module (VSM) management interface or the selectors (aaa authen match, qos match, and so on) are not logged.

Statistics and logging are provided for each flow. A flow is defined by the following IP flows:

- VSM ID
- Virtual Ethernet Module (VEM) ID
- Source interface
- Protocol
- Source IP address
- Source port
- Destination IP address
- Destination port

Scalability is provided through the following functionality:

- Each Cisco Nexus 1000V switch can support up to 64 VEMs.
- Each VEM can support up to 5000 permits and 5000 denies flows. The maximum number of permit/deny flows is a configurable option.
- The flow reporting interval can be set from 5 up to 86,400 seconds (1 day).
- The configuration flow syslog level can be from 0 to 7.
- Up to three syslog servers are supported.

For information about troubleshooting ACL logging, see to the *Cisco Nexus 1000V Troubleshooting Guide, Release 4.2(1)SV1(5.1)*.

ACL Flows

An ACL flow as it pertains to ACL logging has the following characteristics:

- It represents a stream of IPv4 packets with the same packet headers (SrcIP, DstIP, Protocol, SrcPort, DstPort) for which an identical ACL action is enforced. Each flow entry tracks the count of packets that match the flow.
- It is created only if logging is enabled on the corresponding ingress/egress ACL policy. Ingress and egress flows are tracked separately.

- Each VEM tracks a maximum of 10,000 ACL flows; a flow space is shared between permit/deny flows; each has a configurable maximum of 5000.
- Each flow entry contains the following:
  - Packet tuple
  - ACL action
  - Direction
  - Packet count
- The ACL flow life cycle is as follows:
  - A flow is created when the first packet of a unidirectional stream matches a Layer 3 ACL policy. A new flow notification is sent to the syslog server.
  - For all subsequent packets with a tuple that matches the flow-tuple, the per flow packet counter is incremented.
  - Each flow is tracked periodically based on the configured reporting interval. Within each periodic report, all the active flows and the corresponding packet count seen since the last periodic report are reported to the syslog server.
  - If no packets matches a flow for one full periodic interval, the flow entry is purged. This is the only flow-aging scheme.
  - A flow is not stateful. There is no connection tracking for TCP flows.
- The flow reporting process occurs in the following manner:
  - For each flow created, a new flow notification message is sent to the syslog server.
  - A periodic report for each active flow comes next. A flow is active if packets that match the flow are seen since the last periodic report.
  - The flow information is exported to the syslog server and contains the following: packet tuple, ACL action, direction, VEM-ID, VSM-ID, packet count.
  - The periodic time can be as low as 5 seconds with the default setting of 5 minutes. A new user space ACL-Logging thread handles the periodic poll and report functionality.
  - Syslog messages that identify the flow space usage are sent at 75 percent, 90 percent, and 100 percent of the threshold maximum to the syslog server once during each interval.

Syslog Messages

Syslog message characteristics are as follows:

- Syslog messages that contain flow information are exported from each VEM.
- The syslog client functionality is RFC-5424 compliant and communicates to servers over a UDP port (514).
- The host must be configured with a vmknic interface that can reach the remote syslog server.
- On an ESXi-5.0 host, syslog messages are blocked by a firewall. The Cisco Nexus 1000V has installation scripts that open the firewall for port 514.

Prerequisites for IP ACLs

IP ACLs have the following prerequisites:

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

Guidelines and Limitations

IP ACLs have the following configuration guidelines and limitations:

- 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.
- ACLs are not supported in port channels.

Default Settings

Table 9-1 lists the default settings for IP ACL parameters.

Table 9-1 Default IP ACL Parameters

Parameters	Default
IP ACLs	No IP ACLs exist by default
ACL rules	Implicit rules apply to all ACLs (see the "Implicit Rules" section on page 9-3)

Configuring IP ACLs

This section includes the following topics:

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 know or do the following:

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

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

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into CLI Global Configuration mode.
Step 2	**[no] ip access-list** {*name* | **match-local-traffic**} **Example:** n1000v(config)# ip access-list acl-01 n1000v(config-acl)# **Example:** n1000v(config)# ip access-list match-local-traffic n1000v(config-acl)#	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.

	Command	Purpose
Step 3	[*sequence-number*] {**permit** | **deny**} *protocol source destination* **Example:** `n1000v(config-acl)# permit ip 192.168.2.0/24 any`	Creates a rule in the IP ACL. You can create many rules. The *sequence-number* argument can be a whole number between 1 and 4294967295. The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*.
Step 4	**statistics per-entry** **Example:** `n1000v(config-acl)# statistics per-entry`	(Optional) Specifies that the device maintains global statistics for packets that match the rules in the ACL.
Step 5	**show ip access-lists** *name* **Example:** `n1000v(config-acl)# show ip access-lists acl-01`	(Optional) Displays the IP ACL configuration.
Step 6	**copy running-config startup-config** **Example:** `n1000v(config-acl)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

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 recreate it 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. For more information, see the "Changing Sequence Numbers in an IP ACL" section on page 9-12.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **config t**
2. **ip access-list** *name*
3. [*sequence-number*] {**permit | deny**} *protocol source destination*
4. **no** {*sequence-number* | {**permit | deny**} *protocol source destination*}
5. [**no**] **statistics per-entry**
6. **show ip access-list** *name*
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into CLI Global Configuration mode.
Step 2	**ip access-list** *name* **Example:** n1000v(config)# ip access-list acl-01 n1000v(config-acl)#	Places you into IP ACL configuration mode for the specified ACL.
Step 3	[*sequence-number*] {**permit** | **deny**} *protocol source destination* **Example:** n1000v(config-acl)# 100 permit ip 192.168.2.0/24 any	(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 between 1 and 4294967295. The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*
Step 4	**no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*} **Example:** n1000v(config-acl)# no 80	(Optional) Removes the rule that you specified from the IP ACL. The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1).*
Step 5	[**no**] **statistics per-entry** **Example:** n1000v(config-acl)# statistics per-entry	(Optional) 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	**show ip access-lists** *name* **Example:** n1000v(config-acl)# show ip access-lists acl-01	(Optional) Displays the IP ACL configuration.
Step 7	**copy running-config startup-config** **Example:** n1000v(config-acl)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Removing an IP ACL

You can remove an IP ACL from the device.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- Make sure that you know whether the ACL is applied to an interface.
- Removing an ACL does not affect the configuration of the interfaces where applied. Instead, the device considers the removed ACL to be empty.

SUMMARY STEPS

1. **config t**
2. **[no] ip access-list** *name*
3. **show ip access-list** *name* **summary**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into CLI Global Configuration mode.

Step 2	**no ip access-list** *name* **Example:** `n1000v(config)# no ip access-list acl-01`	Removes the IP ACL that you specified by name from the running configuration.
Step 3	**show ip access-list** *name* **summary** **Example:** `n1000v(config)# show ip access-lists acl-01 summary`	(Optional) Displays the IP ACL configuration. If the ACL remains applied to an interface, the command lists the interfaces.
Step 4	**copy running-config startup-config** **Example:** `n1000v(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

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 know or do the following:

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **config t**
2. **resequence ip access-list** *name starting-sequence-number increment*
3. **show ip access-lists** *name*
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into CLI Global Configuration mode.

Step 2	**resequence ip access-list** *name starting-sequence-number increment* **Example:** `n1000v(config)# resequence access-list ip acl-01 100 10`	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 between 1 and 4294967295.
Step 3	**show ip access-lists** *name* **Example:** `n1000v(config)# show ip access-lists acl-01`	(Optional) Displays the IP ACL configuration.
Step 4	**copy running-config startup-config** **Example:** `n1000v(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Applying an IP ACL as a Port ACL

Use this procedure to configure a port ACL by applying an IPv4 or ACL to a Layer 2 interface physical port.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You can apply one port ACL to an interface.
- Make sure that the ACL you want to apply exists and that it is configured to filter traffic in the manner that you need for this application. For more information, see the "Creating an IP ACL" section on page 9-8 or the "Changing an IP ACL" section on page 9-9.
- An IP ACL can also be configured in a port profile. For more information, see the "Adding an IP ACL to a Port Profile" procedure on page 9-14.

SUMMARY STEPS

1. **config t**
2. **interface vethernet** *port*
3. **ip port access-group** *access-list* **[in | out]**
4. **show running-config aclmgr**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into CLI Global Configuration mode.

Step 2	**interface vethernet** *port*
	
	Example:
	`n1000v(config)# interface vethernet 40`
	`n1000v(config-if)#`
		Places you into Interface Configuration mode for the specified vEthernet interface.

Step 3	**ip port access-group** *access-list* [**in** | **out**] **Example:** `n1000v(config-if)# ip port access-group acl-l2-marketing-group in`	Applies an inbound or outbound IPv4 ACL to the interface. You can apply one port ACL to an interface.
Step 4	**show running-config aclmgr** **Example:** `n1000v(config-if)# show running-config aclmgr`	(Optional) Displays the ACL configuration.

	Command	Purpose
Step 5	**copy running-config startup-config** **Example:** `n1000v(config-if)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Adding an IP ACL to a Port Profile

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

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already created the IP ACL to add to this port profile using the "Creating an IP ACL" procedure on page 9-8; and you know its name.
- If using an existing port profile, you have already created it and you know its name.
- If creating a new port profile, you know the interface type (Ethernet or vEthernet) and the name you want to give the profile.
- For more information about port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*;
- You know the name of the IP access control list that you want to configure for this port profile.
- You know the direction of packet flow for the access list.

SUMMARY STEPS

1. **config t**
2. **port-profile** [**type** {**ethernet** | **vethernet**}] *profile-name*
3. **ip port access-group** *name* {**in** | **out**}
4. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Description
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**port-profile** [**type** {**ethernet** | **vethernet**}] *name* **Example:** n1000v(config)# port-profile AccessProf n1000v(config-port-prof)#	Enters port profile configuration mode for the named port profile.
Step 3	**ip port access-group** *name* {**in** | **out**} **Example:** n1000v(config-port-prof)# ip port access-group allaccess4 out	Adds the named ACL to the port profile for either inbound or outbound traffic.
Step 4	**show port-profile name** *profile-name* **Example:** n1000v(config-port-prof)# show port-profile name AccessProf	(Optional) Displays the configuration for verification.
Step 5	**copy running-config startup-config** **Example:** n1000v(config-port-prof)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Applying an IP ACL to the Management Interface

Use this procedure to applying an IPv4 or ACL to the Management interface, mgmt0.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- Make sure that the ACL you want to apply exists and that it is configured to filter traffic in the manner that you need for this application. For more information, see the "Creating an IP ACL" section on page 9-8 or the "Changing an IP ACL" section on page 9-9.

SUMMARY STEPS

1. **config t**
2. **interface mgmt0**
3. **[no] ip access-group** *access-list* **[in | out]**
4. **show ip access-lists** *access-list*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into CLI global configuration mode.
Step 2	**interface mgmt0** **Example:** n1000v(config)# interface mgmt0 n1000v(config-if)#	Places you into interface configuration mode for the management interface.
Step 3	**[no] ip access-group** *access-list* [**in** | **out**] **Example:** n1000v(config-if)# ip access-group telnet in n1000v(config-if)#	Applies a specified inbound or outbound IPv4 ACL to the interface. The no option removes the specified configuration.
Step 4	**show ip access-lists** *access-list* **Example:** n1000v(config-if)# show ip access-lists telnet summary IP access list telnet statistics per-entry Total ACEs Configured:2 Configured on interfaces: mgmt0 - ingress (Router ACL) Active on interfaces: mgmt0 - ingress (Router ACL)	(Optional) Displays the ACL configuration.
Step 5	**copy running-config startup-config** **Example:** n1000v(config-if)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Configuring ACL Logging

ACL logging is the enabled on by default all Virtual Ethernet Modules (VEMs). In addition, the following also apply to ACL logging configuration:

- Any rule can be enabled for logging by adding the **log** keyword.
- Only packets that have a rule with the **log** keyword enabled are logged.

Disabling ACL Logging

You can disable ACL logging on a VEM by entering the following command:

Command	Purpose
[no] logging ip access-list cache module *vem*	Disables ACL logging on the specified VEM.

Configuring a Time Interval for Accumulating Packet Counters

You can configure the time interval for accumulating packet counters before they are reported to the syslog servers. You enter the time range in seconds from 5 to 86,400 seconds (1 day). The default is 300 seconds (5 minutes).

You can configure the amount of time to accumulate packet counters by entering one of the following commands:

Command	Purpose
logging ip access-list cache interval *secs*	Sets the time interval in seconds to accumulate packet counters before they are reported to the syslog servers, where *num* is the number of seconds.
[no] logging ip access-list cache interval *secs*	Reverts the configuration to the default time interval configuration 300 seconds (5 minutes), where *num* is the number of seconds.

EXAMPLES

These examples show the time interval syslog message format that is sent periodically when the time interval expires:

```
ACL-LOGGING-6-PERMIT-FLOW-INTERVAL <VSM-id> <VEM-id> <protocol> <source-interface>
<source-ip/source-port)> <destination-ip/destination-port> Hit-count = <nnn>

ACL-LOGGING-6-DENY-FLOW-INTERVAL <VSM-id> <VEM-id> <protocol> <source-interface>
<source-ip/source-port)> <destination-ip/destination-port> Hit-count = <nnn>
```

These examples show the time interval syslog message format that is sent when the time interval conditions are met:

```
ACL-LOGGING-6-MAX-PERMIT-FLOW-REACHED: The number of ACL log permit-flows has reached 75%
limit (<n>)
ACL-LOGGING-6-MAX-PERMIT-FLOW-REACHED: The number of ACL log permit-flows has reached 90%
limit (<n>)
ACL-LOGGING-6-MAX-PERMIT-FLOW-REACHED: The number of ACL log permit-flows has reached 100%
limit (<n>)

ACL-LOGGING-6-MAX-DENY-FLOW-REACHED: The number of ACL log deny-flows has reached 75%
limit (<n>)
ACL-LOGGING-6-MAX-DENY-FLOW-REACHED: The number of ACL log deny-flows has reached 90%
limit (<n>)
ACL-LOGGING-6-MAX-DENY-FLOW-REACHED: The number of ACL log deny-flows has reached 100%
limit (<n>)
```

Configuring Flows

You can configure the number of deny and permit flows per VEM. The range is from 0 to 5000 flows. The default is 3000. A syslog message is sent when the flow is near the maximum threshold. The first message is sent when the number of flows has reached 75 percent of the maximum threshold and the next message is sent when the number of flows has reached 90 percentof the maximum threshold. The last message is sent when the number of flows reaches the maximum threshold 100 percent.

Configuring Permit Flows

You can configure permit flows by entering one of the following commands:

Command	Purpose
logging ip access-list cache max-permit-flows *num*	Sets the number of permit flows where *num* is the number of flows.
[no] logging ip access-list cache max-permit-flows	Reverts the configuration to the default permit flow value 3000.

EXAMPLES

These examples show permit flow syslog messages:

- New flow notification message

```
-  Aug 28 04:17:19 fish-231-157.cisco.com 1 2011-08-28T11:14:23 - n1k-ecology -
ACLLOG-PERMIT-FLOW-CREATE VSM ID: 172.23.231.150, VEM ID:
86d04494-79e2-11df-a573-d0d0fd093c68, Source IP: 192.168.231.22, Destination IP:
192.168.231.21, Source Port: 42196, Destination Port: 8029, Source Interface: Veth2,
Protocol: "TCP"(6), Hit-count = 1
```

- Periodic flow reporting message

```
-  Aug 28 04:17:20 sfish-231-157.cisco.com 1 2011-08-28T11:14:23 - n1k-acllog -
ACLLOG-PERMIT-FLOW-INTERVAL VSM ID: 172.23.231.150, VEM ID:
86d04494-79e2-11df-a573-d0d0fd093c68, Source IP: 192.168.231.22, Destination IP:
192.168.231.21, Source Port: 42196, Destination Port: 8029, Source Interface: Veth2,
Protocol: "TCP"(6), Hit-count = 1245
```

- Threshold crossing alarm messages

```
-  Aug 28 04:17:22 sfish-231-157.cisco.com 1 2011-08-28T11:14:24 - n1k-acllog -
ACLLOG-MAX-PERMIT-FLOW-REACHED The number of ACL log permit-flows has reached 75 percent
limit (3969)
-  Aug 28 04:17:26 sfish-231-157.cisco.com 1 2011-08-28T11:14:26 - n1k-acllog -
ACLLOG-MAX-PERMIT-FLOW-REACHED The number of ACL log permit-flows has reached 90 percent
limit (4969)
-  Aug 28 04:17:27 sfish-231-157.cisco.com 1 2011-08-28T11:14:31 - n1k-acllog -
ACLLOG-MAX-PERMIT-FLOW-REACHED The number of ACL log permit-flows has reached 100 percent
limit (5000)
```

Configuring Deny Flows

You can configure deny flows by entering one of the following commands:

Command	Purpose
logging ip access-list cache max-deny-flows *num*	Sets the number of deny flows, where *num* is the number of flows
[no] logging ip access-list cache max-deny-flows	Reverts the configuration back to the default deny flow value 3000.

EXAMPLES

These examples show deny flow syslog messages:

- New flow notification message

```
-  Aug 28 04:17:19 sfish-231-157.cisco.com 1 2011-08-28T11:14:23 - n1k-acllog -
ACLLOG-DENY-FLOW-CREATE VSM ID: 172.23.231.150, VEM ID:
86d04494-79e2-11df-a573-d0d0fd093c68, Source IP: 192.168.231.22, Destination IP:
192.168.231.100, Source Port: 48528, Destination Port: 8029, Source Interface: Veth2,
Protocol: "TCP"(6), Hit-count = 1
```

- Periodic flow reporting message

```
-  Aug 28 04:17:20 sfish-231-157.cisco.com 1 2011-08-28T11:14:23 - n1k-acllog -
ACLLOG-DENY-FLOW-INTERVAL VSM ID: 172.23.231.150, VEM ID:
86d04494-79e2-11df-a573-d0d0fd093c68, Source IP: 192.168.231.22, Destination
IP:192.168.231.100, Source Port: 47164, Destination Port: 8029, Source Interface: Veth2,
Protocol: "TCP"(6), Hit-count = 1245
```

- Threshold crossing alarm messages

```
-  Aug 28 04:17:27 sfish-231-157.cisco.com 1 2011-08-28T11:14:31 - n1k-acllog -
ACLLOG-MAX-DENY-FLOW-REACHED The number of ACL log deny-flows has reached 75 percent limit
(4330)
-  Aug 28 04:18:27 sfish-231-157.cisco.com 1 2011-08-28T11:15:31 - n1k-acllog -
ACLLOG-MAX-DENY-FLOW-REACHED The number of ACL log deny-flows has reached 90 percent limit
(4630)
-  Aug 28 04:20:17 sfish-231-157.cisco.com 1 2011-08-28T11:17:20 - n1k-acllog -
ACLLOG-MAX-PERMIT-FLOW-REACHED The number of ACL log permit-flows has reached 100 percent
limit (5000)
```

Configuring Syslog Server Severity Levels

You can configure severity levels of the ACL logging syslog messages for up to three remote syslog servers. The range is from 0 up to 7. The default severity level is 6. See the "Configuring Flows" section on page 9-17 for examples. Table 9-2 lists the severity code, the severity level, and the description of each severity level.

Table 9-2 Severity Levels

Severity code	Severity level	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant condition
6	Informational	Informational messages.
7	Debug	Debug-level messages

You can set the severity level of a syslog message and the server to which you want the message to be sent by entering one of the following commands:

Command	Purpose
acllog match-log-level *level*	Sets the severity level at which syslog messages are sent, where *level* is the severity code from 0 to 7.
[no] logging ip access-list cache max-deny-flows	Reverts the configuration back to the default severity level 6.
logging server *A.B.C.D 0-7*	Specifies the syslog server on which you want to set a severity level, where *A.B.C.D* is the syslog server IP address and *0-7* are the severity levels you can choose.

Verifying the IP ACL Configuration

To display IP ACL configuration information, use the following commands:

Command	Purpose
show running-config aclmgr	Displays the ACL configuration, including 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*] **summary**	Displays a summary of all configured IPv4 ACLs or a named IPv4 ACL.
show running-config interface	Displays the configuration of an interface to which you have applied an ACL.
show logging ip access-list status	Displays the ACL logging configuration for a VSM
vemcmd show acllog config	Displays the VEM ACL logging configuration

Monitoring IP ACL

Use the following commands for IP ACL monitoring:

Command	Purpose
show ip access-lists	Displays IPv4 ACL configuration. If the IPv4 ACL includes the **statistics per-entry** command, then the **show ip access-lists** command output includes the number of packets that have matched each rule.
clear ip access-list counters	Clears statistics for all IPv4 ACLs or for a specific IPv4 ACL.

Example Configurations for IP ACL

This example shows how to create an IPv4 ACL named acl-01 and apply it as a port ACL to vEthernet interface 40:

```
ip access-list acl-01
    permit ip 192.168.2.0/24 any
interface vethernet 40
ip port access-group acl-01 in
```

This example shows how to enable access list matching for locally-generated traffic:

```
ip access-list match-local-traffic
```

This example shows how to verify VSM ACL logging configuration:

```
vsm# show logging ip access-list status
    Max deny flows   = 3000
    Max permit flows = 3000
    Alert interval   = 300
    Match log level  = 6
    VSM IP = 192.168.1.1
    Syslog IP = 10.1.1.1
    Syslog IP = 0.0.0.0
    Syslog IP = 0.0.0.0

    ACL Logging enabled on module(s):
       4   5   6   7   8   9  10  11  12  13  14  15  16  17  18  19
      20  21  22  23  24  25  26  27  28  29  30  31  32  33  34  35
      36  37  38  39  40  41  42  43  44  45  46  47  48  49  50  51
      52  53  54  55  56  57  58  59  60  61  62  63  64  65  66
    ACL Logging disabled on module(s):
       3
```

This example shows how to verify VEM ACL logging configuration:

```
vem# vemcmd show acllog config
ACL-Log Config:
    Status:             enabled
    Reporting Interval: 300
    Max Permit Flows:   3000
    Max Deny   Flows:   3000
    Syslog Facility :   4
    Syslog Severity:    6
    Syslog Srvr 1:      10.1.1.1
    Syslog Srvr 2:      0.0.0.0
    Syslog Srvr 3:      0.0.0.0
    VSM:                192.168.1.1
```

Additional References

For additional information related to implementing IP ACLs, see the following sections:

- Related Documents, page 9-22
- Standards, page 9-22

Related Documents

Related Topic	Document Title
ACL concepts.	*Information About ACLs, page 9-1*
Configuring interfaces.	*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(5.1)*
Configuring port profiles.	*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*
Complete command syntax, command modes, command history, defaults, usage guidelines, and examples for Cisco Nexus 1000V commands.	*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for IP ACL

This section provides the IP ACL release history.

Feature Name	Releases	Feature Information
IP ACL for mgmt0 interface	4.2(1) SV1(4)	
IP ACL	4.0(4)SV1(1)	This feature was introduced.