CHAPTER 17

Configuring Logging for Access Lists

This chapter describes how to configure access list logging for extended access lists and Webytpe access lists, and it describes how to manage deny flows.

This section includes the following topics:

Configuring Logging for Access Lists

This section includes the following topics

Information About Logging Access List Activity

By default, when traffic is denied by an extended ACE or a Webtype ACE, the ASA generates system message 106023 for each denied packet in the following form:

```
%ASA|PIX-4-106023: Deny protocol src [interface_name:source_address/source_port] dst
interface_name:dest_address/dest_port [type {string}, code {code}] by access_group acl_id
```

If the ASA is attacked, the number of system messages for denied packets can be very large. We recommend that you instead enable logging using system message 106100, which provides statistics for each ACE and enables you to limit the number of system messages produced. Alternatively, you can disable all logging.

Note Only ACEs in the access list generate logging messages; the implicit deny at the end of the access list does not generate a message. If you want all denied traffic to generate messages, add the implicit ACE manually to the end of the access list, as shown in the following example:

```
hostname(config)# access-list TEST deny ip any any log
```

The **log** options at the end of the extended **access-list** command enable you to set the following behavior:

- Enable message 106100 instead of message 106023
- Disable all logging
- Return to the default logging using message 106023

System message 106100 uses the following form:

```
%ASA|PIX-n-106100: access-list acl_id {permitted | denied} protocol
interface_name/source_address(source_port) -> interface_name/dest_address(dest_port)
hit-cnt number ({first hit | number-second interval})
```

When you enable logging for message 106100, if a packet matches an ACE, the ASA creates a flow entry to track the number of packets received within a specific interval. The ASA generates a system message at the first hit and at the end of each interval, identifying the total number of hits during the interval. At the end of each interval, the ASA resets the hit count to 0. If no packets match the ACE during an interval, the ASA deletes the flow entry.

A flow is defined by the source and destination IP addresses, protocols, and ports. Because the source port might differ for a new connection between the same two hosts, you might not see the same flow increment because a new flow was created for the connection. See the "Managing Deny Flows" section on page 17-5 to limit the number of logging flows.

Permitted packets that belong to established connections do not need to be checked against access lists; only the initial packet is logged and included in the hit count. For connectionless protocols, such as ICMP, all packets are logged, even if they are permitted, and all denied packets are logged.

See the *Cisco ASA 5500 Series System Log Messages* for detailed information about this system message.

Licensing Requirements for Access List Logging

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature:

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported only in routed and transparent firewall modes.

IPv6 Guidelines

Supports IPv6.

Additional Guidelines and Limitations

ACE logging generates system log message 106023 for denied packets. A deny ACE must be present to log denied packets.

Default Settings

Table 17-1 lists the default settings for extended access list parameters.

Table 17-1 Default Extended Access List Parameters

Parameters	Default
log	When the **log** keyword is specified, the default level for system log message 106100 is 6 (informational), and the default interval is 300 seconds.

Configuring Access List Logging

This sections describes how to configure access list logging.

Note For complete access list command syntax, see the "Configuring Extended Access Lists" section on page 11-4 and the "Adding Webtype Access Lists" section on page 14-2.

To configure logging for an ACE, enter the following command:

Command	Purpose
access-list *access_list_name* [**extended**] {***deny*** | ***permit***}...[**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] **Example:** hostname(config)# access-list outside-acl permit ip host 1.1.1.1 any log 7 interval 600	Configures logging for an ACE. The **access-list** *access_list_name* syntax specifies the access list for which you want to configure logging. The **extended** option adds an ACE. The **deny** keyword denies a packet if the conditions are matched. Some features do not allow deny ACEs, such as NAT. (See the command documentation for each feature that uses an access list for more information.) The **permit** keyword permits a packet if the conditions are matched. If you enter the **log** option without any arguments, you enable system log message 106100 at the default level (6) and for the default interval (300 seconds). See the following options: • *level*—A severity level between 0 and 7. The default is 6. • **interval** *secs*—The time interval in seconds between system messages, from 1 to 600. The default is 300. This value is also used as the timeout value for deleting an inactive flow. • **disable**—Disables all access list logging. • **default**—Enables logging to message 106023. This setting is the same as having no **log** option. (See the **access-list** command in the *Cisco Security Appliance Command Reference* for more information about command options.)

Monitoring Access Lists

To monitor access lists, enter one of the following commands:

Command	Purpose
show access list	Displays the access list entries by number.
show running-config access-list	Displays the current running access-list configuration.

Configuration Examples for Access List Logging

This section includes sample configurations for logging access lists.

You might configure the following access list:

```
hostname(config)# access-list outside-acl permit ip host 1.1.1.1 any log 7 interval 600
hostname(config)# access-list outside-acl permit ip host 2.2.2.2 any
hostname(config)# access-list outside-acl deny ip any any log 2
hostname(config)# access-group outside-acl in interface outside
```

When the first ACE of outside-acl permits a packet, the ASA generates the following system message:

```
%ASA|PIX-7-106100: access-list outside-acl permitted tcp outside/1.1.1.1(12345) ->
inside/192.168.1.1(1357) hit-cnt 1 (first hit)
```

Although 20 additional packets for this connection arrive on the outside interface, the traffic does not have to be checked against the access list, and the hit count does not increase.

If one or more connections by the same host are initiated within the specified 10 minute interval (and the source and destination ports remain the same), then the hit count is incremented by 1, and the following message displays at the end of the 10 minute interval:

```
%ASA|PIX-7-106100: access-list outside-acl permitted tcp outside/1.1.1.1(12345)->
inside/192.168.1.1(1357) hit-cnt 2 (600-second interval)
```

When the third ACE denies a packet, the ASA generates the following system message:

```
%ASA|PIX-2-106100: access-list outside-acl denied ip outside/3.3.3.3(12345) ->
inside/192.168.1.1(1357) hit-cnt 1 (first hit)
```

If 20 additional attempts occur within a 5 minute interval (the default), the following message appears at the end of 5 minutes:

```
%ASA|PIX-2-106100: access-list outside-acl denied ip outside/3.3.3.3(12345) ->
inside/192.168.1.1(1357) hit-cnt 21 (300-second interval)
```

Feature History for Access List Logging

Table 17-2 lists the release history for this feature.

Table 17-2 Feature History for Access List Logging

Feature Name	Releases	Feature Information
Access list logging	7.0	You can enable logging using system message 106100, which provides statistics for each ACE and lets you limit the number of system messages produced. The following command was introduced: **access-list**.

Managing Deny Flows

This section includes the following topics:

Information About Managing Deny Flows

When you enable logging for message 106100, if a packet matches an ACE, the ASA creates a flow entry to track the number of packets received within a specific interval. The ASA has a maximum of 32 K logging flows for ACEs. A large number of flows can exist concurrently at any point of time. To prevent unlimited consumption of memory and CPU resources, the ASA places a limit on the number of concurrent *deny* flows; the limit is placed on deny flows only (not on permit flows) because they can indicate an attack. When the limit is reached, the ASA does not create a new deny flow for logging until the existing flows expire.

For example, if someone initiates a DoS attack, the ASA can create a large number of deny flows in a short period of time. Restricting the number of deny flows prevents unlimited consumption of memory and CPU resources.

When you reach the maximum number of deny flows, the ASA issues system message 106100:

```
%ASA|PIX-1-106101: The number of ACL log deny-flows has reached limit (number).
```

The **access-list alert-interval** command sets the time interval for generating the system log message 106001. The system log message 106001 alerts you that the adaptive security appliance has reached a deny flow maximum. When the deny flow maximum is reached, another system log message 106001 is generated if at least six seconds have passed since the last 106001 message was generated.

Licensing Requirements for Managing Deny Flows

The following table shows the licensing requirements for this feature:

Model	License Requirement
All models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature:

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported only in routed and transparent firewall modes.

IPv6 Guidelines

Supports IPv6.

Additional Guidelines and Limitations

The ASA places a limit on the number of concurrent *deny* flows only—not permit flows.

Default Settings

Table 17-1 lists the default settings for managing deny flows.

Table 17-3 Default Parameters for Managing Deny Flows

Parameters	Default
numbers	The *numbers* argument specifies the maximum number of deny flows. The default is 4096.
secs	The *secs* argument specifies the time, in seconds, between system messages. The default is 300.

Managing Deny Flows

To configure the maximum number of deny flows and to set the interval between deny flow alert messages (106100), enter the following command:

Command	Purpose
access-list deny-flow-max *number* **Example:** `hostname(config)# access-list deny-flow-max 3000`	Sets the maximum number of deny flows. The *numbers* argument specifies the maximum number, which can be between 1 and 4096. The default is 4096.

To set the amount of time between system messages (number 106101), which identifies that the maximum number of deny flows was reached, enter the following command:

Command	Purpose
access-list alert-interval *secs* **Example:** `hostname(config)# access-list alert-interval 200`	Sets the time, in seconds, between system messages. The *secs* argument specifies the time interval between each deny flow maximum message. Valid values are from 1 to 3600 seconds. The default is 300 seconds.

Monitoring Deny Flows

To monitor access lists, enter one of the following commands:

Command	Purpose
`show access-list`	Displays access list entries by number.
`show running-config access-list`	Displays the current running access-list configuration.

Feature History for Managing Deny Flows

Table 17-2 lists the release history for this feature.

Table 17-4 Feature History for Managing Deny Flows

Feature Name	Releases	Feature Information
Managing Deny Flows	7.0	You can configure the maximum number of deny flows and set the interval between deny flow alert messages. The following commands were introduced: **access-list deny-flow** and **access-list alert-interval**.