



CHAPTER 20

Configuring Logging for Access Lists

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

This chapter includes the following sections:

- [Configuring Logging for Access Lists, page 20-1](#)
- [Managing Deny Flows, page 20-5](#)

Configuring Logging for Access Lists

This section includes the following topics:

- [Information About Logging Access List Activity, page 20-1](#)
- [Licensing Requirements for Access List Logging, page 20-2](#)
- [Guidelines and Limitations, page 20-2](#)
- [Default Settings, page 20-3](#)
- [Configuring Access List Logging, page 20-3](#)
- [Monitoring Access Lists, page 20-4](#)
- [Configuration Examples for Access List Logging, page 20-4](#)
- [Feature History for Access List Logging, page 20-5](#)

Information About Logging Access List Activity

By default, when traffic is denied by an extended ACE or a Webtype ACE, the ASA generates syslog 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 syslog messages for denied packets can be very large. We recommend that you instead enable logging using syslog message 106100, which provides statistics for each ACE and enables you to limit the number of syslog 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

Syslog 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 syslog message at the first hit and at the end of each interval, identifying the total number of hits during the interval and the timestamp for the last hit. 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 20-5](#) 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 *syslog message guide* for detailed information about this syslog 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 syslog message 106023 for denied packets. A deny ACE must be present to log denied packets.

Default Settings

Table 20-1 lists the default settings for extended access list parameters.

Table 20-1 Default Extended Access List Parameters

Parameters	Default
log	When the log keyword is specified, the default level for syslog 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 15-2 and the [“Using Webtype Access Lists”](#) section on page 18-2.

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

Command	Purpose
<pre>access-list access_list_name [extended] {deny permit}...[log [[level] [interval secs] disable default]]</pre> <p>Example:</p> <pre>hostname(config)# access-list outside-acl permit ip host 10.0.0.0 any log 7 interval 600</pre>	<p>Configures logging for an ACE.</p> <p>The access-list <i>access_list_name</i> syntax specifies the access list for which you want to configure logging.</p> <p>The extended option adds an ACE.</p> <p>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.)</p> <p>The permit keyword permits a packet if the conditions are matched.</p> <p>If you enter the log option without any arguments, you enable syslog message 106100 at the default level (6) and for the default interval (300 seconds). See the following options:</p> <ul style="list-style-type: none"> • level—A severity level between 0 and 7. The default is 6. • interval secs—The time interval in seconds between syslog 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. <p>(See the access-list command in the <i>Cisco Security Appliance Command Reference</i> for more information about command options.)</p>

Monitoring Access Lists

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

Command	Purpose
<code>show access list</code>	Displays the access list entries by number.
<code>show running-config access-list</code>	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 10.10.0.0 any log 7 interval 600
hostname(config)# access-list outside-acl permit ip host 10.255.255.255 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 syslog message:

```
%ASA|PIX-7-106100: access-list outside-acl permitted tcp outside/10.0.0.0(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 syslog message displays at the end of the 10-minute interval:

```
%ASA|PIX-7-106100: access-list outside-acl permitted tcp outside/10.0.0.0(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 syslog message:

```
%ASA|PIX-2-106100: access-list outside-acl denied ip outside/10.255.255.255(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 syslog message appears at the end of 5 minutes:

```
%ASA|PIX-2-106100: access-list outside-acl denied ip outside/10.255.255.255(12345) ->
inside/192.168.1.1(1357) hit-cnt 21 (300-second interval)
```

Feature History for Access List Logging

Table 20-2 lists each feature change and the platform release in which it was implemented.

Table 20-2 Feature History for Access List Logging

Feature Name	Releases	Feature Information
Access list logging	7.0(1)	You can enable logging using syslog message 106100, which provides statistics for each ACE and lets you limit the number of syslog messages produced. We introduced the following command: access-list .
ACL Timestamp	8.3(1)	The ASA reports the timestamp for the last access rule hit.

Managing Deny Flows

This section includes the following topics:

- [Information About Managing Deny Flows, page 20-6](#)
- [Licensing Requirements for Managing Deny Flows, page 20-6](#)
- [Guidelines and Limitations, page 20-6](#)
- [Managing Deny Flows, page 20-7](#)
- [Monitoring Deny Flows, page 20-7](#)
- [Feature History for Managing Deny Flows, page 20-8](#)

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 syslog 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 syslog message 106001. Syslog message 106001 alerts you that the ASA has reached a deny flow maximum. When the deny flow maximum is reached, another syslog 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 20-1 lists the default settings for managing deny flows.

Table 20-3 Default Parameters for Managing Deny Flows

Parameters	Default
<i>numbers</i>	The <i>numbers</i> argument specifies the maximum number of deny flows. The default is 4096.
<i>secs</i>	The <i>secs</i> argument specifies the time, in seconds, between syslog 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
<code>access-list deny-flow-max <i>number</i></code>	Sets the maximum number of deny flows.
Example: hostname(config)# access-list deny-flow-max 3000	The <i>numbers</i> argument specifies the maximum number, which can be between 1 and 4096. The default is 4096.

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

Command	Purpose
<code>access-list alert-interval <i>secs</i></code>	Sets the time, in seconds, between syslog messages.
Example: hostname(config)# access-list alert-interval 200	The <i>secs</i> 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
<code>show access-list</code>	Displays access list entries by number.
<code>show running-config access-list</code>	Displays the current running access list configuration.

Feature History for Managing Deny Flows

Table 20-2 lists each feature change and the platform release in which it was implemented.

Table 20-4 Feature History for Managing Deny Flows

Feature Name	Releases	Feature Information
Managing Deny Flows	7.0(1)	You can configure the maximum number of deny flows and set the interval between deny flow alert messages. We introduced the following commands: access-list deny-flow and access-list alert-interval .