CHAPTER 17

# Adding an IPv6 Access List

This chapter describes how to configure IPv6 access lists to control and filter traffic through the adaptive security appliance.

This chapter includes the following sections:



## Information About IPv6 Access Lists

The typical access list functionality in IPv6 is similar to access lists in IPv4. Access lists determine which traffic to block and which traffic to forward at router interfaces. Access lists allow filtering based upon source and destination addresses, inbound and outbound to specific interfaces. Each access list has an implicit deny statement at the end. You define IPv6 access lists and set their deny and permit conditions using the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode.

## Licensing Requirements for IPv6 Access Lists

The following table shows the licensing requirements for this feature:

| Model | License Requirement |
|---|---|
| All models | Base License. |

# Prerequisites for Adding IPv6 Access Lists

You should be familiar with IPv6 addressing and basic configuration. See the **ipv6** commands in the *Cisco Security Appliance Command Reference* for more information about configuring IPv6.

# Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

### Context Mode Guidelines

Supported in single and multiple context modes.

### Firewall Mode Guidelines

Supported in routed and transparent firewall modes.

### IPv6 Guidelines

Supports IPv6.

### Additional Guidelines and Limitations

The following guidelines and limitations apply to IPv6 access lists:

- The **ipv6 access-list** command allows you to specify whether an IPv6 address is permitted or denied access to a port or protocol. Each command is called an ACE. One or more ACEs with the same access list name are referred to as an access list. Apply an access list to an interface using the **access-group** command.
- The adaptive security appliance denies all packets from an outside interface to an inside interface unless you specifically permit access using an access list. All packets are allowed by default from an inside interface to an outside interface unless you specifically deny access.
- The **ipv6 access-list** command is similar to the **access-list** command, except that it is IPv6-specific. For additional information about access lists, refer to the **access-list extended** command.
- The **ipv6 access-list icmp** command is used to filter ICMPv6 messages that pass through the adaptive security appliance.To configure the ICMPv6 traffic that is allowed to originate and terminate at a specific interface, use the **ipv6 icmp** command.
- See the **object-group** command for information on how to configure object groups.
- Possible operands for the operator option of the **ipv6 access-list** command include **lt** for less than, **gt** for greater than, **eq** for equal to, **neq** for not equal to, and **range** for an inclusive range. Use the **ipv6 access-list** command without an operator and port to indicate all ports by default.
- ICMP message types are filtered by the access rule. Omitting the *icmp_type* argument indicates all ICMP types. If you specify ICMP types, the value can be a valid ICMP type number (from 0 to 255) or one of the following ICMP type literals:
  - destination-unreachable
  - packet-too-big
  - time-exceeded
  - parameter-problem
  - echo-request

  - echo-reply
  - membership-query
  - membership-report
  - membership-reduction
  - router-renumbering
  - router-solicitation
  - router-advertisement
  - neighbor-solicitation
  - neighbor-advertisement
  - neighbor-redirect
- If the protocol argument is specified, valid values are **icmp**, **ip**, **tcp**, **udp**, or an integer in the range of 1 to 254, representing an IP protocol number.

# Default Settings

Table 17-1 lists the default settings for IPv6 access list parameters.

***Table 17-1 Default IPv6 Access List Parameters***

| Parameters | Default |
|---|---|
| **default** | The **default** option specifies that a syslog message 106100 is generated for the ACE. |
| **interval** *secs* | Specifies the time interval at which to generate a 106100 syslog message; valid values are from 1 to 600 seconds. The default interval is 300 seconds. This value is also used as the timeout value for deleting an inactive flow. |
| *level* | The *level* option specifies the syslog level for message 106100; valid values are from 0 to 7. The default level is 6 (informational). |
| **log** | The **log** option specifies logging action for the ACE. If you do not specify the **log** keyword or you specify the **log default** keyword, then message 106023 is generated when a packet is denied by the ACE. If you specify the **log** keyword alone or with a level or interval, then message 106100 is generated when a packet is denied by the ACE. Packets that are denied by the implicit deny at the end of an access list are not logged. You must implicitly deny packets with an ACE to enable logging. |

# Configuring IPv6 Access Lists

This section includes the following topics:



## Task Flow for Configuring IPv6 Access Lists

Use the following guidelines to create and implement an access list:

- Create an access list by adding an ACE and applying an access list name, as shown in the "Adding IPv6 Access Lists" section on page 17-5.
- Apply the access list to an interface. (See the "Configuring Access Rules" section on page 32-8 for more information.)

# Adding IPv6 Access Lists

You can add a regular IPv6 access list or add an IPv6 access list with TCP.

To add a regular IPv6 access list, enter the following command:

| Command | Purpose |
|---|---|
| **ipv6 access-list** *id* [**line** *line-num*] {**deny** \| **permit**} {*protocol* \| **object-group** *protocol_obj_grp_id*} {*source-ipv6-prefix/prefix-length* \| **any** \| **host** *source-ipv6-address* \| **object-group** *network_obj_grp_id*} [*operator* {*port* [*port*] \| **object-group** *service_obj_grp_id*}] {*destination-ipv6-prefix/prefix-length* \| **any** \| **host** *destination-ipv6-address* \| **object-group** *network_obj_grp_id*} [{*operator port* [*port*] \| **object-group** *service_obj_grp_id*}] [**log** [[*level*] [**interval** *secs*] \| **disable** \| **default**]]<br><br>**Example:**<br>`hostname(config)# ipv6 access-list acl_grp permit tcp any host 3001:1::203:A0FF:FED6:162D` | Configures an IPv6 access list.<br><br>The **any** keyword is an abbreviation for the IPv6 prefix ::/0, indicating any IPv6 address.<br><br>The **deny** keyword denies access if the conditions are matched.<br><br>The *destination-ipv6-address* argument identifies the IPv6 address of the host receiving the traffic.<br><br>The *destination-ipv6-prefix* argument identifies the IPv6 network address where the traffic is destined.<br><br>The **disable** option disables syslog messaging.<br><br>The **host** keyword indicates that the address refers to a specific host.<br><br>The ***id** keyword* specifies the number of an access list.<br><br>The **line** *line-num* option specifies the line number for inserting the access rule into the list. By default, the ACE is added to the end of the access list.<br><br>The *network_obj_grp_id* argument specifies existing network object group identification.<br><br>The **object-group** option specifies an object group.<br><br>The *operator* option compares the source IP address or destination IP address ports. For a list of permitted operands, see the "Guidelines and Limitations" section on page 17-2.<br><br>The **permit** keyword permits access if the conditions are matched.<br><br>The *port* option specifies the port that you permit or deny access. You can specify the port either by a number in the range of 0 to 65535 or by a literal name if the protocol is **tcp** or **udp**. For a list of permitted TCP or UDP literal names, see the "Guidelines and Limitations" section on page 17-2.<br><br>The *prefix-length* argument indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix.<br><br>The *protocol* argument specifies the name or number of an IP protocol.<br><br>The *protocol_obj_grp_id* indicates the existing protocol object group ID.<br><br>The *service_obj_grp_id* option specifies the object group.<br><br>The *source-ipv6-address* specifies the address of the host sending traffic.<br><br>The *source-ipv6-prefix* specifies the IPv6 address of traffic origin. |

To configure an IPv6 access list with ICMP, enter the following command:

| Command | Purpose |
|---|---|
| **ipv6 access-list** *id* [**line** *line-num*] {**deny** \| **permit**} **icmp6** {*source-ipv6-prefix*/*prefix-length* \| **any** \| **host** *source-ipv6-address* \| **object-group** *network_obj_grp_id*} {*destination-ipv6-prefix*/*prefix-length* \| **any** \| **host** *destination-ipv6-address* \| **object-group** *network_obj_grp_id*} [*icmp_type* \| **object-group** *icmp_type_obj_grp_id*] [**log** [[*level*] [**interval** *secs*] \| **disable** \| **default**]]<br><br>**Example:**<br>`hostname(config)# ipv6 access list acl_grp permit tcp any host 3001:1::203:AOFF:FED6:162D` | Configures an IPv6 access list with ICMP.<br><br>The **icmp6** keyword specifies that the access rule applies to ICMPv6 traffic passing through the adaptive security appliance.<br><br>The *icmp_type* argument specifies the ICMP message type being filtered by the access rule. The value can be a valid ICMP type number from 0 to 255. (For a list of the permitted ICMP type literals, see the "Guidelines and Limitations" section on page 17-2.)<br><br>The *icmp_type_obj_grp_id* option specifies the object group ICMP type ID.<br><br>For details about additional **ipv6 access-list** command parameters, see the preceding procedure for adding a regular IPv6 access list, or see the **ipv6 access-list** command in the *Cisco Security Appliance Command Reference*. |

# Adding Remarks to Access Lists

You can include remarks about entries in any access list, including extended, EtherType, IPv6, standard, and Webtype access lists. The remarks make the access list easier to understand.

To add a remark after the last **access-list** command you entered, enter the following command:

| Command | Purpose |
|---|---|
| **`access-list`** *`access_list_name`* **`remark`** *`text`*<br><br>**Example:**<br>`hostname(config)# access-list OUT remark - this is the inside admin address` | Adds a remark after the last access-list command you entered.<br><br>The text can be up to 100 characters in length. You can enter leading spaces at the beginning of the text. Trailing spaces are ignored.<br><br>If you enter the remark before any **access-list** command, then the remark is the first line in the access list.<br><br>If you delete an access list using the **no access-list** *access_list_name* command, then all the remarks are also removed. |

### Example

You can add remarks before each ACE, and the remarks appear in the access list in these locations. Entering a dash (-) at the beginning of a remark helps set it apart from an ACE.

```
hostname(config)# access-list OUT remark - this is the inside admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT remark - this is the hr admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any
```

# Monitoring IPv6 Access Lists

To monitor IPv6 access lists, perform one of the following tasks:

| Command | Purpose |
|---|---|
| **show ipv6 access-list** | Displays all IPv6 access list information. |

# Configuration Examples for IPv6 Access Lists

The following example shows how to configure IPv6 access lists:

The following example allows any host using TCP to access the 3001:1::203:A0FF:FED6:162D server:

```
hostname(config)# ipv6 access-list acl_grp permit tcp any host 3001:1::203:A0FF:FED6:162D
```

The following example uses **eq** and a port to deny access to just FTP:

```
hostname(config)# ipv6 access-list acl_out deny tcp any host 3001:1::203:A0FF:FED6:162D eq
ftp
hostname(config)# access-group acl_out in interface inside
```

The following example uses **lt** to permit access to all ports less than port 2025, which permits access to the well-known ports (1 to 1024):

```
hostname(config)# ipv6 access-list acl_dmz1 permit tcp any host 3001:1::203:A0FF:FED6:162D
lt 1025
hostname(config)# access-group acl_dmz1 in interface dmz1
```

# Where to Go Next

Apply the access list to an interface. (See the "Configuring Access Rules" section on page 32-8 for more information.)

# Feature History for IPv6 Access Lists

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

*Table 17-2 Feature History for IPv6 Access Lists*

| Feature Name | Releases | Feature Information |
|---|---|---|
| IPv6 access lists | 7.0(1) | The following command was introduced: **ipv6 access-list**. |