CHAPTER 15

Adding a Standard Access List

This chapter describes how to configure a standard access list and includes the following sections:

Information About Standard Access Lists

Standard access lists identify the destination IP addresses of OSPF routes and can be used in a route map for OSPF redistribution. Standard access lists cannot be applied to interfaces to control traffic.

Licensing Requirements for Standard Access Lists

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 context mode only.

Firewall Mode Guidelines

Supported in routed and transparent firewall modes.

IPv6 Guidelines

Supports IPv6.

Additional Guidelines and Limitations

The following guidelines and limitations apply for standard Access Lists:

- Standard ACLs identify the destination IP addresses (not source addresses) of OSPF routes and can be used in a route map for OSPF redistribution. Standard ACLs cannot be applied to interfaces to control traffic.
- To add additional ACEs at the end of the access list, enter another **access-list** command, specifying the same access list name.
- When used with the **access-group** command, the **deny** keyword does not allow a packet to traverse the adaptive security appliance. By default, the adaptive security appliance denies all packets on the originating interface unless you specifically permit access.
- When specifying a source, local, or destination address, use the following guidelines:
  - Use a 32-bit quantity in four-part, dotted-decimal format.
  - Use the keyword **any** as an abbreviation for an address and mask of 0.0.0.0.0.0.0.0.
  - Use the **host** *ip_address* option as an abbreviation for a mask of 255.255.255.255.
- You can disable an ACE by specifying the keyword **inactive** in the **access-list** command.

Default Settings

Table 15-1 lists the default settings for standard Access List parameters.

Table 15-1 Default Standard Access List Parameters

Parameters	Default
deny	The adaptive security appliance denies all packets on the originating interface unless you specifically permit access. Access list logging generates system log message 106023 for denied packets. Deny packets must be present to log denied packets.

Adding Standard Access Lists

This section includes the following topics:

Task Flow for Configuring Extended 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. See in the "Adding Standard Access Lists" section on page 15-3.
- Apply the access list to an interface. See the "Configuring Access Rules" section on page 32-8 for more information.

Adding a Standard Access List

To add an access list to identify the destination IP addresses of OSPF routes, which can be used in a route map for OSPF redistribution, enter the following command:

Command	Purpose
`hostname(config)# access-list` *access_list_name* **standard** {**deny** | **permit**} {**any** | *ip_address mask*} **Example:** `hostname(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0`	Adds a standard access list entry. To add another ACE to the end of the access list, enter another **access-list** command, specifying the same access list name. The *access_list_name* argument specifies the name of number of an access list. The **any** keyword specifies access to anyone. The **deny** keyword denies access if the conditions are matched. The **host** *ip_address* syntax specifies access to a host IP address. The *ip_address ip_mask* argument specifies access to a specific IP address and subnet mask. The **line** *line-num* option specifies the line number at which to insert an ACE. The **permit** keyword permits access if the conditions are matched. To remove an ACE, enter the **no access-list** command with the entire command syntax string as it appears in the configuration.

Step 1

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* **Example:** `hostname(config)# access-list OUT remark - this is the inside admin address`	Adds a remark after the last **access-list** command you entered. 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. If you enter the remark before any **access-list** command, then the remark is the first line in the access list. 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 a remark before each ACE, and the remarks appear in the access lists in these location. Entering a dash (-) at the beginning of a remark helps to 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
```

What to Do Next

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

Monitoring Access Lists

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

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 Standard Access Lists

The following example shows how to deny IP traffic through the adaptive security appliance:

```
hostname(config)# access-list 77 standard deny
```

The following example shows how to permit IP traffic through the adaptive security appliance if conditions are matched:

```
hostname(config)# access-list 77 standard permit
```

The following example shows how to specify a destination address:

```
hostname(config)# access-list 77 standard permit host 10.1.10.123
```

Feature History for Standard Access Lists

Table 15-2 lists the release history for this feature.

Table 15-2 Feature History for Standard Access Lists

Feature Name	Releases	Feature Information
Standard access lists	7.0	Standard access listsidentify the destination IP addresses of OSPF routes, which can be used in a route map for OSPF redistribution. The feature and the following command were introduced: **access-list standard**.