Standard Access Control Lists

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

- Information About Standard ACLs, page 23-1
- Licensing Requirements for Standard ACLs, page 23-1
- Guidelines and Limitations, page 23-1
- Default Settings, page 23-2
- Adding Standard ACLs, page 23-3
- What to Do Next, page 23-4
- Monitoring ACLs, page 23-4
- Configuration Examples for Standard ACLs, page 23-4
- Feature History for Standard ACLs, page 23-5

Information About Standard ACLs

Standard ACLs identify the destination IP 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.

Licensing Requirements for Standard ACLs

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASAv</td>
<td>Standard or Premium License.</td>
</tr>
<tr>
<td>All other models</td>
<td>Base License.</td>
</tr>
</tbody>
</table>

Guidelines and Limitations

This section includes the guidelines and limitations for this feature:

- Context Mode Guidelines, page 23-2
• Firewall Mode Guidelines, page 23-2  
• IPv6 Guidelines, page 23-2  
• Additional Guidelines and Limitations, page 23-2

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 ACLs:
• 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 ACL, enter another access-list command, specifying the same ACL name.
• When used with the access-group command, the deny keyword does not allow a packet to traverse the ASA. By default, the ASA 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 23-1 lists the default settings for standard ACL parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default Standard ACL Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny</td>
<td>The ASA denies all packets on the originating interface unless you specifically permit access. ACL logging generates system log message 106023 for denied packets. Deny packets must be present to log denied packets.</td>
</tr>
</tbody>
</table>
Adding Standard ACLs

This section includes the following topics:

- Task Flow for Configuring Extended ACLs, page 23-3
- Adding a Standard ACL, page 23-3
- Adding Remarks to ACLs, page 23-4

Task Flow for Configuring Extended ACLs

Use the following guidelines to create and implement an ACL:

- Create an ACL by adding an ACE and applying an ACL name. See in the Adding Standard ACLs, page 23-3.
- Apply the ACL to an interface. See the firewall configuration guide for more information.

Adding a Standard ACL

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname(config)# access-list access_list_name standard (deny</td>
<td>permit) (any4</td>
</tr>
</tbody>
</table>

Example:

ciscoasa(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
Adding Remarks to ACLs

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>access-list access_list_name remark text</code></td>
<td>Adds a remark after the last <code>access-list</code> 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 <code>access-list</code> command, then the remark is the first line in the ACL. If you delete an ACL using the <code>no access-list access_list_name</code> command, then all the remarks are also removed.</td>
</tr>
</tbody>
</table>

Example:

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

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

What to Do Next

Apply the ACL to an interface. See the firewall configuration guide for more information.

Monitoring ACLs

To monitor ACLs, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show access-list</code></td>
<td>Displays the ACL entries by number.</td>
</tr>
<tr>
<td><code>show running-config access-list</code></td>
<td>Displays the current running access-list configuration.</td>
</tr>
</tbody>
</table>

Configuration Examples for Standard ACLs

The following example shows how to deny IP traffic through the ASA:

```plaintext
ciscoasa(config)# access-list 77 standard deny
```
The following example shows how to permit IP traffic through the ASA if conditions are matched:

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

The following example shows how to specify a destination address:

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

## Feature History for Standard ACLs

Table 23-2 lists the release history for this feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard ACLs</td>
<td>7.0(1)</td>
<td>Standard ACLs identify the destination IP addresses of OSPF routes, which can be used in a route map for OSPF redistribution. We introduced the feature and the following command: <code>access-list standard</code>.</td>
</tr>
</tbody>
</table>