



# CHAPTER 11

## Adding an Extended Access List

---

This chapter describes how to configure extended access lists (also known as access control lists), and it includes the following topics:

- [Information About Extended Access Lists, page 11-1](#)
- [Licensing Requirements for Extended Access Lists, page 11-2](#)
- [Guidelines and Limitations, page 11-2](#)
- [Default Settings, page 11-4](#)
- [Configuring Extended Access Lists, page 11-4](#)
- [What to Do Next, page 11-7](#)
- [Monitoring Extended Access Lists, page 11-7](#)
- [Configuration Examples for Extended Access Lists, page 11-7](#)
- [Feature History for Extended Access Lists, page 11-8](#)

## Information About Extended Access Lists

Access lists are used to control network access or to specify traffic for many features to act upon. An extended access list is made up of one or more access control entries (ACE) in which you can specify the line number to insert the ACE, the source and destination addresses, and, depending upon the ACE type, the protocol, the ports (for TCP or UDP), or the ICMP type (for ICMP). You can identify all of these parameters within the access-list command, or you can use object groups for each parameter. This section describes how to identify the parameters within the command. To simplify access lists with object groups, see [Chapter 16, “Configuring Object Groups.”](#)

For TCP and UDP connections for both routed and transparent mode, you do not need an access list to allow returning traffic because the security appliance allows all returning traffic for established bidirectional connections. For connectionless protocols such as ICMP, however, the security appliance establishes unidirectional sessions, so you either need access lists to allow ICMP in both directions (by applying access lists to the source and destination interfaces), or you need to enable the ICMP inspection engine. The ICMP inspection engine treats ICMP sessions as bidirectional connections.

You can apply only one access list of each type (extended and EtherType) to each direction of an interface. You can apply the same access lists on multiple interfaces.

## Allowing Broadcast and Multicast Traffic through the Transparent Firewall

In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access list, including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Transparent firewall mode can allow any IP traffic through. This feature is especially useful in multiple context mode, which does not allow dynamic routing, for example.

**Note**

Because these special types of traffic are connectionless, you need to apply an extended access list to both interfaces so that returning traffic is allowed through.

Table 11-1 lists common traffic types that you can allow through the transparent firewall.

**Table 11-1**      *Transparent Firewall Special Traffic*

Traffic Type	Protocol or Port	Notes
DHCP	UDP ports 67 and 68	If you enable the DHCP server, then the ASA does not pass DHCP packets.
EIGRP	Protocol 88	—
OSPF	Protocol 89	—
Multicast streams	The UDP ports vary depending on the application.	Multicast streams are always destined to a Class D address (224.0.0.0 to 239.x.x.x).
RIP (v1 or v2)	UDP port 520	—

## Licensing Requirements for Extended 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, page 11-2](#)
- [Firewall Mode Guidelines, page 11-2](#)
- [Additional Guidelines and Limitations, page 11-3](#)

**Context Mode Guidelines**

Supported in single and multiple context mode.

**Firewall Mode Guidelines**

Supported only in routed and transparent firewall modes.

### IPv6 Guidelines

IPv6 is supported.

### Additional Guidelines and Limitations

The following guidelines and limitations apply to creating an extended access list:

- When you enter the **access-list** command for a given access list name, the ACE is added to the end of the access list unless you specify the line number.
- Enter the access list name in uppercase letters so that the name is easy to see in the configuration. You might want to name the access list for the interface (for example, INSIDE), or you can name it for the purpose for which it is created (for example, NO\_NAT or VPN).
- Typically, you identify the **ip** keyword for the protocol, but other protocols are accepted. For a list of protocol names, see the [“Protocols and Applications” section on page C-11](#).
- Enter the **host** keyword before the IP address to specify a single address. In this case, do not enter a mask. Enter the **any** keyword instead of the address and mask to specify any address.
- You can specify the source and destination ports only for the **tcp** or **udp** protocols. For a list of permitted keywords and well-known port assignments, see the [“TCP and UDP Ports” section on page C-11](#). DNS, Discard, Echo, Ident, NTP, RPC, SUNRPC, and Talk each require one definition for TCP and one for UDP. TACACS+ requires one definition for port 49 on TCP.
- You can specify the ICMP type only for the **icmp** protocol. Because ICMP is a connectionless protocol, you either need access lists to allow ICMP in both directions (by applying access lists to the source and destination interfaces), or you need to enable the ICMP inspection engine. (See the [“Adding an ICMP Type Object Group” section on page 16-7](#).) The ICMP inspection engine treats ICMP sessions as stateful connections. To control ping, specify **echo-reply (0)** (ASA to host) or **echo (8)** (host to ASA). See the [“Adding an ICMP Type Object Group” section on page 16-7](#) for a list of ICMP types.
- When you specify a network mask, the method is different from the Cisco IOS software **access-list** command. The ASA uses a network mask (for example, 255.255.255.0 for a Class C mask). The Cisco IOS mask uses wildcard bits (for example, 0.0.0.255).
- To make an ACE inactive, use the **inactive** keyword. To reenab it, enter the entire ACE without the **inactive** keyword. This feature enables you to keep a record of an inactive ACE in your configuration to make reenabling easier.
- Use the **disable** option to disable logging for a specified ACE.

## Default Settings

Table 11-2 lists the default settings for extended access list parameters.

**Table 11-2**      *Default Extended Access List Parameters*

Parameters	Default
ACE logging	ACE logging generates system log message 106023 for denied packets. A deny ACE must be present to log denied packets.
log	When the <b>log</b> keyword is specified, the default level for system log message 106100 is 6 (informational), and the default interval is 300 seconds.

## Configuring Extended Access Lists

This section shows how to add and delete an access control entry and access list, and it includes the following topics:

- [Task Flow for Configuring Extended Access Lists, page 11-4](#)
- [Adding an Extended Access List, page 11-5](#)
- [Adding Remarks to Access Lists, page 11-6](#)
- [Deleting an Extended Access List Entry, page 11-6](#)

## 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 the [“Adding an Extended Access List” section on page 11-5](#).)
- Apply the access list to an interface. (See the [“Applying an Access List to an Interface” section on page 35-4](#) for more information.)

## Adding an Extended Access List

An access list is made up of one or more access control entries (ACEs) with the same access list ID. To create an access list you start by creating an ACE and applying a list name. An access list with one entry is still considered a list, although you can add multiple entries to the list.

To add an extended access list or an ACE, enter the following command:

Command	Purpose
<pre>access-list access_list_name [line line_number] [extended] {deny   permit} protocol source_address mask [operator port] dest_address mask [operator port   icmp_type] [inactive]</pre> <p><b>Example:</b></p> <pre>hostname(config)# access-list ACL_IN extended permit ip any any</pre>	<p>Adds an extended access control entry.</p> <p>The <b>line</b> <i>line_number</i> options specify the line number at which insert the ACE. If you do not specify a line number, the ACE is added to the end of the access list. The line number is not saved in the configuration; it only specifies where to insert the ACE.</p> <p>The <b>extended</b> option adds an ACE.</p> <p>The <b>deny</b> 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 <b>permit</b> keyword permits a packet if the conditions are matched.</p> <p>The protocol argument specifies the IP protocol name or number. For example UDP is 17, TCP is 6, and EGP is 47.</p> <p>The <i>source_address</i> specifies the IP address of the network or host from which the packet is being sent. Enter the <b>host</b> keyword before the IP address to specify a single address. In this case, do not enter a mask. Enter the <b>any</b> keyword instead of the address and mask to specify any address.</p> <p>The <i>operator port</i> option matches the port numbers used by the source or destination. The permitted operators are as follows:</p> <ul style="list-style-type: none"> <li>• <b>lt</b>—less than.</li> <li>• <b>gt</b>—greater than.</li> <li>• <b>dq</b>—equal to.</li> <li>• <b>neq</b>—not equal to.</li> <li>• <b>range</b>—an inclusive range of values. When you use this operator, specify two port numbers, for example: <b>range 100 200</b>.</li> </ul> <p>The <i>dest_address</i> argument specifies the IP address of the network or host to which the packet is being sent. Enter the <b>host</b> keyword before the IP address to specify a single address. In this case, do not enter a mask. Enter the <b>any</b> keyword instead of the address and mask to specify any address.</p> <p>The <i>icmp_type</i> argument specifies the ICMP type if the protocol is ICMP.</p> <p>The <b>inactive</b> keyword disables an ACE. To reenale it, enter the entire ACE without the <b>inactive</b> keyword. This feature enables you to keep a record of an inactive ACE in your configuration to make reenabling easier.</p> <p>(See the <b>access-list extended</b> command in the <i>Cisco Security Appliance Command Reference</i> for more information about command options.)</p>

## 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
<b>access-list</b> <i>access_list_name</i> <b>remark</b> <i>text</i>  <b>Example:</b> hostname(config)# <b>access-list</b> OUT remark - this is the inside admin address	<p>Adds a remark after the last access-list command you entered.</p> <p>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.</p> <p>If you enter the remark before any <b>access-list</b> command, then the remark is the first line in the access list.</p> <p>If you delete an access list using the <b>no access-list</b> <i>access_list_name</i> command, then all the remarks are also removed.</p>

### Example


You can add remarks before each ACE, and the remark appears in the access list in this location. Entering a dash (-) at the beginning of the remark helps set it apart from the ACEs.

```
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
```

## Deleting an Extended Access List Entry

This section shows how to remove an ACE. If the deleted entry is the only entry in the list, then the list and listname are deleted.

To delete an extended ACE, enter the following command:

Command	Purpose
hostname(config)# <b>no access-list</b> <i>access_list_name</i> [ <b>line</b> <i>line_number</i> ] [ <b>extended</b> ] { <b>deny</b>   <b>permit</b> } <i>protocol</i> <i>source_address mask</i> [ <i>operator port</i> ] <i>dest_address mask</i> [ <i>operator port</i>   <i>icmp_type</i> ] [ <b>inactive</b> ]	<p>Deletes and extended access list entry.</p> <p>Enter the <b>no access-list</b> command with the entire command syntax string as it appears in the configuration.</p>
<b>Example:</b> hostname(config)# <b>access-list</b> ACL_IN extended permit ip any any	<p> <b>Note</b> To remove the entire access list, use the <b>clear configure access-list</b> command.</p> <p>(See the “<a href="#">Adding an Extended Access List</a>” section on page 11-5 or the <i>Cisco Security Appliance Command Reference</i> for more information about command options.)</p>

## What to Do Next

Apply the access list to an interface. See the [“Applying an Access List to an Interface”](#) section on page 35-4 for more information.

## Monitoring Extended Access Lists

To monitor extended 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 Extended Access Lists

The following access list allows all hosts (on the interface to which you apply the access list) to go through the adaptive security appliance:

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

The following sample access list prevents hosts on 192.168.1.0/24 from accessing the 209.165.201.0/27 network. All other addresses are permitted.

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

If you want to restrict access to selected hosts only, then enter a limited permit ACE. By default, all other traffic is denied unless explicitly permitted.

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

The following access list restricts all hosts (on the interface to which you apply the access list) from accessing a website at address 209.165.201.29. All other traffic is allowed.

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

The following access list that uses object groups restricts several hosts on the inside network from accessing several web servers. All other traffic is allowed.

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

The following example temporarily disables an access list that permits traffic from one group of network objects (A) to another group of network objects (B):

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

To implement a time-based access list, use the **time-range** command to define specific times of the day and week. Then use the **access-list extended** command to bind the time range to an access list. The following example binds an access list named “Sales” to a time range named “New\_York\_Minute”:

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
```

## Feature History for Extended Access Lists

[Table 11-3](#) lists the release history for this feature.

**Table 11-3** Feature History for Extended Access Lists

Feature Name	Releases	Feature Information
Extended access control lists	7.0	Access lists are used to control network access or to specify traffic for many features to act upon. An extended access control list is made up of one or more access control entries (ACE) in which you can specify the line number to insert the ACE, the source and destination addresses, and, depending upon the ACE type, the protocol, the ports (for TCP or UDP), or the ICMP type (for ICMP).  The following command was introduced: <b>access-list extended</b> .