CHAPTER 15

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 sections:

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. You can identify all of these parameters within the **access-list** command, or you can use objects for each parameter.

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

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:

- 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 B-11.
- 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 B-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.
- 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).

Default Settings

Table 15-1 lists the default settings for extended access list parameters.

Table 15-1 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 **log** 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:

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.

Prerequisites

(Optional) Create an object or onject group according to the "Configuring Objects and Groups" section on page 13-1.

Guidelines

To delete an ACE, enter the **no access-list** command with the entire command syntax string as it appears in the configuration. To remove the entire access list, use the **clear configure access-list** command.

Detailed Steps

Command	Purpose
(For IP traffic, no ports) **access-list** *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {*protocol* | **object-group** *prot_grp_id*} {*source_address mask* | **object** *nw_obj_id* | **object-group** *nw_grp_id*} {*dest_address mask* | **object** *nw_obj_id* | **object-group** *nw_grp_id*} [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*] (For TCP or UDP traffic, with ports) **access-list** *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**tcp** | **udp** | **object-group** *prot_grp_id*} {*source_address mask* | **object** *nw_obj_id* | **object-group** *nw_grp_id*} [*operator port* | **object-group** *svc_grp_id*] {*dest_address mask* | **object** *nw_obj_id* | **object-group** *nw_grp_id*} [*operator port* | **object-group** *svc_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*] (For ICMP traffic) **access-list** *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} **icmp** {*source_address mask* | **object** *nw_obj_id* | **object-group** *nw_grp_id*} {*dest_address mask* | **object** *nw_obj_id* | **object-group** *nw_grp_id*} [*icmp_type* | **object-group** *icmp_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*] **Example:** `hostname(config)# access-list ACL_IN extended permit ip any any`	Adds an extended ACE. The **line** *line_number* option specifies 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. The **deny** keyword denies a packet if the conditions are matched. The **permit** keyword permits a packet if the conditions are matched. Instead of entering the protocol, IP address, or port directly in the command, you can use network objects, or protocol, network, port, or ICMP object groups using the **object** and **object-group** keyword. See "Configuring Objects and Groups" section on page 13-1 for more information about creating objects. The *protocol* argument specifies the IP protocol name or number. For example UDP is 17, TCP is 6, and EGP is 47. The *source_address* specifies the IP address of the network or host from which the packet is being sent. 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. For the TCP and UDP protocols only, the *operator port* option matches the port numbers used by the source or destination. The permitted operators are as follows: • **lt**—less than. • **gt**—greater than. • **eq**—equal to. • **neq**—not equal to. • **range**—an inclusive range of values. When you use this operator, specify two port numbers, for example: **range 100 200**. The *dest_address* argument specifies the IP address of the network or host to which the packet is being sent. 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. The *icmp_type* argument specifies the ICMP type if the protocol is ICMP. The **time-range** keyword specifies when an access list is activated. See the "Scheduling Extended Access List Activation" section on page 13-16 for more information. The **inactive** keyword disables an ACE. To reenable 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. For the **log** keyword, see Chapter 20, "Configuring Logging for Access Lists."

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 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
```

Monitoring Extended Access Lists

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

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 Extended Access Lists

This section includes the following topics:

Configuration Examples for Extended Access Lists (No Objects)

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

```
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
```

Configuration Examples for Extended Access Lists (Using Objects)

The following normal access list that does not use object groups restricts several hosts on the inside network from accessing several web servers. All other traffic is allowed.

```
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.16
eq www
```

```
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

If you make two network object groups, one for the inside hosts, and one for the web servers, then the configuration can be simplified and can be easily modified to add more hosts:

```
hostname(config)# object-group network denied
hostname(config-network)# network-object host 10.1.1.4
hostname(config-network)# network-object host 10.1.1.78
hostname(config-network)# network-object host 10.1.1.89

hostname(config-network)# object-group network web
hostname(config-network)# network-object host 209.165.201.29
hostname(config-network)# network-object host 209.165.201.16
hostname(config-network)# network-object host 209.165.201.78

hostname(config-network)# access-list ACL_IN extended deny tcp port 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
```

Where to Go Next

Apply the access list to an interface. See the "Configuring Access Rules" section on page 32-7 for more information.

Feature History for Extended Access Lists

Table 15-2 lists each feature change and the platform release in which it was implemented.

Table 15-2 Feature History for Extended Access Lists

Feature Name	Releases	Feature Information
Extended access lists	7.0(1)	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 IPCMP type (for ICMP). We introduced the following command: **access-list extended**.