CHAPTER 21

Using the ACL Manager

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

- Information About the ACL Manager, page 21-1
- Licensing Requirements for the ACL Manager, page 21-1
- Guidelines and Limitations, page 21-2
- Adding ACLs and ACEs, page 21-2
- Feature History for the ACL Manager, page 21-5

Information About the ACL Manager

Access control lists (ACLs) are used to control network access or to specify traffic for many features to act upon. An ACL is made up of one or more access control entries (ACEs) 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.

The ACL Manager dialog box lets you define ACLs to control the access of a specific host or network to another host/network, including the protocol or port that can be used.

You can configure ACLs (access control lists) to apply to user sessions. These are filters that permit or deny user access to specific networks, subnets, hosts, and web servers.

- If you do not define any filters, all connections are permitted.
- The ASA supports only an inbound ACL on an interface.

At the end of each ACL, there is an implicit, unwritten rule that denies all traffic that is not permitted. If traffic is not explicitly permitted by an access control entry (ACE), the ASA denies it. ACEs are referred to as rules in this section.

For information about adding ACLs and ACEs, see the "Adding ACLs and ACEs" section on page 21-2.

For information about finding specific ACLs and ACEs in your configuration, see the "Using the Find Function in the ACL Manager Pane" section on page 3-15.

Licensing Requirements for the ACL Manager

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 in routed and transparent firewall modes only.

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).
- 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 A-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.

Adding ACLs and ACEs

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

To add an ACL and then add an ACE to that ACL, perform the following steps:

Step 1 Choose **Configuration > Firewall > Advanced > ACL Manager**.

Step 2 Click **Add**, and choose one of the following options:

- **Add ACL**—Adds an ACL for IPv4 traffic
- **Add IPv6 ACL**—Adds an ACL for IPv6 traffic

Step 3 In the ACL name field, add a descriptive name for the ACL, and click **OK**.

Your newly created ACL appears in the window.

Step 4 Select the newly created ACL, click **Add**, and from the drop-down list, choose **Add ACE**.

Step 5 In the Action field of the Add ACE window, click one of the following radio buttons to choose the action

- **Permit**—Permits access if the conditions are matched.
- **Deny**—Denies access if the conditions are matched.

Step 6 In the Source field, enter an IP address that specifies the network object group, interface IP, or any address from which traffic is permitted or denied.

IPv6 must be enabled on at least one interface before you can configure an ACE with an IPv6 address. For more information about enabling IPv6 on an interface, see the "Configuring IPv6 Addressing" section on page 14-14.

Step 7 Select a destination to specify the IP addresses (host or network) that are permitted or denied to send traffic to the IP addresses listed in the Source section.

Step 8 Specify the service to which this ACE applies. You can type a known service into the window or click browse to select from a list of services.

Service groups let you identify multiple non-contiguous port numbers that you want to match.

For example, if you want to filter HTTP, FTP, and port numbers 5, 8, and 9, define a service group that includes all these ports.Without service groups, you would have to create a separate rule for each port

You can create service groups for TCP, UDP, TCP-UDP, ICMP, and other protocols. A service group with the TCP-UDP protocol contains services, ports, and ranges that might use either the TCP or UDP protocol.

- Protocol—Selects the protocol to which this rule applies. Possible values are ip, tcp, udp, icmp, and other. The remaining available fields in the Protocol and Service area depend upon the protocol you select. The next few bullets describe the consequences of each of these selections:
- Protocol: TCP and UDP—Selects the TCP/UDP protocol for the rule. The Source Port and Destination Port areas allow you to specify the ports that the ACL uses to match packets.
- Source Port/Destination Port—(*Available only for TCP and UDP protocols*) Specifies an operator and a port number, a range of ports, or a well-known service name from a list of services, such as HTTP or FTP. The operator list specifies how the ACL matches the port. Choose one of the following operators: = (equals the port number), not = (does not equal the port number), > (greater than the port number), < (less than the port number), range (equal to one of the port numbers in the range).
- Group—(*Available only for TCP and UDP protocols*) Selects a source port service group. The Browse (...) button opens the Browse Source Port or Browse Destination Port dialog box.
- Protocol: ICMP—Enables you to choose an ICMP type or ICMP group from a preconfigured list or browse (...) for an ICMP group. The Browse button opens the Browse ICMP dialog box.
- Protocol: IP—Specifies the IP protocol for the rule in the IP protocol box. No other fields are available when you make this selection.
- Protocol: Other—Enables you to choose a protocol from a drop-down list, choose a protocol group from a drop-down list, or browse for a protocol group. The Browse (...) button opens the Browse Other dialog box.

Step 9 (Optional) Add text that provides a brief description of this rule. A description line can be up to 100 characters long, yet you can break a description into multiple lines.

Note If you add remarks with non-English characters on one platform (such as Windows) then try to remove them from another platform (such as Linux), you might not be able to edit or delete them because the original characters might not be correctly recognized. This limitation is due to an underlying platform dependency that encodes different language characters in different ways.

Step 10 (Optional) Check the Enable Logging check box to enable or disable logging or specify the use of the default logging settings. If logging is enabled, the Syslog Level and Log Interval fields become available.

a. If logging is enables, choose a logging level to specify logging activity. The default is Informational. For information about logging levels, see the "Severity Levels" section on page 76-3.

b. Choose a logging interval to display the interval, in seconds, that is used to limit how many messages at this logging level can be sent.

Step 11 Set the source service (TCP, UDP, and TCP/UDP only).

Step 12 Set the logging interval to establish the number of seconds between log messages. The default is 300.

Step 13 Set the time range during which the rule is applied.

Step 14 Click **Apply** to save the ACL and ACE to the running configuration.

To see a condensed view of all ACLs in your configuration, click **Collapse All** below the ACL Manager window. To see a comprehensive view of all ACLs and ACEs in your configuration, click **Expand All**.

For information about finding specific ACLs and ACEs in your configuration, see the "Using the Find Function in the ACL Manager Pane" section on page 3-15.

Using Standard ACLs in the ACL Manager

Standard ACLs identify the destination IP addresses (not source addresses). Standard ACLs cannot be applied to interfaces to control traffic.

To add a standard ACL to your configuration, perform the following steps:

Step 1 Click **Add**, and from the drop-down list, choose **Add ACL**.

Step 2 In the Add ACL dialog box, add a name or number (without spaces) to identify the ACL.

Step 3 Click **OK**

The ACL name appears in the main pane.

Step 4 Select the newly created ACL, click **Add**, and from the drop-down list, choose **Add ACE**.

The Add ACE dialog box appears.

Step 5 (Optional) To specify the placement of the new ACE, select an existing ACE, and click Insert... to add the ACE before the selected ACE, or click Insert After... to add the ACE after the selected ACE.

Step 6 Click one of the following radio buttons to choose an action:

- **Permit**—Permits access if the conditions are matched.
- **Deny**—Denies access if the conditions are matched.

Step 7 In the Address field, enter the IP address of the destination to which you want to perform or deny access.

You can also browse for the address of a network object by clicking the ellipsis at the end of the Address field.

Step 8 (Optional) In the Description field, enter a description that makes an ACE easier to understand.

The description can contain multiple lines; however, each line can be no more than 100 characters in length.

Note If you add remarks with non-English characters on one platform (such as Windows) then try to remove them from another platform (such as Linux), you might not be able to edit or delete them because the original characters might not be correctly recognized. This limitation is due to an underlying platform dependency that encodes different language characters in different ways.

Step 9 Click **OK**.

The newly created ACE appears under the ACL.

Step 10 Click **Apply** to save the ACE to your configuration.

Feature History for the ACL Manager

Table 21-1 lists each feature change and the platform release in which it was implemented.

Table 21-1 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 (ACEs) 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).