



# CHAPTER 21

## Configuring Access Rules and ACLs

---

Cisco security appliances provide basic traffic filtering capabilities with access rules and access control lists (ACLs), which control access in your network by preventing certain traffic from entering or exiting.



**Note**

---

ASA documentation uses the terms “ACE” for access rule and “access list” for ACL.

---

This chapter describes how to add access rules to create ACLs, and it shows how to use ASDM to add them to your network configuration to control traffic.

- [Information About Access Rules and ACLs, page 21-1](#)
- [Configuring Access Rules and ACLs, page 21-8](#)

## Information About Access Rules and ACLs

This section describes access rules and ACLs, and it includes the following topics:

- [About Access Rules and ACLs, page 21-1](#)
- [About EtherType ACLs, page 21-3](#)
- [Allowing MPLS, page 21-4](#)
- [Using Access Rules, page 21-4](#)
- [Inbound and Outbound Access Rules and ACLs, page 21-4](#)
- [IP Addresses Used for Access Rules When You Use NAT, page 21-5](#)
- [Access Rules for Returning Traffic, page 21-7](#)
- [Allowing Broadcast and Multicast Traffic through the Transparent Firewall Using Access Rules, page 21-7](#)

## About Access Rules and ACLs

Access rules are used in a variety of features and can be configured for all routed and network protocols (IP, AppleTalk, and so on) to filter the packets of those protocols. Your access policy is made up of one or more access rules per interface. An access rule is a single entry in an ACL that specifies a permit or deny rule (to forward or drop the packet) and is applied to a protocol, to a source and destination IP address or network, and, optionally, to the source and destination ports.

You can configure the following types of access rules and ACLs:

- **Standard Access Rules**—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 configure standard access rules, see the [“Configuring Standard ACLs” section on page 21-8](#).
- **Extended Access Rules**—An extended ACL is made up of one or more access rules in which you can specify the line number to insert the access rule, both the source and destination addresses, and, depending upon the access rule type, the protocol, the ports (for TCP or UDP), or the ICMP type (for ICMP). You can identify all of these parameters by creating an ACL, or you can use object groups and service groups for each parameter. (For more information about network objects and service groups, see the [“Using Network Objects and Groups” section on page 20-1](#) and the [“Configuring Service Groups” section on page 20-5](#). To configure extended access rules, see the [“Configuring Extended ACLs” section on page 21-10](#).
- **Webtype Access Rules**—Webtype access rules are added to a configuration that supports filtering for clientless SSL VPN. To configure webtype access rules, see the [“Configuring Webtype ACLs” section on page 21-14](#).
- **EtherType Access Rules**—For transparent mode only, EtherType access rules are based on packet EtherTypes. EtherType rules are used to configure non-IP related traffic policies through the security appliance when operating in transparent mode. In transparent mode, you can apply both extended and EtherType access rules to an interface. EtherType rules take precedence over the extended access rules. See [“Configuring EtherType ACLs” section on page 21-19](#) for more information.
- **IPv6 Access Rules**—ACL functionality in IPv6 is similar to typical ACLs in IPv4. Extended ACLs, Webtype ACLs, and EtherType ACLs allow you to define IPv6 access lists and set their deny and permit conditions using the IPv6 address of the desired interface. IPv6 does not support standard ACLs.

To access the security appliance interface for management access, you do not need an access rule allowing the host IP address. You only need to configure management access according to [Chapter 18, “Configuring Management Access.”](#)

You can use access rules in routed and transparent firewall mode to control IP traffic. In transparent mode you can use both extended access rules (for Layer 3 traffic) and EtherType rules (for Layer 2 traffic).

**Note**

---

To allow any traffic to enter the security appliance, you must attach an inbound access rule to an interface; otherwise, the security appliance automatically drops all traffic that enters that interface.

---

## About EtherType ACLs

This section includes the following topics:

- [Implicit Deny in Ethertype Rules, page 21-3](#)
- [Supported EtherTypes, page 21-3](#)
- [Implicit Permit of IP and ARPs Only, page 21-3](#)

### Implicit Deny in Ethertype Rules

Lists of EtherType rules have an implicit deny at the end of the list, so unless you explicitly permit it, traffic cannot pass. For example, if you want to allow all users to access a network through the security appliance except for particular addresses, then you need to deny the particular addresses and then permit all others.

For EtherType rules, the implicit deny does not affect IPv4 traffic or ARPs; for example, if you allow EtherType 8037 (the EtherType for IPX), the implicit deny at the end of the list does not block any IP traffic that you previously allowed with an access rule (or implicitly allowed from a high security interface to a low security interface). However, if you explicitly deny all traffic with an EtherType rule, then IP and ARP traffic is denied.

### Supported EtherTypes

An EtherType rule controls any EtherType identified by a 16-bit hexadecimal number.

EtherType rules support Ethernet V2 frames.

802.3-formatted frames are not handled by the rule because they use a length field as opposed to a type field.

BPDUs, which are allowed by default, are the only exception: they are SNAP-encapsulated, and the security appliance is designed to specifically handle BPDUs.

The security appliance receives trunk port (Cisco proprietary) BPDUs. Trunk BPDUs have VLAN information inside the payload, so the security appliance modifies the payload with the outgoing VLAN if you allow BPDUs.

**Note**

---

If you use failover, you must allow BPDUs on both interfaces with an EtherType rule to avoid bridging loops.

---

### Implicit Permit of IP and ARPs Only

IPv4 traffic is allowed through the transparent firewall automatically, without a rule, if it arrives from a higher security interface to a lower security interface. ARPs are allowed through the transparent firewall in both directions without a rule. ARP traffic can be controlled by ARP inspection.

However, to allow any traffic with EtherTypes other than IPv4 and ARP, you need to apply an EtherType access list, even from a high security to a low security interface.

Because EtherTypes are connectionless, you need to apply the rule to both interfaces if you want traffic to pass in both directions.

## Allowing MPLS

If you allow MPLS, ensure that Label Distribution Protocol and Tag Distribution Protocol TCP connections are established through the security appliance by configuring both MPLS routers connected to the security appliance to use the IP address on the security appliance interface as the router ID for LDP or TDP sessions. (LDP and TDP allow MPLS routers to negotiate the labels (addresses) used to forward packets.)

## Using Access Rules

The following general information applies to using access rules:

- Same interface—You can apply access rules to each direction of an interface.
- Rule order—The order of rules is important. When the security appliance decides whether to forward or drop a packet, the security appliance tests the packet against each rule in the order in which the rules are listed. After a match is found, no more rules are checked. For example, if you create an access rule at the beginning of the list, and that rule explicitly permits all traffic for an interface, no further rules are ever checked.
- Disabling—You can disable a rule by making it inactive.
- Implicit deny—An ACL has an implicit deny at the end of the list, so unless you explicitly permit it, traffic cannot pass. For example, if you want to allow all users to access a network through the security appliance except for particular addresses, then you need to deny the particular addresses and then permit all others.

## Inbound and Outbound Access Rules and ACLs

By default, all traffic from a higher-security interface to a lower-security interface is allowed. ACLs either let you allow traffic from lower-security interfaces or restrict traffic from higher-security interfaces.

The security appliance supports two types of ACLs:

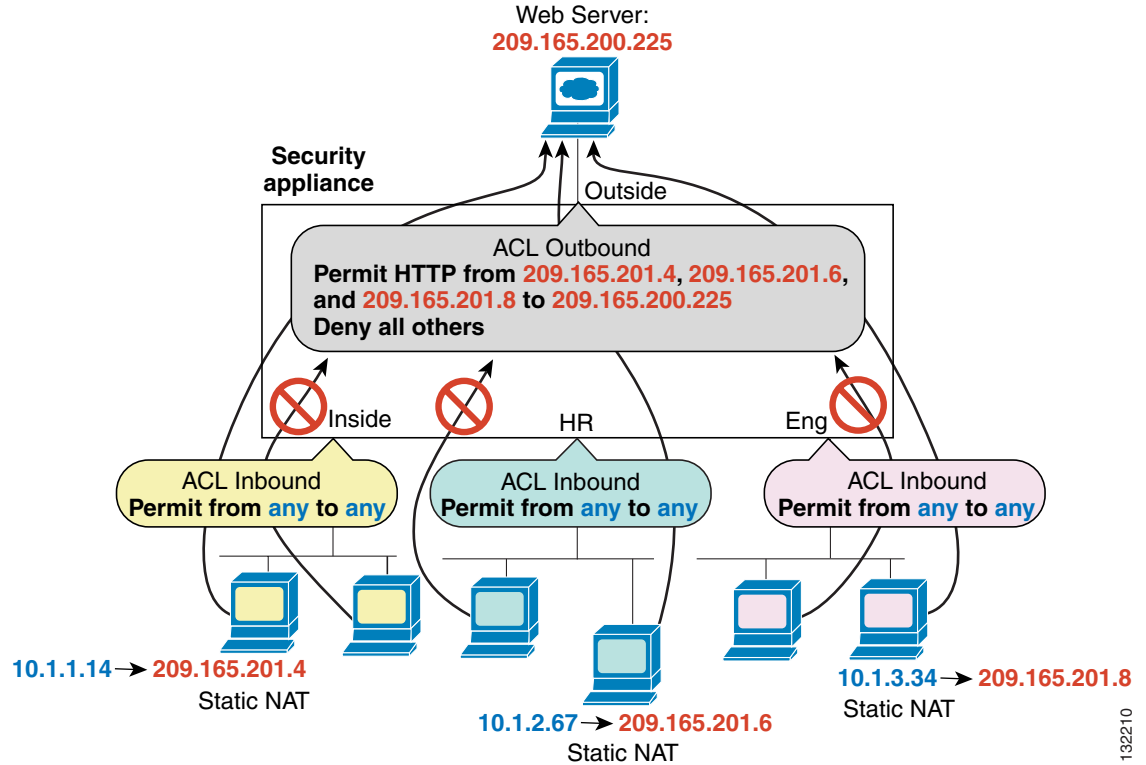
- Inbound—Inbound ACLs apply to traffic as it enters an interface.
- Outbound—Outbound ACLs apply to traffic as it exits an interface.

**Note**

The terms “inbound” and “outbound” refer to the application of an ACL on an interface, either to traffic entering the security appliance on an interface or traffic exiting the security appliance on an interface. These terms do not refer to the movement of traffic from a lower security interface to a higher security interface, commonly known as inbound, or from a higher to lower interface, commonly known as outbound.

An outbound ACL is useful, for example, if you want to allow only certain hosts on the inside networks to access a web server on the outside network. Rather than creating multiple inbound ACLs to restrict access, you can create a single outbound ACL that allows only the specified hosts. (See [Figure 21-1](#).) The outbound ACL prevents any other hosts from reaching the outside network.

Figure 21-1 Outbound ACLs



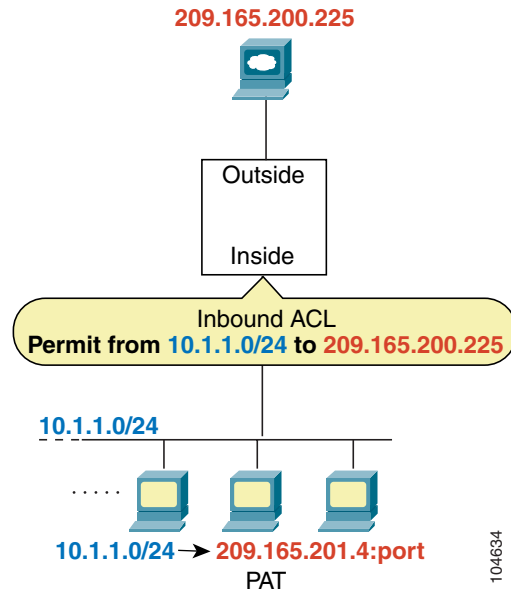
132210

## IP Addresses Used for Access Rules When You Use NAT

When you use NAT, the IP addresses you specify for an access rule depend on the interface to which the access rule is attached; you need to use addresses that are valid on the network that is connected to the interface. This guideline applies for both inbound and outbound access rules: the direction does not determine the address used, only the interface does.

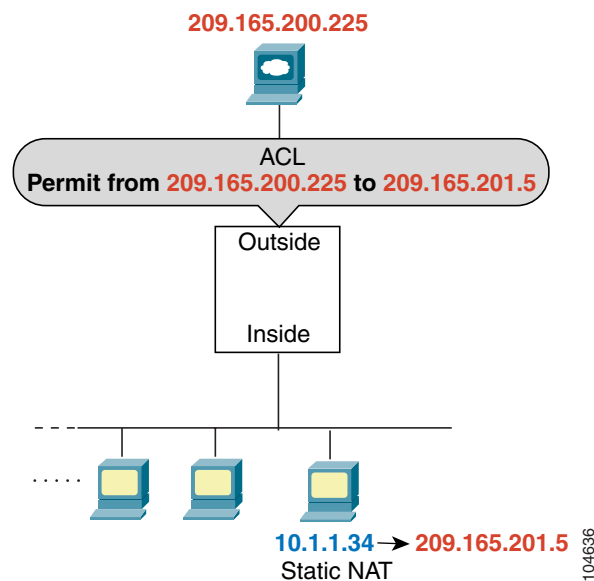
For example, if you want to apply an access rule to the inbound direction of the inside interface, you configure the security appliance to perform NAT on the inside source addresses when they access outside addresses. Because the access rule is applied to the inside interface, the source addresses are the original untranslated addresses. Because the outside addresses are not translated, the destination address used in the access rule is the real address. (See [Figure 21-2](#).)

**Figure 21-2** IP Addresses in ACLs: NAT Used for Source Addresses



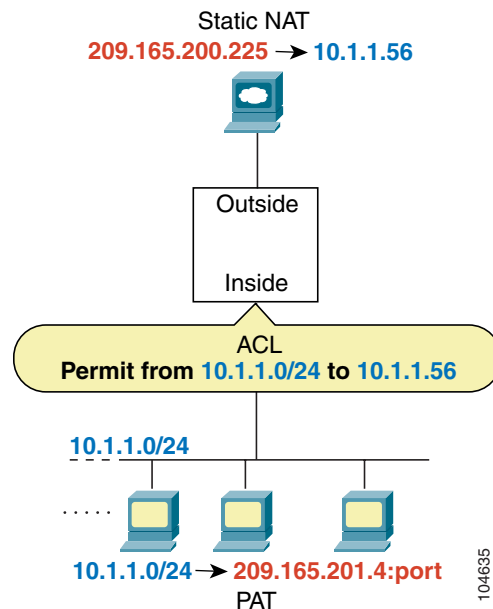
If you want to allow an outside host to access an inside host, you can apply an inbound access rule on the outside interface. You need to specify the translated address of the inside host in the access rule because that address is the address that can be used on the outside network. (See [Figure 21-3](#).)

**Figure 21-3** IP Addresses in ACLs: NAT Used for Destination Addresses.



If you perform NAT on both interfaces, keep in mind the addresses that are visible to a given interface. In Figure 9-4, an outside server uses static NAT so that a translated address appears on the inside network.

**Figure 21-4** IP Addressed in ACLs: NAT Used for Source and Destination Addresses



## Access Rules for Returning Traffic

For TCP and UDP connections for both routed and transparent mode, you do not need an ACL 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 ACLs to allow ICMP in both directions (by applying access rules 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. For more information about allowing ICMP in ACLs, see the [“Adding an Access Rule to Manage a Service Group”](#) section on [page 21-21](#).)

## Allowing Broadcast and Multicast Traffic through the Transparent Firewall Using Access Rules

In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access rule, 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.



### Note

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

Table 21-1 lists common traffic types that you can allow through the transparent firewall.

**Table 21-1** Transparent Firewall Special Traffic

Traffic Type	Protocol or Port	Notes
DHCP	UDP ports 67 and 68	If you enable the DHCP server, then the security appliance 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	—

## Configuring Access Rules and ACLs

The Access Rules pane shows your entire network security policy expressed in rules.

When you choose the Access Rules option, this pane lets you define access rules to control the access of a specific host or network to another host/network, including the protocol or port that can be used.

For more information about access rules, see the [“Information About Access Rules and ACLs” section on page 21-1](#).

This section includes the following topics:

- [Configuring Standard ACLs, page 21-8](#)
- [Configuring Extended ACLs, page 21-10](#)
- [Configuring Webtype ACLs, page 21-14](#)
- [Configuring EtherType ACLs, page 21-19](#)
- [Adding an Access Rule to Manage a Service Group, page 21-21](#)
- [ASDM Field Definitions for Using Access Rules, page 21-23](#)

## Configuring 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. You must first create an ACL and then add an ACE to that ACL.



### Note

IPv6 does not support standard ACLs.

This section includes the following topics:

- [Adding a Standard ACL, page 21-9](#)
- [Adding an ACE to a Standard ACL, page 21-9](#)

## Adding a Standard ACL

To add a standard ACL to your configuration and then add an ACE to the ACL, perform the following steps:

- 
- Step 1** Choose **Configuration > Firewall > Advanced > Standard ACL**.
- Step 2** Click **Add**, and from the drop-down list, choose **Add ACL**.
- Step 3** In the Add ACL dialog box, add a name or number (without spaces) to identify the ACL.
- Step 4** Click **OK**.  
The ACL name appears in the main pane.  
You may add additional ACLs.
- Step 5** Click **Apply** to save the ACLs to your configuration.  
You can now add one or more ACEs to the newly created ACL.  
To add an ACE, see the [“Adding an ACE to a Standard ACL” section on page 21-9](#).
- 

## Adding an ACE to a Standard ACL

Before you can add an ACE to a configuration, you must first add an ACL. For information about adding a standard ACL, see the [“Adding a Standard ACL” section on page 21-9](#). For information about editing ACEs, see the [“Editing an ACE in a Standard ACL” section on page 21-10](#).

To add an ACE to an ACL that exists in your configuration, perform the following steps:

- 
- Step 1** Choose **Configuration > Firewall > Advanced > Standard ACL**.
- Step 2** In the main pane, select the ACL for which you want to add an ACE.
- Step 3** Click **Add**, and choose **Add ACE** from the drop-down list.  
The Add ACE dialog box appears.
- Step 4** (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 5** 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 6** In the Address field, enter the IP address of the destination to which you want to permit 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 7** (Optional) In the Description field, enter a description that makes the ACE easier to understand.  
The description can contain multiple lines; however, each line can be no more than 100 characters in length.
- Step 8** Click **OK**.  
The newly created ACE appears under the ACL.

**Step 9** Click **Apply** to save the ACE to your configuration.

---

## Editing an ACE in a Standard ACL

To edit an ACE in a standard ACL, perform the following steps:

---

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

**Step 2** In the main pane, select the ACE that you want to edit.

**Step 3** Click **Edit**,

The Edit ACE dialog box appears.

**Step 4** Enter the desired changes.

**Step 5** Click **OK**.

---

## Configuring Extended ACLs

Extended ACLs have the ability to filter packets based on source and destination IP addresses. An extended ACL is made up of one or more access rules in which you can specify the line number to insert the access rule, both the source and destination addresses, and, depending upon the access rule type, the protocol, the ports (for TCP or UDP), or the ICMP type (for ICMP). You can identify all of these parameters by creating an ACL, or you can use object groups and service groups for each parameter. (For more information about network objects and service groups, see the [“Using Network Objects and Groups”](#) section on page 20-1 and the [“Configuring Service Groups”](#) section on page 20-5.)

This section includes the following topics:

- [Configuring Extended ACLs for Management Traffic, page 21-10](#)
- [Configuring Extended Access Rules for Network Traffic, page 21-12](#)
- [Editing Extended ACLs for Management Traffic, page 21-12](#)
- [Editing Extended Access Rules for Network Traffic, page 21-13](#)
- [Deleting an Extended ACEs, page 21-14](#)

## Configuring Extended ACLs for Management Traffic

You can configure an interface ACL that supports access control for to-the-box management traffic from a specific peer (or set of peers) to the security appliance. One scenario in which this type of ACL would be useful is when you want to block IKE Denial of Service attacks. (To edit extended ACLs for management traffic, see the [“Editing Extended ACLs for Management Traffic”](#) section on page 21-12.)

To configure an extended ACL that permits or denies packets for to-the-box traffic, perform the following steps:

---

**Step 1** Choose **Configuration > Device Management > Management Access > Management Access Rules**.

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

- **Add Management Access Rule**
- **Add IPv6 Management Access Rule**

The appropriate access rule dialog box appears.

**Step 3** From the Interface drop-down list, choose the interface on which to apply the rule.  
The management interface is for management only and cannot be used to configure an access rule.

**Step 4** In the Action field, 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 5** 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.



---

**Note** IPv6 must be enabled on at least one interface before you can configure an extended ACL with an IPv6 address. For more information about enabling IPv6 on an interface, see [Chapter 9, “Configuring Interfaces.”](#)

---

**Step 6** Select the service type.

For more information about service types, see the [“Adding an Access Rule to Manage a Service Group” section on page 21-21.](#)

**Step 7** (Optional) In the Description field, add a text description about the ACL.

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

**Step 8** (Optional) Logging is enabled by default. You can disable logging by unchecking the check box, or you can change the logging level from the drop-down list. The default logging level is Informational.

For more information about logging options, see the [“Log Options” section on page 21-29.](#)

**Step 9** (Optional) To add a source service (TCP, UDP, and TCP-UDP only) and a time range to your access rule that specifies when traffic can be allowed or denied, click **More Options** to expand the list.

- In the Source Service field, click the browse button.
- In the Browse Source Services window, choose the service to apply to the access rule, and click **Source Service**.

The selected service appears in the Source Service field.

- Click **OK**.

**Step 10** (Optional) To add a time range, perform the following steps under More Options.

- To the right of the Time Range field, click the browse button.

The Browse Time Range dialog box appears.

- Click **Add**.

The Add Time Range dialog box appears.

- In the Time Range Name field, enter a time range name, with no spaces.

- Choose the Start Time and the End Time.

- To specify additional time constraints for the time range, such as specifying the days of the week or the recurring weekly interval in which the time range will be active, click **Add**, and choose the specifications.

f. Click **OK** through all windows to apply the optional time range specifications.

**Step 11** Click **Apply** to save the ACL to your configuration.



**Note**

After you add access rules, you can click the following radio buttons to filter which access rules appear in the main window: IPv4 and IPv6, IPv4 Only, or IPv6 Only.

## Editing Extended ACLs for Management Traffic

To edit an extended ACL for management traffic, perform the following steps:

- 
- Step 1** Choose **Configuration > Device Management > Management Access > Management Access Rules**.
- Step 2** Click **Edit**.  
The Edit Management Access Rule dialog box appears.
- Step 3** Enter the desired changes.  
For information about fields in the ACL, see the [“Configuring Extended ACLs for Management Traffic” section on page 21-10](#) or the [“ASDM Field Definitions for Using Access Rules” section on page 21-23](#).
- Step 4** Click **OK**.
- Step 5** Click **Apply** to save the changes to your configuration.
- 

## Configuring Extended Access Rules for Network Traffic

Extended access rules can also control access through-the box, filtering from hosts through the security appliance and to the outside network. This section shows how to add an extended access rule. To edit an extended ACL for network traffic, see the [“Editing Extended Access Rules for Network Traffic” section on page 21-13](#).

To configure an extended access rule for network traffic, perform the following steps:

- 
- Step 1** Choose **Configuration > Firewall > Access Rules**.
- Step 2** Click **Add**, and choose one of the following options:
- **Add Access Rule**
  - **Add IPv6 Access Rule**
- The appropriate access rule dialog box appears.
- Step 3** From the Interface drop-down list, choose the interface on which to apply the rule.  
The management interface is for management only and cannot be used to configure an access rule.
- Step 4** In the Action field, click one of the following radio buttons next to the desired action:
- **Permit**—Permits access if the conditions are matched.
  - **Deny**—Denies access if the conditions are matched.

- Step 5** 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 to the specified destination.
- For more information about enabling IPv6 on an interface, see [Chapter 9, “Configuring Interfaces.”](#)
- Step 6** In the Destination field, enter an IP address that specifies the network object group, interface IP, or any address to which traffic is permitted or denied from the source specified in the Source field.
- Step 7** Select the service type.
- For more information about service types, see the [“Adding an Access Rule to Manage a Service Group” section on page 21-21.](#)
- Step 8** (Optional) To add a time range to your access rule that specifies when traffic can be allowed or denied, click **More Options** to expand the list.
- To the right of the Time Range drop down list, click the browse button.  
The Browse Time Range dialog box appears.
  - Click **Add**.  
The Add Time Range dialog box appears.
  - In the Time Range Name field, enter a time range name, with no spaces.
  - Choose the Start Time and the End Time.
  - To specify additional time constraints for the time range, such as specifying the days of the week or the recurring weekly interval in which the time range will be active, click **Add**, and choose the specifications.
  - Click **OK** to apply the optional time range specifications.
- Step 9** (Optional) In the Description field, add a text description about the ACL.
- The description can contain multiple lines; however, each line can be no more than 100 characters in length.
- Step 10** (Optional) Logging is enabled by default. You can disable logging by unchecking the check box, or you can change the logging level from the drop-down list. The default logging level is Informational.
- For more information about logging options, see the [“Log Options” section on page 21-29.](#)
- Step 11** Click **OK**. The ACL appears with the newly configured access rules.
- Step 12** Click **Apply** to save the ACL to your configuration.

**Note**

After you add access rules, you can click the following radio buttons to filter which access rules appear in the main pane: IPv4 and IPv6, IPv4 Only, or IPv6 Only.

## Editing Extended Access Rules for Network Traffic

To edit an extended access rule for network traffic, perform the following steps:

- Step 1** Choose **Configuration > Firewall > Access Rules**.
- Step 2** Choose the Access Rule Type to edit by clicking one of the following radio button:
- IPv4 and IPv6**—Shows access rules that have both IPv4 and IPv6 type addresses.

- **IPv4 Only**—Shows access rules that have IPv4 type addresses only.
- **IPv6 Only**—Shows access rules that have IPv6 type addresses only.

The main Access Rule pane displays the available interfaces for the chosen rule type.

**Step 3** Select the ACE to edit.

**Step 4** Click **Edit**.

The Edit Access Rule dialog box appears.

**Step 5** Enter changes to the current configuration.

**Step 6** Click **OK**.

The main Access Rules pane displays the updated access rules.

**Step 7** Click **Apply** to save the changes to your configuration.

---

## Deleting an Extended ACEs

To delete an extended ACE, perform the following steps:

---

**Step 1** Choose **Configuration > Firewall > Access Rules**.

**Step 2** Choose the Access Rule Type to edit by clicking one of the following radio buttons:

- **IPv4 and IPv6**—Shows access rules that have both IPv4 and IPv6 type addresses.
- **IPv4 Only**—Shows access rules that have IPv4 type addresses only.
- **IPv6 Only**—Shows access rules that have IPv6 type addresses only.

**Step 3** Select the existing ACE to delete.

**Step 4** Click **Delete**.

The main Access Rules pane displays without the selected ACE.

**Step 5** Click **Apply** to save the configuration.

---

## Configuring Webtype ACLs

Webtype ACLs are added to a configuration that supports filtering for clientless SSL VPN. The ACL permits or denies access to specific networks, subnets, hosts, and web servers. Each ACE specifies one rule that serves the function of the ACL. If you do not configure any filters, all connections are permitted.

This section includes the following topics:

- [Adding a Webtype ACL and ACE, page 21-15](#)
- [Examples, page 21-16](#)
- [Editing Webtype ACLs and ACEs, page 21-18](#)

## Adding a Webtype ACL and ACE

You must first create the webtype ACL and then add an ACE to the ACL.



### Note

Smart tunnel ACEs filter only on a per-server basis. Thus, you cannot create smart tunnel ACEs to do the following:

- Permit or deny access to directories.
- Permit or deny access to specific smart tunnel-enabled applications.

To configure a webtype access rule, perform the following steps:

- 
- Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs**.
- Step 2** Click **Add**, and choose one of the following ACL types to add:
- **Add ACL**
  - **Add IPv6 ACL**
- The Add ACL dialog box appears.
- Step 3** Enter a name for the ACL (with no spaces), and click **OK**.
- Step 4** To add an entry to the list that you just created, click **Add**, and choose **Add ACE** from the drop-down list.
- Step 5** In the Action field, click the radio button next to the desired action:
- Permit—Permits access if the conditions are matched.
  - Deny—Denies access if the conditions are matched.



### Note

The end of every ACL has an implicit deny rule.

- Step 6** In the Filter field, you can either filter on a URL or filter on an address and Service.
- a. To filter on a URL, choose the URL prefix from the drop-down list, and enter the URL.
- Wild card characters can be used in the URL field:
- An asterisk \* matches none or any number of characters.
  - A question mark (?) matches any one character exactly.
  - Square brackets [] are range operators, matching any character in the range. For example, to match both `http://www.cisco.com:80/` and `http://www.cisco.com:81/`, enter the following:  
`http://www.cisco.com:8[01]/`
- b. To filter on an address and service, click the **Filter address and service** radio button, and enter the appropriate values.
- Wildcard characters can be used in the with regular expression in the address field:
- An asterisk \* matches none or any number of characters.
  - A question mark ? matches any one character exactly.
  - Square brackets [] are range operators, matching any character in the range. For example to permit a range of IP addresses from 10.2.2.20 through 10.2.2.31, enter the following:  
`10.2.2.[20-31]`

You can also browse for the address and service by clicking the browse buttons at the end of the fields.

**Step 7** (Optional) Logging is enabled by default. You can disable logging by unchecking the check box, or you can change the logging level from the drop-down list. The default logging level is Informational.

For more information about logging options, see the “Log Options” section on page 21-29.

**Step 8** (Optional) If you changed the logging level from the default setting, you can specify the logging interval by clicking **More Options** to expand the list.

Valid values are from 1 through 6000 seconds. The default is 300 seconds.

**Step 9** (Optional) To add a time range to your access rule that specifies when traffic can be allowed or denied, click **More Options** to expand the list.

a. To the right of the Time Range drop-down list, click the browse button.

The Browse Time Range dialog box appears.

b. Click **Add**.

The Add Time Range dialog box appears.

c. In the Time Range Name field, enter a time range name, with no spaces.

d. Enter the Start Time and the End Time.

e. To specify additional time constraints for the time range, such as specifying the days of the week or the recurring weekly interval in which the time range will be active, click **Add**, and specify the desired values.

**Step 10** Click **OK** to apply the optional time range specifications.

**Step 11** Click **Apply** to save the configuration.



**Note**

After you add access rules, you can click the following radio buttons to filter which access rules appear in the main pane: IPv4 and IPv6, IPv4 Only, or IPv6 Only.

**Examples**

See the following example ACEs:

- [Example Smart Tunnel ACEs](#)
- [Example Port Forwarding TCP-based ACLs](#)
- [Example Plug-in ACEs](#)
- [Example HTTP and HTTPS ACEs](#)
- [Example CIFS Shares ACEs](#)

**Table 21-2** Example Smart Tunnel ACEs

Function	Action	Filter on URL Values	
		drop-down	:// text box
Permit a basic URL.	Permit	any	http://www.example.com

**Table 21-2** Example Smart Tunnel ACEs

Function	Action	Filter on URL Values	
		drop-down	::/ text box
Permit smart tunnel access to a basic URL.	Permit	any	http://www.example.com
<b>Note:</b> To configure smart tunnel access, add both ACE types, then choose Clientless SSL VPN Access > Portal > Bookmarks, specify the URL in a bookmark entry, and check Enable Smart Tunnel in the Add Bookmark dialog box.	Permit	any	smart-tunnel://www.example.com
Permit smart tunnel access to a basic URL, but deny smart tunnel access to another.	Permit	any	http://www.example.com
	Permit	any	smart-tunnel://www.example.com
	Deny	any	smart-tunnel://images.example.com
Permit smart tunnel access to all URLs ending with ".example.com"	Permit	any	http://*.example.com
	Permit	any	smart-tunnel://*.example.com

**Table 21-3** Example Port Forwarding TCP-based ACLs

Function	Action	Filter on Address and Service Values	
		Address	Service
Permit port forwarding.	Permit	192.168.20.92	2224
Block ports 80 to 90.	Deny	192.168.20.92	80-90
Block all ports.	Deny	192.168.20.92	tcp
Implicitly deny all traffic except that destined to the address specified.	Permit	10.86.192.1	tcp
Specify the default TCP port (3389).	Permit	10.86.192.193	3389

**Note**

Protocols such as RDP, SSH, and VNC are available only if the respective plug-in is imported on the security appliance.

**Table 21-4** Example Plug-in ACEs

Function	Action	Filter on URL Values		Filter on Address and Service Values	
		drop-down	::/ text box	Address	Service
Permit SSH plug-in access to the specified IP address.	Permit	ssh	192.168.20.92		
Permit RDP plug-in access to a range of IP addresses.	Permit	rdp	192.168.20.[1-112]		
Use a wildcard to specify a range of IP addresses to permit RDP plug-in access.	Permit	rdp	192.168.20.*		

**Table 21-4** Example Plug-in ACEs

Function	Action	Filter on URL Values		Filter on Address and Service Values	
		drop-down	:// text box	Address	Service
Provide access to specific URLs.	Permit	http	10.80.192.1/engineering/*		
	Permit	http	10.86.192.1/marketing/*		
	Permit			10.86.192.193	3389
Provide TCP access.	Permit			10.86.192.193	3389

**Table 21-5** Example HTTP and HTTPS ACEs

Function	Action	Filter on URL Values	
		drop-down	:// text box
Provide access to specific URLs.	Permit	http	10.80.192.1/engineering/*
	Permit	http	10.86.192.1/marketing/*
Provide access to any HTTP URL.	Permit	http	*/*
Provide access to any HTTPS URL.	Permit	https	*/*

**Table 21-6** Example CIFS Shares ACEs

Function	Action	Filter on URL Values	
		drop-down	:// text box
Deny access to the shares/Marketing_Reports folder. If this entry were the only one in the ACL for the IP address specified, it would implicitly deny access to the root and all peer and sub-folders of shares/Sales_Reports.	Deny	cifs	172.16.10.39/shares/Marketing_Reports
Permit access to all remaining folders of the specified IP address.	Permit	cifs	172.16.10.40/shares*

## Editing Webtype ACLs and ACEs

To edit a webtype ACL or ACE, perform the following steps:

- Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs**.
- Step 2** Choose the Access Rule Type to edit by clicking one of the following radio buttons:
  - **IPv4 and IPv6**—Shows access rules that have both IPv4 and IPv6 type addresses.
  - **IPv4 Only**—Shows access rules that have IPv4 type addresses only.
  - **IPv6 Only**—Shows access rules that have IPv6 type addresses only.

The main Access Rule pane displays the available interfaces for the chosen rule type.
- Step 3** Select the ACE to edit, and make any changes to the values.

For more information about specific values, see the “[Adding a Webtype ACL and ACE](#)” section on page 21-15 or the “[ASDM Field Definitions for Using Access Rules](#)” section on page 21-23. The “[Examples](#)” section on page 21-16 shows example uses of ACEs.

- Step 4** Click **OK**.
- Step 5** Click **Apply** to save the changes to your configuration.
- 

## Deleting Webtype ACEs

To delete a webtype ACE, perform the following steps:

- Step 1** Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs**.
- Step 2** Choose the Access Rule Type of the rule you want to delete by clicking the radio button:
- IPv4 and IPv6—Shows access rules that have both IPv4 and IPv6 type addresses.
  - IPv4 Only—Shows access rules that have IPv4 type addresses only.
  - IPv6 Only—Shows access rules that have IPv6 type addresses only.
- The main Access Rule pane displays the available interfaces for the chosen rule type.
- Step 3** Select the ACE that you want to delete.



**Note** If you select a specific ACE, only that ACE is deleted. If you select an ACL, that ACL and all of the ACEs under it are deleted.

---

- Step 4** Click **Delete**.
- Step 5** The selected items are removed from the viewing pane.



**Note** If you deleted a rule in error and want to restore it to your configuration, click **Reset** before you click **Apply**. The deleted rules reappear in the viewing pane.

---

- Step 6** Click **Apply** to save the change to the configuration.
- 

## Configuring EtherType ACLs

Ethertype access rules are based on packet EtherTypes. EtherType rules are used to configure non-IP related traffic policies through the security appliance when operating in transparent mode. In transparent mode, you can apply both extended and EtherType access rules to an interface. EtherType rules take precedence over the extended access rules.

For information about EtherType access rules and ACLs, see the “[About EtherType ACLs](#)” section on page 21-3.

This section includes the following topics:

- [Adding EtherType ACLs, page 21-20](#)

- [Editing EtherType Access Rules, page 21-20](#)

## Adding EtherType ACLs

To add an EtherType ACL, perform the following steps:

- 
- Step 1** Choose **Configuration > Firewall > EtherType Rules**.
- Step 2** Click **Add**.
- The Add EtherType rules window appears.
- Step 3** (Optional) To specify the placement of the new EtherType rule, select an existing rule, and click **Insert...** to add the EtherType rule before the selected rule, or click **Insert After ...** to add the EtherType rule after the selected rule.
- Step 4** From the Interface drop-down list, choose the interface on which to apply the rule.
- The management interface is for management only and cannot be used to configure an access rule.
- Step 5** In the Action field, click one of the following radio buttons next to the desired action:
- **Permit**—Permits access if the conditions are matched.
  - **Deny**—Denies access if the conditions are matched.
- Step 6** In the EtherType field, choose an EtherType value from the drop-down list.
- Step 7** (Optional) In the Description field, add a test description about the rule.
- The description can contain multiple lines; however, each line can be no more than 100 characters in length.
- Step 8** (Optional) To specify the direction for this rule, click **More Options** to expand the list, and then specify the direction by clicking one of the following radio buttons:
- **In**—Incoming traffic
  - **Out**—Outgoing traffic
- Step 9** Click **OK**.
- 

## Editing EtherType Access Rules

You can edit the contents of EtherType access rules columns to change a rule or to sort its order in the configuration.

To edit an EtherType ACL, perform the following steps:

- 
- Step 1** Choose **Configuration > Firewall > EtherType Rules**.
- Step 2** Click **Edit**.
- The Edit EtherType Rule dialog box appears.
- Step 3** Enter the desired changes, and click **OK**.
- For specific information about the access rule fields, see the [“Adding EtherType ACLs” section on page 21-20](#).

**Step 4** Click **Apply** to save the changes to your configuration.

---

## Adding an Access Rule to Manage a Service Group

The Service Groups pane lets you associate multiple services into a named group. You can specify any type of protocol and service in one group, or you can create service groups for each of the following types:

- TCP ports
- UDP ports
- TCP-UDP ports
- ICMP types
- IP protocols

Multiple service groups can be nested into a “group of groups” and used as a single group.

You can use a service group for most configurations that require you to identify a port, ICMP type, or protocol. When you configure access rules, the ASDM window includes a Services pane at the right that shows available service groups and other global objects. You can add, edit, or delete objects directly in the Services pane. For more information about managing service groups, see the [“Manage Service Groups” section on page 21-27](#).

To configure an ACL with a service group, perform the following steps:

---

**Step 1** Choose **Configuration > Firewall > Access Rules**.

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

- **Add Access Rule**
- **Add IPv6 Access Rule**

The appropriate access rule dialog box appears.

**Step 3** From the Interface drop-down list, choose the interface on which to apply the rule.

The management interface is for management only and cannot be used to configure an access rule.

**Step 4** In the Action field, click one of the following radio buttons next to the desired action:

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

**Step 5** 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 to the specified destination.

For more information about enabling IPv6 on an interface, see [Chapter 9, “Configuring Interfaces.”](#)

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

**Step 7** In the Service field, click the browse button.

The Browse Service dialog box appears.

**Step 8** From the list Browse Service list, select the service group for which you want to apply the access rule. You can choose either TCP ports, UDP ports, TCP-UDP ports, ICMP types, or IP protocols.

- Step 9** Click **OK**.
- Step 10** (Optional) In the Description pane, add a description of the access rule (up to 200 characters in length).
- Step 11** (Optional) Logging is enabled by default. You can disable logging by unchecking the check box, or you can change the logging level from the drop-down list. The default logging level is Informational.
- For more information about logging options, see the “[Log Options](#)” section on page 21-29.
- Step 12** (Optional) To add a source service (TCP, UDP, and TCP-UDP only) and a time range to your access rule that specifies when traffic can be allowed or denied, click **More Options** to expand the list.
- In the Source Service field, click the browse button to browse for an existing service.
  - In the Browse Source Services dialog box, choose the service to apply to the access rule, and click the Source Service button.
- The selected service appears in the Source Service field.
- Click **OK**.
- Step 13** (Optional) To add a time range, perform the following steps under More Options.
- To the right of the Time Range field, click the browse button.
- The Browse Time Range dialog box appears.
- Click **Add**.
- The Add Time Range dialog box appears.
- In the Time Range Name field, enter a time range name, with no spaces.
  - Enter the Start Time and the End Time.
  - To specify additional time constraints for the time range, such as specifying the days of the week or the recurring weekly interval in which the time range will be active, click **Add**, and specify the desired values.
  - Click **OK** to apply the optional time range specifications.
- Step 14** Click **Add**.
- Step 15** From the Add drop-down list, choose **Service Group**.
- The Add Service Group dialog box appears.
- Step 16** In the Group Name field, enter a meaningful name for the service group.
- Step 17** Click the **Existing Service/Service Group** radio button.
- Step 18** Click **OK**.
- The Browse Service pane displays the newly configured service group.
- Step 19** Click **OK**.
- The Service field appears with the newly configured service group.
- Step 20** Click **OK**.
- Step 21** Click **Apply** to save the configuration.

**Note**

After you add access rules, you can click one of the following radio buttons to filter which access rules appear in the main pane: **IPv4 and IPv6**, **IPv4 Only**, or **IPv6 Only**.

## ASDM Field Definitions for Using Access Rules

This section includes the following topics:

- [Access Rule Field Definitions, page 21-23](#)
- [Rule Queries, page 21-25](#)
- [New/Edit Rule Query, page 21-25](#)
- [Add/Edit Access Rule, page 21-26](#)
- [Manage Service Groups, page 21-27](#)
- [Add/Edit Service Group, page 21-28](#)
- [Advanced Access Rule Configuration, page 21-29](#)
- [Log Options, page 21-29](#)

### Access Rule Field Definitions

You can adjust the table column widths by moving your cursor over a column line until it turns into a double arrow. Click and drag the column line to the desired size.

- **Add**—Adds a new access rule.
- **Edit**—Edits an access rule.
- **Delete**—Deletes an access rule.
- **Move Up**—Moves a rule up. Rules are assessed in the order they appear in this table, so the order can matter if you have overlapping rules.
- **Move Down**—Moves a rule down.
- **Cut**—Cuts a rule.
- **Copy**—Copies the parameters of a rule so that you can start a new rule with the same parameters using the Paste button.
- **Paste**—Opens an Add/Edit Rule dialog box with the copied or cut parameters of a rule prefilled. You can then make any modifications and add it to the table. The Paste button adds the rule above the selected rule. The Paste After item, available from the Paste drop-down list, adds the rule after the selected rule.
- **Find**—Filters the display to show only matching rules. Clicking **Find** opens the Filter field. Click **Find** again to hide the Filter field.
  - **Filter drop-down list**—Choose the criteria to filter, either Interface, Source, Destination, Source or Destination, Destination Service, or Rule Query. A rule query is a collection of multiple criteria that you can save and use repeatedly.
  - **Condition drop-down list**—For criteria Source, Destination, Source or Destination, and Destination Service, choose the condition, either “is” or “includes.”
  - **Filter field**—The Interface type field becomes a drop-down list so that you can choose an interface name. For the Rule Query type, the drop-down list includes all defined rule queries. The Source and Destination types accept an IP address. You can type an address manually or browse for one by clicking the browse button (...) and launching the Browse Address dialog box. The Destination Service type accepts a TCP, UDP, TCP-UDP, ICMP, or IP protocol type. You can enter a type manually or browse for one by clicking the browse button (...) and launching the Browse Service Groups dialog box. The Filter field accepts multiple entries separated by a comma or space. Wildcards are also allowed.

- Filter—Runs the filter.
- Clear—Clears the matches and displays all.
- Rule Query—Opens the Rule Queries dialog box so that you can manage named rule queries.
- Diagram—Shows the Rule Flow Diagram area under the rule table. This diagram shows the networks, type of traffic, interface name, direction of flow, and action.
- Export—Exports to a file in either comma separated value or HTML format.
- Clear Hits—Clears the counted hits for the selected access rule. Logging must be enabled for this field to be active.
- Show Log—Shows the syslogs generated by the selected access rule in the Real-Time Log Viewer.
- Packet Trace—Provides detailed information about packet processing with the adaptive security appliance, as well as information for packet sniffing and network fault isolation.
- IPv4 Only—Shows access rules that have IPv4 type addresses only.
- IPv6 Only—Shows access rules that have IPv6 type addresses only.
- IPv4 and IPv6—Shows access rules that have both IPv4 and IPv6 type addresses.

The following description summarizes the columns in the Access Rules table. You can edit the contents of these columns by double-clicking a table row. Rules are displayed in the order of execution. If you right-click a rule, you see all of the options represented by the buttons above, as well as Insert and Insert After items. These items either insert a new rule before the selected rule (Insert) or after the selected rule (Insert After.)

- No—Indicates the order of evaluation for the rule.
- Enabled—Indicates whether the rule is enabled or disabled.
- Source—Specifies the IP address, network object group, interface IP, or any address from which traffic is permitted or denied to the destination specified in the Destination Type field. An address column might contain an interface name with the word any, such as inside:any. This configuration means that any host on the inside interface is affected by the rule.
- Destination—Specifies the IP address, network object group, interface IP, or any address to which traffic is permitted or denied from the source specified in the Source Type field. An address column might contain an interface name with the word any, such as outside:any. This configuration means that any host on the outside interface is affected by the rule. Also in detail mode, an address column might contain IP addresses in square brackets, for example [209.165.201.1-209.165.201.30]. These addresses are translated addresses. When an inside host makes a connection to an outside host, the firewall maps the address of the inside host to an address from the pool. After a host creates an outbound connection, the firewall maintains this address mapping. The address mapping structure is called an xlate, and it remains in memory for a period of time. During this time, outside hosts can initiate connections to the inside host using the translated address from the pool, if allowed by the access rule. Normally, outside-to-inside connections require a static translation so that the inside host always uses the same IP address.
- Service—Shows the service or protocol specified by the rule.
- Action—The action that applies to the rule, either Permit or Deny.
- Hits—Shows the number of hits for the rule. This column is dynamically updated depending upon the frequency set in the Preferences dialog box. Hit counts are applicable for explicit rules only. No hit count will be displayed for implicit rules in the Access Rules table.
- Logging—Shows the logging level and the interval in seconds between log messages (if you enable logging for the access rule).
- Time—Displays the time range during which the rule is applied.

- **Description**—Shows the description you entered when you added the rule. An implicit rule includes the following description: “Implicit outbound rule.”
- **Addresses**—Enables you to add, edit, delete, or find IP names or network object groups. IP address objects are automatically created based on source and destination entries during rule creation so that they can easily be selected in the creation of subsequent rules. They cannot be added, edited, or deleted manually.
- **Services**—Enables you to add, edit, delete, or find services.
- **Time Ranges**—Enables you to add, edit, or delete time ranges.

### Modes

The following table shows the modes in which ACLs are available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Rule Queries

The Rule Queries dialog box lets you manage named rule queries that you can use in the Filter field when searching for Rules.

### Fields

- **Add**—Adds a rule query.
- **Edit**—Edits a rule query.
- **Delete**—Deletes a rule query.
- **Name**—Lists the names of the rule queries.
- **Description**—Lists the descriptions of the rule queries.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## New/Edit Rule Query

The New/Edit Rule Query dialog box lets you add or edit a named rule query that you can use in the Filter field when searching for rules.

**Fields**

- Name—Enter a name for this rule query.
- Description—Enter a description for this rule query.
- Match Criteria—Lists the criteria you want to filter on.
  - any of the following criteria—Sets the rule query to match any of the listed criteria.
  - all of the following criteria—Sets the rule query to match all of the listed criteria.
  - Field—Lists the type of criteria. For example, an interface or source.
  - Value—Lists the value of the criteria, for example, “inside.”
  - Remove—Removes the selected criteria.
- Define New Criteria—Lets you define new criteria to add to the match criteria.
  - Field—Choose a type of criteria, including Interface, Source, Destination, Service, Action, or another Rule Query to be nested in this rule query.
  - Value—Enter a value to search on. For the Interface type, this field becomes a drop-down list so you can choose an interface name. For the Action type, the drop-down list includes Permit and Deny. For the Rule Query type, the drop-down list includes all defined rule queries. The Source and Destination types accept an IP address. You can type one manually or browse for one by clicking the browse (...) button and launching the Browse Address dialog box. The Service type accepts a TCP, UDP, TCP-UDP, ICMP, or IP protocol type. You can type one manually, or browse for one by clicking the browse (...) button and launching the Browse Service Groups dialog box.
  - Add—Adds the criteria to the Match Criteria table.

**Modes**

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

**Add/Edit Access Rule**

The Add/Edit Rule dialog box lets you create a new rule or modify an existing rule.

For more information about access rules, see the [“Information About Access Rules and ACLs”](#) section on page 21-1.

**Fields**

- Interface—Specifies the interface to which the rule applies.
- Action—Determines the action type of the new rule. Select either permit or deny.
  - Permit—Permits all matching traffic.
  - Deny—Denies all matching traffic.
- Source—Specifies the IP address, network object group, interface IP, or any, from which traffic is permitted or denied to the destination specified in the Destination field.

- ...—Lets you select, add, edit, delete, or find an existing IP address object, IP name, network object group, or all.
- Destination —Specifies the IP address, network object group, interface IP, or any, to which traffic is permitted or denied from the source specified in the Source Type field.
  - ...—Lets you select, add, edit, delete, or find an existing IP address object, IP name, network object group, or all.
- Service—Choose this option to specify a port number, a range of ports, or a well-known service name or group from a list of services.
  - ...—Lets you select, add, edit, delete, or find an existing service from a preconfigured list.
- Description—(Optional) Enter a description of the access rule.
- Enable Logging—Enables logging for the access rule.
  - Logging Level—Specifies default, emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging.
- More Options—Shows additional configuration options for the rule.
  - Enable Rule—Enables or disables the rule.
  - Traffic Direction—Determines which direction of traffic the rule is applied. Options are either incoming or outgoing.
  - Source Service—Specifies a source protocol and service (TCP or UDP service only).
    - ...—Lets you select, add, edit, delete or find a source service from a preconfigured list.
  - Logging Interval—Specifies the interval for logging in seconds if logging is configured.
  - Time Range—Specifies a time range defined for this rule from the drop-down list.
    - ...—Lets you select, add, edit, delete or find a time range from a preconfigured list.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Manage Service Groups

The Manage Service Groups dialog box lets you associate multiple TCP, UDP, or TCP-UDP services (ports) in a named group. You can then use the service group in an access or IPSec rule, a conduit, or other functions within ASDM and the CLI.

The term service refers to higher layer protocols associated with application level services having well known port numbers and “literal” names such as ftp, telnet, and smtp.

The security appliance permits the following TCP literal names:

bgp, chargen, cmd, daytime, discard, domain, echo, exec, finger, ftp, ftp-data, gopher, h323, hostname, http, ident, irc, klogin, kshell, lpd, nntp, pop2, pop3, pptp, smtp, sqlnet, sunrpc, tacacs, talk, telnet, time, uucp, whois, www.

The Name of a service group must be unique to all four types of object groups. For example, a service group and a network group may not share the same name.

Multiple service groups can be nested into a “group of groups” and used the same as a single group. When a service object group is deleted, it is removed from all service object groups where it is used.

If a service group is used in an access rule, do not remove it. A service group used in an access rule cannot be made empty.

#### Fields

- TCP—Choose this option to add TCP services or port numbers to an object group.
- UDP—Choose this option to add UDP services or port numbers to an object group.
- TCP-UDP—Choose this option to add services or port numbers that are common to TCP and UDP to an object group.
- Service Group table—This table contains a descriptive name for each service object group. To modify or delete a group in this list, select the desired group, and click **Edit** or **Delete**. To add a new group to this list, click **Add**.

#### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Add/Edit Service Group

The Add/Edit Service Group dialog box lets you manage a group of TCP/UDP services/ports.

#### Fields

- Service Group Name—Specifies the name of the service group. The name must be unique for all object groups. A service group name cannot share a name with a network group.
- Description—Specifies a description of the service group.
- Service—Lets you choose services for the service group from a predefined drop-down list.
- Range/Port #—Lets you specify a range of ports for the service group.

#### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Advanced Access Rule Configuration

The Advanced Access Rule Configuration dialog box lets you to set global access rule logging options.

When you enable logging, if a packet matches the access rule, the security appliance creates a flow entry to track the number of packets received within a specific interval (see Log Options). The security appliance generates a system log message at the first hit and at the end of each interval, identifying the total number of hits during the interval. At the end of each interval, the security appliance resets the hit count to 0. If no packets match the access rule during an interval, the security appliance deletes the flow entry.

A large number of flows can exist concurrently at any point of time. To prevent unlimited consumption of memory and CPU resources, the security appliance places a limit on the number of concurrent deny flows; the limit is placed only on deny flows (and not permit flows) because they can indicate an attack. When the limit is reached, the security appliance does not create a new deny flow until the existing flows expire. If someone initiates a denial of service attack, the security appliance can create a very large number of deny flows in a very short period of time. Restricting the number of deny-flows prevents unlimited consumption of memory and CPU resources.

For more information about access rules, see the [“Information About Access Rules and ACLs” section on page 21-1](#).

### Prerequisites

These settings only apply if you enable the newer logging mechanism for the access control entry (also known as a rule) for the access rule. See Log Options for more information.

### Fields

- **Maximum Deny-flows**—The maximum number of deny flows permitted before the security appliance stops logging, between 1 and the default value. The default is 4096.
- **Alert Interval**—The amount of time (1-3600 seconds) between system log messages (number 106101) that identify that the maximum number of deny flows was reached. The default is 300 seconds.
- **Per User Override table**—Specifies the state of the per user override feature. If the per user override feature is enabled on the inbound access rule, the access rule provided by a RADIUS server replaces the access rule configured on that interface. If the per user override feature is disabled, the access rule provided by the RADIUS server is combined with the access rule configured on that interface. If the inbound access rule is not configured for the interface, per user override cannot be configured.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Log Options

The Log Options dialog box lets you set logging options for each access rule. See the [“Advanced Access Rule Configuration” section on page 21-29](#) to set global logging options.

This dialog box lets you use the older logging mechanism (only denied traffic is logged), to use the newer logging mechanism (permitted and denied traffic is logged, along with additional information such as how many packet hits), or to disable logging.

The Log option consumes a certain amount of memory when enabled. To help control the risk of a potential Denial of Service attack, you can configure the Maximum Deny-flow setting by choosing **Advanced** in the Access Rules dialog box.

### Fields

- Use default logging behavior—Uses the older access rule logging mechanism: the security appliance logs system log message number 106023 when a packet is denied. Use this option to return to the default setting.
- Enable logging for the rule—Enables the newer access rule logging mechanism: the security appliance logs system log message number 106100 when a packet matches the access rule (either permit or deny).

If a packet matches the access rule, the security appliance creates a flow entry to track the number of packets received within a specific interval. (See the Logging Interval field that follows.) The security appliance generates a system log message at the first hit and at the end of each interval, identifying the total number of hits during the interval. At the end of each interval, the security appliance resets the hit count to 0. If no packets match the access rule during an interval, the security appliance deletes the flow entry.

- Logging Level—Selects the level of logging messages to be sent to the syslog server from this drop-down list. Levels are defined as follows:

Emergency (level 0)—The security appliance does not use this level.

Alert (level 1, immediate action needed)

Critical (level 2, critical condition)

Error (level 3, error condition)

Warning (level 4, warning condition)

Notification (level 5, normal but significant condition)

Informational (level 6, informational message only)

Debugging (level 7, appears during debugging only)

- Logging Interval—Sets the amount of time in seconds (1-600) the security appliance waits before sending the flow statistics to the syslog. This setting also serves as the timeout value for deleting a flow if no packets match the access rule. The default is 300 seconds.
- Disable logging for the rule—Disables all logging for the access rule.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—