



CHAPTER 20

Configuring Access Rules and EtherType Rules

This chapter describes how to configure access rules and EtherType rules, and includes the following topics:

- [Information About Access Rules and EtherType Rules, page 20-1](#)
- [Configuring Access Rules, page 20-7](#)
- [Configuring Ethertype Rules \(Transparent Mode Only\), page 20-16](#)



Note

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

To access the security appliance interface for management access, you do not also need an access rule allowing the host IP address. You only need to configure management access according to [Chapter 16, “Configuring Management Access.”](#)

Information About Access Rules and EtherType Rules

Your access policy is made up of one or more access rules and/or EtherType rules per interface.

You can use access rules in routed and transparent firewall mode to control IP traffic. An access rule permits or denies traffic based on the protocol, a source and destination IP address or network, and optionally the source and destination ports.



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.

For transparent mode only, an EtherType rule controls network access for non-IP traffic. An EtherType rule permits or denies traffic based on the EtherType.

This section includes the following topics:

- [Information About Both Access Rules and EtherType Rules, page 20-2](#)
- [Information About Access Rules, page 20-3](#)
- [Information About EtherType Rules, page 20-6](#)

Information About Both Access Rules and EtherType Rules

This section describes information for both access rules and EtherType rules, and includes the following topics:

- [Using Access Rules and EtherType Rules on the Same Interface, page 20-2](#)
- [Rule Order, page 20-2](#)
- [Implicit Deny, page 20-2](#)
- [Inbound and Outbound Rules, page 20-2](#)

Using Access Rules and EtherType Rules on the Same Interface

You can apply both access rules and EtherType 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 that explicitly permits all traffic for an interface, no further rules are ever checked.

You can disable a rule by making it inactive.

Implicit Deny

Lists of access rules or 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.

Inbound and Outbound Rules

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

The security appliance supports two types of access lists:

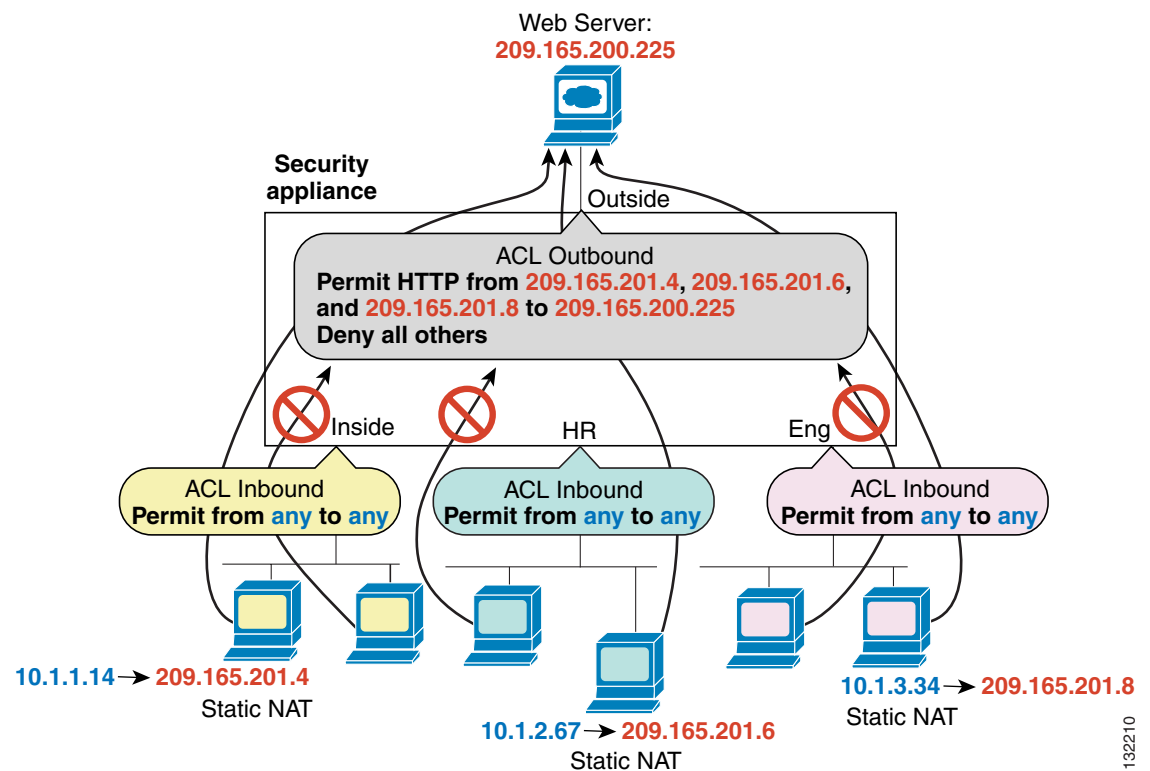
- Inbound—Inbound access lists apply to traffic as it enters an interface.
- Outbound—Outbound access lists apply to traffic as it exits an interface.

**Note**

“Inbound” and “outbound” refer to the application of an access list 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 access list 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 access lists to restrict access, you can create a single outbound access list that allows only the specified hosts (see [Figure 20-1](#)). The outbound access list prevents any other hosts from reaching the outside network.

Figure 20-1 Outbound Access List



132210

Information About Access Rules

This section describes information about access rules, and includes the following topics:

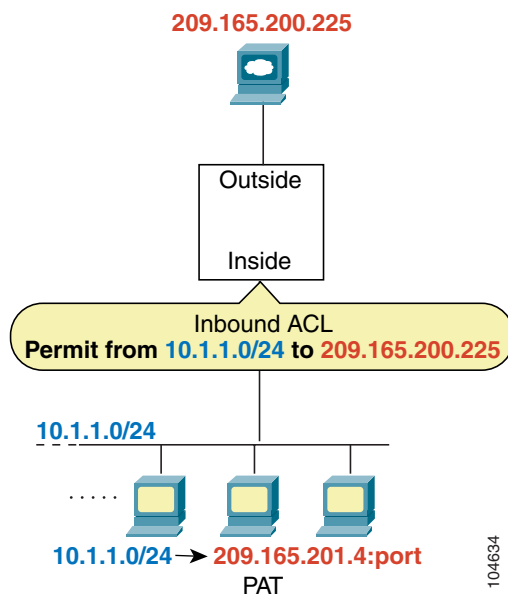
- [IP Addresses Used for Access Rules When You Use NAT](#), page 20-4
- [Access Rules for Returning Traffic](#), page 20-6
- [Allowing Broadcast and Multicast Traffic through the Transparent Firewall Using Access Rules](#), page 20-6

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 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.

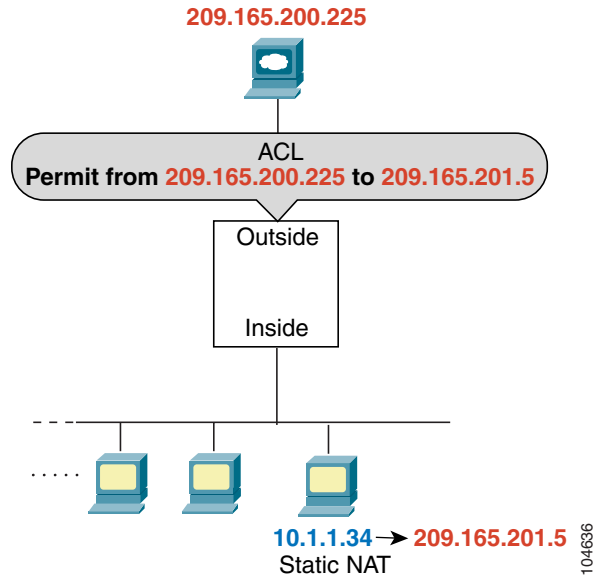
For example, you want to apply an access rule to the inbound direction of the inside interface. You configure the security appliance to perform NAT on the inside source addresses when they access outside addresses. Because the access rule is applied to the inside interface, the source addresses are the original untranslated addresses. Because the outside addresses are not translated, the destination address used in the access rule is the real address (see [Figure 20-2](#)).

Figure 20-2 IP Addresses in Access Rules: NAT Used for Source Addresses



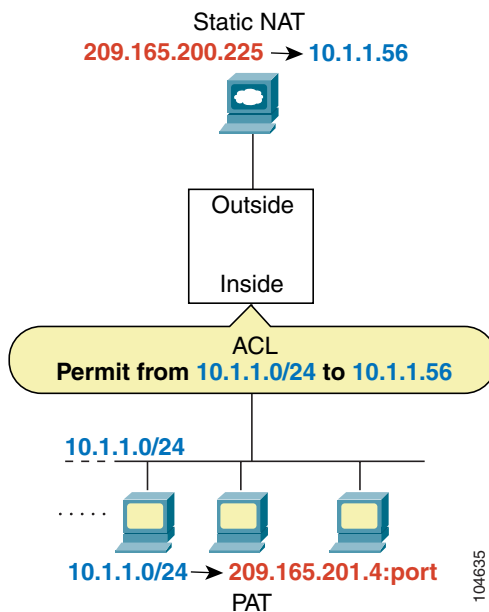
If you want to allow an outside host to access an inside host, you can apply an inbound access rule on the outside interface. You need to specify the translated address of the inside host in the access rule because that address is the address that can be used on the outside network (see Figure 20-3).

Figure 20-3 IP Addresses in Access Rules: 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 20-4, an outside server uses static NAT so that a translated address appears on the inside network.

Figure 20-4 IP Addresses in Access Rules: 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 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.

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, for example.



Note

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

Table 20-1 lists common traffic types that you can allow through the transparent firewall.

Table 20-1 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	—

Information About EtherType Rules

This section describes EtherType rules, and includes the following topics:

- [Supported EtherTypes, page 20-6](#)
- [Implicit Permit of IP and ARPs Only, page 20-7](#)
- [Using Access Rules and EtherType Rules on the Same Interface, page 20-2](#)
- [Allowing MPLS, page 20-7](#)

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 handled by the rule, 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 from a higher security interface to a lower security interface, without a rule. 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.

IPv6 Unsupported

EtherType ACEs do not allow IPv6 traffic, even if you specify the IPv6 EtherType.

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.)

On Cisco IOS routers, enter the appropriate command for your protocol, LDP or TDP. The *interface* is the interface connected to the security appliance.

```
hostname(config)# mpls ldp router-id interface force
```

Or

```
hostname(config)# tag-switching tdp router-id interface force
```

Configuring Access Rules

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

When you choose the **Access Rules** option, this window lets you define access lists 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 EtherType Rules” section on page 20-1](#).

Fields

Note: 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 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 on, 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—For the Interface type, this field becomes a drop-down list so 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 one manually, or browse for one by clicking the ... 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 type one manually, or browse for one by clicking the ... 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 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.

The following description summarizes the columns in the Access Rules table. You can edit the contents of these columns by double-clicking on 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, 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 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, 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 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 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 on 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—If you enable logging for the access rule, this column shows the logging level and the interval in seconds between log messages.
- 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—Tab that lets you 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—Tab that lets you add, edit, delete, or find services.
- Time Ranges—Tab that lets you add, edit, or delete time ranges.

Modes

The following table shows the modes in which this feature is 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—This area 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—This area 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 ... 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 ... 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 EtherType Rules” section on page 20-1](#).

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**—Select this option to add TCP services or port numbers to an object group.
- **UDP**—Select this option to add UDP services or port numbers to an object group.
- **TCP-UDP**—Select 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 on this list, select the 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 select 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 EtherType Rules” section on page 20-1](#).

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 20-13](#) 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 window.

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
•	•	•	•	—

Configuring EtherType Rules (Transparent Mode Only)

The EtherType Rules window shows access rules 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 more information about EtherType rules, see the [“Information About Access Rules and EtherType Rules” section on page 20-1](#).

Fields

- Add—Adds a new EtherType rule. Choose the type of rule you want to add from the drop-down list.
- Edit—Edits an EtherType rule.
- Delete—Deletes an EtherType 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 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 the 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.

The following description summarizes the columns in the EtherType Rules table. You can edit the contents of these columns by double-clicking on a table cell. Double-clicking on a column header sorts the table in ascending alphanumeric order, using the selected column as the sort key. 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.
- Action—Permit or deny action for this rule.
- Ethertype—EtherType value: IPX, BPDU, MPLS-Unicast, MPLS-Multicast, or a 16-bit hexadecimal value between 0x600 (1536) and 0xffff by which an EtherType can be identified.
- Interface—Interface to which the rule is applied.
- Direction Applied—Direction for this rule: incoming traffic or outgoing traffic.
- Description—Optional text description of the rule.

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 EtherType Rule

The Add/Edit EtherType Rules dialog box lets you add or edit an EtherType rule.

For more information about EtherType rules, see the [“Information About Access Rules and EtherType Rules”](#) section on page 20-1.

Fields

- Action—Permit or deny action for this rule.
- Interface—Interface name for this rule.
- Apply rule to—Direction for this rule: incoming traffic or outgoing traffic.
- Ethertype—EtherType value: BPDU, IPX, MPLS-Unicast, MPLS-Multicast, any (any value between 0x600 and 0xffff), or a 16-bit hexadecimal value between 0x600 (1536) and 0xffff by which an EtherType can be identified.
- Description—Optional text description of the rule.

Modes

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

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

