



# CHAPTER 17

## Configuring Access Rules

---

### 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 control lists to control the access of a specific host or network to another host/network, including the protocol or port that can be used. Conduits and outbound lists have been superseded by access lists.

By default on the security appliance, traffic from a higher security level (for example, inside) can access a lower security level (for example, outside): there is an implicit access list on the inside interface allowing all outbound IP traffic from the inside network. (The security appliance denies traffic destined for the inside network from the outside network using the Adaptive Security Algorithm. Adaptive Security Algorithm is a stateful approach to security. Every inbound packet is checked against the Adaptive Security Algorithm and against connection state information in memory.) The implicit access list appears in ASDM, but you cannot edit it. To limit outbound traffic, you can add an access list (in which case, the implicit access list is removed).

Every inbound packet is checked using the Adaptive Security Algorithm unless a connection is already established. By default on the security appliance, no traffic can pass through the firewall unless you add an access list to allow it.

To allow traffic that is normally denied by the Adaptive Security Algorithm, you can add an access list; for example, you can allow public access to a web server on a DMZ network by adding an access list to the outside interface.

#### Restrictions

At the end of each access list, there is an implicit, unwritten rule that denies all traffic that is not permitted. If traffic is not explicitly permitted by an access control entry, it will be denied. ACEs are referred to as rules in this topic.

#### Prerequisites

If desired, create network groups on the **Addresses** tab.

#### 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, Service, or Rule Query. A rule query is a collection of multiple criteria that you can save and use repeatedly.
  - **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 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.
- **Show Rule Flow 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.
- **Packet Trace**—Opens the Packet Tracer tool with the parameters pre-filled with the characteristics of the selected rule.

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 list. 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.
- **Logging**—If you enable logging for the access list, 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 network objects or 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.

### 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.
- **Direction**—Determines which direction of traffic the rule is applied.
  - Incoming—Selects incoming traffic to the source interface.
  - Outgoing—Selects outgoing traffic from the destination interface.
- **Source Type**—**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.**
  - **IP Address**—**Specifies the IP address from which traffic is permitted or denied to the destination specified in the Destination Type field.**
    - IP address**—**Specifies the IP address.**
    - ...—Lets you select, add, edit, delete, or find an existing network object, network object group, or all.
    - Netmask**—**Specifies the netmask.**
  - **Network Object Group**—**Specifies the network object group from which traffic is permitted or denied to the destination specified in the Destination Type field.**
    - Group Name**—**Specifies the network object group name.**
    - ...—Lets you select, add, edit, delete, or find an existing network object, network object group, or all.
  - **Interface IP**—**Specifies the interface IP, or any, from which traffic is permitted or denied to the destination specified in the Destination Type field.**
  - **Interface**—**Specifies the interface.**
- **Destination Type**—**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.**
  - **IP Address**—**Specifies the IP address to which traffic is permitted or denied from the destination specified in the Source Type field.**
    - IP address**—**Specifies the IP address.**
    - ...—Lets you select, add, edit, delete, or find an existing network object, network object group, or all.
    - Netmask**—**Specifies the netmask.**
  - **Network Object Group**—**Specifies the network object group to which traffic is permitted or denied from the source specified in the Source Type field.**
    - Group Name**—**Specifies the network object group name.**
    - ...—Lets you select, add, edit, delete, or find an existing network object, , network object group, or all.

- **Interface IP**—Specifies the interface IP, or any, to which traffic is permitted or denied from the source specified in the Source Type field.
- **Interface**—Specifies the interface.
- **Protocol and Service: TCP and UDP**—Selects the TCP/UDP protocol for the rule. The **Source Port** and **Destination Port** areas allow you to specify the ports that the access list uses to match packets.
  - **Service**—Choose this option to specify a port number, a range of ports, or a well-known service name from a list of services, such as HTTP or FTP. The operator drop-down list specifies how the access list matches the port. Choose one of the following operators:
    - = —Equals the port number.
    - not =** —Does not equal the port number.
    - > —Greater than the port number.
    - < —Less than the port number.
    - range**—Equal to one of the port numbers in the range.
  - **Group**—Choose this option to specify a service group from the Service Group drop-down list, The browse button displays the Browse Source Port dialog box, which lets you select, add, edit, delete or find a source type from a preconfigured list.
- **Protocol and Service: IP**—Specifies the IP protocol for the rule in the IP protocol field.
- **Protocol and Service: ICMP**—Specifies the ICMP type for the rule in the ICMP type field or the ICMP group.
  - The browse button displays the Browse ICMP dialog box, which lets you select, add, edit, delete or find a source type from a preconfigured list.
- **Rule Flow Diagram**—Shows the networks, type of traffic, interface name, direction of flow, and action.
- **Options**—Enables logging for the access list and sets logging options. Logging options:
  - Use default logging behavior.
  - Enable logging for the rule. Sets the level and interval for permit and deny logging. See [Log Options](#) for more information.
    - Syslog Level—Specifies emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging.
    - Log Interval—Specifies the interval for logging.
  - Disable logging for the rule.
  - **Time Range**—Select a time range defined for this rule from the drop-down list. The browse button displays the Browse Time Range dialog box, which lets you select, add, edit, or delete a time range from a preconfigured list.
  - **Description**—(Optional) Enter a description of 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
•	•	•	•	—

## 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 list logging options.

When you enable logging, if a packet matches the ACE, 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 ACE 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.

### 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 list. 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 list, the access list provided by a RADIUS server replaces the access list configured on that interface. If the per user override feature is disabled, the access list provided by the RADIUS server is combined with the access list configured on that interface. If the inbound access list 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 control entry (also called a rule) for an access control list. Conduits and outbound lists do not support logging. See **Advanced Access Rule Configuration** 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 list 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 list logging mechanism: the security appliance logs system log message number 106100 when a packet matches the ACE (either permit or deny).

If a packet matches the ACE, 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 ACE 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 ACE. The default is 300 seconds.
- **Disable logging for the rule**—Disables all logging for the ACE.

### Modes

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

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