Managing Firewall Access Rules

Access rules define the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied (with the exception of less common AAA rules). In that sense, they are your first line of defense.

Tip For some types of devices, you can configure IPv6 access rules in addition to IPv4 access rules. For information on supported device types, see IPv6 Support in Security Manager, page 1-8.

The following topics help you understand and work with access rules:

The following topics can help you with general rule table usage:

Understanding Access Rules

Access rules policies define the rules that allow or deny traffic to transit an interface. Typically, you create access rules for traffic entering an interface, because if you are going to deny specific types of packets, it is better to do it before the device spends a lot of time processing them.

When you deploy access rules to devices, they become one or more entries (ACEs) to access control lists (ACLs) that are attached to interfaces. Typically, these rules are the first security policy applied to packets; they are your first line of defense. You use access rules to filter out undesired traffic based on service (protocol and port numbers) and source and destination addresses, either permitting the traffic or denying (dropping) it. Each packet that arrives at an interface is examined to determine whether to forward or drop the packet based on criteria you specify. If you define access rules in the out direction, packets are also analyzed before they are allowed to leave an interface.

Tip For ASA 8.3+ devices, you can augment interface-specific access rules with global access rules. For more information, see Understanding Global Access Rules, page 16-3.

When you permit traffic in an access rule, subsequent policies might end up dropping it. For example, inspection rules, web filter rules, and zone-based firewall rules are applied after a packet makes it through the interface's access rules. These subsequent rules might then drop the traffic based on a deeper analysis of the traffic; for example, the packet header might not meet your inspection requirements, or the URL for a web request might be for an undesired web site.

Thus, you should carefully consider the other types of firewall rules you intend to create when you define access rules. Do not create a blanket denial in an access rule for traffic that you really want to inspect. On the other hand, if you know that you will never allow a service from or to a specific host or network, use an access rule to deny the traffic.

Keep in mind that access rules are ordered. That is, when the device compares a packet against the rules, it searches from top to bottom and applies the policy for the first rule that matches it, and ignores all subsequent rules (even if a later rule is a better match). Thus, you should place specific rules above more general rules to ensure those rules are not ignored. To help you identify cases where IPv4 rules will never be matched, and to identify redundant rules, you can use the automatic conflict detection and policy query tools. For more information, see Using Automatic Conflict Detection, page 16-28 and Generating Policy Query Reports, page 12-28.

The following are additional ways in which you can evaluate your access rules:

- Combine rules—You can use a tool to evaluate your IPv4 rules and combine them into a smaller number of rules that perform the same functions. This can leave you with a smaller, easier to manage list of rules. For more information, see Combining Rules, page 12-22.
- Generate hit counts—You can use a tool to view the hit count statistics maintained by the device for IPv4 and IPv6 ACLs. This can tell you how often a rule has permitted or denied traffic. For more information, see Viewing Hit Count Details, page 16-37.
- View events collected by CS-MARS—You can analyze real time or historical events related to an IPv4 rule using the Cisco Security Monitoring, Analysis and Response System application if you configured it to monitor the device and you configure the rule to generate syslog messages. For more information, see Viewing CS-MARS Events for an Access Rule, page 72-44.

For more conceptual information on access rules, see the following topics:

- Understanding Global Access Rules, page 16-3
- Understanding Device Specific Access Rule Behavior, page 16-4
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5

Related Topics

- Configuring Access Rules, page 16-7
- Configuring Expiration Dates for Access Rules, page 16-22

- Configuring Settings for Access Control, page 16-23
- Expanding Object Groups During Discovery, page 12-35
- Importing Rules, page 16-41
- Adding and Removing Rules, page 12-9
- Editing Rules, page 12-10
- Enabling and Disabling Rules, page 12-20
- Moving Rules and the Importance of Rule Order, page 12-19

Understanding Global Access Rules

Traditionally, access rules (ACLs), which control which traffic can flow through a device, are applied to device interfaces. However, with ASA devices running software release 8.3+, you have the option to create global access rules for IPv4 and IPv6.

Global access rules are defined as a special ACL that is processed for every interface on the device for traffic entering the interface. Thus, although the ACL is configured once on the device, it acts like a secondary interface-specific ACL defined for the In direction. (Global rules are always for the In direction, never the Out direction.)

When traffic enters an interface on an ASA 8.3+ device, when applying ACLs, the device first applies any interface-specific access rules to the traffic. It then applies global rules. (Overall processing is explained in Understanding the Processing Order of Firewall Rules, page 12-2.)

Global rules are best used for rules that you want to apply to all traffic that enters a device regardless of which interface it enters. For example, there might be a specific host or subnet that you always want to deny or permit. You can create these as global rules, so they are configured once on the device instead of configured again for each interface (although functionally the same as an interface-specific rule configured for the All-Interfaces role, All-Interfaces rules are repeated for each interface rather than being configured once on the device).

Tip If you want to configure the same set of global rules for more than one device, create a shared policy and inherit it in the IPv4 or IPv6 access rules policy for each device. Ensure that all global rules are in the Default section of the shared policy. If you put any global rules in the Mandatory section, you will not be able to inherit it on devices that have local interface-specific access rules defined. For more information on shared and inherited policies, see Local Policies vs. Shared Policies, page 5-3 and Understanding Rule Inheritance, page 5-4.

When you configure access rules for an ASA 8.3+ device in Security Manager, interface-specific and global rules are configured in the same policy. However, because the device always processes interface-specific rules first, Security Manager prevents you from intermixing these different types of rules. Therefore, if you configure both interface-specific and global rules on a device, keep the following in mind:

- Global rules always come last in the access rules policy. All interface-specific rules come before global rules.
- You cannot move rules in a way that violates the required order. For example, you cannot move an interface-specific rule below a global rule, or a global rule above an interface-specific rule.
- You cannot create rules in a location that violates the required order. For example, if you select an interface-specific rule, and another interface-specific rule follows it in the table, you cannot create a global rule. If you try to create the wrong kind of rule, when you save the rule, Security Manager

will ask you if the rule can be created at the nearest valid location. You must accept the suggestion or the rule will not be added to the table. You can always move the rule after creating it if the suggested location is not ideal (but without violating the rules on order).

- You cannot inherit a policy if the rules in the inherited policy will violate the required order. For example, if you create global rules in the device policy, and try to inherit a shared policy that contains interface-specific rules in the Default section, Security Manager will prevent you from inheriting the policy.
- After assigning or inheriting a shared policy, you cannot edit the policy in a way that will violate rule order on any device that uses the policy.
- If you assign or inherit a policy that contains global rules on a device that does not support them, all global rules are ignored and not configured on the device. For example, if you permit all traffic from host 10.100.10.10 in a global rule in a shared policy, and assign that policy to an IOS device, the rule permitting 10.100.10.10 access is not configured on the IOS device, and traffic from that host is handled either by another interface-specific policy, or the default deny all policy. As a good practice, you should not assign shared policies that contain global rules to devices that do not support them, to ensure that you do not mistakenly believe the policy defined in a global rule is being configured on the unsupported device.

There are also some changes in how certain tools work with global rules:

- Find/Replace—You can search for global rules by using the Global interface name. However, there is no way to convert between global and interface-specific rules. Although you can find global rules using the Global interface name, if you try to replace an interface name with the name "Global," you are actually creating an interface-specific access rule that uses a policy object named Global.
- Rule Combiner—Interface-specific and global rules are never combined.

Related Topics

- Understanding Access Rules, page 16-1
- Understanding Device Specific Access Rule Behavior, page 16-4
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5
- Configuring Access Rules, page 16-7
- Moving Rules and the Importance of Rule Order, page 12-19

Understanding Device Specific Access Rule Behavior

If you do not create an access rule policy, the following is the default behavior based on the type of device, and what happens when you create an access rule:

- IOS devices—Permit all traffic through an interface.

  When you create an access rule permitting source A to destination B without configuring TCP/UDP inspection on the inspection rule table, or configuring the **established** advanced option on the rule, the device permits any packet from A to B. However, for any returning packet from B to A, the packet is not allowed, unless there is a corresponding access rule permitting that packet. If you configure TCP/UDP inspection on the traffic the inspection rule table, a rule permitting B to A is not needed in the access rule, as any returning packet from B to A automatically passes the device.
- ASA and PIX devices—Permit traffic from a higher-security interface to a lower-security interface. Otherwise, all traffic is denied.

If an access rule allows TCP/UDP traffic in one direction, the appliance automatically allows return traffic (you do not need to configure a corresponding rule for the return traffic), except for ICMP traffic, which does require a return rule (where you permit the reverse source and destination), or you must create an inspection rule for ICMP.

- FWSM devices—Deny all traffic entering an interface, permit all traffic leaving an interface.

  You must configure access rules to allow any traffic to enter the device.

If you create any rules for an interface for any type of device, the device adds an implicit **deny any** rule at the end of the policy. It is a good practice for you to add this rule yourself so that you remember it is there. Adding the rule also allows you to get hit count information for the rule. For more information, see Viewing Hit Count Details, page 16-37.

Tip When you create the access rule policy, ensure that you include a rule that will permit access to the device from the Security Manager server, or you will not be able to manage the device using the product.

Related Topics

- Understanding Access Rules, page 16-1
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5

Understanding Access Rule Address Requirements and How Rules Are Deployed

One of the complexities of creating access control lists using the operating system commands on the command line interface (CLI) is the fact that different operating systems have different IP address formats for source and destination addresses.

For example, Cisco IOS Software requires that you enter addresses using wildcard masks instead of subnet masks. To create a rule for the 10.100.10.0/24 network (subnet mask 255.255.255.0), you are required to enter the address as 10.100.10.0 0.0.0.255. The 0 and 1 have the reverse meaning in a wildcard mask that they have in a subnet mask. In ASA, PIX, and FWSM software, however, you use subnet masks, so you enter 10.100.10.0 255.255.255.0.

Security Manager simplifies addressing requirements for access rules: you always use the subnet mask. You are not even allowed to enter a wildcard mask. When you deploy the access rules to a device, Security Manager considers the operating system of the device and converts subnet masks to wildcard masks automatically when needed.

This makes it possible for you to create shared rules based on logical policies and to apply those rules to all of your devices. For example, there might be a set of access rules that you want all devices to use, in which case you can create the shared policy and assign it as the inherited policy for all devices. You do not have to worry about defining rules using the “right” syntax for the device type. You can use the same network/host objects that you use in other types of policies to identify targeted hosts and networks.

The specific CLI commands generated in deployed configurations are also based on the type of device. For IOS devices, the **ip access-list** command is used. For ASA, PIX, FWSM devices, the **access-list** or **ipv6 access-list** command is used and the **access-group** command binds it to the interface. With ASA, PIX, FWSM, and IOS 12.4(20)T+ devices, if you use network/host objects to identify the source or destination addresses for a rule, the **object-group** command is used to create object groups for those network/host objects. Object groups are also created for service objects.

Tips

- Because you can use network/host objects to identify a source or destination, and you can configure deployment optimization for rules, there is not always a one-to-one relationship between an access rule and ACEs in the CLI definition of an ACL.
- All access lists created from firewall rules are extended access lists (rather than standard). Security Manager applies a system-generated name to the ACL unless you specify a name for the ACL on the Access Control Settings Page, page 16-24. The name applies to the ACL that includes all of the rules related to the interface and direction for which the name is defined.
- There are several deployment options that control how object groups are deployed. This topic describes the default behavior. On the Deployment Page, page 11-13 (select **Tools > Security Manager Administration > Deployment**), you can deselect the option to create object groups from network/host objects. You can also optimize object groups during deployment (see Optimizing Network Object Groups When Deploying Firewall Rules, page 12-35), create new object groups from rules with multiple services or source and destination addresses, or remove unused object groups.
- The deployment options also include settings that control the names of ACLs generated from access rules and how many ACLs are created. By default, Security Manager creates a unique ACL for each interface, even if this means that several duplicate ACLs are created.

  If you select **Enable ACL Sharing for Firewall Rules**, Security Manager can create a single ACL and apply it to multiple interfaces, thus avoiding the creation of unnecessary duplicate ACLs. However, ACL sharing occurs only if it can be done while preserving your ACL naming requirements:

  - If you specify an ACL name for an interface and direction, that name is always used, even if it means a duplicate ACL must be created. For more information, see Configuring Settings for Access Control, page 16-23.
  - If you select **Reuse existing names** for the Firewall Access-List Names property, the existing names are preserved (unless you override them in the access control settings policy). This means that you might end up with duplicate ACLs under different names if duplicate ACLs already exist on the device.

  Tip: To maximize ACL sharing, ensure that you select **Reset to CS-Manager Generated Names** for the Firewall Access-List Names property, select **Speed** for the Optimize the Deployment of Access Rules For property, and that you do not configure ACL names in the access control settings policy.

  For more detailed information about the **Enable ACL Sharing for Firewall Rules** property, see Deployment Page, page 11-13.
- IPv4 and IPv6 ACLs cannot have the same name.

Related Topics

- Understanding Access Rules, page 16-1
- Configuring Access Rules, page 16-7
- Configuring Settings for Access Control, page 16-23
- Expanding Object Groups During Discovery, page 12-35

Configuring Access Rules

Access rules policies define the rules for allowing traffic to pass through an interface. If you do not configure an access rules policy, the device behavior differs based on device type as explained in Understanding Device Specific Access Rule Behavior, page 16-4.

Note Prior to the release of Security Manager 4.4 and versions 9.0 and later of the ASA, separate pages, policies and policy objects were provided for configuring IPv4 and IPv6 firewall rules and policies. With Security Manager 4.4 and ASA 9.0+, these policies and policy objects were "unified," meaning one set of rules in which you can use either IPv4 or IPv6 addresses, or a mixture of both. (See Policy Object Changes in Security Manager 4.4, page 1-10 for additional information.) However, for the earlier ASA versions, a separate page for IPv6 access rules is still provided in Device view, while in Policy view, IPv4 and unified versions of the access-rule policy types are provided. In addition, a utility that you can use to convert existing IPv4 policies is provided (see Converting IPv4 Rules to Unified Rules, page 12-28). The following descriptions apply to all versions of the access rule table, except where noted.

If you assign an IPv4 access-rule shared policy to a 9.0+ device, you will no longer be able to assign unified versions of those policies to that device. Likewise, if you assign a unified access-rule shared policy to a 9.0+ device, you will no longer be able to assign IPv4 versions of those shared policies to that device--the device will not be included in the list of available devices on the Assignments tab for the shared policy.

Before you configure access rules, consider the other types of firewall rules you will configure. Access rules are processed before all other types of rules except AAA rules. See the following topics for more information about things you should consider:

- Understanding Access Rules, page 16-1
- Understanding Global Access Rules, page 16-3
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5

Before You Begin

You might have a set of access rules that you want to apply to all devices. To do this, you can create a shared rule and inherit its rules to each device's access rules policy. For more information, see Creating a New Shared Policy, page 5-54 and Inheriting or Uninheriting Rules, page 5-47.

Related Topics

- Using Sections to Organize Rules Tables, page 12-20
- Copying Policies Between Devices, page 5-33
- Working with Shared Policies in Device View or the Site-to-Site VPN Manager, page 5-37
- Understanding Networks/Hosts Objects, page 6-80
- Understanding Interface Role Objects, page 6-73
- Understanding and Specifying Services and Service and Port List Objects, page 6-100

Step 1 Do one of the following to open the Access Rules Page, page 16-10:

- (Device view) Select **Firewall > Access Rules** (or **Firewall > Settings > IPv6 Access Rules**) from the Policies selector.

- (Policy view) Select **Firewall > Access Rules** (or **Firewall > Settings > IPv6 Access Rules**) from the Policy Type selector. Select an existing policy or create a new one.

Step 2 Select the row after which you want to create the rule and click the **Add Row** button or right-click and select **Add Row**. This opens the Add and Edit Access Rule Dialog Boxes, page 16-14.

Tip If you do not select a row, the new rule is added at the end of the local scope. You can also select an existing row and edit either the entire row or specific cells. For more information, see Editing Rules, page 12-10. Special rules apply if you mix interface-specific and global rules in a policy; for more information, see Understanding Global Access Rules, page 16-3.

Step 3 Configure the rule. Following are the highlights of what you typically need to decide while configuring your rule. For specific information on configuring the fields, see Add and Edit Access Rule Dialog Boxes, page 16-14.

- Permit or Deny—Whether you are allowing traffic that matches the rule or dropping it.
- Source and Destination addresses—If the rule should apply no matter which addresses generated the traffic or their destinations, use "All-Addresses" as the source or destination. If the rule is specific to a host or network, enter the addresses or network/host objects. For information on the accepted address formats, see Specifying IP Addresses During Policy Definition, page 6-87.
- Source and Destination Security Groups (ASA 9.0+ only)—You can specify TrustSec security groups used to filter traffic in addition to the source and destination addresses. See Selecting Security Groups in Policies, page 14-16, Configuring TrustSec-Based Firewall Rules, page 14-17 and Creating Security Group Objects, page 14-14 for more information about security groups.
- Source Users (ASA 8.4.2+ only)—You can further define the traffic source by specifying Active Directory (AD) user names (in the format NetBIOS_DOMAIN\username), user groups (NetBIOS_DOMAIN\\user_group), or identity user group objects that define the names and groups. The user specification is conjoined to the source address to limit the match to user addresses within the source address range. For more information, see Configuring Identity-Based Firewall Rules, page 13-21 and Creating Identity User Group Objects, page 13-19.
- Services—Use the IP service to apply to any traffic (for example, if you want to deny all traffic from a specific source). Otherwise, select the more specific service, which is a protocol and port combination, that you are targeting.
- Interfaces or Global—The interface or interface role for which you are configuring the rule, or Global to create global access rules on ASA 8.3+ devices (see Understanding Global Access Rules, page 16-3).
- Advanced settings—Click **Advanced** to open the Advanced dialog box for configuring additional settings. You can configure the following options; for detailed information, see Advanced and Edit Options Dialog Boxes, page 16-17.
  - Logging options. If you are using Security Manager or CS-MARS to monitor the device, ensure that you enable logging.
  - The direction of traffic to which this rule should apply (in or out). The default is in. You cannot change this setting for global rules.
  - The time range for the rule, which allows you to configure rules that work only for specific periods of time, such as during working hours. For more information, see Configuring Time Range Objects, page 6-71.
  - IOS device options for fragmentation and allowing the return of traffic for established outbound sessions.

– Rule expiration dates and notification settings. For more information, see Configuring Expiration Dates for Access Rules, page 16-22.

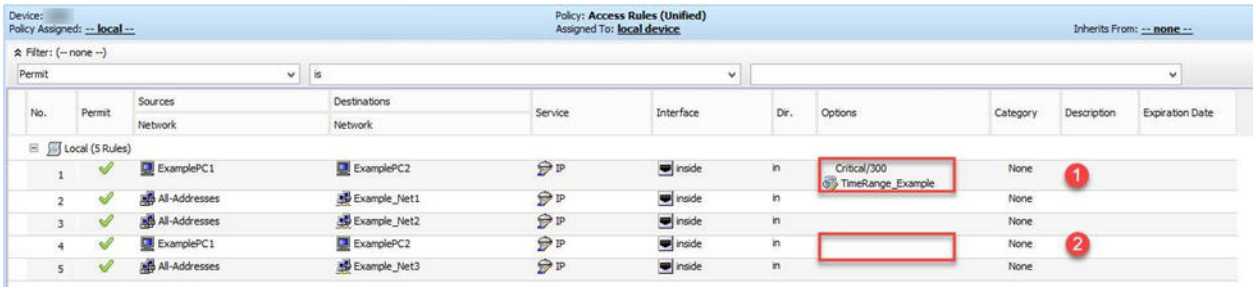
Step 4 Click **OK** when you are finished defining your rule.

Note You can enable conflict detection (see Enable Conflict Detection) to see if the new rule conflicts or overlaps with other rules. For more information, see Using Automatic Conflict Detection, page 16-28.

Note While adding or editing a rule, any two rules might become identical (example shown as 1 and 2 in Figure 16-1) except for differences in time range and/or logging values (defined in Advanced and Edit Options Dialog Boxes)—

- Cisco Security Manager deploys only the rule that is at the bottom (2 in Figure 16-1).
- Only rule (2) is used to identify configuration changes in preview configuration (see Previewing Configurations, page 8-44).
- If rule (2) has been deployed on the device, the preview configuration will not detect any changes.

Figure 16-1 Identical Rules



Step 5 If you are required to find the bottom rule (example, (2) in Figure 16-1), that prevents Cisco Security Manager from deployment of a top rule (1 in Figure 16-1), do the following:

a. Enable Conflict Detection for the device.

b. Generate Report for the conflicts found.

c. In the report, under the Rule No column, find the bottom rule (2), determine the rule number it conflicts with [rule (1)] and delete rule (1), if required.

Step 6 If you did not select the right row before adding the rule, select the new rule and use the up and down arrow buttons to position the rule appropriately. For more information, see Moving Rules and the Importance of Rule Order, page 12-19. There are special restrictions for moving rules when you mix interface-specific and global rules; see Understanding Global Access Rules, page 16-3.

Step 7 If you already have a large number of rules, consider analyzing and combining them before deploying the new rules. You can use the conflict detection tool to analyze your rules (see Using Automatic Conflict Detection, page 16-28). If analysis shows that you have a lot of redundant rules, right-click anywhere in

the rules table and choose **Combine Rules** to combine them. You can either allow Security Manager to evaluate all rules for combination, or just the rules you select before starting the rule combination tool. For more information, see Combining Rules, page 12-22.

Access Rules Page

Use the Access Rules page to configure access control rules for device interfaces. Access rules policies define the rules that allow or deny traffic to transit an interface. Typically, you create access rules for traffic entering an interface, because if you are going to deny specific types of packets, it is better to do it before the device spends a lot of time processing them. Access rules are processed before other types of firewall rules.

Note With the release of Security Manager 4.4 and versions 9.0 and later of the ASA, the separate policies and objects for configuring IPv4 and IPv6 access rules were "unified," meaning one set of access rules in which you can use either IPv4 or IPv6 addresses, or a mixture of both. (See Policy Object Changes in Security Manager 4.4, page 1-10 for additional information.) In Policy view, IPv4 and unified versions of the access policy type are provided. In addition, a utility that you can use to convert existing IPv4 policies is provided (see Converting IPv4 Rules to Unified Rules, page 12-28). The following descriptions apply to apply to all versions of the access rule table, except where noted.

Read the following topics before you configure access rules:

- Understanding Access Rules, page 16-1
- Understanding Global Access Rules, page 16-3
- Understanding Device Specific Access Rule Behavior, page 16-4
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5
- Configuring Access Rules, page 16-7

Tip Disabled rules are grayed out. When you deploy the configuration, disabled rules are removed from the device. For more information, see Enabling and Disabling Rules, page 12-20.

Navigation Path

To open the Access Rules page, do one of the following:

- (Device view) Select a device, then select **Firewall > Access Rules** (or **Firewall > Settings > IPv6 Access Rules**) from the Policies selector.
- (Policy view) Select **Firewall > Access Rules** (or **Firewall > Settings > IPv6 Access Rules**) from the Policy Type selector. Create a new policy or select an existing one.
- (Map view) Right-click a device and select **Edit Firewall Policies > Access Rules** (or **Edit Firewall Policies > IPv6 Access Rules**).

Related Topics

- Configuring Expiration Dates for Access Rules, page 16-22
- Configuring Settings for Access Control, page 16-23
- Adding and Removing Rules, page 12-9

- Editing Rules, page 12-10
- Enabling and Disabling Rules, page 12-20
- Moving Rules and the Importance of Rule Order, page 12-19
- Using Sections to Organize Rules Tables, page 12-20
- Using Rules Tables, page 12-8
- Filtering Tables, page 1-48

Field Reference

Note For details on the fields and user interface elements available as part of the automatic conflict detection feature, see Understanding the Automatic Conflict Detection User Interface, page 16-30.

Table 16-1 Access Rules Page

Element	Description
Expand all rows/Collapse all rows	Use these buttons to expand or collapse all sections in the rules table. **Note** The buttons are located in the upper-right corner of the Filter area above the access rules table.
Conflict Indicator icons	Identifies conflicts and provides a quick visual representation of the type of conflict. For more details, including types of conflicts and the actions you can take from this column, see Understanding the Automatic Conflict Detection User Interface, page 16-30.
No.	The ordered rule number.
Permit	Whether a rule permits or denies traffic based on the conditions set: • Permit—Shown as a green check mark. • Deny—Shown as a red circle with slash.
Sources	The sources of traffic for this rule; can be networks, security groups (ASA 9.0+ only), and users. Multiple entries are displayed on separate lines within the table cell.
Destinations	The destinations for this rule; can be networks and security groups (ASA 9.0+ only). Multiple entries are displayed on separate lines within the table cell.
Service	The services or service objects that specify the protocol and port of the traffic to which the rule applies. Multiple entries are displayed on separate lines within the table cell. See Understanding and Specifying Services and Service and Port List Objects, page 6-100.

Table 16-1 Access Rules Page (continued)

Element	Description
Hit Count	Number of times this rule has been "hit"; that is, number of times it has permitted or denied traffic; it is actually the sum of the hit counts for all accesss control entries (ACEs) created by the rule. This information is useful in debugging the deployed policies. Use the Refresh Hit Count button at the bottom of this page to update the hit information; opens the Hit Count Selection Summary Dialog Box, page 16-20. **Note** The Hit Count of a duplicated ACE, either within the same rule or different rules, is always set to 0. You can right-click this cell and choose Show Hit Count Details to open the Hit Count Details pane at the bottom of the Configuration Manager window. See Viewing Hit Count Details, page 16-37 for more information.
Last Hit Time	Timestamp for the most-recent hit.
Interface	The interfaces or interface roles to which the rule is assigned. Interface role objects are replaced with the actual interface names when the configuration is generated for each device. Multiple entries are displayed on separate lines within the table cell. See Understanding Interface Role Objects, page 6-73. For ASA 8.3+ devices, global rules are indicated with the name **Global** and a special icon to distinguish them from rules that use interface or interface role names (for an explanation of the icons, see Specifying Interfaces During Policy Definition, page 6-76).
Dir.	The direction of the traffic to which this rule applies: • In—Packets entering the interface. • Out—Packets exiting the interface.
Options	Any additional options configured for the rule. These include logging, time range, and some additional IOS rule options. See Advanced and Edit Options Dialog Boxes, page 16-17.
Category	The category assigned to the rule. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Description	The description of the rule, if any.
Expiration Date	The date on which the rule expires. Expired rules show **Expired** in bold text. Expired rules are not automatically deleted.
Last Ticket(s)	Shows the ticket(s) associated with last modification to the rule. You can click the ticket ID in the Last Ticket(s) column to view details of the ticket and to navigate to the ticket. If linkage to an external ticket management system has been configured, you can also navigate to that system from the ticket details (see Ticket Management Page, page 11-72).
Page elements below the rules table	

Table 16-1 Access Rules Page (continued)

Element	Description
Enable conflict detection Generate Report (neither option presented on the IPv6 Access Control page)	Enable or disable automatic conflict detection. This feature is enabled by default and the setting is managed per user. Disabling conflict detection for one access rules table will also disable the feature for other access rules tables. You can disable conflict detection while creating your rule table or making large modifications and then re-enable it when you are ready to verify your changes. See Using Automatic Conflict Detection, page 16-28. **Note** For details on the fields and user interface elements available as part of the automatic conflict detection feature, see Understanding the Automatic Conflict Detection User Interface, page 16-30. If conflict detection is enabled, you can click the **Generate Report** button to create an HTML report of any rule conflicts detected. This report can be printed or exported to another application.
Refresh Hit Count (not presented on the IPv6 Access Control page)	Click this button to update the hit information displayed in the table; opens the Hit Count Selection Summary Dialog Box, page 16-20.
Query (not presented on the IPv6 Access Control page)	Click this button to run a policy query, which can help you evaluate your rules and identify ineffective rules. See Generating Policy Query Reports, page 12-28
Find and Replace button (binoculars icon)	Click this button to search for various types of items within the table and to optionally replace them. See Finding and Replacing Items in Rules Tables, page 12-16.
Up Row and Down Row buttons (arrow icons)	Click these buttons to move the selected rules up or down within a scope or section. For more information, see Moving Rules and the Importance of Rule Order, page 12-19.
Add Row button	Click this button to add a rule to the table after the selected row using the Add and Edit Access Rule Dialog Boxes, page 16-14. If you do not select a row, the rule is added at the end of the local scope. For more information about adding rules, see Adding and Removing Rules, page 12-9.
Edit Row button	Click this button to edit the selected rule. You can also edit individual cells. For more information, see Editing Rules, page 12-10.
Delete Row button	Click this button to delete the selected rule.

Right-click Menu

A right-click menu is also available. This menu provides access to many of the functions listed above; the options presented depend on the location right-clicked:

- If you right-click a rule in the table, the options may include editing functions relative to the specific table cell right-clicked. For example, the command “Show Hit Count Details” is included when you right-click a Hit Count cell. See Editing Rules, page 12-10 for more information.

- You can also navigate from a rule to events associated with that rule in either Event Viewer or CS MARS. For more information, see Viewing Events for an Access Rule, page 69-56 and Viewing CS-MARS Events for an Access Rule, page 72-44.
- The Import Rules and Combine Rules options are also included in the right-click menu. See Importing Rules, page 16-41 and Combining Rules, page 12-22 for more information about these options.

Add and Edit Access Rule Dialog Boxes

Use the Add and Edit Access Rule dialog boxes to add and edit security-device access rules.

Note With the release of Security Manager 4.4 and versions 9.0 and later of the ASA, the separate pages for configuring IPv4 and IPv6 access rules were unified. However, for the earlier ASA versions, a separate page for IPv6 access rules is still provided. The following descriptions apply to apply to all versions of the page, except where noted.

Read the following topics before you configure access rules:

- Understanding Access Rules, page 16-1
- Understanding Global Access Rules, page 16-3
- Understanding Device Specific Access Rule Behavior, page 16-4
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5
- Configuring Access Rules, page 16-7

Navigation Path

On the Access Rules Page, page 16-10, click the **Add Row** button or select a row and click the **Edit Row** button.

Note Prior to Cisco Security Manager 4.13, the **Add Access Rule** dialog was populated with default values. Starting from 4.13, the user can customize the appearance of default values by updating the **csm.properties** file. For more information, see Customizing defaults in the Add Access Rule dialog, page 16-49

Related Topics

- Configuring Expiration Dates for Access Rules, page 16-22
- Editing Rules, page 12-10
- Adding and Removing Rules, page 12-9
- Importing Rules, page 16-41
- Understanding Networks/Hosts Objects, page 6-80
- Understanding and Specifying Services and Service and Port List Objects, page 6-100

Field Reference

Table 16-2 Add and Edit Access Rule Dialog Boxes

Element	Description
Enable Rule	Check this box to enable this rule, which means the rule becomes active when you deploy the configuration to the device. Deselect to disable the rule while keeping the rule definition. Disabled rules are shown overlaid with hash marks in the rule table. See Enabling and Disabling Rules, page 12-20 for more information.
Action	Whether the rule permits or denies traffic based on the conditions you define.

Table 16-2 Add and Edit Access Rule Dialog Boxes (continued)

Element	Description
Sources	Provide traffic sources for this rule; can be networks, security groups, and users. You can enter values or object names, or Select objects, for one or more of the following types of sources: • Network – You can specify a various network, host and interface definitions, either individually or as objects. If you Select an interface object as a source, the dialog box displays tabs to differentiate between hosts/networks and interfaces. The "All-Address" objects do not restrict the rule to specific hosts, networks, or interfaces. These addresses are IPv4 or IPv6 addresses for hosts or networks, network/host objects, interfaces, or interface roles. **Note** You can only specify a fully qualified domain name (FQDN) by providing an FQDN network/host object, or a group object that includes an FQDN object. You cannot directly type in an FQDN. See Understanding Networks/Hosts Objects, page 6-80, Specifying IP Addresses During Policy Definition, page 6-87 and Understanding Interface Role Objects, page 6-73 for additional information about these definitions. • Security Groups (ASA 9.0+) – Enter or Select the name or tag number for one or more source security groups for the rule, if any. See Selecting Security Groups in Policies, page 14-16, Configuring TrustSec-Based Firewall Rules, page 14-17 and Creating Security Group Objects, page 14-14 for more information about security groups. • Users – Enter or Select the Active Directory (AD) user names, user groups, or identity user group objects for the rule, if any. You can enter any combination of the following: – Individual user names: NetBIOS_DOMAIN\username – User groups (note the double \): NetBIOS_DOMAIN\\user_group – Identity user group object names. For more information, see: – Selecting Identity Users in Policies, page 13-21 – Configuring Identity-Based Firewall Rules, page 13-21 – Creating Identity User Group Objects, page 13-19 **Note** Enter more than one value in any of these fields by separating the items with commas. Each specification is combined with any others to limit traffic matches to only those flows that include all definitions. For example, specified user traffic originating from within a specified source address range.

Table 16-2 Add and Edit Access Rule Dialog Boxes (continued)

Element	Description
Destinations	Provide traffic destinations for this rule; can be networks or security groups. As with Sources, you can enter values or object names, or Select objects, for one or more destinations of Network and Security Group (ASA 9.0+) type.
Services	The services that define the type of traffic upon which to act. You can enter or Select any combination of service objects and service types (which are typically a protocol and port combination). Enter more than one value by separating the items with commas. For complete information on how to specify services, see Understanding and Specifying Services and Service and Port List Objects, page 6-100.
Interfaces Global (ASA 8.3+)	Specify whether you are creating an interface-specific or global rule. Global rules are available only for ASA 8.3+ devices, and are handled according to special rules (for detailed information, see Understanding Global Access Rules, page 16-3). If you select **Interfaces**, enter or Select the name of the interface or the interface role to which the rule is assigned, or click **Select** to select the interface or role from a list. An interface must already be defined to appear on the list. For bridge groups in routed mode, you can create access rules for both the Bridge Virtual Interface (BVI) and each bridge group member interface. Interface role objects are replaced with the actual interface names when the configuration is generated for each device. See Understanding Interface Role Objects, page 6-73. Global rules are created as a special global ACL that is not attached to specific interfaces, but are processed for all interfaces in the In direction after interface-specific rules.
Description	An optional description of the rule (up to 1024 characters).
Category	The category assigned to the rule. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.
Advanced button	Click this button to configure other settings for the rule, including logging configuration, traffic direction, time ranges, and rule expiration dates. For more information, see Advanced and Edit Options Dialog Boxes, page 16-17.

Advanced and Edit Options Dialog Boxes

Use the Advanced dialog box to configure additional settings for an access rule. These settings are displayed in three different cells of the access-rule table: direction, options, and rule expiration. You can then edit those settings directly by right-clicking the appropriate cell.

Note With the release of Security Manager 4.4 and versions 9.0 and later of the ASA, the separate pages for configuring IPv4 and IPv6 access rules were unified. However, for the earlier ASA versions, a separate page for IPv6 access rules is still provided. The following descriptions apply to apply to all versions of the page, except where noted.

Navigation Path

To access the Advanced dialog box:

- In the Add and Edit Access Rule Dialog Boxes, page 16-14, click the **Advanced** button.

To access one of the Edit options dialog boxes:

- Right-click the Options or Expiration Date cell in an access rule (on the Access Rules Page, page 16-10) and choose the related Edit command. To change the rule direction, right-click the Dir. cell and choose the opposite direction (in or out).

  If you select multiple rows, your changes replace those options for all selected rules.

Related Topics

- Configuring Access Rules, page 16-7
- Editing Rules, page 12-10
- Understanding Access Rules, page 16-1
- Chapter 16, “Managing Firewall Access Rules”
- Configuring Time Range Objects, page 6-71

Field Reference

Table 16-3 Advanced Dialog Box

Element	Description
Enable Logging (PIX, ASA, FWSM)	Whether to generate syslog messages for the rule entries (also known as access-control entries, or ACEs), for PIX, ASA, and FWSM devices. When selected, these additional options are enabled: • Default Logging—Use the default logging behavior. If a packet is denied, message 106023 is generated. If a packet is permitted, no syslog message is generated. The default logging interval is 300 seconds. • Per ACE Logging—Configure logging specific to this entry. Choose the logging Level you want to use to log events for the ACE, and provide a logging Interval, which can range from 1 to 600 seconds. Syslog message 106100 is generated for the ACE. Available logging levels: – Emergency—(0) System is unstable – Alert—(1) Immediate action is needed – Critical—(2) Critical conditions – Error—(3) Error conditions – Warning—(4) Warning conditions – Notification—(5) Normal but significant condition – Informational—(6) Informational messages only – Debugging—(7) Debugging messages **Note** You can change the firewall and IOS logging options for an existing rule in the table on the Access Rules Page, page 16-10 by right-clicking the Options cell and choosing Edit Options.
Enable Logging (IOS) Log Input (IPv4 only; neither option presented on the IPv6 Access Control page)	Whether to generate an informational logging message about the packet that matches the entry; the message will be sent to the console for IOS devices. Select Log Input to include the input interface and source MAC address or virtual circuit in the logging output.
Traffic Direction	For interface-specific access rules, the direction of the traffic to which this rule applies: • In—Packets entering an interface. • Out—Packets exiting an interface. **Note** You can change the direction for an existing rule in the table on the Access Rules Page, page 16-10 by right-clicking the Dir. cell and choosing the opposite direction. Global rules are always applied in the In direction, so you cannot change this setting when configuring a global rule.

Table 16-3 Advanced Dialog Box (continued)

Element	Description
Time Range	The name of a time range policy object that defines the times when this rule applies. The time is based on the system clock of the device. The feature works best if you use NTP to configure the system clock. Enter the name or Select the object. If the object that you want is not listed, click the Create button to create it. **Note** Time range is not supported on FWSM 2.x or PIX 6.3 devices.
Options (IOS) (IPv4 only; not presented on the IPv6 Access Control page)	Additional options for IOS devices: • none—Do not apply. • Fragment—Allow fragmentation, which provides additional management of packet fragmentation and improves compatibility with NFS. By default, a maximum of 24 fragments is accepted to reconstruct a full IP packet. However, based on your network security policy, you might want to consider configuring the device to prevent fragmented packets from traversing the firewall. • Established—Allow outbound TCP connections return access through the device. This option works with two connections: an original connection outbound from a network protected by the device, and a return connection inbound between the same two devices on an external host.
Rule Expiration	Lets you configure an expiration date for the rule. Click the calendar icon to select a date. For more information, see Configuring Expiration Dates for Access Rules, page 16-22. If you configure an expiration date, you can also configure the number of days before the rule expires to send out a notification of the pending expiration, and e-mail addresses to which to send the notifications. These fields are initially filled with the information configured on the Rule Expiration administrative settings page (select **Tools > Security Manager Administration > Rule Expiration**). You can change these options for an existing rule in the table on the Access Rules Page, page 16-10 by right-clicking the Expiration Date cell and choosing Edit Rule Expiration. **Note** Expired rules are not automatically deleted. You must delete them yourself and redeploy the configuration to the device.

Hit Count Selection Summary Dialog Box

Use the Hit Count Selection Summary dialog box to select the rules for which you want to refresh hit count information. Your options are limited by the rules you selected before clicking the Refresh Hit Count button. When you click OK in this dialog box, updated hit count information is obtained from the device, which can take some time, so you are given the option to abort the operation.

Note The Hit Count of a duplicated ACE, either within the same rule or different rules, is always set to 0.

Tip You can view detailed hit count information for a rule by right-clicking the Hit Count cell for that rule on the Access Rules Page, page 16-10. Detailed hit count information is displayed in the Hit Count Details window, as described in Viewing Hit Count Details, page 16-37.

Navigation Path

(Device view only) On the Access Rules Page, page 16-10, select one access rule in the table for which you want detailed hit count information, then right-click the Hit Count column and choose Show Hit Count Details.

Related Topics

- Viewing Hit Count Details, page 16-37
- Understanding Access Rules, page 16-1

Field Reference

Table 16-4 Hit Count Selection Summary Dialog Box

Element	Description
Policy Selected	Identifies the selected policy. If you do not select a policy, this is Local, which means the rules defined specifically for the device. The policy might also be a scope within a shared or inherited policy. The indication in this field does not actually limit the scope of your hit count report.
Rules Selected	The rules for which you want to obtain hit count details; choose: • Select the **rules** option to obtain information for only those rules you selected. You can select the rows related to the name of a scope, a section name, multiple individual rules, or create a filter and select all filtered rules. This is the default if any row is selected when you initiate the hit count report. • Select **All Rules** to get hit counts for all inherited, shared, and local rules. The option is not restricted to the scope indicated in the Policy Selected field. This is the only available option if you do not select any rules before initiating the hit count report.

Table 16-4 Hit Count Selection Summary Dialog Box (continued)

Element	Description
Fetch Data From	Select one of the following options and then click **Refresh Hit Count**: • Device—Security Manager fetches the Hit Count information from the device and displays the same on the Access Rules policy page. Beginning from version 4.9, Security Manager stores the Hit Count information in its database for ASA and ASASM devices. • History—Security Manager fetches the latest Hit Count information for the particular ACEs from its database (the Hit Count history) and displays the same on the Access Rules policy page. **NOTE:** If there is an open activity the Hit Count data will not be persisted in the Security Manager database. This feature is supported in IPv4 Access Rules starting from ASASM/ASA version 8.3 and Unified Access Rules starting from ASASM/ASA version 9.0. If the Fetch Data From Device is based on Rules Selected option, the Hit Count persistence support will not be enabled. The support of Hit Count persistence will be enabled only if you choose the All Rules option within Fetch Data from Device. While fetching data From history, if the value of Hit Count is zero, Security Manager checks whether the rule was hit earlier based on the Hit Count History of the rule and displays its corresponding values. If Security Manager is not able to find the values of previous Hit from History, it displays the value of Hit Count as zero.

Configuring Expiration Dates for Access Rules

A frequent use of access rules is to provide temporary access to a network. For example, you might configure an access rule to allow a partner access for the duration of a specific project. Ideally, you want to remove the access rule at the completion of the project. However, as access rule lists grow, it is hard to manage them and to remember which rules were meant to be temporary.

To help you deal with this problem, you can configure expiration dates for access rules. By configuring an expiration date, you can project when you believe the rule will no longer be needed.

Expiration dates are not hard and fast dates; Security Manager does not delete rules that reach their expiration date. Instead, when an expiration date is reached, Security Manager displays “Expired” in bold letters in the Expiration Date column for the rule. You can filter the access rules page based on the expiration date field, for example, filtering for “expiration date has passed” to see all expired rules.

If the rule is no longer needed, you can delete it (right-click and select **Delete Row**), or disable it (right-click and select **Disable**), and then redeploy the configuration to the device. You might want to initially disable the rule, which leaves the rule in the table (overlain with hash marks), in case you discover the rule really was still needed after all, saving you the time of recreating the rule. You then just need to re-enable the rule (right-click and select **Enable**) and redeploy the configuration.

When you configure an expiration date, you can also configure notification settings, specifying an e-mail address that should be notified when an expiration date is approaching. You can specify how many days before the expiration date to send the notification e-mail message to allow you time to evaluate the rule.

The notification settings are initially filled with the values configured in the administration settings (select **Tools > Security Manager Administration > Rule Expiration**); you can enter different settings for a given rule.

To configure rule expiration:

- When creating a new rule, or editing an entire rule, click the Advanced button in the Add and Edit Access Rule Dialog Boxes, page 16-14 to get to the rule expiration settings.
- For existing rules, you can add or edit expiration settings without editing the entire rule. Right-click the Expiration Date cell for the rule and select **Edit Rule Expiration**. You can select multiple rows to configure the same rule expiration settings. For more information, see Advanced and Edit Options Dialog Boxes, page 16-17.

Related Topics

- Rule Expiration Page, page 11-69
- Configuring Access Rules, page 16-7

Configuring Settings for Access Control

You can configure various settings that apply to security-device access control lists. These settings work in conjunction with your access rules policy. The main setting of interest is that you can configure your own ACL names for each interface/traffic direction combination, or for the global ACL on ASA 8.3+ devices. For PIX, ASA, and FWSM devices, you can also control the maximum number of concurrent flows and the related syslog interval.

You can also configure an interface to allow per-user downloadable ACLs for PIX, ASA, and FWSM devices. This allows you to configure user-based ACLs in your AAA server to override the ACLs defined on a device.

Note With the release of Security Manager 4.4 and versions 9.0 and later of the ASA, the separate pages for configuring IPv4 and IPv6 access control were unified. However, for the earlier ASA versions, a separate page for IPv6 settings is still provided. The following descriptions apply to apply to all versions of the page, except where noted.

Related Topics

- Configuring Access Rules, page 16-7

Step 1 Do one of the following to open the Access Control Settings Page, page 16-24:

- (Device view) Select **Firewall > Settings > Access Control** (or **Firewall > Settings > IPv6 Access Control**) from the Policies selector.
- (Policy view) Select **Firewall > Settings > Access Control** (or **Firewall > Settings > IPv6 Access Control**) from the Policy Type selector. Select an existing policy or create a new one.

Step 2 Configure the global settings in the top part of the page. For PIX, ASA, and FWSM devices, you can define the maximum number of concurrent deny flows and the related syslog interval. For ASA 8.3+ devices, you can enable object group search to optimize ACL performance when converting from Checkpoint, but this setting is not recommended unless you have a memory-constrained device. (Not available on the IPv6 Access Control page.)

For specific information about these settings, and the platforms that support ACL compilation, see Access Control Settings Page, page 16-24.

Step 3 For each interface on which you want to configure an ACL name, or enable per-user ACLs, add the interface to the interfaces table by clicking the **Add Row** button beneath the table and filling in the Firewall ACL Setting Dialog Box, page 16-26. Keep the following in mind:

- If you configure an ACL name, the name is applied to the specific interface and direction. Security Manager creates system-generated names for any interface/direction combinations that you do not specifically name.
- You can also specify the name of the global ACL for ASA 8.3+ devices.

You can edit existing entries in the list by selecting them and clicking **Edit Row**, or delete them by clicking **Delete Row**.

Access Control Settings Page

Use the Access Control Settings page to configure settings to use in conjunction with your access rules policy. You can control some performance and logging features, and configure ACL names for individual interfaces.

Note With the release of Security Manager 4.4 and versions 9.0 and later of the ASA, the separate policies and objects for configuring IPv4 and IPv6 access control were "unified," meaning one set of rules in which you can use either IPv4 or IPv6 addresses, or a mixture of both. However, for the earlier ASA versions, a separate page for IPv6 settings is still provided. (See Policy Object Changes in Security Manager 4.4, page 1-10 for additional information.) The following descriptions apply to apply to all versions of the page, except where noted.

Thus, many of these settings apply only to specific device types or software versions. If you configure an option and apply the policy to unsupported device types, the option is ignored for those unsupported devices.

Navigation Path

To open the Access Control Page, do one of the following:

- (Device view) Select a device, then select **Firewall > Settings > Access Control** (or **Firewall > Settings > IPv6 Access Control**) from the Policies selector.
- (Policy view) Select **Firewall > Settings > Access Control** (or **Firewall > Settings > IPv6 Access Control**) from the Policy Type selector. Create a new policy or select an existing policy.
- (Map view) Right-click a device and select **Edit Firewall Settings > Access Control** (or **Edit Firewall Settings > IPv6 Access Control**).

Related Topics

- Configuring Settings for Access Control, page 16-23
- Understanding Access Rules, page 16-1
- Understanding Device Specific Access Rule Behavior, page 16-4
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5
- Understanding Access Rules, page 16-1

- Understanding Interface Role Objects, page 6-73

Field Reference

Table 16-5 Access Control Settings Page

Element	Description
Maximum number of concurrent flows (PIX, ASA, FWSM) (not presented on the IPv6 Access Control page)	The maximum number of concurrent deny flows that the device is allowed to create. Syslog message 106101 is generated when the device reaches the number. The range you should use depends on the amount of flash memory available in the device: • More than 64 MB—Values are 1-4096. The default is 4096. • More than 16 MB—Values are 1-1024. The default is 1024. • Less than or equal to 16 MB—Values are 1-256. The default is 256.
Syslog interval (PIX, ASA, FWSM) (not presented on the IPv6 Access Control page)	The interval of time for generating syslog message 106101, which alerts you that the security appliance has reached a deny flow maximum. When the deny flow maximum is reached, another 106101 message is generated if the specified number of seconds has passed since the last 106101 message. Values are 1-3600 milliseconds. The default is 300.
Enable Access List Compilation (Global) (IPv4 only; also not presented on the IPv6 Access Control page)	Whether to compile access lists, which speeds up the processing of large rules tables. Compilation optimizes your policy rules and performance for all ACLs, but is supported on a limited number of older platforms: • Routers (global configuration only): 7120, 7140, 7200, 7304, and 7500. • PIX 6.3 firewalls, in global mode or per interface. An ACL is compiled only if the number of access list elements is greater than or equal to 19. The maximum recommended number of entries is 16,000. To compile access lists, the device must have a minimum of 2.1 MB of memory. Access list compilation is also known as Turbo ACL.
Enable Object Group Search (ASA 8.3+) (not presented on the IPv6 Access Control page)	Whether to enable object group search on ASA 8.3+ devices, which optimizes ACL performance without expanding object groups. Object group search is mainly for use when migrating from Checkpoint to ASA, which can result in a large increase in the number of access rules, when you have a memory-constrained device (that is, you find during operations that memory runs low). If you enable object group search, you cannot use the Hit Count tool to analyze your rules. In most cases, you should not enable this feature. Instead, use the rule combination tool to simplify your access rules, and consider using global rules for rules you want to enforce on all interfaces.

Table 16-5 Access Control Settings Page (continued)

Element	Description
Enable Threshold Object Group Search (IPv4 only; also not presented on the IPv6 Access Control page)	Check this box to enable the threshold limit on object group search. By default the threshold is not enabled.
Access Control settings table	The table lists the interfaces for which you want to configure special processing. The interface name can be a specific interface or an interface role (which can apply settings to more than one interface at a time), or Global for global ACL settings on ASA 8.3+ devices. The main use of this table is to configure names for ACLs if you do not want Security Manager to configure system-generated names. The name applies to the ACL generated for an interface in a specific direction. You can also configure interface-level settings for per user downloadable ACLs, object group search, and ACL compilation. • To add an Access Control interface setting, click the Add Row button and fill in the Firewall ACL Setting Dialog Box, page 16-26. • To edit an Access Control interface setting, select it and click the Edit Row button. • To delete an Access Control interface setting, select it and click the Delete Row button.

Firewall ACL Setting Dialog Box

Use the Firewall ACL Setting dialog box to configure settings for specific interfaces, interface roles, or global rules for use with security-device access rules policies.

Navigation Path

Go to the Access Control Settings Page, page 16-24 and click the **Add Row** button below the interface table, or select a row in the table and click the **Edit Row** button.

Related Topics

- Configuring Settings for Access Control, page 16-23
- Understanding Access Rules, page 16-1
- Understanding Global Access Rules, page 16-3
- Understanding Device Specific Access Rule Behavior, page 16-4
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5
- Understanding Interface Role Objects, page 6-73

Field Reference

Table 16-6 Firewall ACL Setting Dialog Box

Element	Description
Interface Global (ASA 8.3+)	Specify whether you are configuring settings for specific interfaces (or interface roles), or for global rules on ASA 8.3+ devices. If you select **Interface**, specify the name of the interface or interface role for which you are configuring settings. Enter the name or click **Select** to select it from a list or to create a new object. If you select Global, your only option is to specify the name of the global ACL.
Traffic Direction	The direction of the traffic through the interface, In or Out. The settings you configure apply only to this direction, if direction matters. For global ACLs on ASA 8.3+ devices, the direction is always in.
User Defined ACL Name (checkbox not presented on the IPv6 Access Control page) ACL Name	Whether you want to supply the name for the ACL. If you select this option, enter the name you want to use, which is applied to the ACL generated for the interface and direction combination. The name must be unique on the device. If you are configuring the name for the global ACL on ASA 8.3+ devices, the option is automatically selected; simply enter the desired name. **Note** Make sure that the firewall rules ACL name is unique and is not the same name as the ACL object defined in the Policy Object Manager. For more information see Creating Access Control List Objects, page 6-53. If you do not configure a name, Security Manager generates a name for you.
Enable Per User Downloadable ACLs (PIX, ASA, FWSM) (not presented on the IPv6 Access Control page)	Whether to enable the download of per-user ACLs to override the ACLs on the interface. User ACLs are configured in a AAA server; they are not configured in Security Manager. If there are no per-user ACLs, the access rules configured for the interface are applied to the traffic. The option is configured on the device for the specified interface only when the Traffic Direction is in.
Enable Object Group Search (PIX 6.x) (not presented on the IPv6 Access Control page)	Whether to enable object group search on a PIX 6.x interface, which reduces the memory requirement on the device to hold large ACLs. However, object group search impacts performance by making ACL processing slower for each packet. Object group search is recommended when you have very large object groups. **Tip** If you are trying to configure object group search on ASA 8.3+ devices, the setting is on the Access Control Settings Page, page 16-24.

Table 16-6 Firewall ACL Setting Dialog Box (continued)

Element	Description
Enable Access List Compilation (PIX 6.x) (not presented on the IPv6 Access Control page)	Whether to compile access lists on this interface for PIX 6.x devices. This setting overrides the equivalent global setting that you configure on the Access Control Settings page. ACL compilation speeds the processing of large rules tables and optimizes your policy rules and performance for the interface. An ACL is compiled only if the number of access list elements is greater than or equal to 19. The maximum recommended number of entries is 16,000. To compile access lists, the device must have a minimum of 2.1 MB of memory.

Using Automatic Conflict Detection

Security Manager provides an Automatic Conflict Detection feature for access rules. You can use Automatic Conflict Detection to evaluate the logic of your access rules. When enabled, Automatic Conflict Detection identifies rules that overlap or conflict with other rules in the access rule policy. Use this information to identify rules that need to be deleted, moved, or edited.

This section contains the following topics:

Understanding Automatic Conflict Detection

Security Manager provides an automatic conflict detection feature to help identify unnecessary redundant or duplicate rules. Certain conflicting rules might have no effect on a device after they are deployed; however, they create unnecessary clusters in the rules table. By detecting these rules, you can clean up the rule set to develop an easier to use and more efficient access rules policy.

Other conflicting rules, can create unwanted results to your network. By detecting these conflicting rules, you can identify rules that need to be deleted, moved, or edited to implement your security needs as intended.

Note The conflict detection feature will report on the first conflict between two rules. If there are additional rules in the table that also conflict with a rule, they will not be reported until the first conflict is resolved.

Conflicts detected by Security Manager are categorized in the following way:

- Redundant Object—An element in a field of a rule is a subset of one or more elements in the same field of the rule. In the following example, the source cell has two network objects: *net-group2* and *net-group1*. Since *net-group2* is a sub-set of *net-group1*, it is a redundant object and can safely be removed:

```
object-group network net-group1
network-object 10.2.0.0 255.255.0.0

object-group network net-group2
```

```
network-object 10.2.1.1 255.255.255.255
```

- Redundant Rule—Two rules apply the same action to the same type of traffic, and removing the base rule would not change the ultimate result. For example, if a rule permitting FTP traffic for a particular network were followed by a rule allowing IP traffic for that same network, and there were no rules in between denying access, then the first rule is redundant and can be deleted.

  The following is a simple example of redundant rules:

  ```
  access-list acl permit ip 2.1.1.1 255.255.255.255 any
  access-list acl permit ip 2.1.1.0 255.255.255.0 any
  ```

- Partially Redundant Rule—A portion of a compound rule is redundant to a rule or a portion of a compound rule that follows it.
- Shadowed Rule—This is the reverse of a redundant rule. In this case, one rule will match the same traffic as another rule such that the second rule will never be applied to any traffic because it comes later in the access list. If the action for both rules are the same, you can delete the shadowed rule. If the two rules specify different actions for traffic, you might need to move the shadowed rule or edit one of the two rules to implement your desired policy. For example, the base rule might deny IP traffic, and the shadowed rule might permit FTP traffic, for a given source or destination.

  The following is a simple example of shadowed rules:

  ```
  access-list acl permit ip 1.0.0.0 255.0.0.0 any
  access-list acl permit ip 1.1.0.0 255.255.0.0 any
  ```

Note Duplicate rules are reported as shadowed rules by the automatic conflict detection feature.

- Partially Shadowed Rule—A portion of a compound rule is shadowed by a rule before it. If the action for both rules are the same, you can delete the portion of the rule that is shadowed. If the two rules specify different actions for traffic, you might need to move the shadowed rule or edit one of the two rules to implement your desired policy.

Scope of Automatic Conflict Detection

When detecting conflicts, Security Manager evaluates the following pieces of information in your access rules:

- source
- destination
- services
- users
- interfaces

Note Conflict detection is only available for access rules in the Access Rules policy for a device or shared policy. Conflict detection is not available for access rules that are part of other policies, such as AAA or inspection rules.

Note If a rule contains an FQDN network/host object, the FQDN object is ignored, but the rule is otherwise included in the analysis.

Note Disabled rules are not evaluated during conflict detection.

Note Conflict detection does not consider time ranges when evaluating access rules. Make sure that such rules truly conflict before removing any rules flagged during conflict detection.

Related Topics

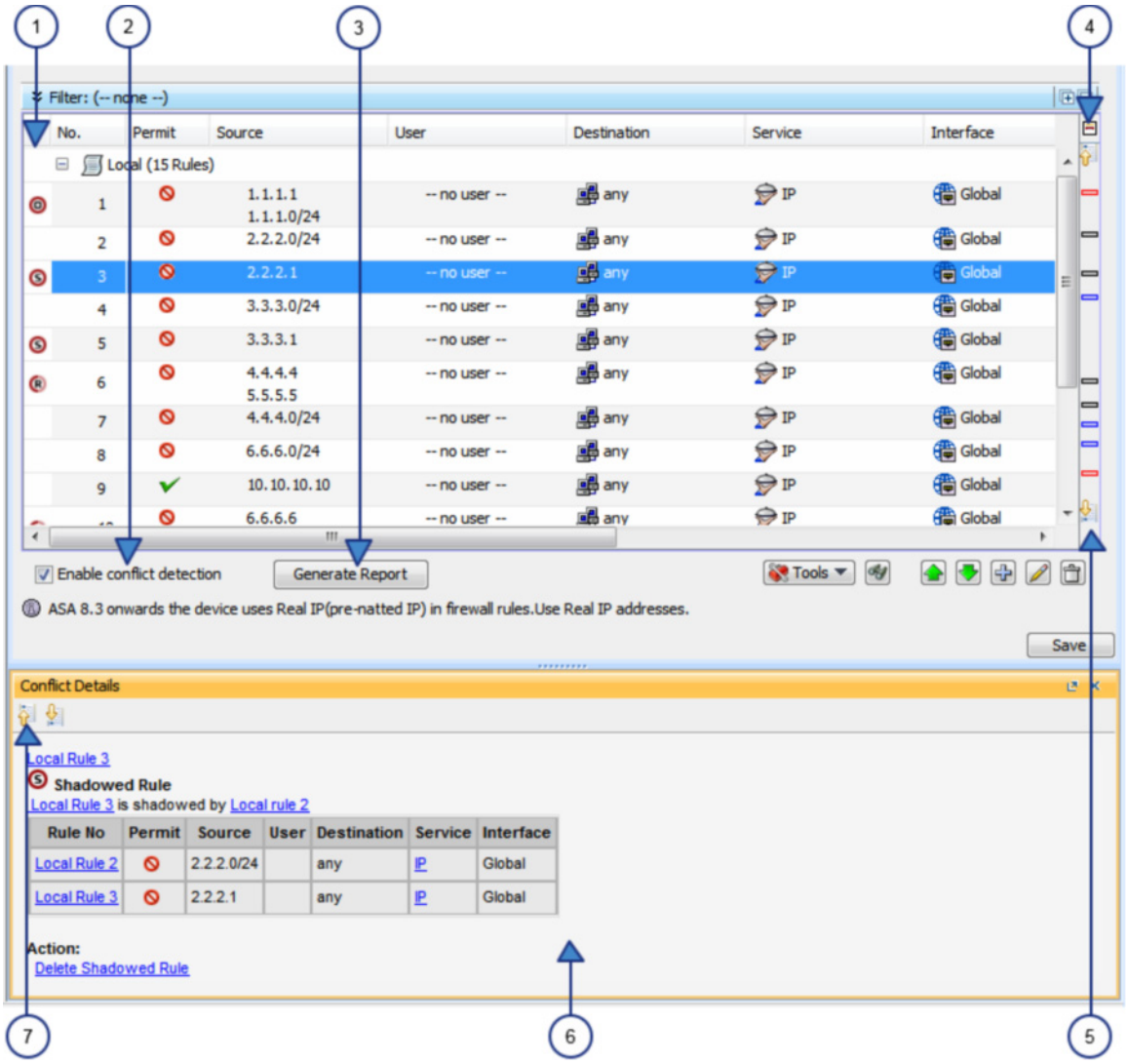
- Understanding the Automatic Conflict Detection User Interface, page 16-30
- Resolving Conflicts, page 16-35
- Understanding Access Rules, page 16-1
- Understanding Device Specific Access Rule Behavior, page 16-4
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5
- Configuring Access Rules, page 16-7

Understanding the Automatic Conflict Detection User Interface

The Automatic Conflict Detection feature is tightly coupled with the access rules table to make identifying conflicts and then resolving those conflicts faster and easier. When conflict detection is enabled, additional user interface elements are available for navigating between the conflicts and for resolving those conflicts.

Note For information on the standard elements of the Access Rules page, see Access Rules Page, page 16-10.

Figure 16-2 Automatic Conflict Detection



1	Conflict Indicator icons	**2**	Enable Conflict Detection
3	Generate Report button	**4**	Annotation Display Options
5	Conflict navigation bar	**6**	Conflict Details area
7	Conflict Navigation buttons		

Conflict Indicator Icons

The Conflict Indicator icons are used to identify conflicts and to provide a quick visual representation of the type of conflict. The following table details the available icons:

Note For an explanation of the types of conflicts, see Understanding Automatic Conflict Detection, page 16-28.

	Redundant Object
	Redundant Rule
	Partially Redundant Rule
	Shadowed Rule
	Partially Shadowed Rule

Note If an access rule has multiple conflicts or if it has a user note attached to it, the conflict indicator icon for that rule will have a small plus sign (+) on it.

You can perform the following actions using the Conflict Indicator icon:

- Hover the mouse pointer over the **Conflict Indicator** icon to view a description of the conflict including any user notes attached to the conflict.
- Click the **Conflict Indicator** icon, or right-click the icon and select **Show Conflict Detail**, to open the Conflict Details pane for the selected conflict.
- Right-click the **Conflict Indicator** icon for a redundant object and select **Remove Redundant Object** to remove the redundant object from a rule.
- Right-click the **Conflict Indicator** icon and select **Add User Note** to open the Add User Note dialog box for the selected conflict. You can use the Add User Note dialog box to enter a note about the conflict that can later be included in the Rule Analysis Detail Report.

  Note User notes are not saved when leaving the access rules page or after editing a rule that has a user note.

Enable Conflict Detection

The Enable Conflict Detection option controls whether automatic conflict detection is enabled. Conflict detection is enabled by default but can be disabled by deselecting this option. The setting is managed per user and enabling or disabling conflict detection for one access rules table, will also enable or disable the feature for other access rules tables.

Caution Conflict detection uses a significant memory size on the CSM client. The memory usage varies based on the number of rules in the policy or the device that is used. Enable the conflict detection functionality on the client UI, only if required. Also, ensure that the CSM client LAX file is configured with adequate memory, based on the system RAM size. By default, it is 2 GB. For example, try configuring the LAX file with 4 GB if the machine's RAM size is 8 GB and with 8 GB if the machine's RAM is 16 GB. It is, however, strongly recommended to configure the client LAX file matching the requirements of the environment.

Use the following parameters based on number of rules and devices requirements:

```
#    LAX.NL.JAVA.OPTION.JAVA.HEAP.SIZE.MAX
#    -------------------------------------
#    2420m
```

```
lax.nl.java.option.java.heap.size.max=2420m
```

Generate Report

If conflict detection is enabled, you can click the **Generate Report** button to create an HTML report of the conflicts that can be printed or exported to another tool. The Rule Analysis Detail Report shows details of all the conflicts in your rules table and includes any user notes that were entered for the conflicts. It does not use the settings you selected in the Annotation Display Options dialog box and does not consider the filter settings defined for the table.

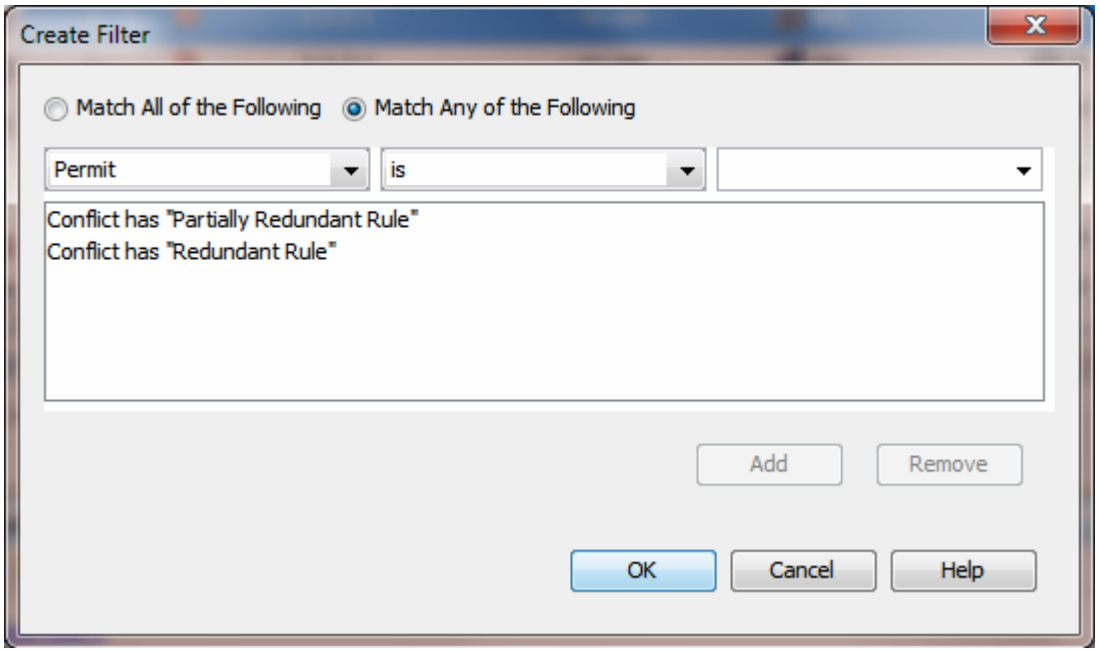
Note User notes are not saved when leaving the access rules page or after editing a rule that has a user note.

When you first open the Access Rules page, the Generate Report button is replaced with a progress bar. After conflict analysis has completed, the Generate Report button becomes available along with the other conflict detection features.

Annotation Display Options button

Click the **Annotation Display Options** button to open the Annotation Display Options dialog box, which is used for selecting the types of conflicts that should be reported. For an explanation of the types of conflicts, see Understanding Automatic Conflict Detection, page 16-28.

Disabling a certain type of conflict does not remove those rules from the access rules table; it only turns off the rule conflict notification for those types of conflicts. To hide or show only conflicting rules of a certain type, you can use the table filter feature. For example, if you only wanted to see redundant and partially redundant rule conflicts, you could set up the following advanced filter:



You can hover the mouse pointer over the Annotation Display Options button to view a summary of the conflicts for each type and also to see which conflict types are disabled.

Note The Annotation Display Options that you select remain in effect until those options are changed. Be sure to verify these settings whenever you are working on resolving conflicts.

Conflict Navigation Bar

Use the Conflict navigation bar to navigate to a conflict. You can use the Previous Conflict and Next Conflict buttons on the Conflict navigation bar to step through the conflicts. You can also click on one of the conflict locators in the Conflict navigation bar to move directly to a specific conflict. This is particularly helpful when working with large rules tables.

Tip Hovering over a conflict locator provides a quick summary of the conflict.

The conflict locators are color-coded as follows:

- **Red locators**—Redundant objects
- **Blue locators**—Redundant and partially redundant rules
- **Black locators**—Shadowed and partially shadowed rules

Conflict Details Area

The Conflict Details pane shows details for the selected conflict. The pane can be docked and undocked as needed. If the Conflict Details pane is docked while the Policy Object Manager pane is also docked, you can navigate between the two features using the tabs at the bottom of the window.

The conflicting rules are shown together in a table for easier direct comparison. The type of conflict is shown above the table. A suggested action is shown below the table for all conflicts except partially redundant rules and partially shadowed rules, which must be resolved manually. Links are provided for direct navigation to the rules involved. Policy objects that are part of the conflicting rules can be expanded by clicking on them to see the object contents. Click again to collapse the policy object.

You can use the links provided to navigate to the conflicting rules. You can also click the link under Action to have Security Manager perform the suggested action automatically.

Conflict Navigation Buttons

The Previous Conflict and Next Conflict buttons at the top of the Conflict Details pane allow you to step through the conflicts that need to be resolved without leaving the Conflict Details pane.

Related Topics

- Understanding Automatic Conflict Detection, page 16-28
- Resolving Conflicts, page 16-35
- Understanding Access Rules, page 16-1
- Understanding Device Specific Access Rule Behavior, page 16-4
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5
- Configuring Access Rules, page 16-7

Resolving Conflicts

The following procedure explains how to use the Automatic Conflict Detection feature to resolve conflicts in your access rules.

Tip You can use the Combine Rules tool to have Security Manager evaluate your rules and find ways to combine them into more efficient rules. For more information, see Combining Rules, page 12-22.

Related Topics

- Understanding Automatic Conflict Detection, page 16-28
- Understanding the Automatic Conflict Detection User Interface, page 16-30
- Understanding Access Rules, page 16-1
- Understanding Device Specific Access Rule Behavior, page 16-4
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 16-5
- Configuring Access Rules, page 16-7

Step 1 Do one of the following:

- (Device view) Select **Firewall > Access Rules** from the Policy selector.
- (Policy view) Select **Firewall > Access Rules** from the Policy Type selector and select an existing policy.

This opens the Access Rules Page, page 16-10. If conflict detection is enabled, the access rules will be analyzed for conflicts after the table has been loaded. If conflict detection is not enabled, select **Enable conflict detection** to begin the conflict analysis.

The analysis progress is shown below the rules table. With the exception of the conflict detection features, you can perform functions on the rules table while the rules are being analyzed. After analysis has completed, the conflict detection features are enabled.

Step 2 Make sure that the rules you are interested in analyzing are being shown in the rules table. This includes expanding sections and making sure that if you are using filters that they are set correctly. Any rules that are being filtered or are in a section that is collapsed will not be included in the conflict detection analysis.

Tip You can use the Expand all rows/Collapse all rows buttons located in the upper-right corner of the Filter area above the access rules table, to quickly expand or collapse all sections in the rules table.

Step 3 Click the **Annotation Display Options** button, which is located above the Conflict navigation bar to the right of the vertical scroll bar, to open the Annotation Display Options dialog box. Verify that the types of conflicts you want detected are all enabled, and then click **OK**.

Tip You can hover the mouse pointer over the Annotation Display Options button to view a summary of the conflicts for each type and also to see which conflict types are disabled.

Note The Annotation Display Options that you select remain in effect until those options are changed. Be sure to verify these settings whenever you are working on resolving conflicts.

Step 4 If you would like to print or save a copy of the conflicts that are found in the rule table, click **Generate Report**.

The Rule Analysis Detail Report is opened in your browser. The Rule Analysis Detail Report shows details of all the conflicts in your rules table. It does not use the settings you selected in the Annotation Display Options dialog box and does not consider the filter settings defined for the table. You can save the report or print it as needed.

Step 5 Use the Conflict navigation bar to navigate to a conflict. You can use the Previous Conflict and Next Conflict buttons on the Conflict navigation bar to step through the conflicts. You can also click on one of the conflict locators in the Conflict navigation bar to move directly to a specific conflict. This is particularly helpful when working with large rules tables.

Tip Hovering over a conflict locator provides a quick summary of the conflict.

The conflict locators are color-coded as follows:

- **Red locators**—Redundant objects
- **Blue locators**—Redundant and partially redundant rules
- **Grey locators**—Shadowed and partially shadowed rules

Step 6 Click on the **Conflict Indicator** icon for the selected conflict to open the Conflict Details pane. For more information on the Conflict Indicator icons, see Understanding the Automatic Conflict Detection User Interface, page 16-30.

The Conflict Details pane shows details for the selected conflict. The conflicting rules are shown together in a table for easier direct comparison. The type of conflict is shown above the table. A suggested action is shown below the table for all conflicts except partially redundant rules and partially shadowed rules, which must be resolved manually. Links are provided for direct navigation to the rules involved. Policy objects that are part of the conflicting rules can be expanded by clicking on them to see the object contents. Click again to collapse the policy object.

Step 7 Use the links provided to navigate to the rules and resolve the conflict as needed or click the link under Action to have Security Manager perform the suggested action automatically.

Note If you do not want to resolve the conflict at this time, you can enter a note about the conflict by right-clicking the **Conflict Indicator** icon to the left of the conflict in the access rule table and then selecting **Add User Note**. User notes are included in the Rule Analysis Detail Report, but are not saved when leaving the access rules page or after editing a rule that has a user note.

Step 8 Use the Conflict navigation bar or the **Previous Conflict** and **Next Conflict** buttons at the top of the Conflict Details pane to access additional conflicts that need to be resolved.

Step 9 If there are any remaining conflicts that you do not want to resolve at this time, you can click **Generate Report** to print or save a copy of the remaining conflicts, if desired.

Viewing Hit Count Details

Use Hit Count Details window to view information about the number of times an access rule was applied to traffic. These rules are the ones that become interface ACLs on the device. The hit count results do not show counts for any other type of ACL (for example, those used with class maps or AAA rules).

For access rules on ASA 8.3(1) devices and later, the detailed hit count report also shows the last time the access rule policy was applied to traffic. This information is helpful for determining rules that might have been superseded by other policy changes.

Use the hit count information to help you debug your access rules. The information can help you identify rules that are never hit (which might mean you do not need them, or that they are duplicates of rules higher in the ACL), and rules that are hit often (which means you might want to refine the rules).

Tip You can click the Refresh Hit Count button at the bottom of the page to update hit count information before viewing the details for a rule. See Hit Count Selection Summary Dialog Box, page 16-20 for more information.

Consider the following points when analyzing the hit count details:

- You get best results if you deploy policies to the device before viewing hit counts. If you discover a device and then generate a hit count report before deployment, the results might be incomplete or hard to interpret. For example, an access rule might not have any hit count information.
- Hit count statistics are based on ACL, not on interface. If you select **Enable ACL Sharing for Firewall Rules** on the Security Manager Administration Deployment page (see Deployment Page, page 11-13), any shared ACL provides statistics that are combined from all interfaces that share the ACL.
- If you enable network object group optimization, as described in Optimizing Network Object Groups When Deploying Firewall Rules, page 12-35, you might not get good hit count information.
- If you enable ACL optimization, as described in Optimizing Access Rules Automatically During Deployment, page 16-47, the hit count results might have problems matching ACEs from the device to access rules. Thus, when you select an access rule, you might not get any hit count results for it.
- FQDN network/host objects are ignored. You cannot obtain hit count information on these objects.
- Hit count and last hit time information is cleared when a device is restarted.
- The Hit Count of a duplicated ACE, either within the same rule or different rules, is always set to 0.

Before You Begin

Hit count reports are subject to the following limitations:

- Hit count reports are device-specific. You can generate the report for one device at a time from Device view only. Ensure that you deploy policies to the device before generating the reports.
- If you enable object group search on an ASA 8.3+ device, you cannot use the Hit Count tool. Object group search is configured on the Access Control Settings Page, page 16-24.
- Although you can select rules that include FQDN network/host objects, the objects are ignored in the hit count results.

Navigation Path

(Device view only) From the Access Rules Page, page 16-10, right-click the Hit Count cell for a rule in the table and choose **Show Hit Count Details**.

The Hit Count Details window opens as a pane at the bottom of the access rules table. Click the expand button on the right side of its title bar to view the hit count details in a separate window.

Related Topics

- Understanding Access Rules, page 16-1
- Table Columns and Column Heading Features, page 1-49
- Using Category Objects, page 6-13

Field Reference

Table 16-7 ACE Hit Count Details Window

Element	Description
Choose	You can choose how to view the hit count information: **Expanded Table** or **Raw ACE** (both are explained below).
Expanded Table	This view lists hit count information for the access control list entry (ACE) for the rule selected in the Access Rules table (on the Access Rules Page, page 16-10) when you opened this window. The list contains more than one ACE if the access rule generated more than one ACE when you deployed the policy to the device. Most of the columns in this table match those of the Access Rules table; many contain the specific data configured in the ACE in place of any network/host, service, or interface role objects contained in the rule, with the exception of IOS 12.4(20)T+ devices, which show data only at the object level. Also, the name of the ACL that contains the ACE is listed. The Delta column the difference in hit count for the ACE since the last refresh. The Hit Count column shows the hits for the specific ACE rather than the overall rule. See Sample Hit Count Details Window, page 16-39 for an example of this table. **Tip** You can sort on multiple columns at the same time by pressing and holding the **Ctrl** key while you click the column headings. You can sort on all columns except Interface, Direction, and ACL Name.
Raw ACE	This view shows the actual CLI for the access control entry, along with the Hit Count and Last Hit Time. Use this information if you are more comfortable evaluating device commands. See Sample Hit Count Details Window, page 16-39 for an example of this table.

Note Beginning with version 4.9, Security Manager enables to view the Hit Count history in the Expanded Table and Raw ACE options. Click the **Show History** link to view the Hit Count history in a new window. This new Hit Count History Details window displays the Hit Count and the Last Hit Time information.

Sample Hit Count Details Window

You can generate hit count reports to determine how often each rule in your access rule policy is matched to traffic. If an access rule is deployed as multiple access control entries (ACEs), for example, when you use interface roles to define rules and the roles apply to more than one interface, you can see the separate hit count information for each ACE deployed. The hit count results do not show counts for any other type of ACL (for example, those used with class maps or AAA rules).

For access rules on ASA 8.3(1) devices and later, the hit count report also shows the last time the access rule policy was applied to traffic. This information is helpful for determining rules that might have been superseded by other policy changes.

Use the hit count information to help you debug your access rules. The information can help you identify rules that are never hit (which might mean you do not need them, or that they are duplicates of rules higher in the ACL), and rules that are hit often (which means you might want to refine the rules).

The following figures show an example of a hit count report and how to use the information.

- Figure 16-3 shows the default view. The upper table lists the rules as they exist in your access rules policy, either all rules or just the ones you selected before generating the report. When you select a rule, the ACEs created on the device for that rule are listed in the expanded table in the lower half of the window. When you initially open the report, the expanded table shows the ACEs for all policies listed in the upper table.

  Hit counts in the expanded table are for each ACE, whereas the count in the rules table is the sum of the hit counts for all ACEs created by the rule. Note that the expanded table for ASA/PIX/FWSM devices, and IOS devices lower than 12.4(20)T, shows hit counts for each element within any policy objects used in the rule, whereas for IOS 12.4(20)T+ devices, the information is only provided at the object group level.
- Figure 16-4 shows the same ACEs in CLI format. These are the ACEs as they exist in the device configuration.

For more information about how to read and interpret hit count reports, see Viewing Hit Count Details, page 16-37.

Figure 16-3 Expanded Table

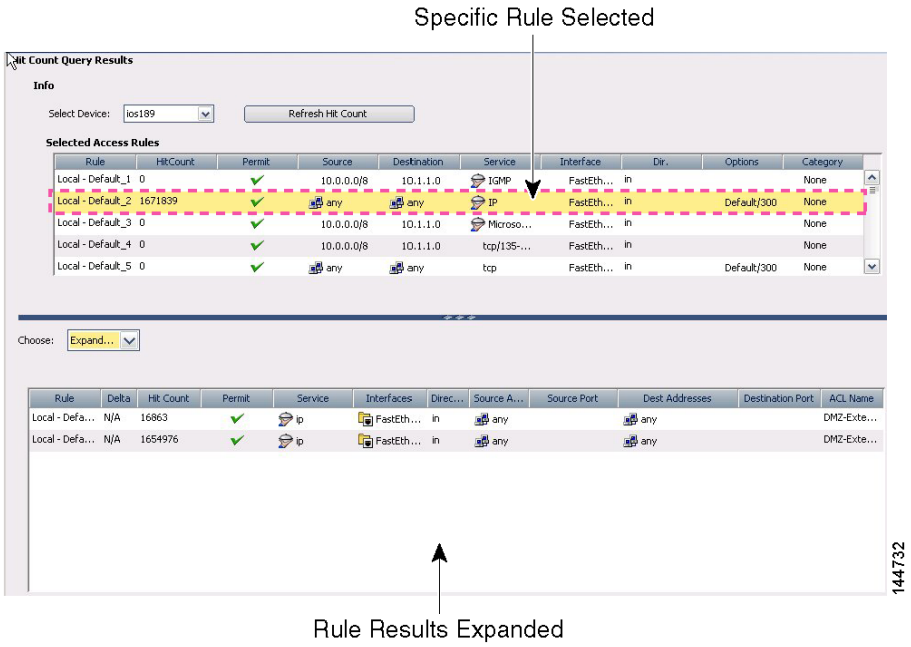


Figure 16-4 Raw ACE Table

Related Topics

- Understanding Access Rules, page 16-1
- Configuring Access Rules, page 16-7

Importing Rules

Typically, when you add a device to Security Manager, you discover policies from the device. This action populates your access rules policy with the access control entries (ACEs) from all active ACLs on the device.

If you find there are other ACLs that have ACEs you want included in your policy, you can define them directly in Security Manager.

Another alternative, however, is to import them by copying and pasting the CLI entries from a device running-configuration, or by typing in the desired commands. Using the Import Rules wizard, you can quickly create ACEs and associated policy objects from ACLs that you know already work. You might also want to use this method if you are more comfortable using CLI commands to define your rules.

The following steps describe using the Import Rules wizard to add CLI-based rules and preview the results.

Step 1 (Device view only) Select **Firewall > Access Rules** to open the Access Rules Page, page 16-10.

Step 2 Select the row after which you want to add the rules. The row must be within the Local scope. If you do not select a row, the rules are added at the end of the Local scope.

Step 3 Right-click anywhere in the rules table and choose **Import Rules** to start the wizard.

The first page—Enter Parameters—of the three-page wizard appears.

Step 4 On the Import Rules Wizard—Enter Parameters Page, page 16-42:

- Enter the desired CLI information in the *running-configuration* format appropriate for the selected device. For examples of importable CLI-based rules, see Examples of Imported Rules, page 16-45.
- Specify whether you are creating an interface-specific rule (and enter the interface or interface role to which you want the rules to apply), or for ASA 8.3+ devices, a global rule (see Understanding Global Access Rules, page 16-3).
- Specify the traffic direction with respect to the interface (the direction is always In for global rules).

Beside access control rules, you should also include the CLI information for the following items if they are referred to by the rules. If you do not include these items, the named objects must already be defined in Security Manager for the import to be successful.

- Time range objects (the **time-range** command with its subcommands), which can create time range policy objects.
- Object groups for PIX, ASA, FWSM, and IOS 12.4(20)T+ devices (the **object-group** command with its subcommands), which can create network/host policy objects.

  For ASA 8.3+ devices, you can also include the **object network** and **object service** commands. However, any object NAT configuration is not imported.

Step 5 Click **Next** to process the rules and open the Import Rules Wizard—Status Page, page 16-43.

You are notified if your CLI input contains errors when you click the Next button. For some detailed tips about what commands you can enter, see Import Rules Wizard—Enter Parameters Page, page 16-42.

The CLI is evaluated and if importable, you are told the types of objects that were created from the CLI.

Step 6 Click **Next** to view the rules and objects on the Import Rules Wizard—Preview Page, page 16-44, or click **Finish** to import the rules without previewing them.

The information on the Preview page is read-only. If the rules are acceptable, click **Finish**.

If you want to make changes, you can click the **Back** button to return to the Enter Parameters page of the wizard, or you can click Finish and edit the rules on the Access Rules page.

Import Rules Wizard—Enter Parameters Page

Use the Import Rules wizard to import a set of access control entries from an ACL in device running-configuration format to your access rules policy. The command syntax you can enter is controlled by the type of device to which you are importing rules.

Beside access control rules, you should also include the CLI for the following items if they are referred to by the rules. If you do not include these items, the named objects must already be defined in Security Manager for the import to be successful.

- Time range objects (the **time-range** command with its subcommands).
- Object groups for PIX, ASA, FWSM, and IOS 12.4(20)T devices (the **object-group** command with its subcommands).

  For ASA 8.3+ devices, you can also include **object network** and **object service** commands. However, any object NAT configuration is not imported.

Navigation Path

(Device view only) Right-click anywhere in the rules table on the Access Rules Page, page 16-10 and choose **Import Rules**.

Related Topics

- Importing Rules, page 16-41
- Understanding Interface Role Objects, page 6-73

Field Reference

Table 16-8 Import Rules - Enter Parameters Dialog Box

Element	Description
CLI	The OS commands that define the rules and related objects that you want to import. These rules must be in running-configuration format, so they are best copied and pasted from a configuration (use Ctrl+V to paste into the field). You can also type in the commands; you will be prompted if they cannot be interpreted. You can import only one ACL at a time. To see some examples of the CLI you can import, see Examples of Imported Rules, page 16-45. **Tips** • If you refer to an object but do not include the CLI, the rule might be created but it will not use the object. • For PIX, FWSM, ASA, and IOS 12.4(20)T+, you can include object group and name commands. • If you import an ACL that is inactive, it is shown as disabled in Security Manager. If you deploy the configuration, it is removed from the device. • You can import extended ACLs for all device types, and standard ACLs for IOS devices. However, standard ACLs are converted to extended ACLs.
Interface Global (ASA 8.3+)	Select whether you are importing an interface-specific or global rule. Global rules are available only for ASA 8.3+ devices, and are handled according to special rules (for detailed information, see Understanding Global Access Rules, page 16-3). If you select **Interfaces**, enter the name of the interface or the interface role for which you are defining this rule, or click **Select** to select the interface or role from a list, or to create a new role. An interface must already be defined to appear on the list. You can enter any combination of interface or interface role names, separated by commas.
Traffic Direction	The direction of the traffic with respect to the interface, in or out.
Category	The category assigned to the rules. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-13.

Import Rules Wizard—Status Page

Use the Status page of the Import Rules wizard to view information about the results of the import process.

Navigation Path

For information on starting the Import Rules wizard, see Import Rules Wizard—Enter Parameters Page, page 16-42

Related Topics

- Importing Rules, page 16-41

Field Reference

Table 16-9 Import Rules Wizard—Status Page

Element	Description
Progress bar	Shows the status of the import process.
Status	The status of the imported configuration.
Rules Imported	The number of rules that will be imported.
Policy Objects Created	The number of policy objects that will be created.
Messages	The warning, error, and informational messages, as indicated by the severity icon. Typical informational messages describe the policy objects created during the operation or the existing policy objects that were reused. When you select an item, the Description box to the right describes the message in detail. The Action box to the right provides information on how you can correct the problem.
Abort button	Click this button to stop the import operation.

Import Rules Wizard—Preview Page

Use the Preview page of the Import Rules wizard to view the rules and objects that will be imported if you click Finish.

This preview is read-only; you cannot edit the rules or objects. If the rules or objects are not exactly what you want, you can click Finish to add the rules and objects, and then edit them from the access rules page. For example, you cannot import rule expiration dates, because those dates have meaning only in Security Manager.

The tabs on this dialog box appear only if the data you are importing includes items to be displayed on the tab.

Tip If your CLI refers to an object that does not exist, such as a time range, the object is not included in the rule. You can either go back and add the CLI for the object, or you can click Finish, create the object yourself, and edit the rule.

Navigation Path

For information on starting the Import Rules wizard, see Import Rules Wizard—Enter Parameters Page, page 16-42.

Related Topics

- Importing Rules, page 16-41
- Access Rules Page, page 16-10
- Understanding Networks/Hosts Objects, page 6-80
- Understanding Interface Role Objects, page 6-73

- Understanding and Specifying Services and Service and Port List Objects, page 6-100
- Filtering Tables, page 1-48

Field Reference

Table 16-10 Import Rules Wizard—Preview Page

Element	Description
Rules tab	The rules that were created from your CLI and that will be imported to the access rules policy. All rules are converted to extended format, even if your CLI was for a standard ACL. Icons indicate the permit and deny status: • Permit—Shown as a green check mark. • Deny—Shown as a red circle with slash. You can right-click the source, destination, services, and interfaces cells and select **Show Contents** to see the detailed information in the cell. You can also right-click and select **Copy** to copy a rule to the clipboard in HTML format, which you can paste into a text editor.
Objects tab	The policy objects created from your CLI, if any. Depending on the CLI, Security Manager might create time range, network/host, service, or port list objects. Right-click an object and select **View Object** to see the object definition in read-only format.

Examples of Imported Rules

The following are some examples of CLI that you can import and the rules and policy objects that are created from them. For information on how to import rules, see Importing Rules, page 16-41.

Example 1: Restrict a network from accessing FTP servers (ASA devices)

The following access list uses object groups and restricts the 10.200.10.0/24 network from accessing some FTP servers. All other traffic is allowed.

```
object-group network ftp_servers
network-object host 172.16.56.195
network-object 192.168.1.0 255.255.255.224
access-list ACL_IN extended deny tcp 10.200.10.0 255.255.255.0 object-group ftp_servers
access-list ACL_IN extended permit ip any any
```

This example creates a network/host object named ftp_servers and two access rules.

No.	Permit	Source	Destination	Service	Interface	Dir.	Category
1		10.200.10.0/24	ftp_servers	TCP	Ethernet0	in	None
2		any	any	IP	Ethernet0	in	None

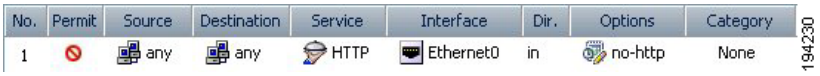
194227

Example 2: Restrict web access during working hours (ASA devices)

The following example denies HTTP requests between the hours of 8 AM and 6 PM, which are typical work hours.

```
time-range no-http
 periodic weekdays 8:00 to 18:00
access-list 101 deny tcp any any eq www time-range no-http
```

This example creates a time range object named no-http and one access rule.

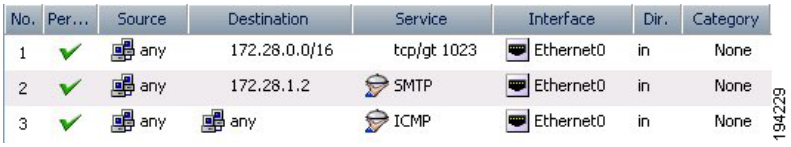


Example 3: Filtering on TCP and ICMP using port numbers (IOS devices)

In the following example, the first line of the extended access list named goodports permits any incoming TCP connections with destination ports greater than 1023. The second line permits incoming TCP connections to the Simple Mail Transfer Protocol (SMTP) port of host 172.28.1.2. The last line permits incoming ICMP messages for error feedback.

```
ip access-list extended goodports
 permit tcp any 172.28.0.0 0.0.255.255 gt 1023
 permit tcp any host 172.28.1.2 eq 25
 permit icmp any 172.28.0.0 255.255.255.255
```

This example creates three access rules. Notice that the wildcard masks used in the IOS ACL syntax are converted to regular subnet masks. Security Manager automatically converts between standard network/host subnet mask designations and the wildcard masks required in IOS ACLs. Because ASA/PIX/FWSM requires the use of subnet masks in ACL commands, this makes it possible for you to create rules that can apply to all devices; Security Manager takes care of converting your rules to the correct syntax.



Example 4: Standard ACLs restricting hosts (IOS devices)

In the following example, the workstation belonging to Jones is allowed access to Ethernet interface 0 and the workstation belonging to Smith is not allowed access:

```
ip access-list standard workstations
 remark Permit only Jones workstation through
 permit 172.16.2.88
 remark Do not allow Smith workstation through
 deny 172.16.3.13
```

This example creates two rules, converting the standard rules to extended rules (to any destination). The remarks are saved in the description field.

For more examples of ACLs in command language format, see the following:

- IOS Devices—http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_create_IP_apply.html#wp1027258.
- ASA Devices—http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/acl_extended.html.

Optimizing Access Rules Automatically During Deployment

You can configure the system to optimize the access control lists (ACLs) that are created from your access rules policies when they are deployed to specific devices or to all devices. This optimization affects only the deployed policies, it does not make any changes to your access rules policy.

Optimization removes redundancies and conflicts and can combine multiple entries (ACEs) into single entries. Although the order of entries might change, the semantics of your policies are preserved; the optimized ACL accepts or denies the same set of packets as did its unoptimized form. Following are the basic cases where changes are made:

- Ineffective ACE—Where one entry is a subset of, or equal to, another entry, the ineffective ACE is removed. Consider the following example:

  ```
  access-list acl_mdc_inside_access deny ip host 10.2.1.1 any
  access-list acl_mdc_inside_access deny ip 10.2.1.0 255.255.255.0 any
  ```

  The first ACE is actually a subset of the second ACE. ACL optimization will deploy only the second entry.

- Superset ACE—Where one entry is a superset of another and the order of the rules does not matter, the redundant rule is removed. Consider the following example:

  ```
  access-list acl_mdc_inside_access permit tcp any any range 110 120
  access-list acl_mdc_inside_access deny tcp any any range 115
  ```

  The second ACE will never be hit. ACL optimization will remove the second ACE and deploy only the first one.

- Adjacent ACEs—Where two entries are similar enough that a single entry can do the same job. There can be no intervening rules that change which packets will hit each rule. Consider the following example:

  ```
  access-list myacl permit ip 1.1.1.0 255.255.255.128 any
  access-list myacl permit ip 1.1.1.128 255.255.255.128 any
  ```

  The two ACEs are merged into one: access-list myacl permit ip 1.1.1.0 255.255.255.0 any.

By configuring ACL deployment optimization, you can create smaller ACLs that are more efficient, which can improve performance on devices with limited, non-expandable memory, such as the FWSM, which can be shared among multiple virtual contexts.

However, there are down sides to configuring ACL deployment optimization:

- Because optimization changes what would normally be deployed for your access rules, it is hard to correlate those rules to the actual deployed ACEs. This can make the results of the hit count tool unusable, and make it very difficult to correlate events in the Cisco Security Monitoring, Analysis and Response System application. If it is important to you that you can monitor your access rules using these tools, do not enable optimization. For more information, see Viewing Hit Count Details, page 16-37 and Viewing CS-MARS Events for an Access Rule, page 72-44.
- Optimization does not address inherent problems in your access rules policy. It is typically better to address redundancies and conflicts proactively by using the automatic conflict detection tool (see Using Automatic Conflict Detection, page 16-28). You can also use the combine rules tool to optimize your rules in the access rules policy before you deploy them (see Combining Rules, page 12-22).

If you decide to configure ACL deployment optimization, consider enabling it only for those devices that are memory constrained.

Step 1 Log into Windows on the Security Manager server.

Step 2 Use a text editor such as NotePad to open the **C:\Program Files\CSCOpx\MDC\athena\config\csm.properties** file. Locate the optimization section and read the instructions.

- To turn on full optimization for all devices, enter the following:

  OPTIMIZE.*=full

- To turn on full optimization for a specific device, replace the asterisk with the Security Manager display name for the device. For example, if the display name is west_coast.cisco.com, enter the following:

  OPTIMIZE.west_coast.cisco.com=full

- To turn on optimization but preserve the object groups used in the ACE, replace the full keyword with preserve_og. For example:

  OPTIMIZE.west_coast.cisco.com=preserve_og

- If you do not want to allow the merger of adjacent entries, enter the following:

  AclOptimization.doMerge=false

Step 3 Save the file. The settings take effect immediately and will be applied to all subsequent deployment jobs.

You can generate optimization reports for deployment jobs by selecting **Capture Discovery/Deployment Debugging Snapshots to File**, which is located in **Tools > Security Manager Administration > Debug Options**.

The deployment results will show optimization results summarized as an informational message that includes the original number of ACEs before optimization and the number of ACEs after optimization. The results are saved to a file on the server in the C:\Program Files\CSCOpx\MDC\temp folder. A job ID is used as part of the file name.

Customizing defaults in the Add Access Rule dialog

Prior to Cisco Security Manager 4.13, the **Add Access Rule** dialog was populated with default values. Starting from 4.13, the user can customize the appearance of default values by updating the **csm.properties** file.

To customize defaults in the Add Access Rule dialog, perform the following steps:

Step 1 Close and exit the Cisco Security Manager interface.

Step 2 Use a text editor such as NotePad to open the **C:\Program Files\CSCOpx\MDC\athena\config\csm.properties** file.

Step 3 Locate the CustDesk.Rule property at the bottom of the csm.properties file and set the values as true or false, based on your requirements:

- CustDesk.Rule.Add.Op.Load.Intf.Default.Values - Set this value as true to load the interface information by default in the Add Access rule dialog.
- CustDesk.Rule.Add.Op.Load.Other.Default.Values - Set this value as true to load the other values by default in the Add Access rule dialog.

Step 4 Save the file.

Note The settings do not take effect immediately. Restart the Cisco Security Manger services for the customized default values to take effect.

Step 5 Launch the Cisco Security Manager interface again.