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 1-6.

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

- Understanding Access Rules, page 14-2
- Understanding Global Access Rules, page 14-3
- Understanding Device Specific Access Rule Behavior, page 14-5
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 14-5
- Configuring Access Rules (IPv4 or IPv6), page 14-7
- Configuring Expiration Dates for Access Rules, page 14-17
- Configuring Settings for Access Control (IPv4 or IPv6), page 14-17
- Generating Analysis Reports, page 14-22
- Generating Hit Count Reports, page 14-24
- Importing Rules, page 14-30
- Optimizing Access Rules Automatically During Deployment, page 14-36

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

- Adding and Removing Rules, page 12-8
- Editing Rules, page 12-9
- Enabling and Disabling Rules, page 12-17
- Moving Rules and the Importance of Rule Order, page 12-16
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.

There are two separate access rules policies based on the IP addressing scheme. The Firewall > Access Rules policy is for IPv4 addresses, and the Firewall > IPv6 Access Rules policy is for IPv6 addresses. Other than the addressing scheme, and the tools available for use with the policies, configuring IPv4 and IPv6 access rules is the same.

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 14-3.

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 analysis and policy query tools. For more information, see Generating Analysis Reports, page 14-22 and Generating Policy Query Reports, page 12-24.

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

- Combining 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 12-19.

- 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 Generating Hit Count Reports, page 14-24.

- 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 65-26.
For more conceptual information on access rules, see the following topics:

- Understanding Global Access Rules, page 14-3
- Understanding Device Specific Access Rule Behavior, page 14-5
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 14-5

Related Topics

- Configuring Access Rules (IPv4 or IPv6), page 14-7
- Configuring Expiration Dates for Access Rules, page 14-17
- Configuring Settings for Access Control (IPv4 or IPv6), page 14-17
- Expanding Object Groups During Discovery, page 12-31
- Importing Rules, page 14-30
- Adding and Removing Rules, page 12-8
- Editing Rules, page 12-9
- Enabling and Disabling Rules, page 12-17
- Moving Rules and the Importance of Rule Order, page 12-16

**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 14-2
- Understanding Device Specific Access Rule Behavior, page 14-5
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 14-5
- Configuring Access Rules (IPv4 or IPv6), page 14-7
- Moving Rules and the Importance of Rule Order, page 12-16
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 *Generating Hit Count Reports*, page 14-24.

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 14-2
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 14-5

Understanding Access Rule Address Requirements and How Rules Are Deployed

One of the complexities of creating IPv4 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.
Understanding Access Rules

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 (IPv4 and IPv6), page 14-19. 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 11-7 (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 12-30), 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 (IPv4 or IPv6), page 14-17.

  - 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 11-7.

- IPv4 and IPv6 ACLs cannot have the same name.

**Related Topics**
- Understanding Access Rules, page 14-2
- Configuring Access Rules (IPv4 or IPv6), page 14-7
- Configuring Settings for Access Control (IPv4 or IPv6), page 14-17
- Expanding Object Groups During Discovery, page 12-31

### Configuring Access Rules (IPv4 or IPv6)

Access rules policies define the rules for allowing traffic to pass through an interface. There are separate policies for IPv4 and IPv6 traffic. 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 14-5.

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 for AAA rules. See the following topics for more information about things you should consider:
- Understanding Access Rules, page 14-2
- Understanding Global Access Rules, page 14-3
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 14-5

**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 5-50 and Inheriting or Uninheriting Rules, page 5-43.

**Related Topics**
- Using Sections to Organize Rules Tables, page 12-17
- Copying Policies Between Devices, page 5-31
- Working with Shared Policies in Device View or the Site-to-Site VPN Manager, page 5-34
- Understanding Network/Host Objects (IPv4 and IPv6), page 6-63
- Understanding Interface Role Objects, page 6-56
- Understanding and Specifying Services and Service and Port List Objects, page 6-72

**Step 1**

Do one of the following to open the Access Rules Page (IPv4 or IPv6), page 14-9:
- (Device view) Select Firewall > Access Rules (for IPv4) or Firewall > IPv6 Access Rules from the Policy selector.
- (Policy view) Select Firewall > Access Rules (for IPv4) or Firewall > 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 (IPv4 and IPv6), page 14-11.
Configuring Access Rules (IPv4 or IPv6)

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 12-9. Special rules apply if you mix interface-specific and global rules in a policy; for more information, see Understanding Global Access Rules, page 14-3.

Step 3 Configure the rule. Following are the highlights of what you typically need to decide. For specific information on configuring the fields, see Add and Edit Access Rule Dialog Boxes (IPv4 and IPv6), page 14-11.

- 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 “any” 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 6-70 or Specifying IPv6 Addresses During Policy Definition, page 6-71.
- Service—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 14-3).
- 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 14-14.
  - 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 6-54.
  - 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 14-17.

Click OK when you are finished defining your rule.

Step 4 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 12-16. There are special restrictions for moving rules when you mix interface-specific and global rules; see Understanding Global Access Rules, page 14-3.
**Step 5** (IPv4 only.) If you already have a large number of rules, consider analyzing and combining them before deploying the new rules:

- Click the **Tools** button and select **Analysis** to analyze whether you have redundant rules or rules that will not be used. Fix problem areas. For more information, see **Generating Analysis Reports**, page 14-22.
- If analysis shows that you have a lot of redundant rules, click the **Tools** button and select **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 combiner tool. For more information, see **Combining Rules**, page 12-19.

---

**Access Rules Page (IPv4 or IPv6)**

Use the Access Rules (for IPv4) or IPv6 Access Rules pages 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.

Read the following topics before you configure access rules:

- Understanding Access Rules, page 14-2
- Understanding Global Access Rules, page 14-3
- Understanding Device Specific Access Rule Behavior, page 14-5
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 14-5
- Configuring Access Rules (IPv4 or IPv6), page 14-7

---

**Tip**

Disabled rules are shown with hash marks covering the table row. When you deploy the configuration, disabled rules are removed from the device. For more information, see **Enabling and Disabling Rules**, page 12-17.

---

**Navigation Path**

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

- (Device view) Select a device, then select **Firewall > Access Rules** (for IPv4) or **Firewall > IPv6 Access Rules** from the Policy selector.
- (Policy view) Select **Firewall > Access Rules** (for IPv4) or **Firewall > 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** (for IPv4) or **Edit Firewall Policies > IPv6 Access Rules**.

**Related Topics**

- Configuring Expiration Dates for Access Rules, page 14-17
- Configuring Settings for Access Control (IPv4 or IPv6), page 14-17
- Adding and Removing Rules, page 12-8
- Editing Rules, page 12-9
Chapter 14  Managing Firewall Access Rules

- Enabling and Disabling Rules, page 12-17
- Moving Rules and the Importance of Rule Order, page 12-16
- Using Sections to Organize Rules Tables, page 12-17
- Using Rules Tables, page 12-7
- Filtering Tables, page 1-37

Field Reference

Table 14-1  Access Rules Page

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>The ordered rule number.</td>
</tr>
</tbody>
</table>
| 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. |
| Source Destination | The source and destination addresses for the rule. The “any” address does 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. Multiple entries are displayed as separate subfields within the table cell. See:  
|                    | - Understanding Network/Host Objects (IPv4 and IPv6), page 6-63  
|                    | - Understanding Interface Role Objects, page 6-56 |
| Service            | The services or service objects that specify the protocol and port of the traffic to which the rule applies. Multiple entries are displayed as separate subfields within the table cell. See Understanding and Specifying Services and Service and Port List Objects, page 6-72. |
| 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 as separate subfields within the table cell. See Understanding Interface Role Objects, page 6-56.  
|                    | 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 6-59). |
| Dir.               | The direction of the traffic to which this rule applies:  
|                    | - In—Packets entering the interface.  
|                    | - Out—Packets exiting the interface. |
| Options            | The 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 14-14. |
| Category           | The category assigned to the rule. Categories help you organize and identify rules and objects. See Using Category Objects, page 6-9. |
| Description        | The description of the rule, if any. |
Add and Edit Access Rule Dialog Boxes (IPv4 and IPv6)

Use the Add and Edit Access Rule dialog boxes to add and edit IPv4 or IPv6 access rules. Read the following topics before you configure access rules:

- Understanding Access Rules, page 14-2
- Understanding Global Access Rules, page 14-3
- Understanding Device Specific Access Rule Behavior, page 14-5
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 14-5
- Configuring Access Rules (IPv4 or IPv6), page 14-7
Navigation Path
From the Access Rules Page (IPv4 or IPv6), page 14-9, click the Add Row button or select a row and click the Edit Row button.

Related Topics
- Configuring Expiration Dates for Access Rules, page 14-17
- Editing Rules, page 12-9
- Adding and Removing Rules, page 12-8
- Importing Rules, page 14-30
- Understanding Network/Host Objects (IPv4 and IPv6), page 6-63
- Understanding and Specifying Services and Service and Port List Objects, page 6-72

Field Reference

Table 14-2    Add and Edit Access Rule Dialog Boxes

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Rule</td>
<td>Whether to enable the rule, which means the rule becomes active when you</td>
</tr>
<tr>
<td></td>
<td>deploy the configuration to the device. Disabled rules are shown overlain</td>
</tr>
<tr>
<td></td>
<td>with hash marks in the rule table. For more information, see Enabling and</td>
</tr>
<tr>
<td></td>
<td>Disabling Rules, page 12-17.</td>
</tr>
<tr>
<td>Action</td>
<td>Whether the rule permits or denies traffic based on the conditions you define.</td>
</tr>
</tbody>
</table>
Chapter 14 Managing Firewall Access Rules

Configuring Access Rules (IPv4 or IPv6)

Table 14-2 Add and Edit Access Rule Dialog Boxes (Continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sources</td>
<td>The source or destination of the traffic. You can enter more than one value by separating the items with commas.</td>
</tr>
<tr>
<td></td>
<td>You can enter any combination of the following address types to define the source or destination of the traffic. You must use either IPv4 or IPv6 addresses, based on which access rules policy you are configuring; you cannot mix address types. For more information, see Specifying IP Addresses During Policy Definition, page 6-70 and Specifying IPv6 Addresses During Policy Definition, page 6-71.</td>
</tr>
<tr>
<td></td>
<td>• Network/host object (IPv4 or IPv6). Enter the name of the object or click Select to select it from a list. You can also create new network/host objects from the selection list.</td>
</tr>
<tr>
<td></td>
<td>• Host IP address, for example, 10.10.10.100 (IPv4) or 2001:DB8::200C:417A (IPv6).</td>
</tr>
<tr>
<td></td>
<td>• IPv4 network address, including subnet mask, in either the format 10.10.10.0/24 or 10.10.10.0/255.255.255.0.</td>
</tr>
<tr>
<td></td>
<td>• IPv6 network address and prefix length in the format 2001:DB8::/32.</td>
</tr>
<tr>
<td></td>
<td>• A range of IP addresses, for example, 10.10.10.100-10.10.10.200 (IPv4) or 2001:DB8::1-2001:DB8::100 (IPv6).</td>
</tr>
<tr>
<td></td>
<td>• (IPv4 only.) An IP address pattern in the format 10.10.0.10/255.255.0.255, where the mask is a discontiguous bit mask (see Contiguous and Discontiguous Network Masks for IPv4 Addresses, page 6-64).</td>
</tr>
<tr>
<td></td>
<td>• Interface role object. Enter the name of the object or click Select to select it from a list (you must select Interface Role as the object type). When you use an interface role, the rule behaves as if you supplied the IPv4 or IPv6 address of the selected interface. This is useful for interfaces that get their address through DHCP, because you do not know what IP address will be assigned to the device. For more information, see Understanding Interface Role Objects, page 6-56.</td>
</tr>
<tr>
<td></td>
<td>If you select an interface role as a source, the dialog box displays tabs to differentiate between hosts or networks and interface roles.</td>
</tr>
<tr>
<td>Destinations</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>The services that define the type of traffic to act on. You can enter more than one value by separating the items with commas.</td>
</tr>
<tr>
<td></td>
<td>You can enter any combination of service objects and service types (which are typically a protocol and port combination). If you type in a service, you are prompted as you type with valid values. You can select a value from the list and press Enter or Tab.</td>
</tr>
<tr>
<td></td>
<td>For complete information on how to specify services, see Understanding and Specifying Services and Service and Port List Objects, page 6-72.</td>
</tr>
</tbody>
</table>
Table 14-2   Add and Edit Access Rule Dialog Boxes (Continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>Select whether you are creating an interface-specific or global rule.</td>
</tr>
<tr>
<td>Global (ASA 8.3+)</td>
<td>Global rules are available only for ASA 8.3+ devices, and are handled</td>
</tr>
<tr>
<td></td>
<td>according to special rules (for detailed information, see Understanding</td>
</tr>
<tr>
<td></td>
<td>Global Access Rules, page 14-3).</td>
</tr>
<tr>
<td></td>
<td>If you select Interfaces, enter the name of the interface or the interface</td>
</tr>
<tr>
<td></td>
<td>role to which the rule is assigned, or click Select to select the interface</td>
</tr>
<tr>
<td></td>
<td>or role from a list, or to create a new role. An interface must already be</td>
</tr>
<tr>
<td></td>
<td>defined to appear on the list.</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description of the rule (up to 1024 characters).</td>
</tr>
<tr>
<td>Category</td>
<td>The category assigned to the rule. Categories help you organize and identify</td>
</tr>
<tr>
<td>Advanced button</td>
<td>Click this button to configure other settings for the rule, including logging</td>
</tr>
<tr>
<td></td>
<td>configuration, traffic direction, time ranges, and rule expiration dates.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Advanced and Edit Options Dialog Boxes, page 14-14</td>
</tr>
</tbody>
</table>

Advanced and Edit Options Dialog Boxes

Use the Advanced and Edit Options dialog boxes to configure additional settings for an IPv4 or IPv6 access rule. When you are in the Advanced dialog box, you have more fields available for configuration than when you edit options, which is a cell-level editing dialog box. The settings in the Advanced dialog box show up in three different cells in an access rule; direction, options, and rule expiration.

Navigation Path

To access the Advanced dialog box, do one of the following:

- Go to the Add and Edit Access Rule Dialog Boxes (IPv4 and IPv6), page 14-11 and click Advanced.
- Right-click the Options cell in an access rule (on the Access Rules Page (IPv4 or IPv6), page 14-9) and select Edit Options. If you select multiple rows, your changes replace the options defined for all selected rules.

Related Topics

- Configuring Access Rules (IPv4 or IPv6), page 14-7
- Editing Rules, page 12-9
- Understanding Access Rules, page 14-2
- Chapter 14, “Managing Firewall Access Rules”
- Configuring Time Range Objects, page 6-54
### Table 14-3 Advanced Dialog Box

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable Logging (PIX, ASA, FWSM) | Whether to generate syslog messages for the rule entries, or ACEs, for PIX, ASA, and FWSM devices. You can select these additional options:  
  - 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. Select the logging level you want to use to log events for the ACE, and the logging interval, which can be from 1-600 seconds. Syslog message 106100 is generated for the ACE.  
  Following are the possible 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 |
| Enable Logging (IOS) Log Input (IPv4 only.) | Whether to generate an informational logging message about the packet that matches the entry to 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 (Advanced dialog box only) | 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.  
  Global rules are always applied in the In direction, so you cannot change this setting when configuring a global rule. |
| 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 click **Select** to 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. |
Configure Access Rules (IPv4 or IPv6)

Edit Firewall Rule Expiration Settings Dialog Box

Use the Edit Firewall Rule Expiration Settings dialog box to edit the expiration settings for an IPv4 or IPv6 access rule.

To set an expiration date for the rule, click the calendar icon to select a date.

If you configure an expiration date, you can also configure the number of days before which 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).

Expired rules are not automatically deleted. You must delete them yourself and redeploy the configuration to the device.

For more information, see Configuring Expiration Dates for Access Rules, page 14-17.

Navigation Path

Right-click the Expiration Date cell in an access rule (on the Access Rules Page (IPv4 or IPv6), page 14-9) and select Edit Rule Expiration. If you select multiple rows, your changes replace the options defined for all selected rules.
Chapter 14      Managing Firewall Access Rules

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 IPv4 or IPv6 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 (overlaid with hash marks), in case you discover the rule really was still needed after all, saving you the time of recreating the rule. You just need to 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 to get to the rule expiration settings. For information on creating access rules, see Configuring Access Rules (IPv4 or IPv6), page 14-7.
- 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 Edit Firewall Rule Expiration Settings Dialog Box, page 14-16.

Related Topics

- Rule Expiration Page, page 11-34
- Contiguous and Discontiguous Network Masks for IPv4 Addresses, page 6-64

Configuring Settings for Access Control (IPv4 or IPv6)

You can configure various settings that apply to IPv4 or IPv6 access control lists. These settings work in conjunction with your IPv4 or IPv6 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 IPv4 deny 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.
There are other settings available, but they pertain to older devices and software releases and are of limited use.

Related Topics
- Configuring Access Rules (IPv4 or IPv6), page 14-7

---

**Step 1**
Do one of the following to open the Access Control Settings Page (IPv4 and IPv6), page 14-19:
- (Device view) Select **Firewall > Settings > Access Control** (for IPv4) or **Firewall > Settings > IPv6 Access Control** from the Policy selector.
- (Policy view) Select **Firewall > Settings > Access Control** (for IPv4) or **Firewall > Settings > IPv6 Access Control** from the Policy Type selector. Select an existing policy or create a new one.

**Step 2**
(IPV4 policy only.) 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.

**Note**
The Enable Object Group Search setting applies to both IPv4 and IPv6 access rules. Your selection in the IPv4 policy applies to all rules; there is not a separate setting for IPv6.

For specific information about these settings, and the platforms that support ACL compilation, see Access Control Settings Page (IPv4 and IPv6), page 14-19.

**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 (IPv4 or IPv6), page 14-21. Keep the following in mind:
- If you configure an ACL name, the name is applied to the specific interface and direction; you cannot use the same name for both IPv4 and IPv6 policies. 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.
- The **Enable Per User Downloadable ACLs** option is not confined to IPv4 or IPv6. If you select the option in either the IPv4 or IPv6 Access Control Settings policy, the option is configured for the specified interface and direction, even if you do not select it in the other access control settings policy.

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 (IPv4 and IPv6)

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. There are separate policies for IPv4 and IPv6, but they are essentially the same.

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 access the Access Control Page, do one of the following:
- (Device view) Select a device, then select Firewall > Settings > Access Control (for IPv4) or Firewall > Settings > IPv6 Access Control from the Policy selector.
- (Policy view) Select Firewall > Settings > Access Control (for IPv4) 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 (for IPv4) or Edit Firewall Settings > IPv6 Access Control.

Related Topics

- Configuring Settings for Access Control (IPv4 or IPv6), page 14-17
- Understanding Access Rules, page 14-2
- Understanding Device Specific Access Rule Behavior, page 14-5
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 14-5
- Understanding Access Rules, page 14-2
- Understanding Interface Role Objects, page 6-56

Field Reference

<table>
<thead>
<tr>
<th>Table 14-4</th>
<th>Access Control Settings Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Element</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| Maximum number of concurrent flows (PIX, ASA, FWSM) (IPv4 only.) | 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) (IPv4 only.) | 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. |
Configuring Settings for Access Control (IPv4 or IPv6)

Chapter 14  Managing Firewall Access Rules

Table 14-4  Access Control Settings Page (Continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable Access List Compilation (Global) (IPv4 only.) | 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+) (On IPv4 policy only, but applies to both IPv4 and IPv6.) | 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 combiner tool to simplify your access rules, and consider using global rules for rules you want to enforce on all interfaces. |
| Interfaces table (IPv4 and IPv6.) | 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 IPv4 or IPv6 ACL generated for an interface in a specific direction.  
  You can also configure interface-level settings for per user downloadable ACLs and for IPv4, object group search and ACL compilation:  
  - To add an interface setting, click the Add Row button and fill in the Firewall ACL Setting Dialog Box (IPv4 or IPv6), page 14-21.  
  - To edit an interface setting, select it and click the Edit Row button.  
  - To delete an interface setting, select it and click the Delete Row button. |
Firewall ACL Setting Dialog Box (IPv4 or IPv6)

Use the Firewall ACL Setting dialog box to configure settings for specific interfaces, interface roles, or global rules for use with IPv4 or IPv6 access rules policies.

Navigation Path
Go to the Access Control Settings Page (IPv4 and IPv6), page 14-19 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 (IPv4 or IPv6), page 14-17
- Understanding Access Rules, page 14-2
- Understanding Global Access Rules, page 14-3
- Understanding Device Specific Access Rule Behavior, page 14-5
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 14-5
- Understanding Interface Role Objects, page 6-56

Field Reference

Table 14-5  Firewall ACL Setting Dialog Box

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Select whether you are configuring settings for specific interfaces (or</td>
</tr>
<tr>
<td>Global (ASA 8.3+)</td>
<td>interface roles), or for global rules on ASA 8.3+ devices. If you select</td>
</tr>
<tr>
<td></td>
<td><strong>Interface</strong>, specify the name of the interface or interface role for which</td>
</tr>
<tr>
<td></td>
<td>you are configuring settings. Enter the name or click <strong>Select</strong> to select it</td>
</tr>
<tr>
<td></td>
<td>from a list or to create a new object. If you select Global, your only</td>
</tr>
<tr>
<td></td>
<td>option is to specify the name of the global ACL.</td>
</tr>
<tr>
<td>Traffic Direction</td>
<td>The direction of the traffic through the interface, in or out. The settings</td>
</tr>
<tr>
<td></td>
<td>you configure apply only to this direction, if direction matters. For global</td>
</tr>
<tr>
<td></td>
<td>ACLs on ASA 8.3+ devices, the direction is always in.</td>
</tr>
<tr>
<td>User Defined ACL Name</td>
<td>Whether you want to supply the name for the ACL. If you select this option,</td>
</tr>
<tr>
<td>ACL Name</td>
<td>enter the name you want to use, which is applied to the ACL generated for</td>
</tr>
<tr>
<td></td>
<td>the interface and direction combination. The name must be unique on the</td>
</tr>
<tr>
<td></td>
<td>device.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> When configuring IPv6 access control settings, there is only the</td>
</tr>
<tr>
<td></td>
<td>ACL Name edit box; there is no User Defined ACL Name check box. Note that</td>
</tr>
<tr>
<td></td>
<td>you cannot use the same ACL name for IPv4 and IPv6 ACLs.</td>
</tr>
<tr>
<td></td>
<td>If you are configuring the name for the global ACL on ASA 8.3+ devices, the</td>
</tr>
<tr>
<td></td>
<td>option is automatically selected; simply enter the desired name.</td>
</tr>
<tr>
<td></td>
<td>If you do not configure a name, Security Manager generates a name for you.</td>
</tr>
</tbody>
</table>
Generating Analysis Reports

You can generate analysis reports to evaluate the logic of your access rules. The report lists 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.

The purpose of analyzing your access rules policy is twofold:

- To identify unnecessary redundant or duplicate rules that you can delete. For example:
  - Redundant Base Rule—Although not identical to the overlapping rule, the rules apply the same action to the same type of traffic, and removing the base rule would not change the ultimate result. For example, the base rule might prohibit a service during a specific time range, but the overlapping rule prohibits the service at all times. Another example is where the overlapping rule might allow any source, whereas the base rule specifies a particular network.


- Redundant Overlapping Rule—This is the reverse of a redundant base rule. In this case, the base rule will match the same traffic as the overlapping rule, meaning the overlapping rule will never be applied to any traffic (because it comes later in the access list). You can delete the overlapping rule.

- Duplicate Rule—The base rule and the overlapping rule are identical. You can delete one of them.

- Conflicting Rule—To identify rules that define conflicting actions for the same traffic. With conflicting rules, the base rule and the overlapping rule specify different actions for traffic. It might not always be apparent that the rules specify different policies. However, because the base rule comes before the overlapping rule, it is the base rule that will decide what happens to the traffic. You might need to move the overlapping rules, or edit the base or overlapping rules, to implement your desired policy.

For example, the base rule might deny IP traffic, and the overlapping rule might permit FTP traffic, for a given source or destination.

By removing unnecessary rules, you can develop an easier to use and more efficient access rules policy. Figure 14-1 shows an example of a redundant rule. In this case, the base rule permits source address 1.2.3.4 to make TFTP connections to destination 2.3.4.5. However, a subsequent rule allows any source address to make TFTP connections to that destination. The base rule is not needed, assuming you want to keep the overlapping rule.

Figure 14-1 Example Rule Analysis Report
Chapter 14  Managing Firewall Access Rules

Generating Hit Count Reports

In addition to analysis, 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 12-19.

Related Topics

- Understanding Access Rules, page 14-2
- Understanding Device Specific Access Rule Behavior, page 14-5
- Understanding Access Rule Address Requirements and How Rules Are Deployed, page 14-5
- Configuring Access Rules (IPv4 or IPv6), page 14-7

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 (IPv4 or IPv6), page 14-9.

Step 2  Click the **Tools** button and select **Analysis**.

The rules are analyzed and the results presented in the Rule Analysis Results window. The report has three window panes.

- Left pane (Base Rules)—Lists conflicting groups of rules identified by the base rule, which is the rule with the lowest rule number.
- Top right pane (Conflict Overview)—Shows the base rule selected in the left pane and all of the rules that overlap, or conflict, with it. The scope indicates whether the rule is local to a device or inherited from a shared rule (mandatory or default). The other columns are the same as the regular access rule attributes (see Access Rules Page (IPv4 or IPv6), page 14-9).

Select an overlapping rule in this pane to view a detailed comparison in the lower right pane.

- Bottom right pane (Overlap Details)—Shows a detailed comparison between the base rule and the overlapping rule selected in the top right pane for easier direct comparison. Conflicting elements are shown in bold text. The types of overlap are explained above.

Use the previous and next buttons to page through the details if necessary.

Generating Hit Count Reports

You can generate hit count reports to determine how often each rule in your IPv4 or IPv6 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).

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 14-2** 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 14-3** shows the same ACEs except 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 Analyzing Hit Count Query Results, page 14-28.
Before You Begin

Hit count reports are device-specific. You can generate the report for a single device at a time from Device view only. Ensure that you deploy policies to the device before generating the reports.

Tip

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 (IPv4 and IPv6), page 14-19.

Related Topics

- Understanding Access Rules, page 14-2
- Configuring Access Rules (IPv4 or IPv6), page 14-7

Step 1  (Device view only.) Select Firewall > Access Rules or Firewall > IPv6 Access Rules to open the Access Rules Page (IPv4 or IPv6), page 14-9.

Step 2  If you want to get the hit count for specific rules, select them in the table. Use Shift+click to select a group of rules, or Ctrl+click to select multiple individual rules.

You can also select rules by selecting a section heading, a scope heading, or by creating a filter to display only those rules that interest you.

Step 3  Click the Tools button located below the table, then select Hit Count to open the Hit Count Selection Summary Dialog Box, page 14-27.

Step 4  Select the rules to include in the report. Select All Rules to include all local, shared, and inherited rules. If you selected rules before initiating the report, select that option.
Step 5  
Click OK.

The tool obtains the ACL and hit count information from the device. You can abort the operation if you want. When the information is obtained, it is displayed in the Hit Count Summary Results Page. For information on reading the report, see Analyzing Hit Count Query Results, page 14-28.

You can click Refresh Hit Count while the report is open to obtain the latest information. The Delta column displays the difference in hit count since the last refresh.

Hit Count Selection Summary Dialog Box

Use the Hit Count Selection Summary dialog box to select the rules for which you want to generate hit count information. Your options are limited by the rules you selected before initiating the hit count report.

When you click OK, the hit count information is obtained from the device, which can take some time so you are given the option to abort the operation. The results are shown in the Hit Count Query Results window. For information on reading the results, see Analyzing Hit Count Query Results, page 14-28.

Navigation Path
(Device view only) Select either Firewall > Access Rules, or Firewall > IPv6 Access Rules, then click the Tools button and select Hit Count. For more information, see Access Rules Page (IPv4 or IPv6), page 14-9.

Related Topics
- Generating Hit Count Reports, page 14-24
- Understanding Access Rules, page 14-2
Field Reference

Table 14-6 Hit Count Selection Summary Dialog Box

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Selected</td>
<td>Identifies the selected policy. If you do not select any policy, this is typically 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.</td>
</tr>
</tbody>
</table>
| Rules Selected   | The rules for which you want to obtain hit counts.  

- 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.  
- Select the option for your selected rules to obtain information for only those rules. 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. |

Analyzing Hit Count Query Results

Use Hit Count Query Results page to view information about the number of times an IPv4 or IPv6 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).

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). For an example of a hit count report, see Generating Hit Count Reports, page 14-24.

Consider the following points when analyzing the hit count results:

- 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 11-7), 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 12-30, you might not get good hit count information.
- If you enable ACL optimization, as described in Optimizing Access Rules Automatically During Deployment, page 14-36, 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.
Navigation Path

(Device view only) From the Access Rules Page (IPv4 or IPv6), page 14-9, click the Tools button, select Hit Count, and then click OK in the Hit Count Selection Summary Dialog Box, page 14-27.

Related Topics

- Generating Hit Count Reports, page 14-24
- Understanding Access Rules, page 14-2
- Table Columns and Column Heading Features, page 1-38
- Using Category Objects, page 6-9

Field Reference

Table 14-7  Hit Count Query Results Page

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Device</td>
<td>The device for which you are displaying hit count information.</td>
</tr>
<tr>
<td>Refresh Hit Count button</td>
<td>Click this button to update the hit count information. The difference between the last hit count and the updated hit count is listed in the Delta column in the expanded table (in the lower pane). The amount of time since the last refresh is shown next to the button to help you evaluate the delta count. Obtaining refreshed information can take some time, so you are given the opportunity to abort the refresh.</td>
</tr>
<tr>
<td>Selected Access Rules table</td>
<td>The rules you selected for obtaining hit count information. The hit count is the sum of the hit counts for all ACEs created by the rule. The other information is the same as in the Access Rules Page (IPv4 or IPv6), page 14-9. Select one or more rules in this table to see detailed information for the access control entries (ACEs) associated with the rule in the tables in the lower half of the window.</td>
</tr>
<tr>
<td>Choose</td>
<td>Select whether you want to see the expanded table or the raw ACE table (both explained below).</td>
</tr>
</tbody>
</table>
Chapter 14  Managing Firewall Access Rules

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 from a device running-configuration or by typing in the desired commands. By using the Import Rules wizard, you can quickly create all of the 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 to define your rules.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expanded table</td>
<td>Lists the device’s access control list entries (ACEs) for the rule selected in the upper table (Selected Access Rules table). The list contains more than one ACE if the access rule generated more than one ACE when you deployed the policy to the device. The columns in the table match those of the upper table, except they 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 additional Delta column contains the number of hits for the ACE since the last time you clicked the Refresh Hit Count button. The Hit Count column shows the hits for the specific ACE rather than the overall rule.</td>
</tr>
<tr>
<td>Raw ACE table</td>
<td>Shows the actual CLI for the access control entry, along with the hit count. Use this information if you are more comfortable evaluating device commands.</td>
</tr>
</tbody>
</table>

**Step 1**
(Device view only) Select Firewall > Access Rules to open the Access Rules Page (IPv4 or IPv6), page 14-9.

**Note** You cannot import IPv6 access rules.

**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**
Click the Tools button and select Import Rules to start the wizard (see Import Rules Wizard—Enter Parameters Page, page 14-31).
Step 4  Enter the CLI in running-configuration format appropriate for the type of device. Select 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 14-3). Also, select the traffic direction with respect to the interface (the direction is always In for global rules).

For examples of importable CLI, see Examples of Imported Rules, page 14-34.

Beside access control rules, you should also include the CLI for the following items if they are referred to by the rules:

- 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 object network and object service commands. However, any object NAT configuration is not imported.

You are prompted if your CLI contains errors when you click the Next button. For some detailed tips about what you can enter, see Import Rules Wizard—Enter Parameters Page, page 14-31.

Step 5  Click Next to process the rules and open the Import Rules Wizard—Status Page, page 14-32.

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

Step 6  Click Finish to import the rules, or click Next to view the rules and objects on the Import Rules Wizard—Preview Page, page 14-33.

The information on the Preview page is read-only. If the rules are acceptable, click Finish. If you want to make changes, you can edit them in the access rules policy.

---

**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:

- 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) Click the Tools button and select Import Rules from the Access Rules Page (IPv4 or IPv6), page 14-9.

**Related Topics**

- Importing Rules, page 14-30
- Understanding Interface Role Objects, page 6-56
Field Reference

Table 14-8 Import Rules - Enter Parameters Dialog Box

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI</td>
<td>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 14-34.</td>
</tr>
<tr>
<td>CLI</td>
<td>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 14-34.</td>
</tr>
<tr>
<td>CLI</td>
<td>Tips</td>
</tr>
<tr>
<td>interface</td>
<td>Interface</td>
</tr>
<tr>
<td>global (ASA 8.3+)</td>
<td>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 14-3). 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.</td>
</tr>
<tr>
<td>traffic direction</td>
<td>The direction of the traffic with respect to the interface, in or out.</td>
</tr>
</tbody>
</table>

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 14-31

Related Topics
- Importing Rules, page 14-30
Field Reference

Table 14-9 Import Rules Wizard—Status Page

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Progress bar</td>
<td>Shows the status of the import process.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the imported configuration.</td>
</tr>
<tr>
<td>Rules Imported</td>
<td>The number of rules that will be imported.</td>
</tr>
<tr>
<td>Policy Objects Created</td>
<td>The number of policy objects that will be created.</td>
</tr>
<tr>
<td>Messages</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Abort button</td>
<td>Click this button to stop the import operation.</td>
</tr>
</tbody>
</table>

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 14-31.

Related Topics

- Importing Rules, page 14-30
- Access Rules Page (IPv4 or IPv6), page 14-9
- Understanding Network/Host Objects (IPv4 and IPv6), page 6-63
- Understanding Interface Role Objects, page 6-56
- Understanding and Specifying Services and Service and Port List Objects, page 6-72
- Filtering Tables, page 1-37
Field Reference

Table 14-10  Import Rules Wizard—Preview Page

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. Google Ads? 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 14-30.

**Note**

You cannot import IPv6 access control rules.

**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.

```plaintext
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.
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.

<table>
<thead>
<tr>
<th>No.</th>
<th>Permit</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Interface</th>
<th>Dir.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✓</td>
<td>172.16.2.38</td>
<td>any</td>
<td>TCP</td>
<td>Ethernet0</td>
<td>in</td>
<td>Permit only for TCP traffic from 172.16.2.38.</td>
</tr>
<tr>
<td>2</td>
<td>✓</td>
<td>172.16.3.10</td>
<td>any</td>
<td>TCP</td>
<td>Ethernet0</td>
<td>in</td>
<td>Do not allow TCP traffic from 172.16.3.10.</td>
</tr>
</tbody>
</table>

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


## 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.

**Note**

The optimization described in this topic applies to IPv4 ACLs only. Optimization does not work with IPv6 ACLs.

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:

```plaintext
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:

```plaintext
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 downsides 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 Generating Hit Count Reports, page 14-24 and Viewing CS-MARS Events for an Access Rule, page 65-26.

- Optimization does not address inherent problems in your access rules policy. It is typically better to address redundancies and conflicts proactively by using the rule analysis tool (see Generating Analysis Reports, page 14-22). 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 12-19).

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 \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 filename.