

Tuning Traffic Flow Using Access Control Rules

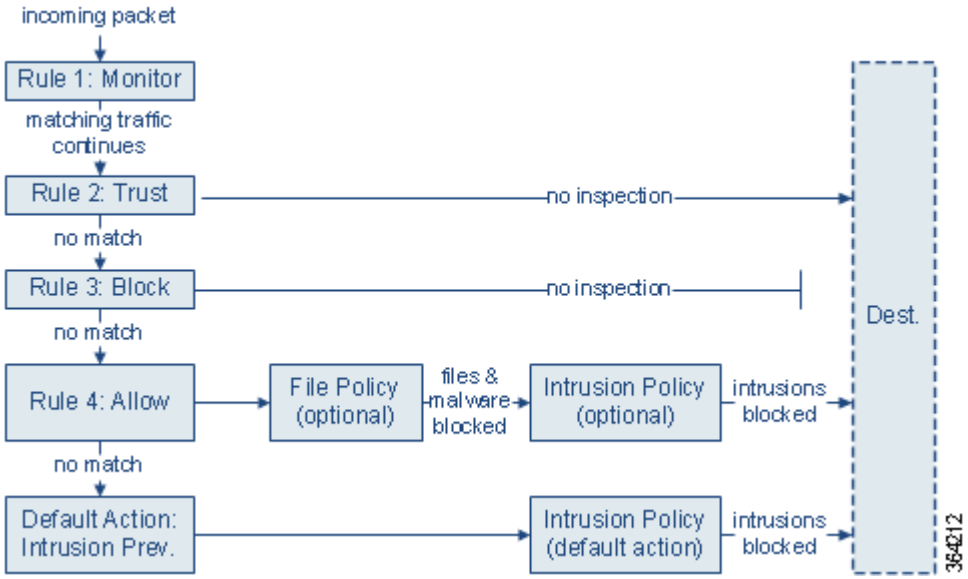
Within an access control policy, *access control rules* provide a granular method of handling network traffic.

Note Security Intelligence-based traffic filtering, and some decoding and preprocessing occur **before** network traffic is evaluated by access control rules. You can also configure the *SSL inspection* feature to block or decrypt encrypted traffic before access control rules evaluate it.

The system matches traffic to access control rules in the order you specify. In most cases, the system handles network traffic according to the *first* access control rule where *all* the rule's conditions match the traffic. Conditions can be simple or complex; you can control traffic by security zone, network or geographical location, port, application, requested URL, and user.

Each rule also has an *action*, which determines whether you monitor, trust, block, or allow matching traffic. When you allow traffic, you can specify that the system first inspect it with intrusion or file policies to block any exploits, malware, or prohibited files before they reach your assets or exit your network. However, after the system trusts or blocks traffic, it does **not** perform further inspection.

The following scenario summarizes the ways that traffic can be evaluated by access control rules in an inline, intrusion prevention deployment.



In this scenario, traffic is evaluated as follows:

- **Rule 1: Monitor** evaluates traffic first. Monitor rules track and log network traffic but do not affect traffic flow. The system continues to match traffic against additional rules to determine whether to permit or deny it.
- **Rule 2: Trust** evaluates traffic next. Matching traffic is allowed to pass to its destination without further inspection. Traffic that does not match continues to the next rule.
- **Rule 3: Block** evaluates traffic third. Matching traffic is blocked without further inspection. Traffic that does not match continues to the final rule.
- **Rule 4: Allow** is the final rule. For this rule, matching traffic is allowed; however, prohibited files, malware, intrusions, and exploits within that traffic are detected and blocked. Remaining non-prohibited, non-malicious traffic is allowed to its destination. Note that you might have additional Allow rules that perform only file inspection, or only intrusion inspection, or neither.
- **Default Action** handles all traffic that does not match any of the rules. In this scenario, the default action performs intrusion prevention before allowing non-malicious traffic to pass. In a different deployment, you might have a default action that trusts or blocks all traffic, without further inspection. (You cannot perform file or malware inspection on traffic handled by the default action.)

For more information on access control rules, see:

- Creating and Editing Access Control Rules, page 6-2
- Managing Access Control Rules in a Policy, page 6-11
- Troubleshooting Access Control Policies and Rules, page 4-12

Creating and Editing Access Control Rules

License: Any

Within an access control policy, access control rules provide a granular method of handling network traffic. In addition to its unique name, each access control rule has the following basic components:

State

By default, rules are enabled. If you disable a rule, the system does not use it to evaluate network traffic, and stops generating warnings and errors for that rule.

Position

Rules in an access control policy are numbered, starting at 1. The system matches traffic to rules in top-down order by ascending rule number. With the exception of Monitor rules, the first rule that traffic matches is the rule that handles that traffic.

Conditions

Conditions specify the specific traffic the rule handles. Conditions can match traffic by security zone, network or geographical location, port, application, requested URL, or user. Conditions can be simple or complex; their use often depends on license.

Action

A rule's action determines how the system handles matching traffic. You can monitor, trust, block, or allow (with or without further inspection) matching traffic. Note that the system does **not** perform inspection on trusted or blocked traffic.

Inspection

Inspection options for an access control rule govern how the system inspects and blocks malicious traffic you would otherwise allow. When you allow traffic with a rule, you can specify that the system first inspect it with intrusion or file policies to block any exploits, malware, or prohibited files before they reach your assets or exit your network.

Logging

A rule's logging settings govern the records the system keeps of the traffic it handles. You can keep a record of traffic that matches a rule. In general, you can log sessions at the beginning and end of a connection. You can log connections to the ASA FirePOWER module, as well as to the system log (syslog) or to an SNMP trap server.

Comments

Each time you save changes to an access control rule, you can add a comment.

Use the access control rule editor to add and edit access control rules; access the rule editor from the Rules tab of the access control policy editor. In the rule editor, you:

- Configure basic properties such as the rule's name, state, position, and action in the upper portion of the editor.
- Add conditions using the tabs on the left side of the lower portion of the editor.
- Use the tabs on the right side of the lower portion to configure inspection and logging options, and also to add comments to the rule. For your convenience, the editor lists the rule's inspection and logging options regardless of which tab you are viewing.



Note Properly creating and ordering access control rules is a complex task, but one that is essential to building an effective deployment. If you do not plan your policy carefully, rules can preempt other rules, require additional licenses, or contain invalid configurations. To help ensure that the system handles traffic as

you expect, the access control policy interface has a robust warning and error feedback system for rules. For more information, see Troubleshooting Access Control Policies and Rules, page 4-12.

To create or modify an access control rule:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**.

Step 2 Click the edit icon ( ) next to the access control policy where you want to add a rule.

Step 3 You have the following options:

- To add a new rule, click **Add Rule**.
- To edit an existing rule, click the edit icon ( ) next to the rule you want to edit.

Step 4 Enter a **Name** for the rule.

Each rule must have a unique name. You can use up to thirty printable characters, including spaces and special characters, with the exception of the colon (:).

Step 5 Configure the rule components, as summarized above. You can configure the following, or accept the defaults:

- Specify whether the rule is **Enabled**.
- Specify the rule position; see Specifying a Rule's Order of Evaluation, page 6-4.
- Specify a rule **Action**; see Using Rule Actions to Determine Traffic Handling and Inspection, page 6-7.
- Configure the rule's conditions; see Using Conditions to Specify the Traffic a Rule Handles, page 6-5.
- For Allow and Interactive Block rules, configure the rule's **Inspection** options; see Controlling Traffic Using Intrusion and File Policies, page 11-1.
- Configure content restriction settings by clicking the Safe Search ( ) or YouTube EDU ( ) icon on the **Applications** tab. If the icons are dimmed, content restriction is disabled for the rule. For more information, see Using Access Control Rules to Enforce Content Restriction, page 13-1.
- Specify **Logging** options; see Logging Connections in Network Traffic, page 36-1.
- Add **Comments**; see Adding Comments to a Rule, page 6-10.

Step 6 Click **Store FirePOWER Changes** to save the rule.

Your rule is saved. You can click the delete icon ( ) to delete the rule. You must apply the access control policy for your changes to take effect; see Deploying Configuration Changes, page 4-11.

Specifying a Rule's Order of Evaluation

License: Any

When you first create an access control rule, you specify its position using the **Insert** drop-down list in the rule editor. Rules in an access control policy are numbered, starting at 1. The system matches traffic to access control rules in top-down order by ascending rule number.

In most cases, the system handles network traffic according to the *first* access control rule where *all* the rule's conditions match the traffic. Except in the case of Monitor rules (which log traffic but do not affect traffic flow), the system does **not** continue to evaluate traffic against additional, lower-priority rules after that traffic matches a rule.

Tip Proper access control rule order reduces the resources required to process network traffic, and prevents rule preemption. Although the rules you create are unique to every organization and deployment, there are a few general guidelines to follow when ordering rules that can optimize performance while still addressing your needs. For more information, see Ordering Rules to Improve Performance and Avoid Preemption, page 4-14.

In addition to ordering rules by number, you can group rules by category. By default the system provides three categories: Administrator, Standard, and Root. You can add custom categories, but you cannot delete the Cisco-provided categories or change their order. For information on changing the position or category of an existing rule, see Changing a Rule's Position or Category, page 6-13.

To add a rule to a category while editing or creating a rule:

Step 1 In the access control rule editor, from the **Insert** drop-down list, select **Into Category**, then select the category you want to use.

When you save the rule, it is placed last in that category.

To position a rule by number while editing or creating a rule:

Step 1 In the access control rule editor, from the **Insert** drop-down list, select **above rule** or **below rule**, then type the appropriate rule number.

When you save the rule, it is placed where you specified.

Using Conditions to Specify the Traffic a Rule Handles

License: feature dependent

An access control rule's conditions identify the type of traffic that rule handles. Conditions can be simple or complex; you can control traffic by security zone, network or geographical location, port, application, requested URL, and user.

When adding conditions to access control rules, keep the following points in mind:

- You can configure multiple conditions per rule. Traffic must match **all** the conditions in the rule for the rule to apply to traffic. For example, you can use a single rule to perform URL filtering (URL condition) for specific hosts (zone or network condition).
- For each condition in a rule, you can add up to 50 criteria. Traffic that matches **any** of a condition's criteria satisfies the condition. For example, you can use a single rule to perform user control for up to 50 users and groups.

Note that you can constrain zone and network conditions by source and destination, using up to 50 source and up to 50 destination criteria. If you add both source and destination criteria to a zone or network condition, matching traffic must originate from one of the specified source zones/networks **and** egress through one of the destination zones/networks. In other words, the system links multiple condition criteria of the same type with an OR operation, and links multiple condition types with an AND operation. For example, if your rule conditions are:

```
Source Networks: 10.0.0.0/8, 192.168.0.0/16
Application Category: peer to peer
```

the rule would match peer-to-peer application traffic from a host on one of your private IPv4 networks—a packet must originate from either one **OR** the other source network, **AND** represent peer-to-peer application traffic. Both of the following connections trigger the rule:

```
10.42.0.105 to anywhere, using LimeWire
192.168.42.105 to anywhere, using Kazaa
```

If you do not configure a particular condition for a rule, the system does not match traffic based on that criterion. For example, a rule with a network condition but no application condition evaluates traffic based on its source or destination, regardless of the application used in the session.

Note When you apply an access control policy, the system evaluates all its rules and creates an expanded set of criteria that the ASA FirePOWER module uses to evaluate network traffic. Complex access control policies and rules can command significant resources. For tips on simplifying access control rules and other ways to improve performance, see Troubleshooting Access Control Policies and Rules, page 4-12.

When you add or edit an access control rule, use the tabs on the left side of the lower portion of the rule editor to add and edit rule conditions. The following table summarizes the types of conditions you can add.

Table 6-1 Access Control Rule Condition Types

These Conditions...	Match Traffic...	Details
Zones	entering or leaving a device via an interface in a specific security zone	A security zone is a logical grouping of one or more interfaces according to your deployment and security policies. To build a zone condition, see Controlling Traffic by Security Zone, page 7-1.
Networks	by its source or destination IP address, country, or continent	You can explicitly specify IP addresses or address blocks. The geolocation feature also allows you to control traffic based on its source or destination country or continent. To build a network condition, see Controlling Traffic by Network or Geographical Location, page 7-3.
Ports	by its source or destination port	For TCP and UDP, you can control traffic based on the transport layer protocol. For ICMP and ICMPv6 (IPv6-ICMP), you can control traffic based on its Internet layer protocol plus an optional type and code. Using port conditions, you can also control traffic using other protocols that do not use ports. To build a port condition, see Controlling Traffic by Port and ICMP Codes, page 7-5.
Applications	by the application detected in a session	You can control access to individual applications, or filter access according to basic characteristics: type, risk, business relevance, categories, and tags. To build an application condition, see Controlling Application Traffic, page 8-2.

Table 6-1 Access Control Rule Condition Types (continued)

These Conditions...	Match Traffic...	Details
URLs	by the URL requested in the session	You can limit the websites that users on your network can access either individually or based on the URL's general classification and risk level. To build a URL condition, see Blocking URLs, page 8-7.
Users	by the user involved in the session	You can control traffic based on the LDAP user logged into a host involved in a monitored session. You can control traffic based on individual users or groups retrieved from a Microsoft Active Directory server. To build a user condition, see Access Control Rules: Realms and Users, page 9-1.

Note that although you can create access control rules with any license, certain rule conditions require that you enable specific licensed capabilities before you can apply the policy. For more information, see License Requirements for Access Control, page 4-2.

Using Rule Actions to Determine Traffic Handling and Inspection

License: Any

Every access control rule has an *action* that determines the following for matching traffic:

- handling—foremost, the rule action governs whether the system will monitor, trust, block, or allow traffic that matches the rule's conditions
- inspection—certain rule actions allow you, when properly licensed, to further inspect matching traffic before allowing it to pass
- logging—the rule action determines when and how you can log details about matching traffic

The access control policy's *default action* handles traffic that does not meet the conditions of any non-Monitor access control rule; see Setting Default Handling and Inspection for Network Traffic, page 4-4.

Keep in mind that only devices deployed inline can block or modify traffic. Devices deployed passively can analyze and log, but not affect, the flow of traffic. For detailed information on rule actions and how they affect traffic handling, inspection, and logging, see the following sections:

- Monitor Action: Postponing Action and Ensuring Logging, page 6-8
- Trust Action: Passing Traffic Without Inspection, page 6-8
- Blocking Actions: Blocking Traffic Without Inspection, page 6-8
- Interactive Blocking Actions: Allowing Users to Bypass Website Blocks, page 6-9
- Allow Action: Allowing and Inspecting Traffic, page 6-10
- Controlling Traffic Using Intrusion and File Policies, page 11-1
- Logging Connections Based on Access Control Handling, page 36-9

Monitor Action: Postponing Action and Ensuring Logging

License: Any

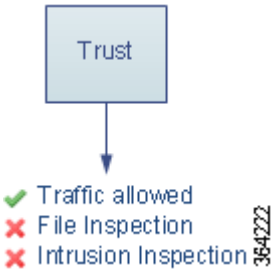
The **Monitor** action does not affect traffic flow; matching traffic is neither immediately permitted nor denied. Rather, traffic is matched against additional rules to determine whether to permit or deny it. The first non-Monitor rule matched determines traffic flow and any further inspection. If there are no additional matching rules, the system uses the default action.

Because the primary purpose of Monitor rules is to track network traffic, the system automatically logs end-of connection events for monitored traffic. That is, connections are logged even if the traffic matches no other rules and you do not enable logging on the default action. For more information, see Understanding Logging for Monitored Connections, page 36-5.

Trust Action: Passing Traffic Without Inspection

License: Any

The **Trust** action allows traffic to pass without further inspection of any kind.

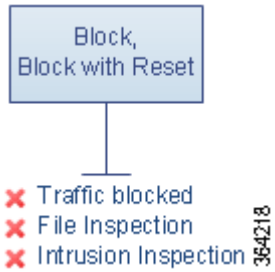


You can log trusted network traffic at both the beginning and end of connections. For more information, see Understanding Logging for Trusted Connections, page 36-5.

Blocking Actions: Blocking Traffic Without Inspection

License: Any

The **Block** and **Block with reset** actions deny traffic without further inspection of any kind. Block with reset rules also reset the connection.



For decrypted HTTP traffic, when the system blocks a web request, you can override the default browser or server page with a custom page that explains that the connection was denied. The system calls this custom page an *HTTP response page*; see Displaying a Custom Web Page for Blocked URLs, page 8-14.

You can log blocked network traffic only at the beginning of connections. Note that only devices deployed inline can block traffic. Because blocked connections are not actually blocked in passive deployments, the system may report multiple beginning-of-connection events for each blocked connection. For more information, see Understanding Logging for Blocked and Interactively Blocked Connections, page 36-5.

Caution Logging blocked TCP connections during a Denial of Service (DoS) attack can affect system performance with multiple similar events. Before you enable logging for an Block rule, consider whether the rule monitors traffic on an Internet-facing interface or other interface vulnerable to DoS attack.

Interactive Blocking Actions: Allowing Users to Bypass Website Blocks

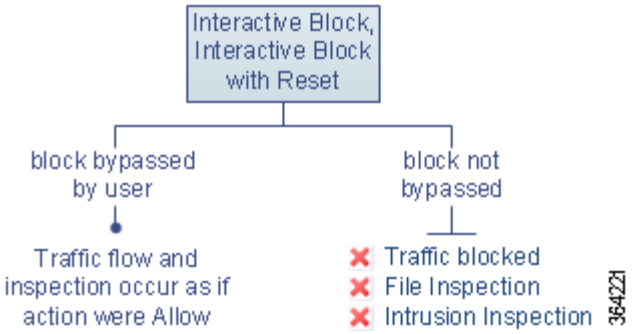
License: Any

For decrypted HTTP traffic, the **Interactive Block** and **Interactive Block with reset** actions give users a chance to bypass a website block by clicking through a customizable warning page, called an *HTTP response page*. Interactive Block with reset rules also reset the connection.

If you configure SSL inspection to decrypt web traffic and that traffic matches an Interactive Block rule, the system encrypts the response page and sends it at the end of the reencrypted SSL response stream.

For all interactively blocked traffic, the system's handling, inspection, and logging depend on whether the user bypasses the block:

- If a user does not (or cannot) bypass the block, the rule mimics a Block rule. Matching traffic is denied without further inspection and you can log only the beginning of the connection. These beginning-of-connection events have an `Interactive Block` or `Interactive Block with Reset` action.
- If a user bypasses the block, the rule mimics an Allow rule. Therefore, you can associate either type of Interactive Block rule with a file and intrusion policy to inspect this user-allowed traffic. The system can also log both beginning and end-of-connection events. These connection events have an action of `Allow`.



Allow Action: Allowing and Inspecting Traffic

License: Any

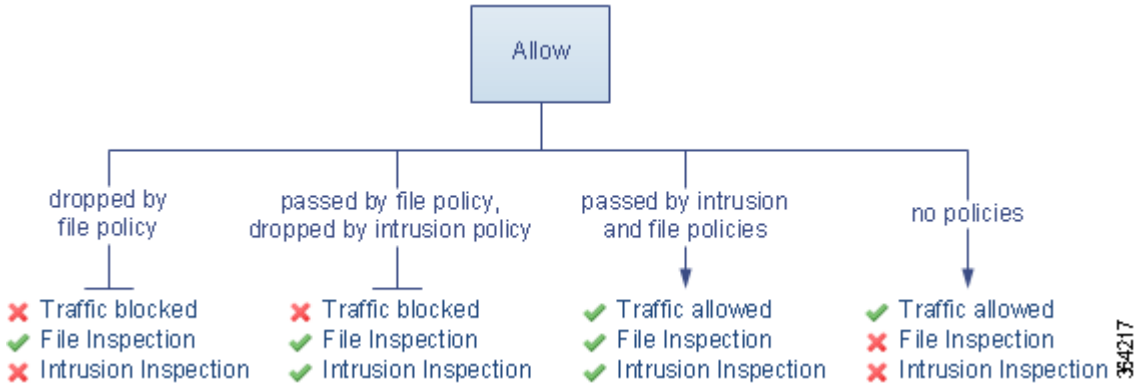
The **Allow** action allows matching traffic to pass. When you allow traffic, you can use an associated intrusion or file policy (or both) to further inspect and block unencrypted or decrypted network traffic:

- With a Protection license, you can use an intrusion policy to analyze network traffic according to intrusion detection and prevention configurations and, optionally, drop offending packets.
- Also with a Protection license, you can perform file control using a file policy. File control allows you to detect and block your users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols.
- With a Malware license, you can perform network-based advanced malware protection (AMP), also using a file policy. Network-based AMP can inspect files for malware, and optionally block detected malware.

For instructions on how to associate an intrusion or file policy with an access control rule, see Controlling Traffic Using Intrusion and File Policies, page 11-1.

The diagram below illustrates the types of inspection performed on traffic that meets the conditions of an Allow rule (or a user-bypassed Interactive Block rule; see Interactive Blocking Actions: Allowing Users to Bypass Website Blocks, page 6-9). Notice that file inspection occurs before intrusion inspection; blocked files are not inspected for intrusion-related exploits.

For simplicity, the diagram displays traffic flow for situations where both (or neither) an intrusion and a file policy are associated with an access control rule. You can, however, configure one without the other. Without a file policy, traffic flow is determined by the intrusion policy; without an intrusion policy, traffic flow is determined by the file policy.



You can log allowed network traffic at both the beginning and end of connections.

Adding Comments to a Rule

License: Any

When you create or edit an access control rule, you can add a comment. For example, you might summarize the overall configuration for the benefit of other users, or note when you change a rule and the reason for the change. You can display a list of all comments for a rule along with the user who added each comment and the date the comment was added.

When you save a rule, all comments made since the last save become read-only.

To add a comment to a rule:

Step 1 In the access control rule editor, select the **Comments** tab.

The Comments page appears.

Step 2 Click **New Comment**.

The New Comment pop-up window appears.

Step 3 Type your comment and click **OK**.

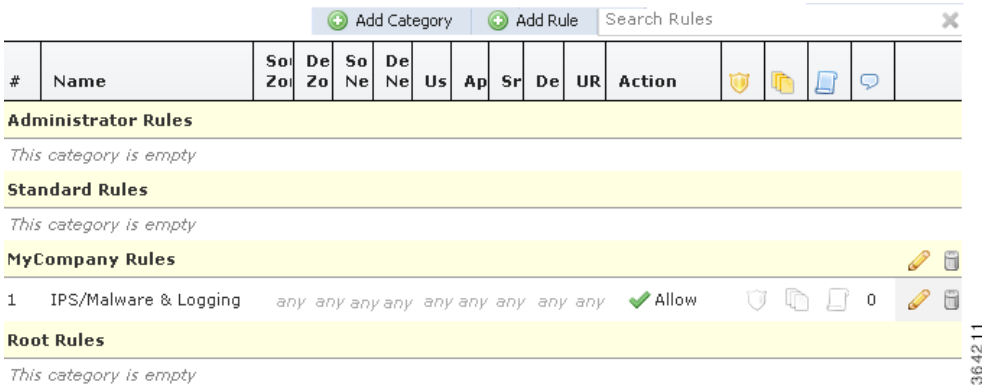
Your comment is saved. You can edit or delete this comment until you save the rule.

Step 4 Save or continue editing the rule.

Managing Access Control Rules in a Policy

License: Any

The Rules tab of the access control policy editor, shown in the following graphic, allows you to add, edit, search, move, enable, disable, delete, and otherwise manage access control rules within your policy.



For each rule, the policy editor displays its name, a summary of its conditions, the rule action, plus icons that communicate the rule's inspection and logging options. Other icons represent comments, warnings, errors, and other important information, as described in the following table. Disabled rules are grayed and marked `(disabled)` beneath the rule name.

Table 6-2 Understanding the Access Control Policy Editor

Icon	Description	You can...
	intrusion inspection	Click an active (yellow) inspection icon to edit the inspection options for the rule; see Controlling Traffic Using Intrusion and File Policies, page 11-1. If the icon is inactive (white), no policy of that type is selected for the rule.
	file and malware inspection	

Table 6-2 Understanding the Access Control Policy Editor (continued)

Icon	Description	You can...
	logging	Click an active (blue) logging icon to edit the logging options for the rule; see Logging Connections Based on Access Control Handling, page 36-9. If the icon is inactive (white), connection logging is disabled for the rule.
	comment	Click the number in the comment column to add a comment to a rule; see Adding Comments to a Rule, page 6-10. The number indicates how many comments the rule already contains.
	warning	In the access control policy editor, click **Show Warnings** to display a pop-up window that lists all the warnings for the policy; see Troubleshooting Access Control Policies and Rules, page 4-12.
	error	
	information	

For information on managing access control rules, see:

- Creating and Editing Access Control Rules, page 6-2
- Searching Access Control Rules, page 6-12
- Enabling and Disabling Rules, page 6-13
- Changing a Rule's Position or Category, page 6-13

Searching Access Control Rules

License: Any

You can search the list of access control rules for matching values using an alphanumeric string, including spaces and printable, special characters. The search inspects the rule name and any rule condition you have added to the rule. For rule conditions, the search matches any name or value you can add for each condition type (zone, network, application, and so on). This includes individual object names or values, group object names, individual object names or values within a group, and literal values.

You can use complete or partial search strings. The column for matching values is highlighted for each matching rule. For example, if you search on all or part of the string `100Bao`, at a minimum, the Applications column is highlighted for each rule where you have added the 100Bao application. If you also have a rule named 100Bao, both the Name and Applications columns are highlighted.

You can navigate to each previous or next matching rule. A status message displays the current match and the total number of matches.

Matches may occur on any page of a multi-page rule list. When the first match is not on the first page, the page where the first match occurs is displayed. Selecting the next match when you are at the last match takes you to the first match, and selecting the previous match when you are at the first match takes you to the last match.

To search for rules:

Step 1 In the access control policy editor for the policy you want to search, click the **Search Rules** prompt, type a search string, then press Enter. You can also use the Tab key or click a blank page area to initiate the search.

Columns for rules with matching values are highlighted, with differentiated highlighting for the indicated (first) match.

Step 2 Find the rules you are interested in:

- To navigate between matching rules, click the next-match (▼) or previous-match (▲) icon.
- To refresh the page and clear the search string and any highlighting, click the clear icon (✖).

Enabling and Disabling Rules

License: Any

When you create an access control rule, it is enabled by default. If you disable a rule, the system does not use it to evaluate network traffic and stops generating warnings and errors for that rule. When viewing the list of rules in an access control policy, disabled rules are grayed out, although you can still modify them. Note that you can also enable or disable an access control rule using the rule editor; see Creating and Editing Access Control Rules, page 6-2.

To change an access control rule's state:

Step 1 In the access control policy editor for the policy that contains the rule you want to enable or disable, right-click the rule and choose a rule state:

- To enable an inactive rule, select **State > Enable**.
- To disable an active rule, select **State > Disable**.

Step 2 Click **Store FirePOWER Changes** to save the policy.

You must apply the access control policy for your changes to take effect; see Deploying Configuration Changes, page 4-11.

Changing a Rule's Position or Category

License: Any

To help you organize access control rules, every access control policy has three system-provided rule categories: Administrator Rules, Standard Rules, and Root Rules. You cannot move, delete, or rename these categories, although you can create custom categories.

For more information, see:

- Moving a Rule, page 6-14
- Adding a New Rule Category, page 6-14

Moving a Rule

License: Any

Proper access control rule order reduces the resources required to process network traffic, and prevents rule preemption.

The following procedure explains how to move one or more rules at a time using the access control policy editor. You can also move individual access control rules using the rule editor; see Creating and Editing Access Control Rules, page 6-2.

To move a rule:

Step 1 In the access control policy editor for the policy that contains the rules you want to move, select the rules by clicking in a blank area for each rule. Use the Ctrl and Shift keys to select multiple rules.

The rules you selected are highlighted.

Step 2 Move the rules. You can cut and paste or drag and drop.

To cut and paste rules into a new location, right-click a selected rule and select **Cut**. Then, right-click a blank area for a rule next to where you want to paste the cut rules and select **Paste above** or **Paste below**. Note that you cannot copy and paste access control rules between two different access control policies.

Step 3 Click **Store FirePOWER Changes** to save the policy.

You must apply the access control policy for your changes to take effect; see Deploying Configuration Changes, page 4-11.

Adding a New Rule Category

License: Any

To help you organize access control rules, every access control policy has three system-provided rule categories: Administrator Rules, Standard Rules, and Root Rules. You cannot move, delete, or rename these categories, although you can create custom categories between the Standard Rules and Root Rules.

Adding custom categories allows you to further organize your rules without having to create additional policies. You can rename and delete categories that you add. You cannot move these categories, but you can move rules into, within, and out of them.

To add a new category:

Step 1 In the access control policy editor for the policy where you want to add a rule category, click Add Category.

Tip If your policy already contains rules, you can click a blank area in the row for an existing rule to set the position of the new category before you add it. You can also right-click an existing rule and select **Insert new category**.

The Add Category pop-up window appears.

Step 2 Type a unique category **Name**.

You can enter an alphanumeric name, including spaces and special printable characters, with up to 30 characters.

Step 3 You have the following choices:

- To position the new category immediately above an existing category, select **above Category** from the first **Insert** drop-down list, then select the category above which you want to position the rule from the second drop-down list.
- To position the new category rule below an existing rule, select **below rule** from the drop-down list, then enter an existing rule number. This option is valid only when at least one rule exists in the policy.
- To position the rule above an existing rule, select **above rule** from the drop-down list, then, enter an existing rule number. This option is valid only when at least one rule exists in the policy.

Step 4 Click **OK**.

Your category is added. You can click the edit icon ( ) next to a custom category to edit its name, or click the delete icon ( ) to delete the category. Rules in a category you delete are added to the category above.

Step 5 Click **Store FirePOWER Changes** to save the policy.