



Access Control Rules

The following topics describe how to configure access control rules:

- [Introduction to Access Control Rules, page 1](#)
- [Adding an Access Control Rule Category, page 6](#)
- [Creating and Editing Access Control Rules, page 6](#)
- [Enabling and Disabling Access Control Rules, page 8](#)
- [Positioning an Access Control Rule, page 8](#)
- [Access Control Rule Conditions and Traffic Handling, page 9](#)
- [Access Control Rule Actions, page 10](#)
- [Access Control Rule Comments, page 15](#)
- [Searching Access Control Rules, page 15](#)
- [Access Control Rules and Affected Devices, page 16](#)

Introduction to Access Control Rules

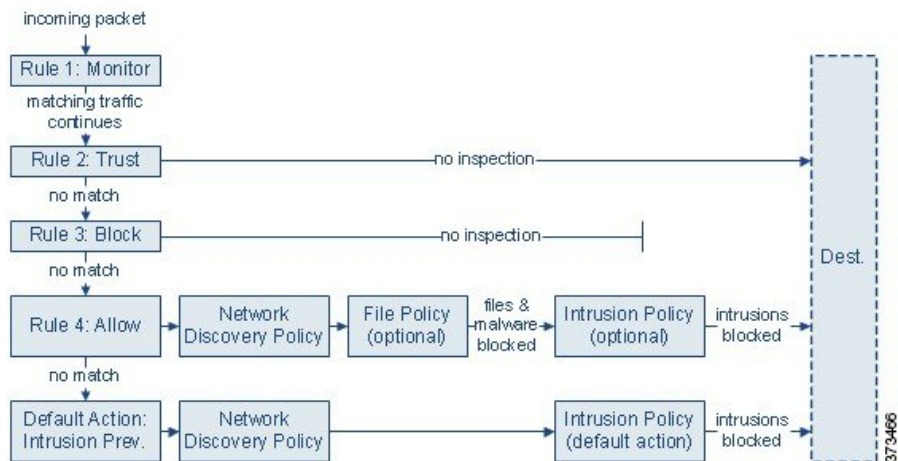
Within an access control policy, *access control rules* provide a granular method of handling network traffic across multiple managed devices.

Hardware-based fast-path rules, Security Intelligence-based traffic filtering, SSL inspection, user identification, and some decoding and preprocessing occur before access control rules evaluate network traffic.

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.

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.

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.)

Traffic you allow, whether with an access control rule or the default action, is automatically eligible for inspection for host, application, and user data by the network discovery policy. You do not explicitly enable discovery, although you can enhance or disable it. However, allowing traffic does not automatically guarantee discovery data collection. The system performs discovery only for connections involving IP addresses that are explicitly monitored by your network discovery policy; additionally, application discovery is limited for encrypted sessions.

Note that access control rules handle encrypted traffic when your SSL inspection configuration allows it to pass, or if you do not configure SSL inspection. However, some access control rule conditions require unencrypted traffic, so encrypted traffic may match fewer rules. Also, by default, the system disables intrusion and file inspection of encrypted payloads. This helps reduce false positives and improve performance when an encrypted connection matches an access control rule that has intrusion and file inspection configured.

Access Control Rule Management

The **Rules** tab of the access control policy editor allows you to add, edit, categorize, search, move, enable, disable, delete, and otherwise manage access control rules in the current policy.

For each access control 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 (ℹ). Disabled rules are dimmed and marked (disabled) beneath the rule name.

To create or edit a rule, use the access control rule editor. You can:

- 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.

Access Control Rule Inheritance

Each access control policy has two system-provided rule sections: Mandatory and Default. All access control rules must belong to one of those sections. An access control policy's rules are nested between its parent policy's Mandatory and Default rule sections.

You can only add and edit rules in the policy you are currently editing, which appears as the innermost policy. You cannot view or edit rules in descendant policies; you can view but not edit the rules in ancestor policies.

In a typical deployment, where you deploy the innermost access control policy, the system matches traffic against Mandatory rules in every policy, starting with the outermost and working inwards. If traffic does not match any Mandatory rules, the system uses the Default rules in every policy, starting with the innermost and working outwards.

Although you can strictly enforce other settings on descendant policies, you cannot enforce Default rules or the default action:

- Mandatory access control rules preempt rules in descendant policies. The system matches traffic against the Mandatory rules in every ancestor policy before it matches traffic against the rules in the deployed policy. Place a rule in the Mandatory section if you want the rule to handle traffic before any descendant policy's rules.
- Default access control rules preempt rules in ancestor policies. Place a rule in the Default section if you want to allow descendant policies' rules to handle the target traffic a different way.

- If traffic matches none of the (non-Monitor) rules in either the deployed policy or the deployed policy's ancestors, the system uses the deployed policy's default action. Although an access control policy can inherit its default action from an ancestor policy, you cannot enforce this inheritance.

For example, nested access control policies might display the following rule evaluation order while editing the innermost policy:

- Mandatory rules - Global Policy
 - Mandatory rules - Subdomain Policy
 - Default rules - Subdomain Policy
- Default rules - Global Policy
- Default action - Subdomain Policy

Access Control Rule Components

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 and stops generating warnings and errors for that rule.

Position

Rules in an access control policy are numbered, starting at 1. If you are using policy inheritance, rule 1 is the first rule in the outermost policy. 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.

Rules can also belong to a section and a category, which are organizational only and do not affect rule position. Rule position goes across sections and categories.

Section and Category

To help you organize access control rules, every access control policy has two system-provided rule sections, Mandatory and Default. To further organize access control rules, you can create custom rule categories inside the Mandatory and Default sections.

If you are using policy inheritance, the current policy's rules are nested between its parent policy's Mandatory and Default sections.

Conditions

Conditions specify the specific traffic the rule handles. 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. The system does **not** perform deep inspection on trusted, blocked, or encrypted traffic.

Inspection

Deep inspection options 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 or end of a connection, or both. You can log connections to the database, 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 comments.

Access Control Rule Order

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 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.

To help you organize access control rules, every access control policy has two system-provided rule sections, Mandatory and Default. To further organize, you can create custom rule categories inside the Mandatory or Default sections. After you create a category, you cannot move it, although you can delete it, rename it, and move rules into, out of, within, and around it. The system assigns rule numbers across sections and categories.

If you use policy inheritance, the current policy's rules are nested between its parent policy's Mandatory and Default rule sections. Rule 1 is the first rule in the outermost policy, not the current policy, and the system assigns rule numbers across policies, sections, and categories.

Any predefined user role that allows you to modify access control policies also allows you to move and modify access control rules within and among rules categories. You can, however, create custom roles that restrict users from moving and modifying rules. Any user who is allowed to modify access control policies can add rules to custom categories and modify rules in them without restriction.



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.

Adding an Access Control Rule Category

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin

You can divide an access control policy's Mandatory and Default rule sections into custom categories. After you create a category, you cannot move it, although you can delete it, rename it, and move rules into, out of, within, and around it. The system assigns rule numbers across sections and categories.

Procedure

-
- Step 1** In the access control policy editor, 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**.
- Step 2** Enter a **Name**.
- Step 3** From the **Insert** drop-down list, choose where you want to add the category:
- To insert a category below all existing categories in a section, choose **into Mandatory** or **into Default**.
 - To insert a category above an existing category, choose **above category**, then choose a category.
 - To insert a category above or below an access control rule, choose **above rule** or **below rule**, then enter an existing rule number.
- Step 4** Click **OK**.
- Step 5** Click **Save** to save the policy.
-

What to Do Next


- Deploy configuration changes; see [Deploying Configuration Changes](#).


Creating and Editing Access Control Rules

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin

Procedure




Step 1 In the access control policy editor, you have the following options:

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

If a view icon () appears next to a rule instead, the rule belongs to an ancestor policy, or you do not have permission to modify the rule.

Step 2 Type a **Name**.

Step 3 Configure the rule components, or accept the defaults:

- **Enabled** — Specify whether the rule is **Enabled**.
- **Position** — Specify the rule position; see [Access Control Rule Order](#), on page 5.
- **Action** — Select a rule **Action**; see [Access Control Rule Actions](#), on page 10.
- **Conditions** — Configure the rule's conditions; see [Access Control Rule Conditions and Traffic Handling](#), on page 9.
- **Deep Inspection** — For Allow and Interactive Block rules, click the intrusion inspection icon () or the file and malware inspection icon () to configure the rule's **Inspection** options. If the icons are inactive (white), no policy of that type is selected for the rule. See [Access Control Using Intrusion and File Policies](#) for more information.
- **Logging** — Click an active (blue) logging icon () to specify **Logging** options. If the icon is inactive (white), connection logging is disabled for the rule. See [Connection Logging](#) for more information.
- **Comments** — Click the number in the comment column to add **Comments**. The number indicates how many comments the rule already contains. See [Access Control Rule Comments](#), on page 15 for more information.

Step 4 Click **Save**.

Step 5 Click **Save** to save the policy.

What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).

Enabling and Disabling Access Control Rules

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin


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.


Tip

You can also enable or disable an access control rule using the rule editor.

Procedure

Step 1 In the access control policy editor, right-click the rule and choose a rule state.

If a view icon () appears next to a rule instead, the rule belongs to an ancestor policy, or you do not have permission to modify the rule.

Step 2 Click **Save**.

What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).

Positioning an Access Control Rule

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin

You can move an existing rule within, but not between, access control policies. When you add or move a rule to a category, the system places it last in the category.


Tip

You can move multiple rules at once by selecting the rules then cutting and pasting using the right-click menu.

Procedure

- Step 1** In the access control rule editor, you have the following options:
- If you are adding a new rule, use the **Insert** drop-down list.
 - If you are editing an existing rule, click **Move**.
- Step 2** Choose where you want to move or insert the rule:
- Choose **into Mandatory** or **into Default**.
 - Choose a **into Category**, then choose the user-defined category.
 - Choose **above rule** or **below rule**, then type the appropriate rule number.
- Step 3** Click **Save**.
- Step 4** Click **Save** to save the policy.
-

What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).

Access Control Rule Conditions and Traffic Handling

An access control rule's conditions identify the type of traffic that rule handles.

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.

When adding conditions to access control rules:

- 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.
- Although you can configure the system without licensing your deployment, many features require that you enable the appropriate licenses before you deploy. Also, some features are only available on certain device models. Warning icons and confirmation dialog boxes designate unsupported features.



- Note** When you deploy an access control policy, the system evaluates all its rules and creates an expanded set of criteria that targeted devices use to evaluate network traffic. Complex access control policies and rules can command significant resources.
-

Access Control Rule Condition Types

When you build access control rules, each condition type has its own tab in the access control rule editor.

Zones

Matches traffic 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. Interfaces in a zone may be located across multiple devices.

Networks

Matches traffic by its source or destination IP address, country, or continent (geolocation).

Ports

Matches traffic 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.

VLAN Tags

Matches VLAN-tagged traffic. For access control, the system uses the innermost VLAN tag.

Applications

Matches traffic 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.

URLs

Matches traffic by the URL requested in the session. You can control access to individual websites, use lists and feeds, or filter access based on a site's general classification and risk level.

Users and Realms

Matches traffic by the user, user group, or realm involved in the session.

ISE Attributes

Matches traffic by ISE attribute (**Security Group Tag (SGT)**, **Endpoint Profile**, or **Endpoint Location**).

Access Control Rule Actions

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.

Only devices deployed inline (that is, using routed, switched, or transparent interfaces, or inline interface pairs) can block or modify traffic. Devices deployed passively or in tap mode can analyze and log, but not affect, the flow of traffic.

Access Control Rule Monitor Action

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.



Note

If locally-bound traffic matches a Monitor rule in a Layer 3 deployment, that traffic may bypass inspection. To ensure inspection of the traffic, enable **Inspect Local Router Traffic** in the advanced device settings for the managed device routing the traffic.

Access Control Rule Trust Action

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. Note that the system logs TCP connections handled by a Trust rule differently depending on the model of the device that detected the connection.

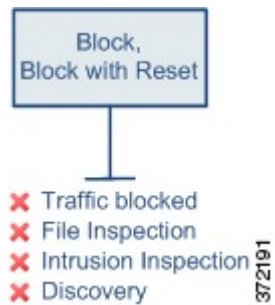


Caution

For most devices, the system processes certain Trust rules before an access control policy's Security Intelligence blacklist, which can allow blacklisted traffic to pass uninspected.

Access Control Rule Blocking Actions

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



For unencrypted 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*.

For decrypted and encrypted (HTTPS) traffic, Interactive Block rules block matching connections without interaction and the system does **not** display a response page.

Note that the system does not display the configured response page for some successfully blocked traffic handled by 7000 and 8000 Series devices. Instead, users requesting prohibited URLs have their connection either reset or time out.

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.



Caution

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

Access Control Rule Interactive Blocking Actions

For unencrypted 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.

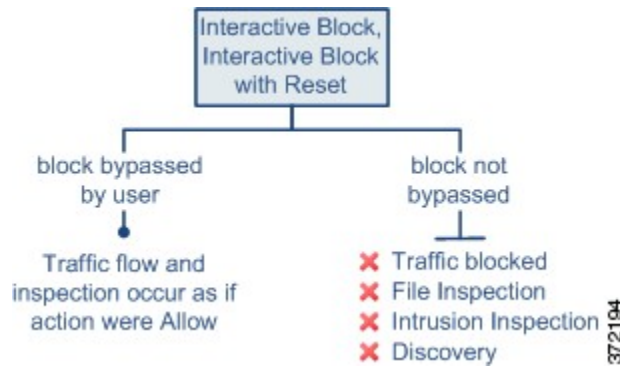


Note

For decrypted and encrypted (HTTPS) traffic, Interactive Block rules block matching connections without interaction and the system does **not** display a response page.

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 use network discovery to inspect it, and you can log both beginning and end-of-connection events. These connection events have an action of `Allow`.



Access Control Rule Allow Action

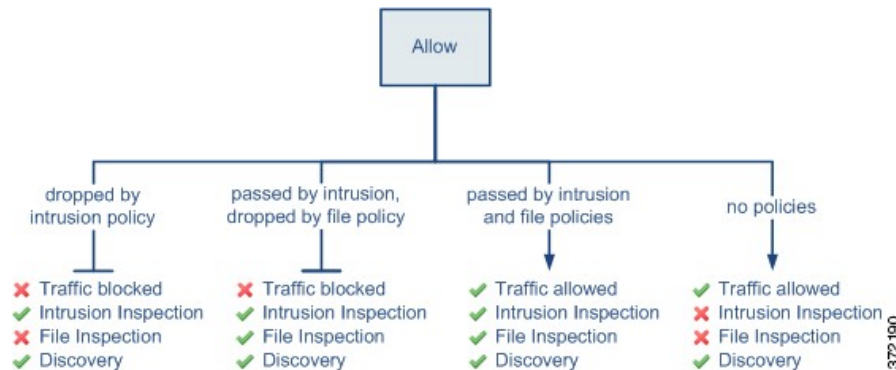
The **Allow** action allows matching traffic to pass. But, depending on your license, you can perform deep inspection to further inspect and block unencrypted or decrypted network traffic before it reaches its destination:

- You can use an intrusion policy to analyze network traffic according to intrusion detection and prevention configurations, and drop offending packets depending on the configuration.
- 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.
- You can perform network-based advanced malware protection (AMP), also using a file policy. AMP for Firepower can inspect files for malware, and block detected malware depending on the configuration.

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. 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.

Regardless of whether the traffic is inspected or dropped by an intrusion or file policy, the system can inspect it using network discovery. However, allowing traffic does not automatically guarantee discovery inspection. The system performs discovery only for connections involving IP addresses that are explicitly monitored by your network discovery policy; additionally, application discovery is limited for encrypted sessions.



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

Limitations to Trusting or Blocking Traffic

On any managed devices except NGIPSv and ASA FirePOWER, the system may *promote* access control rules that meet specific criteria. Promoted rules immediately divert or block traffic that does not require deep packet inspection. Their advantage is the speed at which they determine the correct path for the traffic.

Because this evaluation takes place at a basic level, the system can only use limited information to quickly handle connections by promoting rules. Supported devices promote rules that meet all of the following criteria:

- have the **Trust**, **Block**, or **Block with reset** action
- use **only** simple, network-based conditions: security zone, IP address, VLAN tag, and port
- are placed above **all** other access control rules (regardless of action) that perform deep packet inspection, that is, that have application, URL, user, or geolocation-based conditions
- are also placed above **all** Monitor rules

Therefore, rules promoted to improve performance are most likely simple Trust or Block rules that are placed either near the top of an access control policy (rules with a low number), or anywhere in a policy that uses only simple, network-based rules. However, the performance benefits realized from rule promotion can cause some unexpected behavior.

Preempting Security Intelligence

The system processes promoted rules before an access control policy's Security Intelligence blacklist. This means that promoted Trust rules can allow blacklisted traffic to pass uninspected.

Preventing HTTP Response Page Display

Web traffic blocked by a promoted Block rule does not cause the system to display the configured HTTP response page to your users, even though the system successfully blocks the traffic. Instead, users requesting prohibited URLs have their connection either reset or time out.

IPv6 Traffic Handling

The system can inspect both IPv4 and IPv6 traffic. IPv6 inspection includes the 4in6, 6in4, 6to4, and 6in6 tunneling schemes, and also includes Teredo tunneling when the UDP header specifies port 3544. When evaluating traffic using access control rules with IP address conditions, in most cases devices match the IP address you specify against the IP address in the innermost packet header.

However, promoted rules use the IP address in the **outermost** header to evaluate IPv6 traffic, regardless of whether that traffic is tunneled, and regardless of where the IPv6 header is: innermost or outermost. In other words, when promoted rules evaluate tunneled traffic, only 4in4 traffic uses the innermost header to match against access control rule criteria.

For example, consider a scenario where you are using examining 6in4 tunneled traffic sent over an IPv4 network. You create a simple, network-based access control rule that blocks traffic to or from a specific IPv6 address. If the system promotes the rule as a result of its position in the access control policy, the rule has no effect. This is because the system matches the outermost IPv4 header of a tunneled packet to the IPv6 rule condition, which can never trigger. The system handles the traffic as if the rule did not exist, using either a subsequent access control rule or the policy's default action.

Access Control Rule Comments

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.

Adding Comments to an Access Control Rule

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin

Procedure

-
- Step 1** In the access control rule editor, click the **Comments** tab.
 - Step 2** Click **New Comment**.
 - Step 3** Enter your comment and click **OK**. You can edit or delete this comment until you save the rule.
 - Step 4** Click **Save**.
 - Step 5** Click **Save** to save the policy.
-

What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).

Searching Access Control Rules

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin

You can search access control rules either by name or condition value, including referenced object names, values, and groups. You cannot search for values in a Security Intelligence or URL list or feed.

In a multidomain deployment, searching access control rules searches the current policy and any ancestor policies.

Procedure

-
- Step 1** In the access control policy editor, click the **Search Rules** prompt, enter a search string, then press Enter. You can use a complete or partial search string.
- The column for matching values is highlighted for each matching rule. A status message displays the current match and the total number of matches.
- 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 (✕).
-

Access Control Rules and Affected Devices

You can filter the access control rules listed in your access control policy to display only the rules that govern traffic for one or more specified devices.

To determine the rules that affect a device, the system uses the access control rules' zone conditions. A security zone is a logical grouping of interfaces, so, if a zone condition includes an interface, the device that handles traffic where that interface is located is affected by that rule. Rules with no zone condition apply to any zone, and therefore every device.

Filtering Access Control Rules by Device

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin

Procedure

-
- Step 1** In the access control policy editor, click the **Rules** tab, then click **Filter by Device**. A list of targeted devices and device groups appears.
- Step 2** Check one or more check boxes to display only the rules that apply to those devices or groups. Or, check **All** to reset and display all of the rules.
- Tip** Hover your pointer over a rule criterion to see its value. If the criterion represents an object with device-specific overrides, the system displays the override value when you filter the rules list by only that device. If the criterion represents an object with domain-specific overrides, the system displays the override value when you filter the rules list by devices in that domain.

Step 3 Click **OK**.
