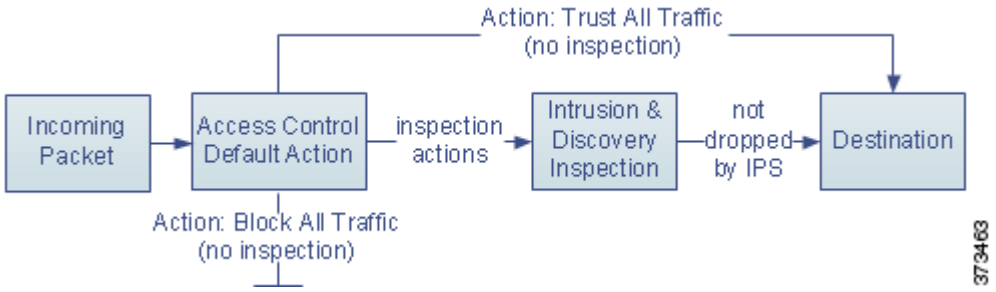
Getting Started with Access Control Policies

An *access control policy* determines how the system handles non-fast-pathed traffic on your network. You can configure one or more access control policies, which you can then apply to one or more managed devices. Each device can have one currently applied policy.

The simplest access control policy directs its target devices to handle all traffic using its *default action*. You can set this default action to block or trust all traffic without further inspection, or to inspect traffic for intrusions and discovery data.



Note that only devices deployed inline can affect the flow of traffic. Applying an access control policy configured to block or alter traffic to passively deployed devices can have unexpected results. In some cases, the system prevents you from applying inline configurations to passively deployed devices.

This chapter explains how to create and apply a simple access control policy. It also contains basic information on managing access control policies: editing, updating, comparing, and so on. For more information, see:

A more complex access control policy can blacklist traffic based on Security Intelligence data, as well as use *access control rules* to exert granular control over network traffic logging and handling. These rules can be simple or complex, matching and inspecting traffic using multiple criteria. Advanced access control policy options control decryption, preprocessing, performance, and other general preferences.

After you create a basic access control policy, see the following chapters for more information on tailoring it to your deployment:

- Blacklisting Using Security Intelligence IP Address Reputation, page 13-1 explains how to immediately blacklist (block) connections based on the latest reputation intelligence.
- Understanding Traffic Decryption, page 19-1 explains how to use an SSL policy to block encrypted traffic without inspecting it, or to pass it on to access control rules, optionally after decrypting it.
- Understanding Network Analysis and Intrusion Policies, page 23-1 explains how network analysis and intrusion policies preprocess and examine packets, as part of the system's intrusion detection and prevention feature.
- Tuning Traffic Flow Using Access Control Rules, page 14-1 explains how access control rules provide a granular method of handling network traffic across multiple managed devices.
- Controlling Traffic Using Intrusion and File Policies, page 18-1 explains how intrusion and file policies provide the last line of defense before traffic is allowed to its destination, by detecting and optionally blocking intrusions, prohibited files, and malware.

Access Control License and Role Requirements

Although you can create access control policies regardless of the licenses on your Defense Center, many features require that you enable the appropriate licenses before you apply the policy. Additionally, some features are only available on certain models.

Also note that available access control-related features and actions depend on your user role. The system includes predefined user roles designed for a variety of administrators and analysts, and you can create custom user roles with specialized access privileges.

For more information, see:

- License and Model Requirements for Access Control, page 12-2
- Managing Your Deployment with Custom User Roles, page 12-4

License and Model Requirements for Access Control

Although you can create access control policies regardless of the licenses on your Defense Center, certain aspects of access control require that you enable specific licensed capabilities on target devices before you can apply the policy. Additionally, some features are only available on certain models.

Warning icons and confirmation dialog boxes designate unsupported features for your deployment. For details, hover your pointer over a warning icon and see Troubleshooting Access Control Policies and Rules, page 12-22.

The following table explains the license and appliance model requirements to apply access control policies. Note that Series 2 devices automatically have most Protection capabilities; you do not have to explicitly enable Protection on those devices.

Table 12-1 License and Model Requirements for Access Control

To apply an access control policy that...	License	Supported Defense Centers	Supported Devices
performs access control based on zone, network, VLAN, or port performs URL filtering using literal URLs and URL objects	Any	Any	Any, except: • Series 2 devices cannot perform URL filtering • ASA FirePOWER devices cannot perform VLAN filtering
performs SSL inspection; see Table 12-2 on page 12-3	Any	Any, except the DC500 is limited to network, application, and SSL-related control	Series 3
performs access control using geolocation data (source or destination country or continent)	FireSIGHT	Any except DC500	Series 3 Virtual ASA FirePOWER
performs intrusion detection and prevention, file control, or Security Intelligence filtering	Protection	Any	Any, except Series 2 devices cannot perform Security Intelligence filtering
performs advanced malware protection, that is, network-based malware detection and blocking	Malware	Any except DC500	Any except Series 2 or X-Series
performs user or application control	Control	Any, except the DC500 cannot perform user control	Any except Series 2 or X-Series
performs URL filtering using category and reputation data	URL Filtering	Any except DC500	Any except Series 2

The following table explains the licenses you must have to apply an access control policy that performs SSL inspection by invoking an SSL policy.

Table 12-2 License and Model Requirements for SSL Inspection

To apply an SSL policy that...	License	Supported Defense Centers	Supported Devices
handles encrypted traffic on the basis of zone, network, VLAN, port, or SSL-related criteria	Any	Any	Series 3
handles encrypted traffic using geolocation data	FireSIGHT	Any except DC500	Series 3
handles encrypted traffic using application or user criteria	Control	Any, except the DC500 cannot perform user control	Series 3
filters encrypted traffic using URL category and reputation data	URL Filtering	Any except DC500	Series 3

Managing Your Deployment with Custom User Roles

License: feature dependent

As described in Managing Custom User Roles, page 61-53, you can create custom user roles with specialized access privileges. Custom user roles can have any set of menu-based and system permissions, and may be completely original or based on a predefined user role. Custom roles for access control-related features determine whether users can view, modify, and apply access control, intrusion, and file policies, as well as insert or modify rules in the Administrator Rules or Root Rules categories.

The following table shows five example custom roles that determine how FireSIGHT System users interact with access control features. The table lists, in the order they appear when creating custom user roles, the privileges required for each custom role.

Table 12-3 Example Access Control Custom Roles

Custom Role Permission	Access Control & SSL Editor	Intrusion & Network Analysis Editor	File Policy Editor	Policy Applier (All)	Intrusion Policy Applier
Access Control	yes	no	no	yes	yes
Access Control List	yes	no	no	yes	yes
Modify Access Control Policy	yes	no	no	no	no
Apply Intrusion Policies	no	no	no	yes	yes
Apply Access Control Policies	no	no	no	yes	no
Intrusion (also grants network analysis privileges)	no	yes	no	no	no
Intrusion Policy	no	yes	no	no	no
Modify Intrusion Policy	no	yes	no	no	no
File Policy	no	no	yes	no	no
Modify File Policy	no	no	yes	no	no
SSL	yes	no	no	no	no
Modify SSL Policy	yes	no	no	no	no
Apply SSL Policy	no	no	no	yes	no

Note that you can create and edit network analysis as well as intrusion policies if your FireSIGHT System user account's role is restricted to Intrusion Policy or Modify Intrusion Policy.

The system renders the web interface differently depending on whether a user can apply full access control policies (including intrusion policies), only intrusion policies, or neither. For example, Intrusion Policies Appliers in the table above can view access control policies and apply intrusion policies but cannot edit either. They also cannot apply access control policies, nor view file or SSL policies. In the web interface in this case:

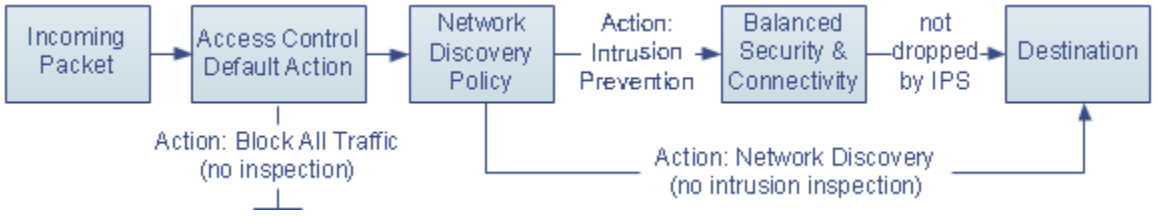
- the edit icon ( ) does not appear on the Access Control Policy page
- the delete icon ( ) does not appear on the Access Control Policy page
- the quick-apply pop-up window applies only the intrusion policy
- access control policy check boxes in the detailed apply pop-up window are disabled

Creating a Basic Access Control Policy

License: Any

When you create a new access control policy you must give it a unique name and specify a default action. At this point, the default action determines how the policy's target devices handles all non-fastpathed traffic; you will add other configurations that affect traffic flow later. Although you are not required to identify the policy targets at creation time, you must perform this step before you can apply the policy.

When you create a new policy, you can set the default action to block all traffic without further inspection, or to inspect traffic for intrusions and discovery data, as shown in the following diagram.



Tip When you first create an access control policy, you cannot choose to trust traffic as the default action. If you want to trust all traffic by default, change the default action after you create the policy.

Use the Access Control Policy page (**Policies > Access Control**) to create new and manage existing access control policies. Depending on whether and how you registered devices to the Defense Center, either of two predefined access control policies might appear and already be applied to your devices:

- The Default Access Control policy blocks all traffic without further inspection.
- The Default Intrusion Prevention policy allows all traffic, but also inspects with the Balanced Security and Connectivity intrusion policy and default intrusion variable set.

You can use and modify either of these access control policies. Note that neither of these default policies has logging enabled.

Caution Applying an access control policy for the first time restarts the Snort process, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. See How Snort Restarts Affect Traffic, page 1-9 for more information.

To create an access control policy:

Access: Admin/Access Admin/Network Admin

Step 1 Select **Policies > Access Control**.

The Access Control Policy page appears.

Tip You can also copy an existing policy from this Defense Center or import a policy from another Defense Center. To copy a policy, click the copy icon ( ). To import a policy, see Importing and Exporting Configurations, page A-1.

Step 2 Click **New Policy**.

The New Access Control Policy pop-up window appears.

Step 3 Give the policy a unique **Name** and, optionally, a **Description**.

You can use all printable characters, including spaces and special characters, except for the pound sign (#), a semi-colon (;), or either brace ({}). The name must include at least one non-space character.

Step 4 Specify the initial **Default Action**:

- **Block all traffic** creates a policy with the **Access Control: Block All Traffic** default action.
- **Intrusion Prevention** creates a policy with the **Intrusion Prevention: Balanced Security and Connectivity** default action.
- **Network Discovery** creates a policy with the **Network Discovery Only** default action.

For guidance on choosing an initial default action, as well as how to change it later, see Setting Default Handling and Inspection for Network Traffic, page 12-6.

Step 5 Select the **Available Devices** where you want to apply the policy.

Use Ctrl and Shift to select multiple devices, or right-click to **Select All**. To narrow the devices that appear, type a search string in the **Search** field. If you skip adding target devices, see Setting Target Devices for an Access Control Policy, page 12-9 for information on adding them later.

Step 6 Click **Add to Policy** to add the selected devices.

You can also drag and drop selected objects.

Step 7 Click **Save**.

The access control policy editor appears. For information on configuring your new policy, see Editing Access Control Policies, page 12-11. Note that you must apply the policy for it to take effect; see Applying an Access Control Policy, page 12-15.

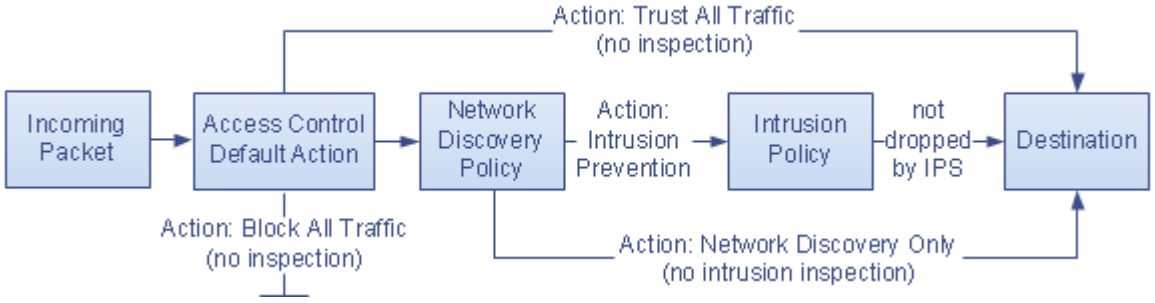
Setting Default Handling and Inspection for Network Traffic

License: Any

When you create an access control policy, you must select a default action. The default action for an access control policy determines how the system handles traffic that:

- is not blacklisted by Security Intelligence
- is not blocked by SSL inspection (encrypted traffic only)
- matches none of the rules in the policy (except Monitor rules, which match and log—but do not handle or inspect—traffic)

Therefore, when you apply an access control policy that does not contain any access control rules or Security Intelligence configurations, and that does not invoke an SSL policy to handle encrypted traffic, the default action determines how *all* traffic on your network is handled. You can block or trust all traffic without further inspection, or inspect traffic for intrusions and discovery data. Your options are shown in the following diagram.

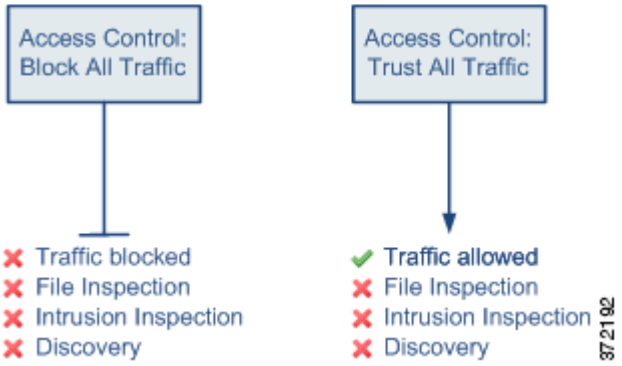


The following table describes how the different default actions handle traffic, and lists the types of inspection you can perform on traffic handled by each default action. Note that you **cannot** perform file or malware inspection on traffic handled by the default action. For more information, see Controlling Traffic Using Intrusion and File Policies, page 18-1.

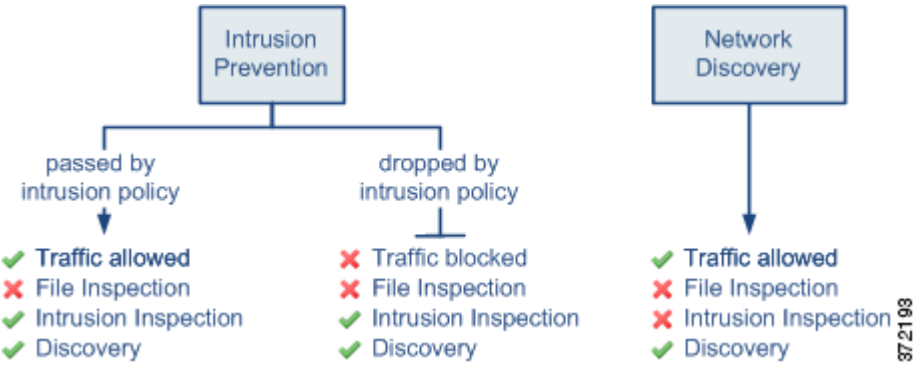
Table 12-4 Access Control Policy Default Actions

Default Action	Effect on Traffic	Inspection Type and Policy
Access Control: Block All Traffic	block without further inspection	none
Access Control: Trust All Traffic	trust (allow to its final destination without further inspection)	none
Intrusion Prevention	allow, as long as it is passed by the intrusion policy you specify (requires Protection)	intrusion, using the specified intrusion policy and associated variable set, and discovery, using the network discovery policy
Network Discovery Only	allow	discovery only, using the network discovery policy

The diagram below illustrates the **Block All Traffic** and **Trust All Traffic** default actions.



The diagram below illustrates the **Intrusion Prevention** and **Network Discovery Only** default actions.



Tip The purpose of **Network Discovery Only** is to improve performance in a discovery-only deployment. Different configurations can disable discovery if you are only interested in intrusion detection and prevention. See IPS or Discovery-Only Performance Considerations, page 12-20 for more information, including other guidelines you must follow.

When you first create an access control policy, logging connections that are handled by the default action is disabled by default. If you select a default action that performs intrusion inspection, the system automatically associates the default intrusion variable set with the intrusion policy you select. You can change either of these options, as well as the default action itself, after you create the policy.

To change an access control policy's default action and related options:

Access: Admin/Access Admin/Network Admin

Step 1 Select **Policies > Access Control**.

The Access Control Policy page appears.

Step 2 Click the edit icon ( ) next to the access control policy you want to configure.

The access control policy editor appears.

Step 3 Select a **Default Action**.

- To block all traffic, select **Access Control: Block All Traffic**.

- To trust all traffic, select **Access Control: Trust All Traffic**.
- To allow all traffic and inspect it with network discovery, select **Network Discovery Only**.
- To inspect all traffic with both network discovery and intrusion policies, select an intrusion policy, all of which begin with the label **Intrusion Prevention**. Keep in mind that an intrusion policy can block traffic.

Step 4 If you selected an **Intrusion Prevention** default action, click the variables icon ( ) to change the variable set associated with the intrusion policy you selected.

In the pop-up window that appears, select a new variable set and click **OK**. You can also edit the selected variable set in a new window by clicking the edit icon ( ). If you do not change the variable set, the system uses a default set. For more information, see Working with Variable Sets, page 3-17.

Step 5 Click the logging icon ( ) to change logging options for connections handled by the default action.

Depending on the default action, you can log a matching connection at its beginning, end, or both. You can log connections to the Defense Center database, external system log (syslog), or SNMP trap server. For more information, see Logging Connections Handled by the Access Control Default Action, page 38-17.

Setting Target Devices for an Access Control Policy

License: Any

Before you can apply an access control policy you must identify the managed devices where you want to apply the policy. You can identify the devices you want to target with your policy while creating a policy, or you can add them later.

The following table summarizes the actions you can take when managing targeted devices.

Table 12-5 Targeted Device Management Actions

To...	You can...
search a list of available devices	click inside the search field, then type a search string. The list of devices updates as you type to display matching device names.
clear a search for available devices	click the clear icon ( ) in the search field.
select available devices to add to the list of selected targets	click the device name; use the Ctrl and Shift keys to select multiple devices. You can also right-click an available device, then click **Select All**.
add selected devices	click **Add to Policy** or drag and drop into the list of selected devices.
delete a single device from the Selected Devices list	click the delete icon ( ) next to the device, or right-click the device and select **Delete**.
delete multiple devices from the Selected Devices list	use the Ctrl and Shift keys to select multiple devices, right-click to highlight the row for a selected device, then click **Delete Selected**.

Note that you cannot target stacked devices running different versions of the system (for example, if an upgrade on one of the devices fails). You can target a device stack, but not individual devices within the stack. See Managing Stacked Devices, page 4-42 for more information.

To manage targeted devices in an access control policy:

Access: Admin/Access Admin/Network Admin

Step 1 Select **Policies > Access Control**.

The Access Control Policy page appears.

Step 2 Click the edit icon ( ) next to the access control policy you want to configure.

The access control policy editor appears.

Step 3 Click the device targets link, then click **Manage Targets**.

The Manage Device Targets pop-up window appears.

Step 4 Build your target list.

Use the actions summarized in Table 12-5 on page 12-9.

Step 5 Click **OK**.

Your configuration is added to the policy and the access control policy editor appears.

Managing Access Control Policies

License: Any

On the Access Control Policy page (**Policies > Access Control**) you can view your current custom access control policies, along with the following information, when appropriate:

- the number of devices using each access control policy to inspect traffic, including information on whether a policy is applied to only some of its targets, or is applied to a device not currently targeted by that policy
- the number of targeted devices where each policy is out of date, as well as information about who (if anyone) is currently editing each policy

In addition to custom policies that you create, the system can provide three custom policies: Default Access Control, Default Intrusion Prevention, and Default Network Discovery. The system creates these policies during initial device registration, depending on the detection modes you selected for your devices during their initial configuration. You can edit and use these system-provided custom policies. Note that a device's detection mode is not a setting you can change later; it is simply an option you choose during setup that helps the system tailor that device's initial configurations.

Options on the Access Control Policy page allow you to take the actions in the following table.

Table 12-6 Access Control Policy Management Actions

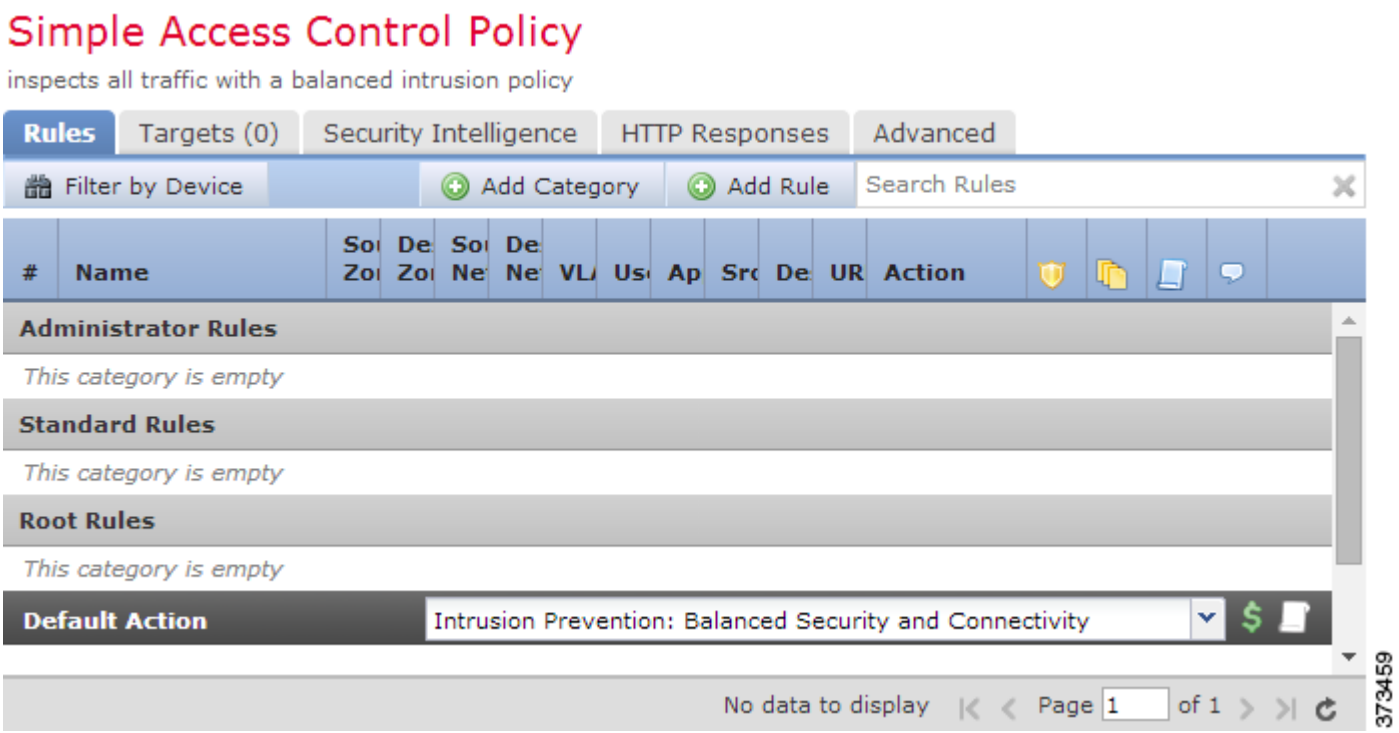
To...	You can...	See...
create a new access control policy	click **New Policy**.	Creating a Basic Access Control Policy, page 12-5
edit an existing access control policy	click the edit icon ( ).	Editing Access Control Policies, page 12-11
reapply an access control policy to your managed devices	click the apply icon ( ).	Applying an Access Control Policy, page 12-15
export an access control policy to import on another Defense Center	click the export icon ( )	Exporting Configurations, page A-1
view a PDF report that lists the current configuration settings in a access control policy	click the report icon ( ).	Generating a Report of Current Access Control Settings, page 12-26
compare access control policies	click **Compare Policies**.	Comparing Access Control Policies, page 12-27
delete an access control policy	click the delete icon ( ), then confirm that you want to delete the policy. You cannot delete an applied access control policy or one that is currently applying.	

Editing Access Control Policies

License: Any

When you first create a new access control policy, the access control policy editor appears, focused on the Rules tab. The following graphic shows a newly created policy. Because a new policy does not yet have rules or other configurations, the default action handles *all* traffic. In this case, the default action

inspects unencrypted traffic with the system-provided Balanced Security and Connectivity intrusion policy before allowing it to its final destination. Note that by default, the system disables file and intrusion inspection on encrypted payloads.



Use the access control policy editor to add and organize rules, specify the devices that will use the policy, and so on. The following list provides information on the policy configurations you can change.

Name and Description

To change the policy's name and description, click the appropriate field and type the new name or description.

Targets

Before you can apply an access control policy, use the Targets tab to identify the managed devices, including device groups, where you want to apply the policy. For more information, see Setting Target Devices for an Access Control Policy, page 12-9.

Security Intelligence

Security Intelligence is a first line of defense against malicious Internet content. This feature allows you to immediately blacklist (block) connections based on the latest reputation intelligence. To ensure continual access to vital resources, you can override blacklists with custom whitelists. This traffic filtering takes place **before** any other policy-based inspection, analysis, or traffic handling, including rules and the default action. For more information, see Blacklisting Using Security Intelligence IP Address Reputation, page 13-1.

Rules

Rules provide a granular method of handling network traffic. 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. These conditions include security zone, network or geographical location, VLAN, port, application, requested URL, or user. Conditions can be simple or complex; their use often depends on certain licenses and appliance models.

Use the Rules tab to add, categorize, enable, disable, filter, and otherwise manage rules. For more information, see Tuning Traffic Flow Using Access Control Rules, page 14-1.

Default Action

The default action determines how the system handles traffic that is not blacklisted by Security Intelligence and does not match any access control rules. Using the default action, you can block or trust all traffic without further inspection, or inspect traffic for intrusions and discovery data. You can also select an custom variable set if you have created one, and enable or disable logging of connections handled by the default action.

For more information, see Setting Default Handling and Inspection for Network Traffic, page 12-6 and Logging Connections Based on Access Control Handling, page 38-15.

HTTP Responses

You can specify what the user sees in a browser when the system blocks that user's website request—either display a generic system-provided response page, or enter custom HTML. You can also display a page that warns users, but also allows them to click a button to continue or refresh the page to load the originally requested site. For more information, see Displaying a Custom Web Page for Blocked URLs, page 16-17.

Advanced Access Control Options

Advanced access control policy settings typically require little or no modification. The default settings are appropriate for most deployments. Advanced settings you can modify include:

- the number of characters you store in the Defense Center database for each URL requested by your users; see Logging URLs Detected in Connections, page 38-19
- the length of time before you re-block a website after a user bypasses an initial block; see Setting the User Bypass Timeout for a Blocked Website, page 16-16
- an SSL policy to monitor, decrypt, block, or allow application layer protocol traffic encrypted with Secure Socket Layer (SSL) or Transport Layer Security (TLS); see Applying Decryption Settings Using Access Control, page 20-8
- allow traffic inspection during policy apply or disable traffic inspection for secure connectivity; see Applying an Access Control Policy, page 12-15
- network analysis and intrusion policy settings that allow you to tailor many preprocessing options to networks, zones, and VLANs, as well as set default intrusion inspection behavior; see Customizing Traffic Preprocessing, page 25-1
- advanced transport and network preprocessor settings that apply globally to all networks, zones, and VLANs where you apply the access control policy; see Configuring Advanced Transport/Network Settings, page 29-2
- adaptive profiles to improve reassembly of packet fragments and TCP streams in passive deployments, based on your network's host operating systems; see Tuning Preprocessing in Passive Deployments, page 30-1
- performance options for intrusion inspection, file control, file storage, dynamic analysis, and advanced malware protection; see Tuning Intrusion Prevention Performance, page 18-8 and Tuning File and Malware Inspection Performance and Storage, page 18-20

When you edit an access control policy, a message indicates that you have unsaved changes. To retain your changes, you must save the policy before exiting the policy editor. If you attempt to exit the policy editor without saving your changes, you are cautioned that you have unsaved changes; you can then discard your changes and exit the policy, or return to the policy editor.

To protect the privacy of your session, after sixty minutes of inactivity on the policy editor, changes to your policy are discarded and you are returned to the Access Control Policy page. After the first thirty minutes of inactivity, a message appears and updates periodically to provide the number of minutes remaining before changes are discarded. Any activity on the page cancels the timer.

When you attempt to edit the same policy in two browser windows, you are prompted whether to resume your edit in the new window, discard your changes in the original window and continue editing in the new window, or cancel the second window and return to the policy editor.

When multiple users edit the same policy concurrently, a message for each on the policy editor identifies other users who have unsaved changes. Any user who attempts to save their changes is cautioned that their changes will overwrite changes by other users. When the same policy is saved by multiple users, the last saved changes are retained.

To edit an access control policy:

Access: Admin/Access Admin/Network Admin

Step 1 Select **Policies > Access Control**.

The Access Control Policy page appears.

Step 2 Click the edit icon ( ) next to the access control policy you want to configure.

The access control policy editor appears.

Step 3 Edit your policy. Take any of the actions summarized above.

Step 4 Save or discard your configuration:

- To save your changes and continue editing, click **Save.**
- To save your changes and apply your policy, click **Save and Apply**. See Applying an Access Control Policy, page 12-15.
- To discard your changes, click **Cancel** and, if prompted, click **OK**.

Understanding Out-of-Date Policy Warnings

License: Any

On the Access Control Policy page (**Policies > Access Control**), out-of-date policies are marked with red status text that indicates how many of its targeted devices need a policy update.

In almost every case, whenever you change an access control policy, you must reapply it for the change to take effect. If the access control policy invokes other policies or relies on other configurations, changing those also requires that you reapply the access control policy (or, for intrusion policy changes, you can reapply just the intrusion policy).

Configuration changes that require a policy reapply include:

- Modifying the access control policy itself: any changes to access control rules, the default action, policy targets, Security Intelligence filtering, advanced options including NAP rules, and so on.

- Changing any of the policies that the access control policy invokes: the SSL policy, network analysis policies, intrusion policies, and file policies.
- Changing any reusable object or configuration used in the access control policy or the policies it invokes: network, port, VLAN tag, URL, and geolocation objects; Security Intelligence lists and feeds; application filters or detectors; intrusion policy variable sets; file lists; decryption-related objects, security zones, and so on.
- Updating the system software, intrusion rules, or the vulnerability database (VDB).

Keep in mind that you can change some of these configurations from multiple places in the web interface. For example, you can modify security zones using the object manager (**Objects > Object Management**), but modifying an interface type in a device's configuration (**Devices > Device Management**) can also change a zone and require a policy reapply.

Note that the following updates do **not** require policy reapply:

- automatic updates to Security Intelligence feeds and additions to the Security Intelligence global blacklist or whitelist using the context menu
- automatic updates to URL filtering data
- scheduled geolocation database (GeoDB) updates

To determine why an access control or intrusion policy is out of date, use the comparison viewer.

To determine why an access control policy is out of date:

Access: Admin/Security Approver

Step 1 Select **Policies > Access Control**.

The Access Control Policy page appears. Policies that are out of date are marked with red status text that indicates how many of its targeted devices need a policy update.

Step 2 Click the policy status for an out-of-date policy.

The detailed Apply Access Control Policy pop-up window appears.

Step 3 Click **Out-of-date** next to the changed component you are interested in.

A policy comparison report appears in a new window. For more information, see Comparing Access Control Policies, page 12-27 and Comparing Two Intrusion Policies or Revisions, page 31-10.

Step 4 Optionally, reapply the policy.

See the next section, Applying an Access Control Policy.

Applying an Access Control Policy

License: Any

After you change an access control policy, you must apply the policy to one or more target devices to implement the change on the networks monitored by the devices. Although you can apply any combination of an access control policy and its associated intrusion policies, applying an access control policy automatically applies all associated SSL, network analysis, and file policies. You cannot apply these policies independently.

Caution When you apply an access control policy, resource demands may result in a small number of packets dropping without inspection. Additionally, applying some configurations requires the Snort process to restart, which temporarily interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. See How Snort Restarts Affect Traffic, page 1-9.

Tip If you are using Cisco NGIPS for Blue Coat X-Series deployed inline and you configure a multi-VAP VAP group for load-balancing and redundancy, you can avoid processing pauses by removing the affected VAP from the load-balanced list until the device restarts, then reinstate it.

Note that only devices deployed inline can affect the flow of traffic. Applying an access control policy configured to block or alter traffic to passively deployed devices can have unexpected results. For example, because blocked connections are not actually blocked in passive deployments, the system may report multiple beginning-of-connection events for each blocked connection.

In some cases, the system prevents you from applying inline configurations to passively deployed devices, including inline devices in tap mode. For example, in an passive deployment, you cannot apply an access control policy that references an SSL policy that blocks encrypted traffic, or that is configured to re-sign decrypted traffic. Also, passive deployments do not support decrypting traffic encrypted with the ephemeral Diffie-Hellman (DHE) or the elliptic curve Diffie-Hellman (ECDHE) cipher suites.

Keep the following additional points in mind when applying access control policies:

- Some features require specific licenses, minimum versions of the system, or specific device models. For more information, see License and Model Requirements for Access Control, page 12-2, as well as the release notes for the version of the system you are running on your managed devices. If an access control policy requires licenses enabled through recently applied device configurations, the system queues the access control policy apply until the device configurations finish applying.
- You cannot apply an access control policy to stacked devices running different versions of the system (for example, if an upgrade on one of the devices fails).
- When you apply an access control policy, the system evaluates all the rules together and creates an expanded set of criteria that target devices use to evaluate network traffic. A pop-up window may warn that you have exceeded the maximum number of access control rules or intrusion policies supported by a target device. This maximum depends on a number of factors, including the physical memory and the number of processors on the device. On devices with less computing resources, note that limited memory may require that you select as few as three intrusion policies across an entire access control policy. For more information, see Simplifying Rules to Improve Performance, page 12-23.
- If you are performing application control, at least one detector must be enabled for each application used as a criterion in either an access control or SSL rule. If no detector is enabled for an application, the system automatically enables all system-provided detectors for the application; if none exist, the system enables the most recently modified user-defined detector for the application.
- When you import an intrusion rule update, you can automatically reapply access control and intrusion policies after the import completes. This allows you to use the most up-to-date intrusion rules and advanced settings, as well as preprocessor rules and preprocessor settings. This is especially useful if you allow rule updates to modify system-provided base policies. Note that rule updates can also modify default values for the advanced preprocessing and performance options in your access control policies. For more information, see Importing Rule Updates and Local Rule Files, page 66-15.

- On devices with limited memory, the number of intrusion policies may not be paired with more than one variable set. In the case where you can apply an access control policy that references only one intrusion policy, verify every reference to the intrusion policy is paired with the same variable set.

See the following sections for more information:

- Applying a Complete Policy, page 12-17 explains how to use the quick-apply option to apply the access control policy along with all associated SSL, network analysis, intrusion, and file policies.
- Applying Selected Policy Configurations, page 12-17 explains how to apply specific access control policy configurations, including individual intrusion policies.

Applying a Complete Policy

License: Any

Supported Devices:

You can apply an access control policy to its target devices at any time. Applying an access control policy also applies any associated policies that are different from those currently running:

- SSL policy
- network analysis policies
- intrusion policies
- file policies

A pop-up window allows you to apply all together as a single quick-apply action. Unchanged policies are not applied when you use the quick-apply option.

The label for the apply button on the quick-apply pop-up window can differ depending on whether you are permitted to apply an access control policy, intrusion policy, or both; see Managing Your Deployment with Custom User Roles, page 12-4.

To quick-apply a complete access control policy:

Access: Admin/Security Approver

Step 1 Select **Policies > Access Control**.

The Access Control Policy page appears.

Step 2 Click the apply icon ( ) next to the policy you want to apply.

The Apply Access Control Policy pop-up window appears.

Alternatively, you can click **Save and Apply** while editing a policy; see Editing Access Control Policies, page 12-11.

Step 3 Click **Apply All**.

Your policy apply task is queued. Click **OK** to return to the Access Control Policy page. You can monitor the progress of the policy apply task on the Task Status page (**System > Monitoring > Task Status**).

Applying Selected Policy Configurations

License: Any

You can use the detailed policy apply page to apply changes to your access control policy and to any associated intrusion policies. The detailed page lists each device targeted by the policy and provides a column for the access control policy by device, and a column for associated intrusion policies by device. You can specify whether to apply changes to an access control policy, to associated intrusion policies individually or in combination, or both, for each targeted device.

You must apply both an access control policy and an associated intrusion policy in either of the following cases:

- when the access control policy is being applied to the device for the first time
- when an intrusion policy has been newly added to the access control policy

In both cases, the states of the access control policy and the intrusion policies are linked; that is, you must apply both or neither.

Note that regardless of the intrusion policies you apply, applying an access control policy automatically applies all associated SSL, network analysis, and file policies that are different from those currently running on devices targeted by the policy. You cannot apply these policies independently.

The Access Control Policy Column

The Access Control Policy column provides a check box for indicating whether to apply the access control policy.

Tip Although you can reapply a policy while it is still in the task queue, that is, while the apply task has not yet completed, there is no benefit in doing this.

A status message indicates whether the policy is currently up to date or out of date. When the policy is out of date, you can conveniently display a comparison of the policy to the currently running policy in a new browser window. The comparison does not include differences in an intrusion policy associated with the access control policy.

The Intrusion Policies Column

The Intrusion Policies column provides one or more check boxes for indicating whether to apply intrusion policies associated with the access control policy to a device. A single grayed check box indicates that all associated intrusion policies are identical to currently running policies, in which case the check box is cleared and cannot be selected. You cannot apply an unchanged intrusion policy; only changed intrusion policies are listed, and can be selected individually. When the same intrusion policy is associated with multiple rules in a policy, the intrusion policy is listed only once for each device.

The check box for an intrusion policy is selected and the check box is grayed and cannot be changed when the access control policy and the intrusion policy must be applied together, as described above, in either of the following cases:

- when the access control policy is being applied to the device for the first time
- when an intrusion policy has been newly added to the access control policy

Status messages indicate whether intrusion policies are currently up to date or out of date. An intrusion policy is out of date when it is not identical to an intrusion policy currently running on the listed device. An identical intrusion policy on the device is up to date. When the policy is out of date, you can conveniently display a comparison of the policy to the currently running policy in a new browser window.

To apply selected access control policy configurations:

Access: Admin/Security Approver

Step 1 Select **Policies > Access Control**.

The Access Control Policy page appears.

Step 2 Click the apply icon ( ) next to the policy you want to apply.

The Apply Access Control Policy pop-up window appears.

Alternatively, you can click **Save and Apply** while editing a policy; see Editing Access Control Policies, page 12-11.

Step 3 Click **Details**.

The detailed Apply Access Control Policy pop-up window appears. Note that you can also open the pop-up window from the Access Control Policy page (**Policies > Access Control**) by clicking on an out-of-date message in the **Status** column for the policy.

Step 4 Select or clear the access control policy check box next to the device name to specify whether to apply the access control policy to a targeted device.

Step 5 Select or clear the intrusion policy check box next to the device name to specify whether to apply an intrusion policy to a targeted device.

Step 6 Click **Apply Selected Configurations**.

Your policy apply task is queued. Click **OK** to return to the Access Control Policy page.

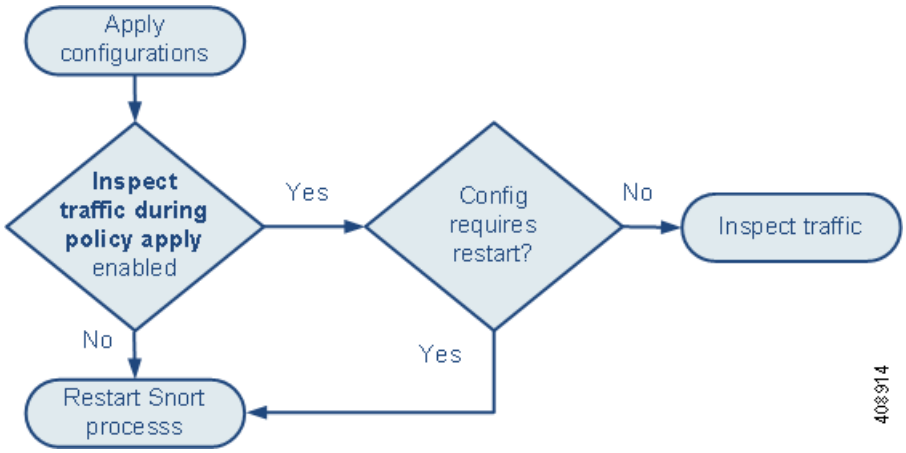
Note that a pop-up window may warn that you have exceeded the maximum number of intrusion policies supported by the device. You must reevaluate your access control policy and consolidate intrusion policies. You cannot apply the access control policy until the number of associated intrusion policies (including the default action) falls within the maximum.

You can monitor the progress of the policy apply task on the Task Status page (**System > Monitoring > Task Status**).

Traffic Inspection During Access Control Policy Apply

The following graphic illustrates how restarting the Snort process can occur when you enable or disable the **Inspect traffic during policy apply** advanced access control policy option.

Caution Restarting the Snort process temporarily interrupts traffic inspection. Whether traffic drops during this interruption or passes without inspection depends on the model of the managed device and how it handles traffic. See Configurations that Restart the Snort Process, page 1-7.



Note the following:

- When you enable **Inspect traffic during policy apply**:
  - Certain configurations can require the Snort process to restart.
  - When the configurations you apply do not require a Snort restart, the system initially uses the currently applied access control policy to inspect traffic, and switches during the application process to the policy you are applying
- When you disable **Inspect traffic during policy apply**, the Snort process always restarts when you apply the policy.
- How a Snort restart affects traffic depends on the model of the managed device and how it handles traffic. See How Snort Restarts Affect Traffic, page 1-9.

IPS or Discovery-Only Performance Considerations

License: FireSIGHT or Protection

A FireSIGHT license is included with your Defense Center and allows you to perform host, application, and user discovery. Discovery data allows the system to create a complete, up-to-the-minute profile of your network. With Protection licenses applied to your managed devices, the system can act as an intrusion detection and prevention system (IPS). You can analyze network traffic for intrusions and exploits and, optionally, drop offending packets.

Combining discovery and IPS gives context to your network activity and allows you to take advantage of many features, including:

- impact flags and indications of compromise, which can tell you which of your hosts are vulnerable to a particular exploit, attack, or piece of malware
- adaptive profiles and FireSIGHT recommendations, which allow you to examine traffic differently depending on the destination host
- correlation, which allows you to respond to intrusions (and other events) differently depending on the affected host

However, if your organization is interested in performing only IPS, or only discovery, there are a few configurations that can optimize the performance of the system, as described in the following sections:

Optimizing a Network Discovery-Only Deployment

License: FireSIGHT

The *discovery* feature allows you to monitor network traffic and determine the number and types of hosts (including network devices) on your network, as well as the operating systems, active applications, and open ports on those hosts. You can also configure managed devices and User Agents to monitor user activity on your network. You can use discovery data to perform traffic profiling, assess network compliance, and respond to policy violations.

In a basic deployment (discovery and simple, network-based access control only), you can improve a device's performance by following a few important guidelines when configuring its access control policy.

Note You must apply an access control policy, even if it simply allows all traffic. The network discovery policy can **only** examine traffic that the access control policy allows to pass.

First, make sure your access control policy does not require complex processing and uses only simple, network-based criteria to handle network traffic. You must implement **all** of the following guidelines; misconfiguring any one of these options eliminates the performance benefit:

- Do **not** use the Security Intelligence feature. Remove any populated global whitelist or blacklist from the policy's Security Intelligence configuration.
- Do **not** include access control rules with Monitor or Interactive Block actions. Use only Allow, Trust, and Block rules. Keep in mind that allowed traffic can be inspected by discovery; trusted and blocked traffic cannot.
- Do **not** include access control rules with application, user, URL, or geolocation-based network conditions, even if your devices are appropriately licensed. Use only simple network-based conditions: zone, IP address, VLAN tag, and port.
- Do **not** include access control rules that perform file, malware, or intrusion inspection, even if your devices are appropriately licensed. In other words, do not associate a file policy or intrusion policy with any access control rule.
- Make sure that the default intrusion policy for the access control policy is set to **No Rules Active**; see Setting the Default Intrusion Policy for Access Control, page 25-1.
- Select **Network Discovery Only** as the policy's default action. Do **not** choose a default action for the policy that performs intrusion inspection.

Note that with the exception of geolocation-based access control, the options described above require at least a Protection license. If you have only a FireSIGHT license, the system prevents you from applying an access control policy using these features.

After you configure and apply the access control policy, you can configure and apply the network discovery policy, which specifies the network segments, ports, and zones that the system examines for discovery data, as well as whether hosts, applications, and users are discovered on the segments, ports, and zones.

Performing Intrusion Detection and Prevention without Discovery

License: Protection

The intrusion detection and prevention feature allows you to analyze network traffic for intrusions and exploits and, optionally, drop offending packets. If you want to perform intrusion inspection but do not need to take advantage of discovery data, you can improve a device's performance by disabling discovery.

Note If you are performing application, user, or URL control, you **cannot** disable discovery for a performance benefit. Although you can prevent the system from storing it, the system **must** collect and examine discovery data to implement those features.

To disable discovery, implement **all** of the following guidelines; misconfiguring any eliminates the performance benefit:

- In your access control policy, do **not** include rules with application, user, URL, or geolocation-based network conditions, even if your devices are appropriately licensed. Use only simple network-based conditions: zone, IP address, VLAN tag, and port.
- Delete all rules from your network discovery policy.

After you apply the access control policy and then the network discovery policy, new discovery halts on target devices. The system gradually deletes information in your network map according to the timeout periods you specified in the network discovery policy. Or, you can purge all discovery data immediately, see Purging Discovery Data from the Database, page B-1.

Troubleshooting Access Control Policies and Rules

License: Any

Properly configuring access control policies, especially creating and ordering access control rules, is a complex task. However, it is a task that is essential to building an effective deployment. If you do not plan your policy carefully, rules can preempt other rules or contain invalid configurations. Both rules and other policy settings can require additional licenses.

To help ensure that the system handles traffic as you expect, the access control policy interface has a robust feedback system. Icons in the access control policy and rule editors mark warnings and errors, as described in the Access Control Error Icons table. Hover your pointer over an icon to read the warning, error, or informational text.

Tip In the access control policy editor, click **Show Warnings** to display a pop-up window that lists all the warnings for the policy.

Additionally, the system warns you at apply-time of any issues that could affect traffic analysis and flow.

Table 12-7 Access Control Error Icons

Icon	Description	Details
	error	If a rule or configuration has an error, you cannot apply the policy until you correct the issue, even if you disable any affected rules.
	warning	You can apply an access control policy that displays rule or other warnings. However, misconfigurations marked with warnings have no effect. For example, you can apply a policy that contains preempted rules or rules that cannot match traffic due to misconfiguration—conditions using empty object groups, application filters that match no applications, configuring URL conditions without having enabled cloud communications, and so on. These rules do not evaluate traffic. If you disable a rule with a warning, the warning icon disappears. It reappears if you enable the rule without correcting the underlying issue. As another example, many features require a specific license or device model. An access control policy successfully applies only to eligible target devices.
	information	Information icons convey helpful information about configurations that may affect the flow of traffic. These issues do not prevent you from applying the policy. For example, if you are performing application control or URL filtering, the system may skip matching the first few packets of a connection against some access control rules, until the system identifies the application or web traffic in that connection. This allows connections to be established so that applications and HTTP requests can be identified. For more information, see Limitations to Application Control, page 16-7 and Limitations to URL Detection and Blocking, page 16-14.

Properly configuring access control policies and rules can also reduce the resources required to process network traffic. Creating complex rules, invoking many different intrusion policies, and mis-ordering rules can all affect performance.

For more information, see:

- Access Control License and Role Requirements, page 12-2
- Simplifying Rules to Improve Performance, page 12-23
- Understanding Rule Preemption and Invalid Configuration Warnings, page 12-24
- Ordering Rules to Improve Performance and Avoid Preemption, page 12-25

Simplifying Rules to Improve Performance

Complex access control policies and rules can command significant resources. When you apply an access control policy, the system evaluates all the rules together and creates an expanded set of criteria that target devices use to evaluate network traffic. A pop-up window may warn that you have exceeded the maximum number of access control rules or intrusion policies supported by a target device. This maximum depends on a number of factors, including the physical memory and the number of processors on the device.

Simplifying Access Control Rules

The following guidelines can help you simplify access control rules and improve performance:

- When constructing a rule, use as few individual elements in your conditions as possible. For example, in network conditions, use IP address blocks rather than individual IP addresses. In port conditions, use port ranges. Use application filters and URL categories and reputations to perform application control and URL filtering, and LDAP user groups to perform user control.

  Note that combining elements into objects that you then use in access control rule conditions does not improve performance. For example, using a network object that contains 50 individual IP addresses gives you only an organizational—not a performance—benefit over including those IP addresses in the condition individually.
- Restrict rules by security zones whenever possible. If a device's interfaces are not in one of the zones in a zone-restricted rule, the rule does not affect performance on that device.
- Do not overconfigure rules. If one condition is enough to match the traffic you want to handle, do not use two.

Avoiding Intrusion Policy and Variable Set Proliferation

The number of unique intrusion policies you can use to inspect traffic in an access control policy depends on the resources on your device and the complexity of your policies: you can associate one intrusion policy with each Allow and Interactive Block rule, as well as with the default action. Every unique **pair** of intrusion policy and variable set counts as one policy.

If you exceed the number of intrusion policies supported by your device, reevaluate your access control policy. You may want to consolidate intrusion policies or variable sets so you can associate a single intrusion policy-variable set pair with multiple access control rules.

Check to see how many policies you select and how many variable sets those policies use in each of the following locations in your access control policy: the **Intrusion Policy used before Access Control rule is determined** option in the Advanced access control policy settings, the default action for the access control policy, and the inspection settings for any access control rules in the policy.

Understanding Rule Preemption and Invalid Configuration Warnings

License: Any

Properly configuring and ordering access control rules (and, in advanced deployments, network analysis rules) is essential to building an effective deployment. Within an access control policy, access control rules can preempt other rules or contain invalid configurations. Similarly, network analysis rules, which you configure using the access control policy's advanced settings, can have the same issues. The system uses warning and error icons to mark these.

Understanding Rule Preemption Warnings

The conditions of an access control rule may preempt a subsequent rule from matching traffic. For example:

```
Rule 1: allow Admin users
Rule 2: block Admin users
```

The second rule above will never block traffic because the first rule will have already allowed the traffic.

Any type of rule condition can preempt a subsequent rule. For example, the VLAN range in the first rule below includes the VLAN in the second rule, so the first rule preempts the second rule:

```
Rule 1: allow VLAN 22-33
Rule 2: block VLAN 27
```

In the following example, Rule 1 matches any VLAN because no VLANs are configured, so Rule 1 preempts Rule 2, which attempts to match VLAN 2:

```
Rule 1: allow Source Network 10.4.0.0/16
```

```
Rule 2: allow Source Network 10.4.0.0/16, VLAN 2
```

A rule also preempts an identical subsequent rule where all configured conditions are the same. For example:

```
Rule 1: allow VLAN 1 URL www.example.com
Rule 2: allow VLAN 1 URL www.example.com
```

A subsequent rule would not be preempted if any condition is different. For example:

```
Rule 1: allow VLAN 1 URL www.example.com
Rule 2: allow VLAN 2 URL www.example.com
```

Understanding Invalid Configuration Warnings

Because outside settings that the access control policy depends on may change, an access control policy setting that was valid may become invalid. Consider the following examples:

- A rule that performs URL filtering might be valid until you target a device that does not have a URL Filtering license. At that point, an error icon appears next to the rule, and you cannot apply the policy to that device until you edit or delete the rule, retarget the policy, or enable the appropriate license.
- If you add a port group to the source ports in a rule, then change the port group to include an ICMP port, the rule becomes invalid and a warning icon appears next to it. You can still apply the policy, but the rule will have no effect on network traffic.
- If you add a user to a rule, then change your LDAP user awareness settings to exclude that user, the rule will have no effect because the user is no longer an access controlled user.

Ordering Rules to Improve Performance and Avoid Preemption

License: Any

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.

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.

Order Rules from Most to Least Critical

First, you must order rules to suit your organization's needs. Place priority rules that must apply to all traffic near the top of the policy. For example, if you want to inspect traffic from a single user for intrusions (using an Allow rule), but trust all other users in the department (using a Trust rule), place two access control rules in that order.

Order Rules from Specific to General

You can improve performance by placing specific rules earlier, that is, rules that narrowly define the traffic they handle. This is also important because rules with broad conditions can match many different types of traffic, and can preempt later, more specific rules.

Consider a scenario where you want to block most social networking sites, but allow access to certain others. For example, you may want your graphic designers to be able to access Creative Commons Flickr and deviantART content, but not access other sites such as Facebook or Google+. You should order your rules as follows:

```
Rule 1: Allow Flickr, deviantART for the "Design" LDAP user group
Rule 2: Block social networking
```

If you reverse the rules:

```
Rule 1: Block social networking
Rule 2: Allow Flickr, deviantART for the "Design" LDAP user group
```

the first rule blocks all social networking traffic, including Flickr and deviantART. Because no traffic will ever match the second rule, your designers cannot access the content you wanted to make available.

Place Rules that Inspect Traffic Later

Because discovery, intrusion, file, and malware inspection require processing resources, placing rules that do not inspect traffic (Trust, Block) before rules that do (Allow, Interactive Block) can improve performance. This is because Trust and Block rules can divert traffic that the system might otherwise have inspected. All other factors being equal, that is, given a set of rules where none is more critical and preemption is not an issue, consider placing them in the following order:

- Monitor rules that log matching connections, but take no other action on traffic
- Trust and Block rules that handle traffic without further inspection
- Allow and Interactive Block rules that do not inspect traffic further
- Allow and Interactive Block rules that optionally inspect traffic for malware, intrusions, or both

Generating a Report of Current Access Control Settings

License: Any

An access control policy report is a record of the policy and rules configuration at a specific point in time. You can use the report, which contains the following information, for auditing purposes or to inspect the current configuration.

Table 12-8 Access Control Policy Report Sections

Section	Description
Policy Information	Provides the name and description of the policy, the name of the user who last modified the policy, and the date and time the policy was last modified.
Device Targets	Lists the managed devices targeted by the policy.
HTTP Block Response HTTP Interactive Block Response	Provides details on the pages you display to users when you block a website using the policy.
Security Intelligence	Provides details on the policy's Security Intelligence whitelist and blacklist.
Default Action	Lists the default action and associated variable set, if any.
Rules	Lists each access control rule in the policy, and provides details about its configuration.

Table 12-8 Access Control Policy Report Sections (continued)

Section	Description
Advanced Settings	Detailed information on the policy's advanced settings, including: • network analysis policies used to preprocess traffic for the access control policy, as well as global preprocessing options • adaptive profile settings for passive deployments • performance settings for detecting files, malware, and intrusions • other policy-wide settings
Referenced Objects	Provides details on the reusable objects referenced by the access control policy, including intrusion policy variable sets and objects used by the SSL policy.

You can also generate an access control comparison report that compares a policy with the currently applied policy or with another policy. For more information, see Comparing Access Control Policies, page 12-27.

To view an access control policy report:

Access: Admin/Access Admin/Network Admin

Step 1 Select **Policies > Access Control**.

The Access Control Policy page appears.

Step 2 Click the report icon () next to the policy for which you want to generate a report. Remember to save any changes before you generate an access control policy report; only saved changes appear in the report.

The system generates the report. Depending on your browser settings, the report may appear in a pop-up window, or you may be prompted to save the report to your computer.

Comparing Access Control Policies

License: Any

To review policy changes for compliance with your organization's standards or to optimize system performance, you can examine the differences between two access control policies. You can compare any two policies or the currently applied policy with another policy. Optionally, after you compare, you can then generate a PDF report to record the differences between the two policies.

There are two tools you can use to compare policies:

- The comparison view displays only the differences between two policies in a side-by-side format. The name of each policy appears in the title bar on the left and right sides of the comparison view except when you select **Running Configuration**, in which case a blank bar represents the currently active policy.

  You can use this to view and navigate both policies on the web interface, with their differences highlighted.

- The comparison report creates a record of only the differences between two policies in a format similar to the policy report, but in PDF format.

You can use this to save, copy, print, and share your policy comparisons for further examination.

For more information on understanding and using the policy comparison tools, see:

- Using the Access Control Policy Comparison View, page 12-28
- Using the Access Control Policy Comparison Report, page 12-28

Using the Access Control Policy Comparison View

License: Any

The comparison view displays both policies in a side-by-side format, with each policy identified by name in the title bar on the left and right sides of the comparison view. When comparing two policies other than the running configuration, the time of last modification and the last user to modify are displayed with the policy name.

Differences between the two policies are highlighted:

- Blue indicates that the highlighted setting is different in the two policies, and the difference is noted in red text.
- Green indicates that the highlighted setting appears in one policy but not the other.

You can perform any of the actions in the following table.

Table 12-9 Access Control Policy Comparison View Actions

To...	You can...
navigate individually through changes	click **Previous** or **Next** above the title bar. The double-arrow icon ( ) centered between the left and right sides moves, and the **Difference** number adjusts to identify which difference you are viewing.
generate a new policy comparison view	click **New Comparison**. The **Select Comparison** window appears. See Using the Access Control Policy Comparison Report, page 12-28 for more information.
generate a policy comparison report	click **Comparison Report**. The policy comparison report creates a PDF document that lists only the differences between the two policies.

Using the Access Control Policy Comparison Report

License: Any

An access control policy comparison report is a record of all differences between two access control policies or a policy and the currently applied policy identified by the policy comparison view, presented in PDF format. You can use this report to further examine the differences between two policy configurations and to save and disseminate your findings.

You can generate an access control policy comparison report from the comparison view for any policies to which you have access. Remember to save any changes before you generate a policy report; only saved changes appear in the report.

The format of the policy comparison report is the same as the policy report with one exception: the policy report contains all configurations in the policy, and the policy comparison report lists only those configurations that differ between the policies. An access control policy comparison report contains the

sections described in Table 12-8 on page 12-26.

Tip You can use a similar procedure to compare SSL, network analysis, intrusion, file, system, or health policies.

To compare two access control policies:

Access: Admin/Access Admin/Network Admin

Step 1 Select **Policies > Access Control**.

The Access Control Policy page appears.

Step 2 Click **Compare Policies**.

The Select Comparison window appears.

Step 3 From the **Compare Against** drop-down list, select the type of comparison you want to make:

- To compare two different policies, select **Other Policy**.

  The page refreshes and the Policy A and Policy B drop-down lists appear.
- To compare another policy to the currently active policy, select **Running Configuration.**

  The page refreshes and the Target/Running Configuration A and Policy B drop-down lists appear.

Step 4 Depending on the comparison type you selected, you have the following choices:

- If you are comparing two different policies, select the policies you want to compare from the Policy A and Policy B drop-down lists.
- If you are comparing the running configuration to another policy, select the second policy from the Policy B drop-down list.

Step 5 Click **OK** to display the policy comparison view.

The comparison view appears.

Step 6 Optionally, click **Comparison Report** to generate the access control policy comparison report.

The access control policy comparison report appears. Depending on your browser settings, the report may appear in a pop-up window, or you may be prompted to save the report to your computer.