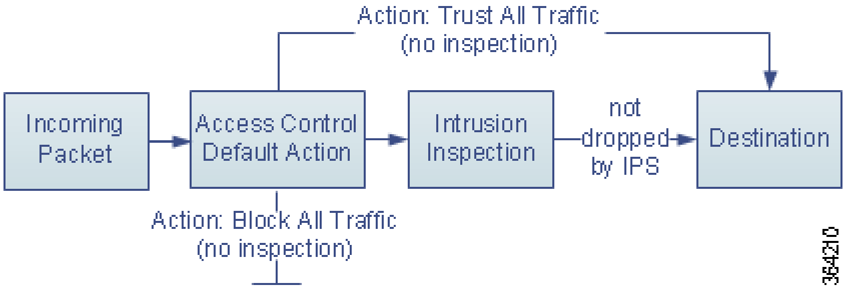
CHAPTER 4

Getting Started with Access Control Policies

An *access control policy* determines how the system handles traffic on your network. Each ASA FirePOWER module can have one currently applied policy.

The simplest access control policy handles 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.



Note that only ASA FirePOWER modules 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 ASA FirePOWER modules.

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:

- Access Control License and Role Requirements, page 4-2
- Creating a Basic Access Control Policy, page 4-3
- Managing Access Control Policies, page 4-6
- Editing Access Control Policies, page 4-7
- Understanding Out-of-Date Policy Warnings, page 4-9
- Applying an Access Control Policy, page 4-10
- Troubleshooting Access Control Policies and Rules, page 4-14
- Generating a Report of Current Access Control Settings, page 4-17
- Comparing Access Control Policies, page 4-18

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 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 5-1 explains how to immediately blacklist (block) connections based on the latest reputation intelligence.
- Understanding Network Analysis and Intrusion Policies, page 11-1 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 6-1 explains how access control rules provide a granular method of handling network traffic across multiple ASA FirePOWER modules.
- Controlling Traffic Using Intrusion and File Policies, page 10-1 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 ASA FirePOWER module, many features require that you enable the appropriate licenses before you apply the policy.

For more information, see License Requirements for Access Control, page 4-2.

License Requirements for Access Control

Although you can create access control policies regardless of the licenses on your ASA FirePOWER module, certain aspects of access control require that you enable specific licensed capabilities before you can apply the policy.

Warning icons and confirmation dialog boxes designate unsupported features for your deployment. For details, see Troubleshooting Access Control Policies and Rules, page 4-14.

The following table explains the license requirements to apply access control policies.

Table 4-1 License Requirements for Access Control

To apply an access control policy that...	License
performs access control based on zone, network, or port performs URL filtering using literal URLs and URL objects	Any
performs access control using geolocation data (source or destination country or continent)	Any
performs intrusion detection and prevention, file control, or Security Intelligence filtering	Protection
performs advanced malware protection, that is, network-based malware detection and blocking	Malware

Table 4-1 License Requirements for Access Control (continued)

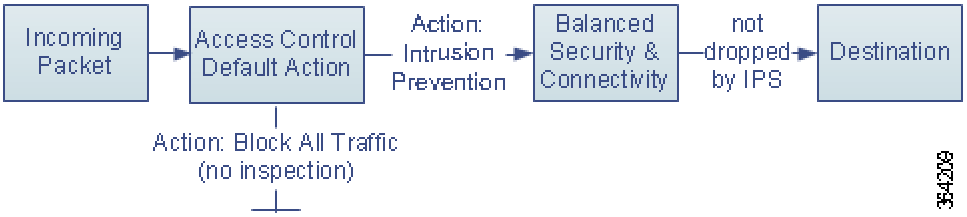
To apply an access control policy that...	License
performs user or application control	Control
performs URL filtering using category and reputation data	URL Filtering

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 ASA FirePOWER modules handles all traffic; you will add other configurations that affect traffic flow later.

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, as shown in the following diagram.


Incoming Packet
Access Control Default Action
Action: Intrusion Prevention
Balanced Security & Connectivity
not dropped by IPS
Destination
Action: Block All Traffic (no inspection)
354209

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.

Optionally, you can use and modify the initial system-provided policy named Default Trust All Traffic.

To create an access control policy:

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

The Access Control Policy page appears.

Tip You can also copy an existing policy from this ASA FirePOWER module or import a policy from another ASA FirePOWER module. To copy a policy, click the copy icon (). To import a policy, see Importing and Exporting Configurations, page B-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.

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 4-4.

Step 5 Click **Store ASA FirePOWER Changes**.

The access control policy editor appears. For information on configuring your new policy, see Editing Access Control Policies, page 4-7. Note that you must apply the policy for it to take effect; see Applying an Access Control Policy, page 4-10.

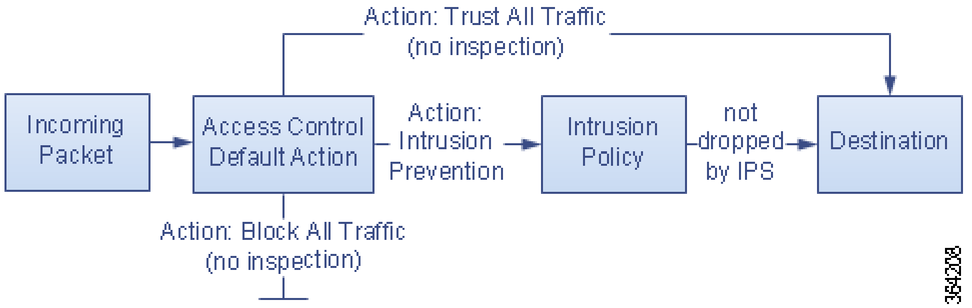
Setting Default Handling and Inspection for Network Traffic

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
- 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, 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. Your options are shown in the following diagram.


Action: Trust All Traffic
(no inspection)
Incoming Packet
Access Control Default Action
Action: Intrusion Prevention
Intrusion Policy
not dropped by IPS
Destination
Action: Block All Traffic
(no inspection)
364208

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 10-1.

:

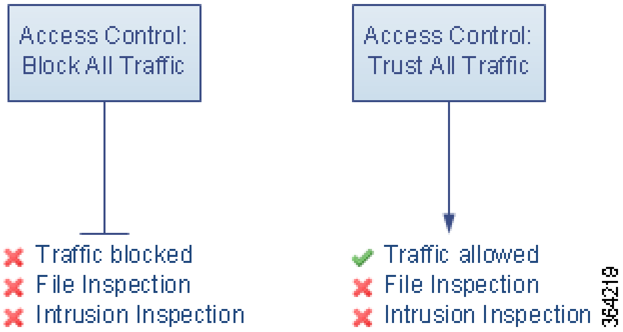
Table 4-2 Access Control Policy Default Actions

Default Action	Effect on Traffic	Inspection Type and Policy
Access Control: Block All Traffic	block without further inspection	none

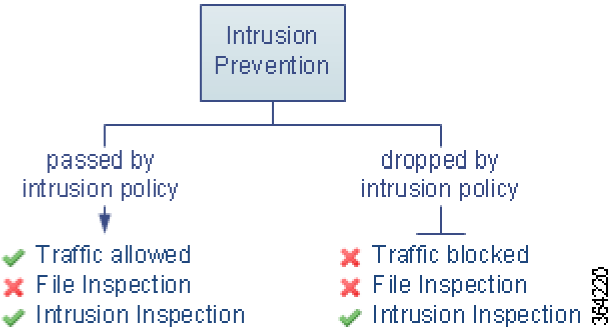
Table 4-2 Access Control Policy Default Actions (continued)

Default Action	Effect on Traffic	Inspection Type and Policy
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 a Protection license)	intrusion, using the specified intrusion policy and associated variable set

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



The diagram below illustrates the **Intrusion Prevention** default actions.



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:

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

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 inspect all traffic with an intrusion policy, select an intrusion policy, all of which begin with the label **Intrusion Prevention**. Keep in mind that an intrusion policy can block traffic.

⚠ **Caution** Do **not** use `Experimental Policy 1` unless instructed to do so by a Cisco representative. Cisco uses this policy for testing.

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 2-13.

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

You can log a matching connection at its beginning and end. Note that the system cannot log the end of blocked traffic. You can log connections to the ASA FirePOWER module event viewer, external system log (syslog) or SNMP trap server. For more information, see Logging Connections Handled by the Access Control Default Action, page 25-11.

Managing Access Control Policies

License: Any

On the Access Control Policy page (**Configuration > ASA FirePOWER Configuration > Policies > Access Control**) you can view your current custom access control policies, along information on whether a policy is applied.

In addition to custom policies that you create, the system provides a custom policy Default Allow All Traffic that you can edit and use.

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

Table 4-3 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 4-3
edit an existing access control policy	click the edit icon (✎).	Editing Access Control Policies, page 4-7
reapply an access control policy	click the apply icon (✓).	Applying an Access Control Policy, page 4-10
export an access control policy to import on another ASA FirePOWER module	click the export icon (📤)	Exporting Configurations, page B-1
view a PDF report that lists the current configuration settings in an access control policy	click the report icon (📄).	Generating a Report of Current Access Control Settings, page 4-17

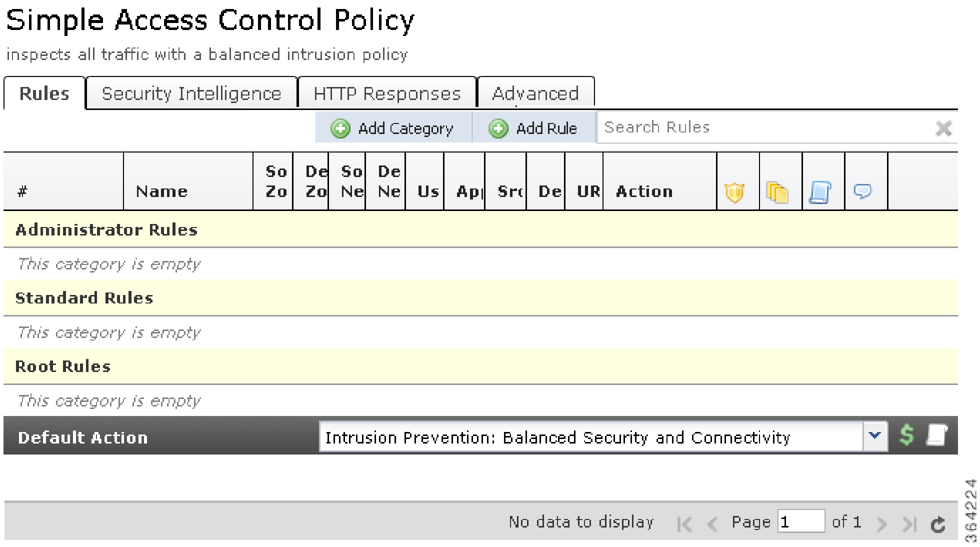
Table 4-3 Access Control Policy Management Actions (continued)

To...	You can...	See...
compare access control policies	click **Compare Policies**.	Comparing Access Control Policies, page 4-18
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 traffic with the system-provided Balanced Security and Connectivity intrusion policy before allowing it to its final destination.



Simple Access Control Policy

inspects all traffic with a balanced intrusion policy

Administrator Rules

This category is empty

Standard Rules

This category is empty

Root Rules

This category is empty

Default Action: Intrusion Prevention: Balanced Security and Connectivity

No data to display

Use the access control policy editor to add and organize rules, 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.

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 5-1.

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, port, application, requested URL, or user. Conditions can be simple or complex; their use often depends on certain licenses.

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 6-1.

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. You can also enable or disable logging of connections handled by the default action.

For more information, see Setting Default Handling and Inspection for Network Traffic, page 4-4 and Logging Connections Based on Access Control Handling, page 25-9.

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 8-14.

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 ASA FirePOWER module database for each URL requested by your users; see Logging URLs Detected in Connections, page 25-13
- 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 8-13
- network analysis and intrusion policy settings that allow you to tailor many preprocessing options to networks and zones, as well as set default intrusion inspection behavior; see Customizing Traffic Preprocessing, page 13-1
- advanced transport and network preprocessor settings that apply globally to all networks and zones where you apply the access control policy; see Configuring Advanced Transport/Network Settings, page 17-1
- 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 18-1
- performance options for intrusion inspection, file control, file storage, and advanced malware protection; see Tuning Intrusion Prevention Performance, page 10-6 and Tuning File and Malware Inspection Performance and Storage, page 10-16

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.

To edit an access control policy:

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

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 **Store ASA FirePOWER Changes.**
- To save your changes and apply your policy, click **Apply ASA FirePOWER Changes**. See Applying an Access Control Policy, page 4-10.
- 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 (**Configuration > ASA FirePOWER Configuration > Policies > Access Control**), out-of-date policies are marked with red status text.

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, Security Intelligence filtering, advanced options including NAP rules, and so on.
- Changing any of the intrusion and file policies that the access control policy invokes: 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, URL, and geolocation objects; Security Intelligence lists and feeds; application filters or detectors; intrusion policy variable sets; file lists; 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 ASA FirePOWER module interface. For example, you can modify security zones using the object manager (**Configuration > ASA FirePOWER Configuration > Object Management**).

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

- 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:

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

The Access Control Policy page appears. Policies that are out of date are marked with red status text that indicates that the ASA FirePOWER module needs 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 4-18 and Comparing Two Intrusion Policies or Revisions, page 19-9.

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 implement the change on the networks monitored by the ASA FirePOWER module. 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, network analysis and file policies. You cannot apply these policies independently.

Caution Leaving the **Inspect Traffic During Policy Apply** option checked via the advanced tab does not allow any uninspected traffic through with a brief disruption in connectivity during policy apply. If you value connectivity over inspected traffic, uncheck the **Inspect Traffic During Policy Apply** option to allow uninspected traffic with no disruption. On 3D7010, 3D7020, and 3D7030 managed devices, applying an access control policy can take up to five minutes. To minimize inconvenience, apply access control policies during a change window or leave the **Inspect Traffic During Policy Apply** option checked.

Traffic interruption occurs when the Snort® process restarts; for example, the process restarts when you apply an access control policy that includes a new version of Snort following an ASA FirePOWER module upgrade, when you apply a policy for the first time after a rule import that includes shared object rules, and, in some cases, when you install a VDB update.

Note that only devices deployed inline can affect the flow of traffic. Applying an access control policy configured to block or alter traffic to a passively deployed device 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.

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

- Some features require specific licenses or minimum versions of the system. For more information, see License Requirements for Access Control, page 4-2, as well as the release notes for the version of the system you are running. 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.
- When you apply an access control policy, the system evaluates all the rules together and creates an expanded set of criteria 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. You might be able to select as few as three intrusion policies across an entire access control policy. For more information, see Simplifying Rules to Improve Performance, page 4-15.
- 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 35-9.

See the following sections for more information:

- Applying a Complete Policy, page 4-11 explains how to use the quick-apply option to apply the access control policy along with all associated network analysis, intrusion and file policies.
- Applying Selected Policy Configurations, page 4-12 explains how to apply specific access control policy configurations, including individual intrusion policies.

Applying a Complete Policy

License: Any

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

- 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.

To quick-apply a complete access control policy:

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

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 **Apply ASA FirePOWER Changes** while editing a policy; see Editing Access Control Policies, page 4-7.

Step 3 Click **Apply All**.

Note that the **Inspect Traffic During Policy Apply** option is checked by default and allows traffic inspection during a policy apply. If you value connectivity over traffic inspection, uncheck this option via the advanced tab.

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 (**Monitoring > ASA FirePOWER 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 provides a column for the access control policy and a column for associated intrusion policies. You can specify whether to apply changes to an access control policy, to associated intrusion policies individually or in combination, or both.

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 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 network analysis and file policies that are different from those currently running. 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. 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. 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.

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 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 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.

To apply selected access control policy configurations:

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

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 **Apply ASA FirePOWER Changes** while editing a policy; see Editing Access Control Policies, page 4-7.

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 (**Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**) 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 to specify whether to apply the access control policy.

Step 5 Select or clear the intrusion policy check box to specify whether to apply an intrusion policy.

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. 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.

Note that the **Inspect Traffic During Policy Apply** option is checked by default and allows traffic inspection during a policy apply. If you value connectivity over traffic inspection, uncheck this option via the advanced tab.

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

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.

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 4-4 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, 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. An access control policy successfully applies only to an eligible device.
ℹ	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 8-6 and Limitations to URL Detection and Blocking, page 8-11.

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 4-2
- Simplifying Rules to Improve Performance, page 4-15
- Understanding Rule Preemption and Invalid Configuration Warnings, page 4-16
- Ordering Rules to Improve Performance and Avoid Preemption, page 4-16

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 the ASA FirePOWER module uses 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.

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 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. You might be able to select as few as three intrusion policies across an entire access control policy.

If you exceed the number of intrusion policies supported, reevaluate your access control policy. You may want to consolidate intrusion policies or variable sets.

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.

Note the following:

- Any type of rule condition can preempt a subsequent rule.
- A rule also preempts an identical subsequent rule where all configured conditions are the same.
- A subsequent rule would not be preempted if any condition is different.

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:

- 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 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 4-5 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.
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 4-5 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.

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 4-18.

To view an access control policy report:

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

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. You are 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 module 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 4-19
- Using the Access Control Policy Comparison Report, page 4-19

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 4-6 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 4-19 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 4-5 on page 4-17.

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

To compare two access control policies:

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

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. You are prompted to save the report to your computer.