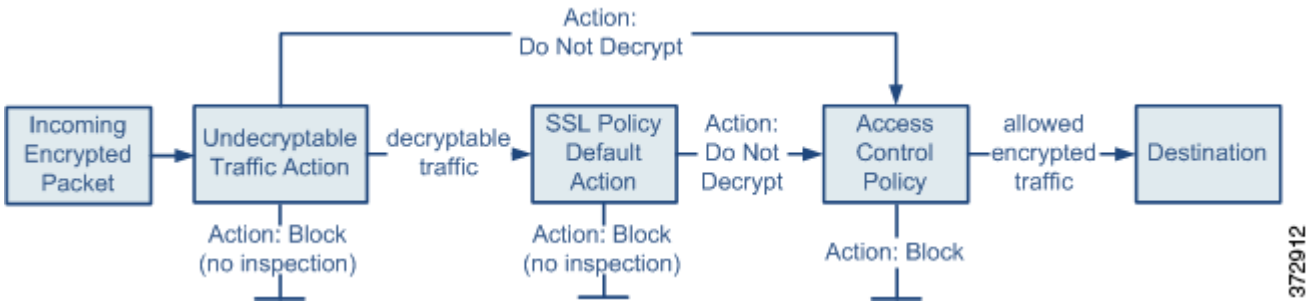


Getting Started with SSL Policies

An *SSL policy* determines how the system handles encrypted traffic on your network. You can configure one or more SSL policies. You associate an SSL policy with an access control policy, then apply the access control policy. When the ASA FirePOWER module detects a TCP handshake, the access control policy first handles and inspects the traffic. If it subsequently identifies an SSL-encrypted session over the TCP connection, the SSL policy takes over, handling and decrypting the encrypted traffic. You can have one currently applied SSL policy.

The simplest SSL policy, as shown in the following diagram, directs the device where it is applied to handle encrypted traffic with a single default action. You can set the default action to block decryptable traffic without further inspection, or inspect undecrypted decryptable traffic with access control. The system can then either allow or block the encrypted traffic. If the ASA FirePOWER module detects undecryptable traffic, it either blocks the traffic without further inspection or does not decrypt it, inspecting it with access control.



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

- Creating a Basic SSL Policy, page 13-2
- Editing an SSL Policy, page 13-6
- Applying Decryption Settings Using Access Control, page 13-8
- Generating a Report of Current Traffic Decryption Settings, page 13-9
- Comparing SSL Policies, page 13-10

A more complex SSL policy can handle different types of undecryptable traffic with different actions, control traffic based on whether a certificate authority (CA) issued or trusts the encryption certificate, and use SSL rules to exert granular control over encrypted traffic logging and handling. These rules can be simple or complex, matching and inspecting encrypted traffic using multiple criteria. After you create a basic SSL policy, see the following chapters for more information on tailoring it to your deployment:

- Managing Reusable Objects, page 2-1 describes how to configure reusable public key infrastructure (PKI) objects and other SSL inspection-related objects to enhance encrypted traffic control and decrypt traffic.
- Logging Connections in Network Traffic, page 34-1 describes how to configure logging for encrypted traffic, whether decryptable or undecryptable.
- Applying Decryption Settings Using Access Control, page 13-8 describes how to associate an SSL policy with an access control policy.
- Getting Started with Access Control Policies, page 4-1 describes how to apply an access control policy to a device.
- Tuning Traffic Flow Using Access Control Rules, page 6-1 describes how to configure access control rules to inspect decrypted traffic.
- Getting Started with SSL Rules, page 14-1 describes how to configure SSL rules to handle and log encrypted traffic.
- Tuning Traffic Decryption Using SSL Rules, page 15-1 describes how to configure SSL rule conditions to better match specific encrypted traffic.

Creating a Basic SSL Policy

License: Any

When you create a new SSL policy you must, at minimum, give it a unique name and specify a policy default action. You have the following options when selecting a default action for a new policy:

- **Do not decrypt** creates a policy with the Do not decrypt default action.
- **Block** creates a policy with the Block default action.
- **Block with reset** creates a policy with the Block with reset default action.

After you create the SSL policy, you can modify the default action. For guidance on choosing a default action, see Setting Default Handling and Inspection for Encrypted Traffic, page 13-3.

The new SSL policy also contains default actions for traffic the system cannot decrypt: either it inherits the default action you just selected for undecryptable traffic, blocks it, or does not decrypt the traffic and inspects it with access control. You can modify the undecryptable traffic actions after you create the SSL policy. For guidance on selecting undecryptable traffic actions, see Setting Default Handling for Undecryptable Traffic, page 13-4

On the SSL policy page (**Configuration > ASA FirePOWER Configuration > Policies > SSL**) you can view all your current SSL policies by name with optional description. Options on this page allow you to compare policies, create a new policy, copy a policy, view a report that lists all of the most recently saved settings in each policy, edit a policy, or delete a policy.

The following table describes the actions you can take to manage your policies on the SSL Policy page:

Table 13-1 SSL Policy Management Actions

To...	You can...
create a new SSL policy	click **New Policy**. See Creating a Basic SSL Policy, page 13-2 for more information.
modify the settings in an existing SSL policy	click the edit icon ( ). See Editing an SSL Policy, page 13-6 for more information.

Table 13-1 SSL Policy Management Actions (continued)

To...	You can...
compare SSL policies	click **Compare Policies**. See Comparing SSL Policies, page 13-10 for more information.
copy an SSL policy	click the copy icon ( ). See Editing an SSL Policy, page 13-6 for more information on editing a copied policy.
view a PDF report that lists the current configuration settings in an SSL policy	click the report icon ( ). See Generating a Report of Current Traffic Decryption Settings, page 13-9 for more information.
delete an SSL policy	click the delete icon ( ), then click **OK**. When prompted whether to continue, you are also informed if another user has unsaved changes in the policy.

To create an SSL policy:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > SSL**.

The SSL Policy page appears.

Step 2 Give the policy a unique **Name** and, optionally, a **Description**.

You can use all printable characters, including spaces and special characters.

Step 3 Specify the **Default Action**.

Note that you can modify your selected default action after you create your SSL policy. See Setting Default Handling and Inspection for Encrypted Traffic, page 13-3 for more information.

Step 4 Click **Store ASA FirePOWER Changes**.

The SSL Policy Editor page appears. See Editing an SSL Policy, page 13-6 for more information.

Setting Default Handling and Inspection for Encrypted Traffic

License: Any

The default action for an SSL policy determines how the system handles decryptable encrypted traffic that does not match any non-Monitor rule in the policy. When you apply an SSL policy that does not contain any SSL rules, the default action determines how all decryptable traffic on your network is handled. See Setting Default Handling for Undecryptable Traffic, page 13-4 for more information on how the system handles undecryptable encrypted traffic.

The following table lists the default actions you can choose, as well as their effect on encrypted traffic. Note that the system does not perform any kind of inspection on encrypted traffic blocked by the default action.

Table 13-2 SSL Policy Default Actions

Default Action	Effect on Encrypted Traffic
Block	block the SSL session without further inspection
Block with reset	block the SSL session without further inspection and reset the TCP connection
Do not decrypt	inspect the encrypted traffic with access control

When you first create an SSL policy, logging connections that are handled by the default action is disabled by default. You can change this, as well as the default action itself, after you create the policy.

The following procedure explains how to set the default action for an SSL policy while editing the policy. See Editing an SSL Policy, page 13-6 for the complete procedure for editing an SSL policy.

To set the default action of an SSL policy:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > SSL**.

The SSL policy page appears.

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

The SSL policy editor appears.

Step 3 Select a **Default Action**. See the SSL Policy Default Actions table for more information.

Step 4 Configure logging options for the default action as described in Logging Decryptable Connections with SSL Rules, page 34-14.

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

The SSL Policy Editor page appears. See Editing an SSL Policy, page 13-6 for more information.

Setting Default Handling for Undecryptable Traffic

License: Any

You can set undecryptable traffic actions at the SSL policy level to handle certain types of encrypted traffic the system cannot decrypt or inspect. When you apply an SSL policy that does not contain any SSL rules, the undecryptable traffic actions determine how all undecryptable encrypted traffic on your network is handled.

Depending on the type of undecryptable traffic, you can choose to:

- block the connection
- block the connection, then reset it
- inspect the encrypted traffic with access control
- inherit the default action from the SSL policy

The following table describes the undecryptable traffic types:

Table 13-3 Undecryptable Traffic Types

Type	Description	Default Action	Available Actions
Compressed Session	The SSL session applies a data compression method.	Inherit default action	Do not decrypt Block Block with reset Inherit default action
SSLv2 Session	The session is encrypted with SSL version 2. Note that traffic is decryptable if the client hello message is SSL 2.0, and the remainder of the transmitted traffic is SSL 3.0.	Inherit default action	Do not decrypt Block Block with reset Inherit default action
Unknown Cipher Suite	The system does not recognize the cipher suite.	Inherit default action	Do not decrypt Block Block with reset Inherit default action
Unsupported Cipher Suite	The system does not support decryption based on the detected cipher suite.	Inherit default action	Do not decrypt Block Block with reset Inherit default action
Session not cached	The SSL session has session reuse enabled, the client and server reestablished the session with the session identifier, and the system did not cache that session identifier.	Inherit default action	Do not decrypt Block Block with reset Inherit default action
Handshake Errors	An error occurred during SSL handshake negotiation.	Inherit default action	Do not decrypt Block Block with reset Inherit default action
Decryption Errors	An error occurred during traffic decryption.	Block	Block Block with Reset

When you first create an SSL policy, logging connections that are handled by the default action is disabled by default. Because the logging settings for the default action also apply to undecryptable traffic handling, logging connections handled by the undecryptable traffic actions is disabled by default. For more information on configuring default logging, see Logging Decryptable Connections with SSL Rules, page 34-14.

Note The system cannot decrypt traffic if an HTTP proxy is positioned between a client and your device, and the client and server establish a tunneled SSL connection using the CONNECT HTTP method. The **Handshake Errors** undecryptable action determines how the system handles this traffic. See Decrypt Actions: Decrypting Traffic for Further Inspection, page 14-9 for more information.

Note that if your browser uses certificate pinning to verify a server certificate, you cannot decrypt this traffic by re-signing the server certificate. Because you can still inspect this traffic with access control, it is not handled by the undecryptable traffic actions. If you want to allow this traffic, configure an SSL rule with the Do not decrypt action to match the server certificate common name or distinguished name.

To set the default handling for undecryptable traffic:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > SSL**.

The SSL Policy page appears.

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

The SSL policy editor appears.

Step 3 Select the **Undecryptable Actions** tab.

The Undecryptable Actions tab appears.

Step 4 For each field, select the action you want to take on the type of undecryptable traffic, or if you want to apply the SSL policy's default action. See the SSL Policy Default Actions table for more information.

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

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

Editing an SSL Policy

License: Any

On the SSL policy editor, you can configure your policy and organize SSL rules. To configure an SSL policy, you must give the policy a unique name and specify a default action. You can also:

- add, edit, delete, enable, and disable SSL rules
- add trusted CA certificates
- determine the handling for encrypted traffic the system cannot decrypt
- log traffic that is handled by the default action and undecryptable traffic actions

After you create or modify an SSL policy, you can associate it with an access control policy, then apply the access control policy. You can also create custom user roles that allow you to assign different permissions to different users for configuring, organizing, and applying policies.

The following table summarizes the configuration actions you can take on the SSL policy editor.

Table 13-4 SSL Policy Configuration Actions

To...	You can...
modify the policy name or description	click the name or description field, delete any characters as needed, then type the new name or description.
set the default action	find more information at Setting Default Handling and Inspection for Encrypted Traffic, page 13-3.
set default handling for undecryptable traffic	find more information at Setting Default Handling for Undecryptable Traffic, page 13-4.

Table 13-4 SSL Policy Configuration Actions (continued)

To...	You can...
log connections for the default action and undecryptable traffic actions	find more information at Logging Decryptable Connections with SSL Rules, page 34-14.
add trusted CA certificates	find more information at Trusting External Certificate Authorities, page 15-21.
assign different rights to different users	find more information at Collecting Prerequisite Information to Configure SSL Rules, page 12-3.
save your policy changes	click **Save**.
cancel your policy changes	click **Cancel**, then, if you have made changes, click **OK**.
add a rule to a policy	click **Add Rule**. See Understanding and Creating SSL Rules, page 14-4 for more information. **Tip** You can also right-click a blank area in the row for a rule and select **Insert new rule**.
edit an existing rule	click the edit icon ( ) next to the rule. See Understanding and Creating SSL Rules, page 14-4 for more information. **Tip** You can also right-click the rule and select **Edit**.
delete a rule	click the delete icon ( ) next to the rule, then click **OK**. **Tip** You can also right-click a blank area in the row for a selected rule, select **Delete**, then click **OK** to delete one or more selected rules.
enable or disable an existing rule	right-click a selected rule, select **State**, then select **Disable** or **Enable**. Disabled rules are grayed and marked `(disabled)` beneath the rule name.
display the configuration page for a specific rule attribute	click the name, value, or icon in the column for the condition on the row for the rule. For example, click the name or value in the **Source Networks** column to display the Networks page for the selected rule. See Tuning Traffic Decryption Using SSL Rules, page 15-1 for more information.

When you change your configuration, 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 SSL 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 multiple users edit the same policy concurrently, a message on the policy editor identifies other users who have unsaved changes. Any user who attempts to save changes is cautioned that his 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 SSL policy:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > SSL**.

The SSL Policy page appears.

Step 2 You have the following choices:

- To configure your policy, you can take any of the actions summarized in the SSL Policy Configuration Actions table.
- To organize rules in your policy, you can take any of the actions described in Managing SSL Rules in a Policy, page 14-11.

Step 3 Save or discard your configuration. You have the following choices:

- To save your changes and continue editing, click **Store ASA FirePOWER Changes**.
- To discard your changes, click **Cancel** and, if prompted, click **OK**.

  Your changes are discarded and the SSL Policy page appears.

Applying Decryption Settings Using Access Control

License: Any

After making any changes to an SSL policy, you must apply the access control policy it is associated with. For more information, see Deploying Configuration Changes, page 4-11.

Keep the following points in mind when applying SSL policies:

- You cannot delete an SSL policy that has been applied or is currently applying.
- Applying an access control policy automatically applies the associated SSL policy. You cannot apply an SSL policy independently.

Note In a passive deployment, the system cannot influence the flow of traffic. If you attempt to apply an access control policy that references an SSL policy that blocks encrypted traffic, or that is configured to decrypt traffic by re-signing the server certificate, the system displays a warning. Also, passive deployments do not support decrypting traffic encrypted with the ephemeral Diffie-Hellman (DHE) or the elliptic curve Diffie-Hellman (ECDHE) cipher suites.

To associate an SSL policy with 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 Select the **Advanced** tab.

Advanced settings for the access control policy appear.

Step 4 Click the edit icon ( ) next to General Settings.

The General Settings pop-up window appears.

Step 5 Select an SSL policy from the **SSL Policy to use for inspecting encrypted connections** drop-down.

Step 6 Click **OK**.

Advanced settings for the access control policy appear.

Step 7 Click **Store ASA FirePOWER Changes**.

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

Generating a Report of Current Traffic Decryption Settings

License: Any

An SSL policy report is a record of the policy and rules configuration at a specific point in time. You can use the report for auditing purposes or to inspect the current configuration.

Tip You can also generate an SSL comparison report that compares a policy with the currently applied policy or with another policy. For more information, see Comparing SSL Policies, page 13-10.

An SSL policy report contains the sections described in the following table.

Table 13-5 SSL Policy Report Sections

Section	Description
Title Page	Identifies the name of the policy report, the date and time the policy was last modified, and the name of the user who made that modification.
Table of Contents	Describes the contents of the report.
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.
Default Action	Provides the default action.
Default Logging	Provides the default connection logging settings.
Rules	Provides the rule action and conditions for each rule in the policy, by rule category.
Trusted CA Certificates	Provides the CA certificates that are automatically trusted if detected traffic is encrypted using these certificates or other certificates within the chain of trust.
Undecryptable Actions	Provides the action taken on detected types of traffic that cannot be decrypted.
Referenced Objects	Provides the name and configuration of all individual objects and group objects used in the policy, by type of condition (networks, ports, and so on) where the object is configured.

To view an SSL policy report:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > SSL**.

The SSL 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 SSL 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 SSL 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 SSL 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 SSL Policy Comparison View, page 13-10
- Using the SSL Policy Comparison Report, page 13-11

Using the SSL 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 13-6 SSL 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 SSL Policy Comparison Report, page 13-11 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 SSL Policy Comparison Report

License: Any

An SSL policy comparison report is a record of all differences between two SSL 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 SSL 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 SSL policy comparison report contains the sections described in Generating a Report of Current Traffic Decryption Settings, page 13-9.

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

To compare two SSL policies:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > SSL.**

The SSL Policy 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 SSL policy comparison report.

The SSL 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.