Start Creating SSL Policies

The following topics provide an overview of SSL policy creation, configuration, management, and logging.

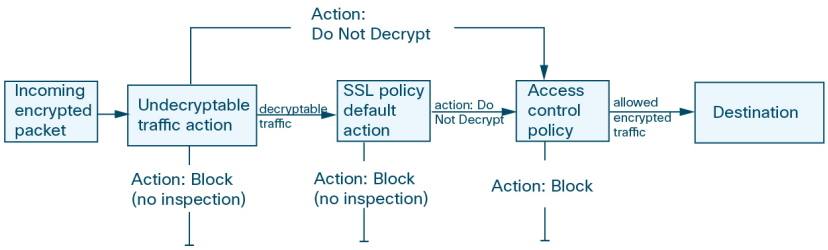
- SSL Policies Overview, on page 1
- SSL Policy Default Actions, on page 2
- Default Handling Options for Undecryptable Traffic, on page 3
- Requirements and Prerequisites for SSL Policies, on page 4
- Manage SSL Policies, on page 4
- Create Basic SSL Policies, on page 5
- Set Default Handling for Undecryptable Traffic, on page 6
- Editing an SSL Policy, on page 7

SSL Policies Overview

An *SSL policy* determines how the system handles encrypted traffic on your network. You can configure one or more SSL policies, associate an SSL policy with an access control policy, then deploy the access control policy to a managed device. When the device detects a TCP handshake, the access control policy first handles and inspects the traffic. If it subsequently identifies a TLS/SSL-encrypted session over the TCP connection, the SSL policy takes over, handling and decrypting the encrypted traffic.

Caution Adding or removing an SSL policy restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See Snort® Restart Traffic Behavior for more information.

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



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.

Note Because TLS and SSL are often used interchangeably, we use the expression *TLS/SSL* to indicate that either protocol is being discussed. The SSL protocol has been deprecated by the IETF in favor of the more secure TLS protocol, so you can usually interpret *TLS/SSL* as referring to TLS only.

The exception is SSL policies. Because the FMC configuration option is **Policies** > **Access Control** > **SSL**, we use the term *SSL policies* although these policies are used to define rules for TLS and SSL traffic.

For more information about SSL and TLS protocols, see a resource such as SSL vs. TLS - What's the Difference?.

Related Topics

TLS/SSL Rule Conditions

SSL Policy Default Actions

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 deploy an SSL policy that does not contain any TLS/SSL rules, the default action determines how all decryptable traffic on your network is handled. Note that the system does not perform any kind of inspection on encrypted traffic blocked by the default action.

Table 1: SSL Policy Default Actions

Default Action	Effect on Encrypted Traffic
Block	Block the TLS/SSL session without further inspection.
Block with reset	Block the TLS/SSL session without further inspection and reset the TCP connection. Choose this option if traffic uses a connectionless protocol like UDP. In that case, the connectionless protocol tries to reestablish the connection until it is reset. This action also displays a connection reset error in the browser so the user is informed that the connection is blocked.
Do not decrypt	Inspect the encrypted traffic with access control.

Related Topics

Create Basic SSL Policies, on page 5

Default Handling Options for Undecryptable Traffic

Table 2: Undecryptable Traffic Types

Type	Description	Default Action	Available Action
Compressed Session	The TLS/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 ClientHello 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 TLS/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 TLS/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.

Note that if your browser uses certificate pinning to verify a server certificate, you cannot decrypt this traffic by re-signing the server certificate. For more information, see TLS/SSL Rule Guidelines and Limitations.

Related Topics

Set Default Handling for Undecryptable Traffic, on page 6

Requirements and Prerequisites for SSL Policies

Model Support

Any except NGIPSv.

Supported Domains

Any

User Roles

- Admin
- Access Admin
- Network Admin

Manage SSL Policies

In the SSL policy editor, you can:

- Configure your policy.
- Add, edit, delete, enable, disable, and organize TLS/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.

In a multidomain deployment, the system displays policies created in the current domain, which you can edit. It also displays policies created in ancestor domains, which you cannot edit. To view and edit policies created in a lower domain, switch to that domain.

Step 1 Choose **Policies** > **Access Control** > **SSL**.

Step 2 Manage SSL policies:

- Associate—To associate an SSL policy with an access control policy, see Associating Other Policies with Access Control.

- Compare—Click **Compare Policies**; see Comparing Policies.
- Copy—Click **Copy** ( ).
- Create—Click **New Policy**; see Create Basic SSL Policies, on page 5.
- Delete—Click **Delete** ( ). If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
- Deploy—Click **Deploy**; see Deploy Configuration Changes.
- Edit—Click **Edit** ( ); see Editing an SSL Policy, on page 7. If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
- Import/Export—See About Configuration Import/Export.
- Report—Click **Report** ( ); see Generating Current Policy Reports.

Create Basic SSL Policies

To configure an SSL policy, you must give the policy a unique name and specify a default action.

Step 1 Choose **Policies** > **Access Control** > **SSL**.

Step 2 Click **New Policy**.

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

Step 4 Specify the **Default Action**; see SSL Policy Default Actions, on page 2.

Step 5 Configure logging options for the default action as described in Logging Connections with a Policy Default Action.

Step 6 Click **Save**.

What To Do Next

- Configure rules to add to your SSL policy; see Creating and Modifying TLS/SSL Rules.
- Set the default handling for undecryptable traffic; see Set Default Handling for Undecryptable Traffic, on page 6.
- Configure logging options for default handling of undecryptable traffic; see Logging Connections with a Policy Default Action.
- Associate the SSL policy with an access control policy as described in Associating Other Policies with Access Control.
- Deploy configuration changes; see Deploy Configuration Changes.

Set Default Handling for Undecryptable Traffic

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 deploy an SSL policy that contains no TLS/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. This option is preferrable for connectionless protocols like UDP, which keep trying to connect until the connection is blocked.
- Inspect the encrypted traffic with access control.
- Inherit the default action from the SSL policy.

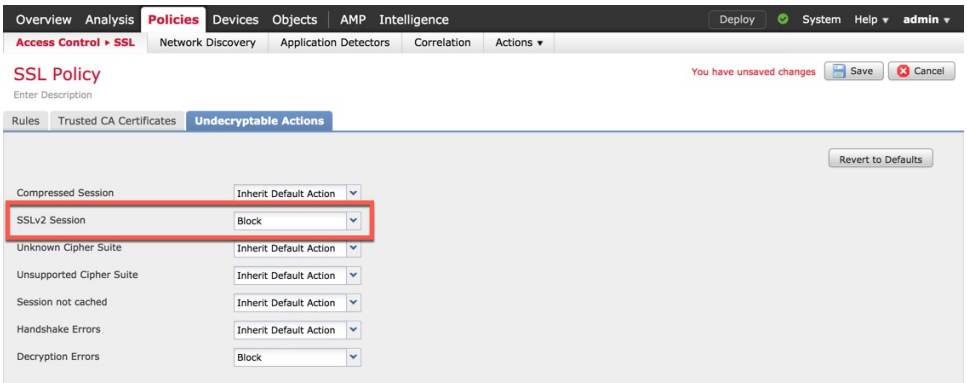
Step 1 In the SSL policy editor, click **Undecryptable Actions**.

Step 2 For each field, choose either the SSL policy's default action or another action you want to take on the type of undecryptable traffic. See Default Handling Options for Undecryptable Traffic, on page 3 and SSL Policy Default Actions, on page 2 for more information.

Step 3 Click **Save** to save the policy.

Example

For example, to block all SSLv2 traffic, set the options as follows:



What to do next

- Configure default logging for connections handled by the undecryptable traffic actions; see Logging Connections with a Policy Default Action.
- Deploy configuration changes; see Deploy Configuration Changes.

Editing an SSL Policy

Only one person should edit a policy at a time, using a single browser window. If multiple users save the same policy, the last saved changes are retained. For your convenience, the system displays information on who (if anyone) is currently editing each policy. To protect the privacy of your session, a warning appears after 30 minutes of inactivity on the policy editor. After 60 minutes, the system discards your changes.

Step 1 Choose **Policies** > **Access Control** > **SSL**.

Step 2 Click **Edit** ( ) next to the SSL policy you want to configure.

If **View** ( ) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 Configure the SSL policy:

- Describe—If you want to update your SSL policy description, click the **Description** field and enter the new description.
- Log—If you want to log connections for undecryptable traffic handling and traffic that does not match SSL rules, see Logging Connections with a Policy Default Action.
- Rename—If you want to rename your SSL policy, click the **Name** field and enter the new name.
- Set the default action—If you want to configure how your SSL policy handles traffic that does not match SSL rules, see SSL Policy Default Actions, on page 2.
- Set the default action for undecryptable traffic—If you want to configure how your SSL policy handles undecryptable traffic, see Set Default Handling for Undecryptable Traffic, on page 6.
- Trust—If you want to add trusted CA certificates to your SSL policy, see Trusting External Certificate Authorities.

Step 4 Edit the rules in your SSL policy:

- Add—If you want to add a rule, click **Add Rule**.
- Copy—If you want to copy a rule, right-click a selected rule and choose **Copy**.
- Cut—If you want to cut a rule, right-click a selected rule and choose **Cut**.
- Delete—To delete a rule, click **Delete** ( ) next to the rule, then click **OK**.
- Disable—To disable an enabled rule, right-click a selected rule, choose **State**, then choose **Disable**.
- Display—To display the configuration page for a specific rule attribute, click the name or value 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 Network Conditions.
- Edit—To edit a rule, click **Edit** ( ) next to the rule.
- Enable—To enable a disabled rule, right-click a selected rule, choose **State**, then choose **Enable**. Disabled rules are dimmed and marked `(disabled)` beneath the rule name.
- Paste—To paste a cut or copied rule, right-click a selected rule and choose **Paste Above** or **Paste Below**.

Step 5 Save or discard your configuration:

- To save your changes and continue editing, click **Save**.
- To discard your changes, click **Cancel** and, if prompted, click **OK**.

What to do next

- If the SSL policy is not already associated with an access control policy, associate it as described in Associating Other Policies with Access Control.
- Deploy configuration changes; see Deploy Configuration Changes.

Related Topics

Creating and Modifying TLS/SSL Rules