

SSL Policies

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

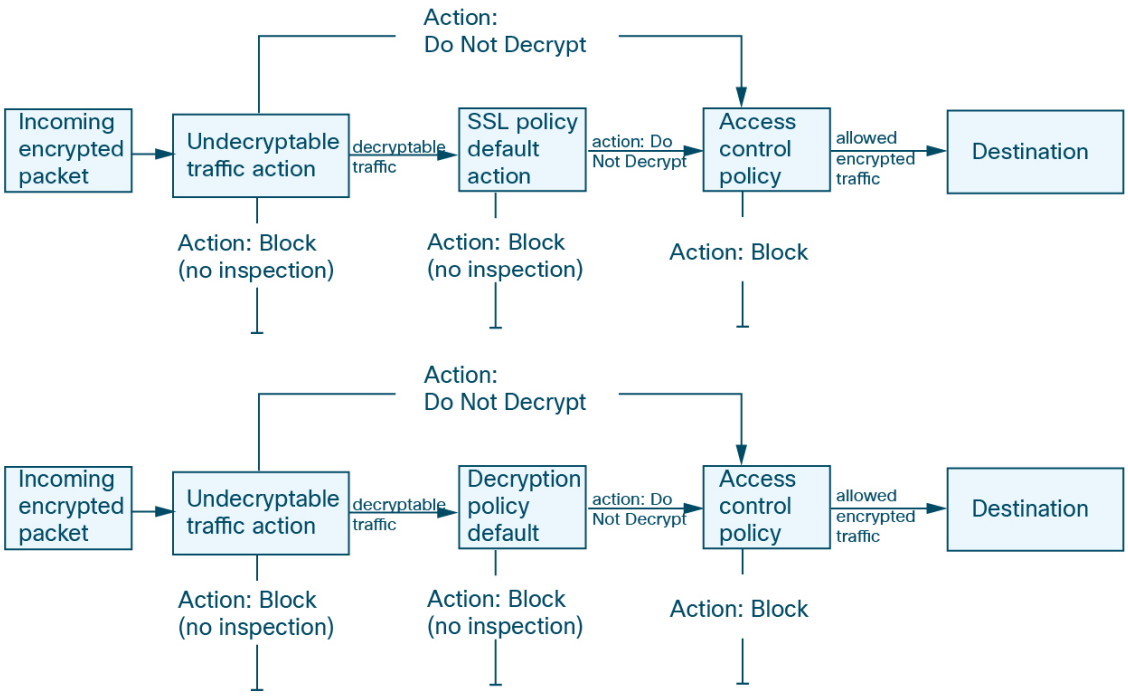
- SSL Policies Overview, on page 1
- SSL Policy Default Actions, on page 2
- Default Handling Options for Undecryptable Traffic, on page 3
- SSL Policy Advanced Options, on page 4
- Requirements and Prerequisites for SSL Policies, on page 5
- Create Basic SSL Policies, on page 5
- Set Default Handling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

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 *Snort 2 only*. 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 TLS/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 heading** > **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

Type	Description	Default Action	Available 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

SSL Policy Advanced Options

An SSL policy 's **Advanced Settings** page has global settings that are applied to all managed devices that are configured for Snort 3 to which the policy is applied.

An SSL policy advanced settings are all ignored on any managed device that runs:

- A version earlier than 7.1
- Snort 2

Block flows requesting ESNI

Encrypted Server Name Indication (ESNI (link to draft proposal)) is a way for a client to tell a TLS 1.3 server what the client is requesting. Because the SNI is encrypted, you can optionally block these connections because the system cannot determine what the server is.

Disable HTTP/3 advertisement

This option strips HTTP/3 (RFC 9114) from the ClientHello in TCP connections. HTTP/3 is part of the QUIC transport protocol, not the TCP transport protocol. Blocking clients from advertising HTTP/3 provides protection against attacks and evasion attempts potentially burried within QUIC connections.

Propagate untrusted server certificates to clients

This applies only to traffic matching a **Decrypt - Resign** rule action.

Enable this option to substitute the certificate authority (CA) on the managed device for the server's certificate in cases where the server certificate is untrusted. An *untrusted* server certificate is one that is not listed as a trusted CA in the Firepower Management Center. (**Objects** > **Object Management** > **PKI** > **Trusted CAs**).

Requirements and Prerequisites for SSL Policies

Supported Domains

Any

User Roles

- Admin
- Access Admin
- Network Admin

Create Basic SSL Policies

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

Procedure

Step 1 Log in to the FMC if you haven't already done so.

Step 2 Click **Policies** > **Access Control heading** > **SSL**.

Step 3 Click **New Policy**.

Step 4 Give the policy a unique **Name** and, optionally, a **Description**.

Step 5 Specify the **Default Action**; see SSL Policy Default Actions, on page 2.

Step 6 Configure logging options for the default actionas described in *Logging Connections with a Policy Default Action* in the Firepower Management Center Administration Guide .

Step 7 Click **Save**.

What To Do Next

- 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* in the Firepower Management Center Administration Guide.
- Set advanced policy properties: SSL Policy Advanced Options, on page 4.

- 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.

Procedure

Step 1 Log in to Firepower Management Center if you haven't already done so.

Step 2 Click **Policies** > **Access Control heading** > **SSL**.

Step 3 Click **Edit** (✎) next to the name of the SSL policy.

Step 4 In the SSL policy editor, click **Undecryptable Actions**.

Step 5 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 6 Click **Save** to save the policy.

What to do next

- Configure default logging for connections handled by the undecryptable traffic actions; see *Logging Connections with a Policy Default Action* in the Firepower Management Center Administration Guide.
- Deploy configuration changes; see Deploy Configuration Changes.

Manage SSL Policies

In the SSL policy editor, you can:

- 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.
- Set advanced options.

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.

Procedure

Step 1 Log in to the FMC if you haven't already done so.

Step 2 Click **Policies** > **Access Control heading** > **SSL**.

Step 3 Manage SSL policies:

- 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.
- Report—Click **Report** (); see Generate Current Policy Reports.
- Edit—Click **Edit** (). If **View** () appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
- To add trusted CA certificates to your SSL policy, see Trusting External Certificate Authorities.
- To configure how your SSL policy handles undecryptable traffic, see Set Default Handling for Undecryptable Traffic, on page 6.
- SSL policy advanced settings—See SSL Policy Advanced Options, on page 4.
- Import/Export—See the section on importing and exporting the configuration in the Secure Firewall Management Center and Threat Defense Management Network Administration.
- To log connections for undecryptable traffic handling and traffic that does not match SSL rules, see *Logging Connections with a Policy Default Action* in the Firepower Management Center Administration Guide .
- Deploy—Choose **Deploy** > **Deployment**; see Deploy Configuration Changes.