

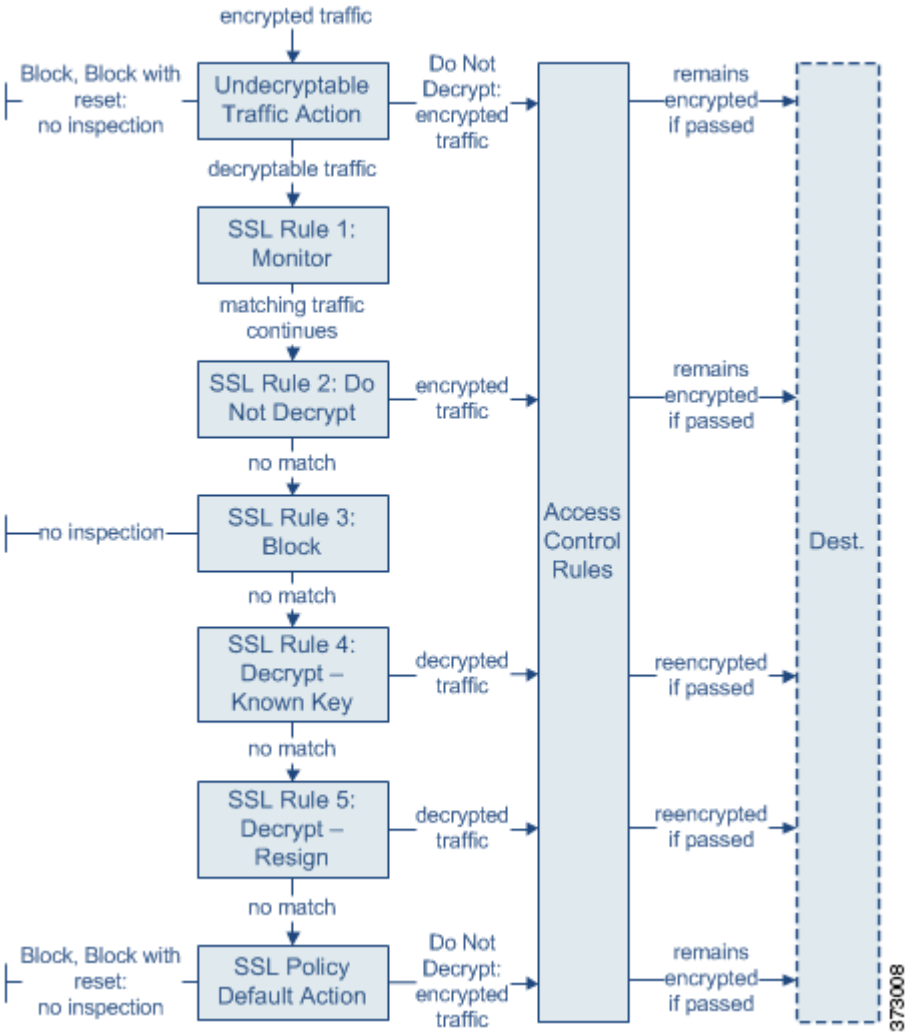
Getting Started with SSL Rules

Within an SSL policy, *SSL rules* provide a granular method of handling encrypted traffic, whether blocking the traffic without further inspection, not decrypting the traffic and inspecting it with access control, or decrypting the traffic for access control analysis.

The ASA FirePOWER module matches traffic to SSL rules in the order you specify. In most cases, the module handles encrypted traffic according to the *first* SSL rule where *all* the rule's conditions match the traffic. Conditions can be simple or complex; you can control traffic by security zone, network or geographical location, port, application, requested URL, user, certificate, certificate distinguished name, certificate status, cipher suite, or encryption protocol version.

Each rule also has an *action*, which determines whether you monitor, block, or inspect matching traffic with access control, optionally after decrypting matching traffic. Note that the module does **not** further inspect encrypted traffic it blocks. It does inspect encrypted and undecryptable traffic with access control. However, some access control rule conditions require unencrypted traffic, so encrypted traffic may match fewer rules. Also, by default, the module disables intrusion and file inspection of encrypted payloads.

The following scenario summarizes the ways that SSL rules handle traffic in an inline deployment.



In this scenario, traffic is evaluated as follows:

- **Undecryptable Traffic Action** evaluates encrypted traffic first. For traffic the module cannot decrypt, the module either blocks it without further inspection or passes it for access control inspection. Encrypted traffic that does not match continues to the next rule.
- **SSL Rule 1: Monitor** evaluates encrypted traffic next. Monitor rules track and log encrypted traffic but do not affect traffic flow. The module continues to match traffic against additional rules to determine whether to permit or deny it.
- **SSL Rule 2: Do Not Decrypt** evaluates encrypted traffic third. Matching traffic is not decrypted; the module inspects this traffic with access control, but not file or intrusion inspection. Traffic that does not match continues to the next rule.
- **SSL Rule 3: Block** evaluates encrypted traffic fourth. Matching traffic is blocked without further inspection. Traffic that does not match continues to the next rule.
- **SSL Rule 4: Decrypt - Known Key** evaluates encrypted traffic fifth. Matching traffic incoming to your network is decrypted using a private key you upload. The decrypted traffic is then evaluated against access control rules. Access control rules handle decrypted and unencrypted traffic

identically. The module can block traffic as a result of this additional inspection. All remaining traffic is reencrypted before being allowed to the destination. Traffic that does not match the SSL rule continues to the next rule.

- **SSL Rule 5: Decrypt - Resign** is the final rule. If traffic matches this rule, the module re-signs the server certificate with an uploaded CA certificate, then acts as a man-in-the-middle to decrypt traffic. The decrypted traffic is then evaluated against access control rules. Access control rules treat decrypted and unencrypted traffic identically. The module can block traffic as a result of this additional inspection. All remaining traffic is reencrypted before being allowed to the destination. Traffic that does not match the SSL rule continues to the next rule.
- **SSL Policy Default Action** handles all traffic that does not match any of the SSL rules. The default action either blocks encrypted traffic without further inspection or does not decrypt it, passing it for access control inspection.

For more information, see the following sections:

- Configuring Supporting Inspection Information, page 16-3
- Understanding and Creating SSL Rules, page 16-4
- Managing SSL Rules in a Policy, page 16-12

Configuring Supporting Inspection Information

License: Any

You must create reusable public key infrastructure (PKI) objects to control encrypted traffic based on encrypted session characteristics and decrypt encrypted traffic. You can add this information on the fly when uploading trusted certificate authority (CA) certificates to the SSL policy and creating SSL rule conditions, creating the associated object in the process. However, configuring these objects ahead of time reduces the chance of improper object creation.

Decrypting Encrypted Traffic with Certificates and Paired Keys

The ASA FirePOWER module can decrypt incoming encrypted traffic if you configure an internal certificate object by uploading the server certificate and private key used to encrypt the session. If you reference that object in an SSL rule with an action of **Decrypt - Known Key** and traffic matches that rule, the module uses the uploaded private key to decrypt the session.

The module can also decrypt outgoing traffic if you configure an internal CA object by uploading a CA certificate and private key. If you reference that object in an SSL rule with an action of **Decrypt - Resign** and traffic matches that rule, the module re-signs the server certificate passed to the client browser, then acts as a man-in-the-middle to decrypt the session.

See the following for more information:

- Working with Internal Certificate Objects, page 3-41
- Working with Internal Certificate Authority Objects, page 3-35

Controlling Traffic Based on Encrypted Session Characteristics

The ASA FirePOWER module can control encrypted traffic based on the cipher suite or server certificate used to negotiate the session. You can configure one of several different reusable objects and reference the object in an SSL rule condition to match traffic. The following table describes the different types of reusable objects you can configure:

If you configure...	You can control encrypted traffic based on whether...
a cipher suite list containing one or more cipher suites	the cipher suite used to negotiate the encrypted session matches a cipher suite in the cipher suite list
a trusted CA object by uploading a CA certificate your organization trusts	the trusted CA trusts the server certificate used to encrypt the session, whether: • the CA issued the certificate directly • the CA issued a certificate to an intermediate CA that issued the server certificate
an external certificate object by uploading a server certificate	the server certificate used to encrypt the session matches the uploaded server certificate
a distinguished name object containing a certificate subject or issuer distinguished name	the subject or issuer common name, country, organization, or organizational unit on the certificate used to encrypt the session matches the configured distinguished name

See the following for more information:

- Working with Geolocation Objects, page 3-42
- Working with Trusted Certificate Authority Objects, page 3-39
- Working with External Certificate Objects, page 3-41
- Working with Distinguished Name Objects, page 3-33

Understanding and Creating SSL Rules

License: Any

Within an SSL policy, SSL rules provide a granular method of handling network traffic. In addition to its unique name, each SSL rule has the following basic components.

State

By default, rules are enabled. If you disable a rule, the module does not use it to evaluate network traffic, and stops generating warnings and errors for that rule.

Position

Rules in an SSL policy are numbered, starting at 1. The module 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.

Conditions

Conditions specify the specific traffic the rule handles. Conditions can match traffic by security zone, network or geographical location, port, application, requested URL, user, certificate, certificate subject or issuer, certificate status, cipher suite, or encryption protocol version. Conditions can be simple or complex; their use can depends on device licenses.

Action

A rule's action determines how the module handles matching traffic. You can monitor, trust, block, or decrypt matching traffic. Decrypted traffic is subject to further inspection. Note that the module does **not** perform inspection on blocked or trusted encrypted traffic.

Logging

A rule's logging settings govern the records the module keeps of the traffic it handles. You can keep a record of traffic that matches a rule. You can log a connection when the module blocks an encrypted session or allows it to pass uninspected, according to the settings in an SSL policy. You can also force the module to log connections that it decrypts for further evaluation by access control rules, regardless of how the module later handles or inspects the traffic. You can log connections to the module log (syslog) or to an SNMP trap server.

Tip Properly creating and ordering SSL rules is a complex task, but one that is essential to building an effective deployment. If you do not plan your policy carefully, rules can preempt other rules, require additional licenses, or contain invalid configurations. To help ensure that the module handles traffic as you expect, the SSL policy interface has a robust warning and error feedback system for rules. For more information, see Troubleshooting SSL Rules, page 16-15.

To create or modify an SSL rule:

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 where you want to add a rule.

The SSL policy editor appears, focused on the Rules tab.

Step 3 You have the following options:

- To add a new rule, click **Add Rule**.
- To edit an existing rule, click the edit icon ( ) next to the rule you want to edit.

The SSL rule editor appears.

Step 4 Type a **Name** for the rule.

Each rule must have a unique name. You can use up to thirty printable characters, including spaces and special characters, with the exception of the colon (:).

Step 5 Configure the rule components, as summarized above. You can configure the following, or accept the defaults:

- Specify whether the rule is **Enabled**.
- Specify the rule position; see Specifying an SSL Rule's Order of Evaluation, page 16-6.
- Select a rule **Action**; see Using Rule Actions to Determine Encrypted Traffic Handling and Inspection, page 16-8.
- Configure the rule's conditions; see Using Conditions to Specify the Encrypted Traffic a Rule Handles, page 16-6.
- Specify **Logging** options; see Logging Decryptable Connections with SSL Rules, page 36-14.

Step 6 Click **Save** to save the rule.

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

Specifying an SSL Rule's Order of Evaluation

License: Any

When you first create an SSL rule, you specify its position using the **Insert** drop-down list in the rule editor. SSL rules in an SSL policy are numbered, starting at 1. The ASA FirePOWER module matches traffic to SSL rules in top-down order by ascending rule number.

In most cases, the module handles network traffic according to the *first* SSL rule where *all* the rule's conditions match the traffic. Except in the case of Monitor rules (which log traffic but do not affect traffic flow), the module does **not** continue to evaluate traffic against additional, lower-priority rules after that traffic matches a rule.

Tip Proper SSL 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. For more information, see Ordering SSL Rules to Improve Performance and Avoid Preemption, page 16-16.

In addition to ordering rules by number, you can group rules by category. By default the module provides three categories: Administrator, Standard, and Root. You can add custom categories, but you cannot delete the ASA FirePOWER module-provided categories or change their order. For information on changing the position or category of an existing rule, see Changing an SSL Rule's Position or Category, page 16-13.

To add a rule to a category while editing or creating a rule:

Step 1 In the SSL rule editor, from the **Insert** drop-down list, select **Into Category**, then select the category you want to use.

When you save the rule, it is placed last in that category.

To position a rule by number while editing or creating a rule:

Step 1 In the SSL rule editor, from the **Insert** drop-down list, select **above rule** or **below rule**, then type the appropriate rule number.

When you save the rule, it is placed where you specified.

Using Conditions to Specify the Encrypted Traffic a Rule Handles

License: feature dependent

An SSL rule's conditions identify the type of encrypted traffic that rule handles. Conditions can be simple or complex, and you can specify more than one condition type per rule. Only if traffic meets all the conditions in a rule does the rule apply to the traffic.

If you do not configure a particular condition for a rule, the module does not match traffic based on that criterion. For example, a rule with a certificate condition but no version condition evaluates traffic based on the server certificate used to negotiate the session, regardless of the session SSL or TLS version.

When you add or edit an SSL rule, use the tabs on the left side of the lower portion of the rule editor to add and edit rule conditions. The conditions you can add to an SSL rule are described in the following table.

Table 16-1 SSL Rule Condition Types

This Condition...	Matches Encrypted Traffic...	Details
Zones	entering or leaving a device via an interface in a specific security zone	A security zone is a logical grouping of one or more interfaces according to your deployment and security policies. To build a zone condition, see Controlling Encrypted Traffic by Network Zone, page 17-2.
Networks	by its source or destination IP address, country, or continent	You can explicitly specify IP addresses. The geolocation feature also allows you to control traffic based on its source or destination country or continent. To build a network condition, see Controlling Encrypted Traffic by Network or Geographical Location, page 17-3.
Ports	by its source or destination port	You can control encrypted traffic based on the TCP port. To build a port condition, see Controlling Encrypted Traffic by Port, page 17-5.
Users	by the user involved in the session	You can control encrypted traffic based on the LDAP user logged into a host involved in an encrypted, monitored session. You can control traffic based on individual users or groups retrieved from a Microsoft Active Directory server. To build a user condition, see Controlling Encrypted Traffic Based on User, page 17-6.
Applications	by the application detected in a session	You can control access to individual applications in encrypted sessions, or filter access according to basic characteristics: type, risk, business relevance, and categories. To build an application condition, see Controlling Encrypted Traffic Based on Application, page 17-8.
Categories	by the URL requested in the session, based on the certificate subject distinguished name	You can limit the websites that users on your network can access based on the URL's general classification and risk level. To build a URL condition, see Controlling Encrypted Traffic by URL Category and Reputation, page 17-13.
Distinguished Names	by the subject or issuer distinguished name of the server certificate used to negotiate the encrypted session	You can control encrypted traffic based on the CA that issued a server certificate, or the server certificate holder. To build a distinguished name condition, see Controlling Encrypted Traffic by Certificate Distinguished Name, page 17-17.
Certificates	by the server certificate used to negotiate the encrypted session	You can control encrypted traffic based on the server certificate passed to the user's browser in order to negotiate the encrypted session. To build a certificate condition, see Controlling Encrypted Traffic by Certificate Status, page 17-20.

Table 16-1 SSL Rule Condition Types (continued)

This Condition...	Matches Encrypted Traffic...	Details
Certificate Status	by properties of the server certificate used to negotiate the encrypted session	You can control encrypted traffic based on a server certificate's status. To build a certificate status condition, see Controlling Encrypted Traffic by Certificate Status, page 17-20.
Cipher Suites	by the cipher suite used to negotiate the encrypted session	You can control encrypted traffic based on the cipher suite selected by the server to negotiate the encrypted session. To build a cipher suite condition, see Controlling Encrypted Traffic by Cipher Suite, page 17-25.
Versions	by the version of SSL or TLS used to encrypt the session	You can control encrypted traffic based on the version of SSL or TLS used to encrypt the session. To build a version condition, see Controlling Traffic by Encryption Protocol Version, page 17-26.

Note that while you can control and inspect encrypted traffic, controlling traffic using detected application, URL category, or user requires additional licenses. Also, overly complex rules can consume excessive resources and in some cases prevent you from applying the policy. For more information, see Troubleshooting SSL Rules, page 16-15.

Using Rule Actions to Determine Encrypted Traffic Handling and Inspection

License: Any

Every SSL rule has an associated action that determines the following for matching encrypted traffic:

- handling — foremost, the rule action governs whether the ASA FirePOWER module will monitor, trust, block, or decrypt encrypted traffic that matches the rule's conditions
- logging — the rule action determines when and how you can log details about matching encrypted traffic.

Your SSL inspection configuration handles, inspects, and logs decrypted traffic:

- The SSL policy's undecryptable actions handle traffic that the ASA FirePOWER module cannot decrypt; see Setting Default Handling for Undecryptable Traffic, page 15-4.
- The policy's default action handles traffic that does not meet the condition of any non-Monitor SSL rule; see Setting Default Handling and Inspection for Encrypted Traffic, page 15-3.

You can log a connection event when the ASA FirePOWER module blocks or trusts an encrypted session. You can also force the module to log connections that it decrypts for further evaluation by access control rules, regardless of how the module later handles or inspects the traffic. Connection logs for encrypted sessions contain details about the encryption, such as the certificate used to encrypt that session. You can log only end-of-connection events, however:

- for blocked connections (Block, Block with reset), the module immediately ends the sessions and generates an event
- for trusted connections (Do not decrypt), the module generates an event when the session ends

For detailed information on rule actions and how they affect handling and logging, see the following sections:

- Monitor Action: Postponing Action and Ensuring Logging, page 16-9

- Do Not Decrypt Action: Passing Encrypted Traffic Without Inspection, page 16-9
- Blocking Actions: Blocking Encrypted Traffic Without Inspection, page 16-9
- Decrypt Actions: Decrypting Traffic for Further Inspection, page 16-10
- Managing SSL Rules in a Policy, page 16-12

Monitor Action: Postponing Action and Ensuring Logging

License: Any

The **Monitor** action does not affect encrypted traffic flow; matching traffic is neither immediately permitted nor denied. Rather, traffic is matched against additional rules, if present, to determine whether to trust, block, or decrypt it. The first non-Monitor rule matched determines traffic flow and any further inspection. If there are no additional matching rules, the ASA FirePOWER module uses the default action.

Because the primary purpose of Monitor rules is to track network traffic, the module automatically logs end-of connection events for monitored traffic. That is, the module always logs the end of the connection, regardless of the logging configuration of the rule or default action that later handles the connection. In other words, if a packet matches a Monitor rule, the connection is always logged, even if the packet matches no other rules and you do not enable logging on the default action.

Do Not Decrypt Action: Passing Encrypted Traffic Without Inspection

License: Any

The **Do not decrypt** action passes encrypted traffic for evaluation by the access control policy's rules and default action. Because some access control rule conditions require unencrypted traffic, this traffic may match fewer rules. The module cannot perform deep inspection on encrypted traffic, such as intrusion or file inspection.

Blocking Actions: Blocking Encrypted Traffic Without Inspection

License: Any

The **Block** and **Block with reset** actions are analogous to the access control rule actions Block and Block with reset. These actions prevent the client and server from establishing the SSL-encrypted session and passing encrypted traffic. Block with reset rules also reset the connection.

Note that the ASA FirePOWER module does not display the configured response page for blocked encrypted traffic. Instead, users requesting prohibited URLs have their connection either reset or time out. See Displaying a Custom Web Page for Blocked URLs, page 8-14 for more information.

Tip Note that you cannot use the Block or Block with reset action in a passive or inline (tap mode) deployment, as the device does not directly inspect the traffic. If you create a rule with the Block or Block with reset action that contains passive or inline (tap mode) interfaces within a security zone condition, the policy editor displays a warning icon ( ) next to the rule.

Decrypt Actions: Decrypting Traffic for Further Inspection

License: Any

The **Decrypt - Known Key** and **Decrypt - Resign** actions decrypt encrypted traffic. The ASA FirePOWER module inspects decrypted traffic with access control. Access control rules handle decrypted and unencrypted traffic identically — you can detect and block intrusions, prohibited files, and malware. The module reencrypts allowed traffic before passing it to its destination.

When you configure the **Decrypt - Known Key** action, you can associate one or more server certificates and paired private keys with the action. If traffic matches the rule, and the certificate used to encrypt the traffic matches the certificate associated with the action, the module uses the appropriate private key to obtain the session encryption and decryption keys. Because you must have access to the private key, this action is best suited to decrypt traffic incoming to servers your organization controls.

Similarly, you can associate one Certificate Authority certificate and private key with the **Decrypt - Resign** action. If traffic matches this rule, the module re-signs the server certificate with the CA certificate, then acts as a man-in-the-middle. It creates two SSL sessions, one between client and device, one between device and server. Each session contains different cryptographic session details, and allows the module to decrypt and reencrypt traffic. This action is more suited for outgoing traffic, as you replace the certificate's private key with one you control to obtain the session keys.

Re-signing a server certificate involves either replacing the certificate's public key with a CA certificate public key, or replacing the entire certificate. Normally, if you replace an entire server certificate, the client browser warns the certificate is not signed by a trusted authority when establishing the SSL connection. However, if your client's browser trusts the CA in the policy, the browser does not warn that the certificate is not trusted. If the original server certificate is self-signed, the ASA FirePOWER module replaces the entire certificate, and trusts the re-signing CA, but the user's browser does not warn that the certificate is self-signed. In this case, replacing only the server certificate public key causes the client browser does warn that the certficate is self-signed.

If you configure a rule with the **Decrypt - Resign** action, the rule matches traffic based on the referenced internal CA certificate's signature algorithm type, in addition to any configured rule conditions. Because you associate one CA certificate with a **Decrypt - Resign** action, you cannot create an SSL rule that decrypts multiple types of outgoing traffic encrypted with different signature algorithms. In addition, any external certificate objects and cipher suites you add to the rule must match the associated CA certificate encryption algorithm type.

For example, outgoing traffic encrypted with an elliptic curve (EC) algorithm matches a **Decrypt - Resign** rule only if the action references an EC-based CA certificate; you must add EC-based external certificates and cipher suites to the rule if you want to create certificate and cipher suite rule conditions. Similarly, a **Decrypt - Resign** rule that references an RSA-based CA certificate matches only outgoing traffic encrypted with an RSA algorithm; outgoing traffic encrypted with an EC algorithm does not match the rule, even if all other configured rule conditions match.

Note the following:

- You cannot use the **Decrypt - Known Key** action in a passive deployment if the cipher suite used to establish the SSL connection applies either the Diffie-Hellman ephemeral (DHE) or the elliptic curve Diffie-Hellman ephemeral (ECDHE) key exchange algorithm. If your SSL policy targets passive or inline (tap mode) interfaces, and contains a **Decrypt - Known Key** rule with a cipher suite condition containing either a DHE or an ECDHE cipher suite, the ASA FirePOWER module displays an information icon ( ) next to the rule. If you later add a zone condition to the SSL rule that contains passive or inline (tap mode) interfaces, the module displays a warning icon ( ).
- You cannot use the **Decrypt - Resign** action in a passive or inline (tap mode) deployment, as the device does not directly inspect traffic. If you create a rule with the **Decrypt - Resign** action that contains passive or inline (tap mode) interfaces within a security zone, the policy editor displays a warning

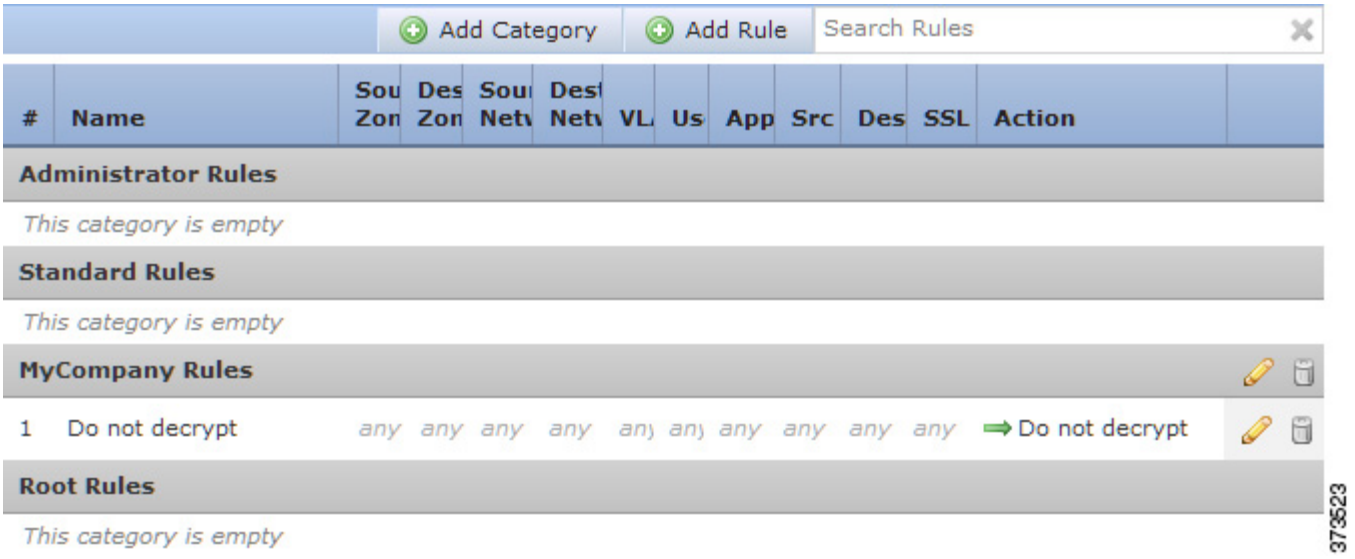
icon ( ) next to the rule. If your SSL policy targets passive or inline (tap mode) interfaces, and contains a **Decrypt - Resign** rule, the module displays an information icon ( ) next to the rule. If you later add a zone condition to the SSL rule that contains passive or inline (tap mode) interfaces, the module displays a warning icon ( ). If you apply an SSL policy that contains a Decrypt - Resign rule to a device with passive or inline (tap mode) interfaces, any SSL sessions that match the rule fail.

- If the client does not trust the CA used to re-sign the server certificate, it warns the user that the certificate should not be trusted. To prevent this, import the CA certificate into the client trusted CA store. Alternatively, if your organization has a private PKI, you can issue an intermediate CA certificate signed by the root CA which is automatically trusted by all clients in the organization, then upload that CA certificate to the device.
- You can add an anonymous cipher suite to the **Cipher Suite** condition in an SSL rule, but keep in mind:
  - The system automatically strips anonymous cipher suites during ClientHello processing. For the system to use the rule, you must also configure your SSL rules in an order that prevents ClientHello processing. For more information, see Ordering SSL Rules to Improve Performance and Avoid Preemption, page 16-16.
  - You cannot use the **Decrypt - Resign** or **Decrypt - Known Key** action in the rule, because the system cannot decrypt traffic encrypted with an anonymous cipher suite.
- The ASA FirePOWER module 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 module handles this traffic. See Setting Default Handling for Undecryptable Traffic, page 15-4 for more information.
- You cannot match on **Distinguished Name** or **Certificate** conditions when creating an SSL rule with a **Decrypt - Known Key** action. The assumption is that if this rule matches traffic, the certificate, subject DN, and issuer DN already match the certificate associated with the rule. For more information, see Using Rule Actions to Determine Encrypted Traffic Handling and Inspection, page 16-8.
- If you create an internal CA object and choose to generate a certificate signing request (CSR), you cannot use this CA for a **Decrypt - Resign** action until you upload the signed certificate to the object. For more information, see Obtaining and Uploading a New Signed Certificate, page 3-37.
- If you configure a rule with the **Decrypt - Resign** action, and mismatch signature algorithm type for one or more external certificate objects or cipher suites, the policy editor displays an information icon ( ) next to the rule. If you mismatch signature algorithm type for all external certificate objects, or all cipher suites, the policy displays a warning icon ( ) next to the rule, and you cannot apply the access control policy associated with the SSL policy. For more information, see Controlling Encrypted Traffic by Certificate, page 17-19 and Controlling Encrypted Traffic by Cipher Suite, page 17-25.
- If decrypted traffic matches an access control rule with an action of **Interactive Block** or **Interactive Block with reset**, the ASA FirePOWER module blocks the matching connection without interaction and the module does **not** display a response page.
- If you enable the **Normalize Excess Payload** option in the inline normalization preprocessor, when the preprocessor normalizes decrypted traffic, it may drop a packet and replace it with a trimmed packet. This does not end the SSL session. If the traffic is allowed, the trimmed packet is encrypted as part of the SSL session. For more information on this option, see Normalizing Inline Traffic, page 24-6.
- If your browser uses certificate pinning to verify a server certificate, you cannot decrypt this traffic by re-signing the server certificate. 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.

Managing SSL Rules in a Policy

License: Any

The Rules tab of the SSL policy editor, shown in the following graphic, allows you to add, edit, search, move, enable, disable, delete, and otherwise manage SSL rules within your policy.



For each rule, the policy editor displays its name, a summary of its conditions, and the rule action. Icons represent warnings, errors, and other important information. Disabled rules are grayed out and marked `(disabled)` beneath the rule name. See Troubleshooting SSL Rules, page 16-15 for more information about the icons.

For information on managing SSL rules, see:

- Searching SSL Rules, page 16-12
- Enabling and Disabling SSL Rules, page 16-13
- Changing an SSL Rule's Position or Category, page 16-13

Searching SSL Rules

License: Any

You can search the list of SSL rules for matching values using an alphanumeric string, including spaces and printable, special characters. The search inspects the rule name and any rule condition you have added to the rule. For rule conditions, the search matches any name or value you can add for each condition type (zone, network, application, and so on). This includes individual object names or values, group object names, individual object names or values within a group, and literal values.

You can use complete or partial search strings. The column for matching values is highlighted for each matching rule. For example, if you search on all or part of the string `100Bao`, at a minimum, the Applications column is highlighted for each rule where you have added the 100Bao application. If you also have a rule named `100Bao`, both the Name and Applications columns are highlighted.

You can navigate to each previous or next matching rule. A status message displays the current match and the total number of matches.

Matches may occur on any page of a multi-page rule list. When the first match is not on the first page, the page where the first match occurs is displayed. Selecting the next match when you are at the last match takes you to the first match, and selecting the previous match when you are at the first match takes you to the last match.

To search for rules:

Step 1 In the SSL policy editor for the policy you want to search, click the **Search Rules** prompt, type a search string, then press Enter. You can also use the Tab key or click a blank page area to initiate the search.

Columns for rules with matching values are highlighted, with differentiated highlighting for the indicated (first) match.

Step 2 Find the rules you are interested in:

- To navigate between matching rules, click the next-match (▼) or previous-match (▲) icon.
- To refresh the page and clear the search string and any highlighting, click the clear icon (✖).

Enabling and Disabling SSL Rules

License: Any

When you create an SSL rule, it is enabled by default. If you disable a rule, the ASA FirePOWER module does not use it to evaluate network traffic and stops generating warnings and errors for that rule. When viewing the list of rules in an SSL policy, disabled rules are grayed out, although you can still modify them. Note that you can also enable or disable an SSL rule using the rule editor; see Understanding and Creating SSL Rules, page 16-4.

To change an SSL rule's state:

Step 1 In the SSL policy editor for the policy that contains the rule you want to enable or disable, right-click the rule and choose a rule state:

- To enable an inactive rule, select **State > Enable**.
- To disable an active rule, **State > Disable**.

Step 2 Click **Store ASA FirePOWER Changes**.

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

Changing an SSL Rule's Position or Category

License: Any

To help you organize SSL rules, every SSL policy has three ASA FirePOWER module-provided rule categories: Administrator Rules, Standard Rules, and Root Rules. You cannot move, delete, or rename these categories, although you can create custom categories.

For more information, see:

- Moving an SSL Rule, page 16-14
- Adding a New SSL Rule Category, page 16-14

Moving an SSL Rule

License: Any

Proper SSL rule order reduces the resources required to process network traffic, and prevents rule preemption.

The following procedure explains how to move one or more rules at a time using the SSL policy editor. You can also move individual SSL rules using the rule editor; see Understanding and Creating SSL Rules, page 16-4.

To move a rule:

Step 1 In the SSL policy editor for the policy that contains the rules you want to move, select the rules by clicking in a blank area for each rule. Use the Ctrl and Shift keys to select multiple rules.

The rules you selected are highlighted.

Step 2 Move the rules. You can cut and paste or drag and drop.

To cut and paste rules into a new location, right-click a selected rule and select **Cut**. Then, right-click a blank area for a rule next to where you want to paste the cut rules and select **Paste above** or **Paste below**. Note that you cannot copy and paste SSL rules between two different SSL policies.

Step 3 Click **Store ASA FirePOWER Changes**..

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

Adding a New SSL Rule Category

License: Any

To help you organize SSL rules, every SSL policy has three ASA FirePOWER module-provided rule categories: Administrator Rules, Standard Rules, and Root Rules. You cannot move, delete, or rename these categories, although you can create custom categories between the Standard Rules and Root Rules.

Adding custom categories allows you to further organize your rules without having to create additional policies. You can rename and delete categories that you add. You cannot move these categories, but you can move rules into, within, and out of them.

To add a new category:

Step 1 In the SSL policy editor for the policy where you want to add a rule category, click **Add Category**.

Tip If your policy already contains rules, you can click a blank area in the row for an existing rule to set the position of the new category before you add it. You can also right-click an existing rule and select **Insert new category**.

The Add Category pop-up window appears.

Step 2 Type a unique category **Name**.

You can enter an alphanumeric name, including spaces and special printable characters, with up to 30 characters.

Step 3 You have the following choices:

- To position the new category immediately above an existing category, select **above Category** from the first **Insert** drop-down list, then select the category above which you want to position the rule from the second drop-down list.
- To position the new category rule below an existing rule, select **below rule** from the drop-down list, then enter an existing rule number. This option is valid only when at least one rule exists in the policy.
- To position the rule above an existing rule, select **above rule** from the drop-down list, then, enter an existing rule number. This option is valid only when at least one rule exists in the policy.

Step 4 Click **OK**.

Your category is added. You can click the edit icon ( ) next to a custom category to edit its name, or click the delete icon ( ) to delete the category. Rules in a category you delete are added to the category above.

Step 5 Click **Store ASA FirePOWER Changes** to save the policy.

Troubleshooting SSL Rules

License: Any

Properly creating and ordering SSL rules is a complex task, but one that is essential to building an effective deployment. If you do not plan your policy carefully, rules can preempt other rules, require additional licenses, or contain invalid configurations. To help ensure that the ASA FirePOWER module handles traffic as you expect, the SSL policy interface has a robust warning and error feedback system for rules.

For each rule, icons in the policy editor mark warnings and errors, as described in the following table. Hover your pointer over the icon to read the warning, error, or informational text.

Table 16-2 SSL Error Icons

Icon	Description	Details
	warning	Depending on the issue, you may be able to apply an SSL policy that displays rule or other warnings. In these cases, the misconfigured settings will have no effect. For example, a preempted rule never evaluates traffic. However, if a warning icon marks a licensing error or model mismatch, you cannot apply the policy until you correct the issue. If you disable a rule with a warning, the warning icon disappears. It reappears if you enable the rule without correcting the underlying issue.

Table 16-2 SSL Error Icons (continued)

Icon	Description	Details
	error	If a rule or other SSL policy configuration has an error, you cannot apply the policy until you correct the issue.
	information	Information icons convey helpful information about configurations that may affect the flow of traffic. These issues are minor and will not prevent you from applying the policy.

Properly configuring SSL rules can also reduce the resources required to process network traffic. Creating complex rules and mis-ordering rules can affect performance.

For more information, see:

- Understanding Rule Preemption and Invalid Configuration Warnings, page 16-16
- Ordering SSL Rules to Improve Performance and Avoid Preemption, page 16-16

Understanding Rule Preemption and Invalid Configuration Warnings

License: Any

Properly configuring and ordering SSL rules is essential to building an effective deployment. Within an SSL policy, SSL rules can preempt other rules or contain invalid configurations. The module uses warning and error icons to mark these issues.

Understanding Rule Preemption Warnings

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

```
Rule 1: do not decrypt Administrators
Rule 2: block Administrators
```

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

Understanding Invalid Configuration Warnings

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

- A rule that contains a URL category condition might be valid until you target a module that does not have a URL Filtering license. At that point, an error icon appears next to the rule, and you cannot apply the policy to that device until you edit or delete the rule, retarget the policy, or enable the appropriate license.
- If you create a Decrypt - Resign rule, and later add a security zone with passive interfaces to a zone condition, the module displays a warning icon next to the rule. Because you cannot decrypt traffic by re-signing a certificate in a passive deployment, the rule has no effect until you remove the passive interfaces from the rule or change the rule action.
- 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 SSL Rules to Improve Performance and Avoid Preemption

License: Any

Rules in an SSL policy are numbered, starting at 1. The ASA FirePOWER module 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 SSL 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 decrypt outgoing traffic from a single user for further analysis (using a Decrypt - Resign rule), but not decrypt traffic from all other users in the department (using a Do not decrypt rule), place two SSL 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 a trusted CA (Good CA) mistakenly issued a CA certificate to a malicious entity (Bad CA), but has not yet revoked that certificate. You want to block traffic encrypted with certificates issued by the untrusted CA, but otherwise allow traffic within the trusted CA's chain of trust. You should upload the CA certificates and all intermediate CA certificates, then order your rules as follows:

```
Rule 1: Block issuer CN=www.badca.com
Rule 2: Do not decrypt issuer CN=www.goodca.com
```

If you reverse the rules:

```
Rule 1: Do not decrypt issuer CN=www.goodca.com
Rule 2: Block issuer CN=www.badca.com
```

the first rule matches all traffic trusted by Good CA, including traffic trusted by Bad CA. Because no traffic ever matches the second rule, malicious traffic may be allowed instead of blocked.

Order Rules to Allow Traffic from Certificate Pinned Sites

Certificate pinning forces a client's browser to verify that a server's public key certificate matches a certificate the browser already associated with the server before establishing an SSL session. Because the Decrypt - Resign action involves modifying a server certificate before passing it to the client, these modified certificates are rejected if the browser already pinned that certificate.

For example, if a client browser connects to `windowsupdate.microsoft.com`, a site that uses certificate pinning, and you configure an SSL rule that matches that traffic with a Decrypt - Resign action, the ASA FirePOWER module re-signs the server certificate before passing it to the client browser. Because this modified server certificate does not match the browser's pinned certificate for `windowsupdate.microsoft.com`, the client browser rejects the connection.

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. In the SSL policy, order this rule before all Decrypt - Resign rules that also match the traffic. You can retrieve the pinned certificate from the client's browser after a successful connection to the website. You can also view the certificate from the logged connection event, whether the connection succeeded or failed.

Place Rules that Decrypt Traffic Later

Because traffic decryption requires processing resources, placing rules that do not decrypt traffic (Do not decrypt, Block) before rules that do (Decrypt - Known Key, Decrypt - Resign) can improve performance. This is because traffic decryption can command significant resources. In addition, Block rules can divert traffic that the ASA FirePOWER module might otherwise have decrypted or 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
- Block rules that block traffic without further inspection
- Do not decrypt rules that do not decrypt encrypted traffic
- Decrypt - Known Key rules that decrypt incoming traffic with a known private key
- Decrypt - Resign rules that decrypt outgoing traffic by re-signing the server certificate

Prioritize ClientHello Modifications

To prioritize ClientHello modifications, place rules that match on conditions that are available in the ClientHello message before rules that match on ServerHello or server Certificate conditions.

When a managed device processes an SSL handshake, it can modify the ClientHello message to increase the likelihood of decryption. For example, it may remove compression methods because the Firepower System cannot decrypt compressed sessions.

The system only modifies ClientHello messages if it can conclusively match them to an SSL rule with a Decrypt - Resign action. The first time the system detects an encrypted session to a new server, server Certificate data is not available for ClientHello processing, which can result in an undecrypted first session. For subsequent connections from the same client, the system can match the ClientHello message conclusively to rules with server Certificate conditions and process the message to maximize decryption potential.

If you place rules that match on ServerHello or server Certificate conditions (certificate, distinguished names, certificate status, cipher suites, version) before rules that match on ClientHello conditions (zones, networks, VLAN tags, ports, users, applications, URL categories), you can preempt ClientHello modification and increase the number of undecrypted sessions.

Configuring SSL Inspection to Improve Performance

License: Any

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

Simplifying Rules

The following guidelines can help you simplify your SSL 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 SSL 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.

Configuring Traffic Decryption

Keep the following guidelines in mind when configuring traffic decryption:

- Traffic decryption requires processing resources to decrypt the traffic, and to inspect it with access control. Create narrowly focused decrypt rules over broad decrypt rules to reduce the amount of traffic the ASA FirePOWER module decrypts, and as a result, reduce the processing resources required to decrypt traffic. Rather than decrypting then later allowing or blocking traffic using an access control rule, block or choose not to decrypt encrypted traffic where possible.
- If you configure certificate status conditions to trust traffic based on the root issuer CA, upload the root CA certificate and all intermediate CA certificates within the root CA's chain of trust to your SSL policy. All traffic within a trusted CA's chain of trust can be allowed without decryption, rather than unnecessarily decrypting it.