

Tuning Traffic Decryption Using SSL Rules

A basic SSL rule applies its rule action to all encrypted traffic inspected by the ASA FirePOWER module. To better control and decrypt encrypted traffic, you can configure rule conditions to handle and log specific types of traffic. Each SSL rule can contain 0, 1, or more rule conditions; a rule only matches traffic if the traffic matches every condition in that SSL rule.

Note When traffic matches a rule, the ASA FirePOWER module applies the configure rule action to the traffic. When the connection ends, the module logs the traffic if configured to do so. For more information, see Using Rule Actions to Determine Encrypted Traffic Handling and Inspection, page 16-8 and Logging Connections Based on Access Control Handling, page 36-9.

Each rule condition allows you to specify one or more properties of traffic you want to match against; these properties include details of:

- the flow of traffic, including the security zone through which it travels, IP address and port, and country of origin or destination
- the user associated with a detected IP address
- the traffic payload, including the application detected in the traffic
- the connection encryption, including the SSL/TLS protocol version and cipher suite and server certificate used to encrypt the connection
- the category and reputation of the URL specified in the server certificate's distinguished name

For more information, see the following sections:

- Logging Decryptable Connections with SSL Rules, page 36-14
- Controlling Encrypted Traffic with Network-Based Conditions, page 17-1
- Controlling Encrypted Traffic by Reputation, page 17-7
- Controlling Traffic Based on Server Certificate Characteristics, page 17-16

Controlling Encrypted Traffic with Network-Based Conditions

License: Any

SSL *rules* within *SSL policies* exert granular control over encrypted traffic logging and handling. Network-based conditions allow you to manage which encrypted traffic can traverse your network, using one or more of the following criteria:

- source and destination security zones
- source and destination IP addresses or geographical locations
- source and destination port

You can combine network-based conditions with each other and with other types of conditions to create an SSL rule. These SSL rules can be simple or complex, matching and inspecting traffic using multiple conditions. For detailed information on SSL rules, see Getting Started with SSL Rules, page 16-1.

For more information, see the following sections:

- Controlling Encrypted Traffic by Network Zone, page 17-2
- Controlling Encrypted Traffic by Network or Geographical Location, page 17-3
- Controlling Encrypted Traffic by Port, page 17-5

Controlling Encrypted Traffic by Network Zone

License: Any

Zone conditions in SSL rules allow you to control encrypted traffic by its source and destination security zones.

A *security zone* is a grouping of one or more interfaces. An option you choose during a device's initial setup, called its *detection mode*, determines how the ASA FirePOWER module initially configures the device's interfaces, and whether those interfaces belong to a security zone.

As a simple example, when you register a device with an **Inline** detection mode, the ASA FirePOWER module creates two zones: Internal and External, and assigns the first pair of interfaces on the device to those zones. Hosts connected to the network on the Internal side represent your protected assets.

Tip You are not required to group all internal (or external) interfaces into a single zone. Choose the grouping that makes sense for your deployment and security policies. For more information on creating zones, see Working with Security Zones, page 3-32.

In this deployment, you may decide that although you want these hosts to have unrestricted access to the Internet, you nevertheless want to protect them by decrypting and inspecting incoming encrypted traffic.

To accomplish this with SSL inspection, configure an SSL rule with a zone condition where the **Destination Zone** is set to **Internal**. This simple SSL rule matches traffic that leaves the device from any interface in the Internal zone.

If you want to build a more complex rule, you can add a maximum of 50 zones to each of the **Sources Zones** and **Destination Zones** in a single zone condition:

- To match encrypted traffic *leaving* the device from an interface in the zone, add that zone to the **Destination Zones**.

  Because devices deployed passively do not transmit traffic, you cannot use a zone comprised of passive interfaces in a **Destination Zone** condition.
- To match encrypted traffic *entering* the device from an interface in the zone, add that zone to the **Source Zones**.

If you add both source and destination zone conditions to a rule, matching traffic must originate from one of the specified source zones **and** egress through one of the destination zones.

Note that just as all interfaces in a zone must be of the same type (all inline, all passive, all switched, or all routed), all zones used in a zone condition for an SSL rule must be of the same type. That is, you cannot write a single rule that matches encrypted traffic to or from zones of different types.

Warning icons indicate invalid configurations, such as zones that contain no interfaces. For details, hover your pointer over the icon.

To control encrypted traffic by zone:

Step 1 In the SSL policy where you want to control encrypted traffic by zone, create a new SSL rule or edit an existing rule.

For detailed instructions, see Understanding and Creating SSL Rules, page 16-4.

Step 2 In the SSL rule editor, select the Zones tab.

The Zones tab appears.

Step 3 Find and select the zones you want to add from the **Available Zones**.

To search for zones to add, click the **Search by name** prompt above the **Available Zones** list, then type a zone name. The list updates as you type to display matching zones.

Click to select a zone. To select multiple zones, use the Shift and Ctrl keys, or right-click and then select **Select All**.

Step 4 Click **Add to Source** or **Add to Destination** to add the selected zones to the appropriate list.

You can also drag and drop selected zones.

Step 5 Save or continue editing 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.

Controlling Encrypted Traffic by Network or Geographical Location

License: Any

Network conditions in SSL rules allow you to control and decrypt encrypted traffic by its source and destination IP address. You can either:

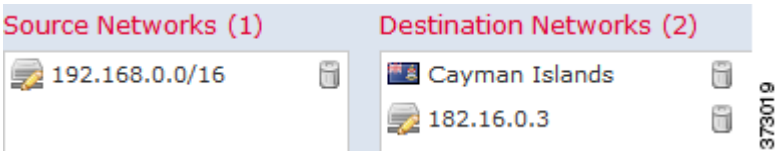
- explicitly specify the source and destination IP addresses for the encrypted traffic you want to control, or
- use the geolocation feature, which associates IP addresses with geographical locations, to control encrypted traffic based on its source or destination country or continent

When you build a network-based SSL rule condition, you can manually specify IP address and geographical locations. Alternately, you can configure network conditions with network and geolocation *objects*, which are reusable and associate a name with one or more IP addresses, address blocks, countries, continents, and so on.

Tip After you create a network or geolocation object, you can use it not only to build SSL rules, but also to represent IP addresses in various other places in the module interface. You can create these objects using the object manager; you can also create network objects on-the-fly while you are configuring SSL rules. For more information, see Managing Reusable Objects, page 3-1.

Note that if you want to write rules to control traffic by geographical location, to ensure you are using up-to-date geolocation data to filter your traffic, Cisco **strongly** recommends you regularly update the geolocation database (GeoDB) on your ASA FirePOWER module; see Updating the Geolocation Database, page 46-19.

The following graphic shows the network condition for an SSL rule that blocks encrypted connections originating from your internal network and attempting to access resources either in the Cayman Islands or an offshore holding corporation server at 182.16.0.3.



The example manually specifies the offshore holding corporation's server IP address, and uses a ASA FirePOWER module-provided Cayman Islands geolocation object to represent Cayman Island IP addresses.

You can add a maximum of 50 items to each of the **Source Networks** and **Destination Networks** in a single network condition, and you can mix network and geolocation-based configurations:

- To match encrypted traffic *from* an IP address or geographical location, configure the **Source Networks**.
- To match encrypted traffic *to* an IP address or geographical location, configure the **Destination Networks**.

If you add both source and destination network conditions to a rule, matching encrypted traffic must originate from one of the specified IP addresses **and** be destined for one of the destination IP addresses.

When building a network condition, warning icons indicate invalid configurations. For details, hover your pointer over the icon.

To control traffic by network or geographical location:

Access: Admin/Access Admin/Network Admin

Step 1 In the SSL policy where you want to control encrypted traffic by network, create a new SSL rule or edit an existing rule.

For detailed instructions, see Understanding and Creating SSL Rules, page 16-4.

Step 2 In the SSL rule editor, select the Networks tab.

The Networks tab appears.

Step 3 Find and select the networks you want to add from the **Available Networks**, as follows:

- Click the Networks tab to display network objects and groups to add; click the Geolocation tab to display geolocation objects.

- To add a network object on the fly, which you can then add to the condition, click the add icon ( ) above the Available Networks list; see Working with Network Objects, page 3-3.
- To search for network or geolocation objects to add, select the appropriate tab, click the **Search by name or value** prompt above the **Available Networks** list, then type an object name or the value of one of the object's components. The list updates as you type to display matching objects.

To select an object, click it. To select multiple objects, use the Shift and Ctrl keys, or right-click and then select **Select All**.

Step 4 Click **Add to Source** or **Add to Destination** to add the selected objects to the appropriate list.

You can also drag and drop selected objects.

Step 5 Add any source or destination IP addresses or address blocks that you want to specify manually.

Click the **Enter an IP address** prompt below the **Source Networks** or **Destination Networks** list; then type an IP address or address block and click **Add**.

Step 6 Save or continue editing 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.

Controlling Encrypted Traffic by Port

License: Any

Port conditions in SSL rules allow you to control encrypted traffic by its source and destination TCP port. When you build a port-based SSL rule condition, you can manually specify TCP ports. Alternately, you can configure port conditions with port *objects*, which are reusable and associate a name with one or more ports.

Tip After you create a port object, you can use it not only to build SSL rules, but also to represent ports in various other places in the module interface. You can create port objects either using the object manager or on-the-fly while you are configuring SSL rules. For more information, see Working with Port Objects, page 3-9.

You can add a maximum of 50 items to each of the **Selected Source Ports** and **Selected Destination Ports** lists in a single network condition:

- To match encrypted traffic *from* a TCP port, configure the **Selected Source Ports**.
- To match encrypted traffic *to* a TCP port, configure the **Selected Destination Ports**.
- To match encrypted traffic both originating from TCP **Selected Source Ports** *and* destined for TCP **Selected Destination Ports**, configure both.

You can only configure the **Selected Source Ports** and **Selected Destination Ports** lists with TCP ports. Port objects containing non-TCP ports are greyed out in the **Available Ports** list.

When building a port condition, warning icons indicate invalid configurations. For example, you can use the object manager to edit in-use port objects so that the rules that use those object groups become invalid. For details, hover your pointer over the icon.

To control traffic by port:

Step 1 In the SSL policy where you want to control encrypted traffic by TCP port, create a new SSL rule or edit an existing rule.

For detailed instructions, see Understanding and Creating SSL Rules, page 16-4.

Step 2 In the SSL rule editor, select the Ports tab.

The Ports tab appears.

Step 3 Find and select the TCP ports you want to add from the **Available Ports**, as follows:

- To add a TCP port object on the fly, which you can then add to the condition, click the add icon ( ) above the Available Ports list; see Working with Port Objects, page 3-9.
- To search for TCP-based port objects and groups to add, click the **Search by name or value** prompt above the **Available Ports** list, then type either the name of the object, or the value of a port in the object. The list updates as you type to display matching objects. For example, if you type 443, the ASA FirePOWER module displays the ASA FirePOWER module-provided HTTPS port object.

To select a TCP-based port object, click it. To select multiple TCP-based port objects, use the Shift and Ctrl keys, or right-click and then select **Select All**. If the object includes non-TCP-based ports, you cannot add it to your port condition.

Step 4 Click **Add to Source** or **Add to Destination** to add the selected objects to the appropriate list.

You can also drag and drop selected objects.

Step 5 Enter a **Port** under the **Selected Source Ports** or **Selected Destination Ports** list to manually specify source or destination ports. You can specify a single port with a value from 0 to 65535.

Step 6 Click **Add**.

Note that the ASA FirePOWER module will not add a port to a rule condition that results in an invalid configuration.

Step 7 Save or continue editing 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.

Controlling Encrypted Traffic Based on User

License: Control

You can configure SSL rules to match traffic for users retrieved from a Microsoft Active Directory Server. User conditions in SSL rules allow you perform *user control*—to manage which traffic can traverse your network, by limiting traffic based on the LDAP user logged into a host.

User control works by associating *access controlled users* with IP addresses. Deployed agents monitor specified users as they log in and out of hosts or authenticate with Active Directory credentials for other reasons. For example, your organization may use services or applications that rely on Active Directory for centralized authentication.

For traffic to match an SSL rule with a user condition, the IP address of either the source or destination host in the monitored session must be associated with a logged in access controlled user. You can control traffic based on individual users or the groups those users belong to.

You can combine user conditions with each other and with other types of conditions to create an SSL rule. These SSL rules can be simple or complex, matching and inspecting traffic using multiple conditions. For detailed information on SSL rules, see Understanding and Creating SSL Rules, page 16-4.

User control requires a Control license and is supported only for LDAP users and groups (*access controlled users*), using login and logoff records reported by a User Agent monitoring Microsoft Active Directory servers.

Before you can write SSL rules with user conditions, you must configure a connection between the ASA FirePOWER module and at least one of your organization's Microsoft Active Directory servers. This configuration, called an authentication object, contains connection settings and authentication filter settings for the server. It also specifies the users you can use in user conditions.

In addition, you must install User Agents. The agents monitor users when they authenticate against Active Directory credentials, and send records of those logins to the ASA FirePOWER module. These records associate users with IP addresses, which is what allows SSL rules with user conditions to trigger.

To control encrypted traffic by user:

Step 1 In the SSL policy where you want to control encrypted traffic by user, create a new SSL rule or edit an existing rule.

For detailed instructions, see Understanding and Creating SSL Rules, page 16-4.

Step 2 In the SSL rule editor, select the Users tab.

The Users tab appears.

Step 3 To search for users to add, click the **Search by name or value** prompt above the **Available Users** list, then type the username. The list updates as you type to display matching users.

To select a user, click it. To select multiple users, use the Shift and Ctrl keys, or right-click and then select **Select All**.

Step 4 Click **Add to Rule** or to add the selected users to the **Selected Users** list.

You can also drag and drop selected users.

Step 5 Save or continue editing 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.

Controlling Encrypted Traffic by Reputation

License: Control or URL Filtering

Reputation-based conditions in SSL rules allow you to manage which encrypted traffic can traverse your network, by contextualizing your network traffic and limiting it where appropriate. SSL rules govern the following types of reputation-based control:

- Application conditions allow you to perform *application control*, which controls application traffic based on not only individual applications, but also applications' basic characteristics: type, risk, business relevance, and categories.
- URL conditions allow you to control web traffic based on a websites' assigned category and reputation.

You can combine reputation-based conditions with each other and with other types of conditions to create an SSL rule. These SSL rules can be simple or complex, matching and inspecting traffic using multiple conditions.

For more information, see the following sections:

- Controlling Encrypted Traffic Based on Application, page 17-8
- Controlling Encrypted Traffic by URL Category and Reputation, page 17-13

Controlling Encrypted Traffic Based on Application

License: Control

When the Firepower system analyzes encrypted IP traffic, it can identify and classify commonly used encrypted applications on your network prior to decrypting the encrypted session. The ASA FirePOWER module uses this discovery-based *application awareness* feature to allow you to control encrypted application traffic on your network.

Application conditions in SSL rules allow you to perform this *application control*. Within a single SSL rule, there are a few ways you can specify applications whose traffic you want to control:

- You can select individual applications, including custom applications.
- You can use ASA FirePOWER module-provided *application filters*, which are named sets of applications organized according to its basic characteristics: type, risk, business relevance, and categories.
- You can create and use custom application filters, which group applications (including custom applications) in any way you choose.

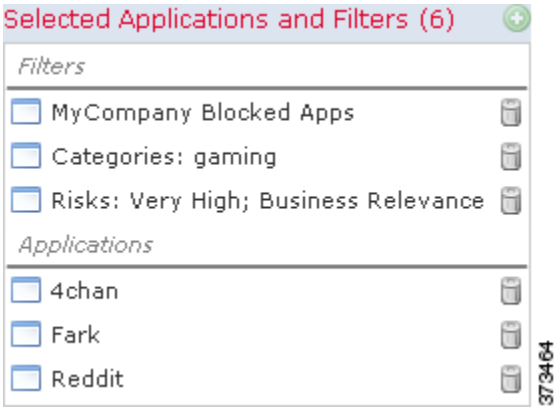
Note When you filter application traffic using access control rules, you can use application tags as a criterion. to filter. However, you cannot use application tags to filter encrypted traffic because there is no benefit. All applications that the ASA FirePOWER module can detect in encrypted traffic are tagged **SSL Protocol**; applications without this tag can only be detected in unencrypted or decrypted traffic.

Application filters allow you to quickly create application conditions for SSL rules. They simplify policy creation and administration, and grant you assurance that the module will control web traffic as expected. For example, you could create an SSL rule that identifies and decrypts all high risk, low business relevance applications in encrypted traffic. If a user attempts to use one of those applications, the session is decrypted and inspected with access control.

In addition, Cisco frequently updates and adds additional detectors via system and vulnerability database (VDB) updates. You can also create your own detectors and assign characteristics (risk, relevance, and so on) to the applications they detect. By using filters based on application characteristics, you can ensure that the module uses the most up-to-date detectors to monitor application traffic.

For traffic to match an SSL rule with an application condition, the traffic must match one of the filters or applications that you add to a **Selected Applications and Filters** list.

The following graphic shows the application condition for an SSL rule that decrypts a custom group of applications for MyCompany, all applications with high risk and low business relevance, gaming applications, and some individually selected applications.



In a single application condition, you can add a maximum of 50 items to the **Selected Applications and Filters** list. Each of the following counts as an item:

- One or more filters from the **Application Filters** list, individually or in custom combination. This item represents set of applications, grouped by characteristic.
- A filter created by saving search of the applications in the **Available Applications** list. This item represents a set of applications, grouped by substring match.
- An individual application from the **Available Applications** list.

In the module interface, filters added to a condition are listed above and separately from individually added applications.

Note that when you apply an SSL policy, for each rule with an application condition, the ASA FirePOWER module generates a list of unique applications to match. In other words, you may use overlapping filters and individually specified applications to ensure complete coverage.

For more information, see the following sections:

- Matching Encrypted Traffic with Application Filters, page 17-9
- Matching Traffic from Individual Applications, page 17-10
- Adding an Application Condition to an SSL Rule, page 17-11
- Limitations to Encrypted Application Control, page 17-12

Matching Encrypted Traffic with Application Filters

License: Control

When building an application condition in an SSL rule, use the **Application Filters** list to create a set of applications, grouped by characteristic, whose traffic you want to match.

For your convenience, the ASA FirePOWER module characterizes each application that it detects using a specified criteria. You can use these criteria as filters or create custom combinations of filters to perform application control.

Note that the mechanism for filtering applications within an SSL rule is the same as that for creating reusable, custom application filters using the object manager; see Working with Application Filters, page 3-11. You can also save many filters you create on-the-fly in access control rules as new, reusable filters. You cannot save a filter that includes another user-created filter because you cannot nest user-created filters.

Understanding How Filters Are Combined

When you select filters, singly or in combination, the **Available Applications** list updates to display only the applications that meet your criteria. You can select ASA FirePOWER module-provided filters in combination, but not custom filters.

The module links multiple filters of the same filter type with an OR operation. For example, if you select the Medium and High filters under the Risks type, the resulting filter is:

```
Risk: Medium OR High
```

If the Medium filter contained 110 applications and the High filter contained 82 applications, the module displays all 192 applications in the **Available Applications** list.

The module links different types of filters with an AND operation. For example, if you select the Medium and High filters under the Risks type, and the Medium and High filters under the Business Relevance type, the resulting filter is:

```
Risk: Medium OR High
AND
Business Relevance: Medium OR High
```

In this case, the module displays only those applications that are included in both the Medium or High Risk type AND the Medium or High Business Relevance type.

Finding and Selecting Filters

To select filters, click the arrow next to a filter type to expand it, then select or clear the check box next to each filter whose applications you want to display or hide. You can also right-click a Cisco-provided filter type (**Risks**, **Business Relevance**, **Types**, or **Categories**) and select **Check All** or **Uncheck All**.

To search for filters, click the **Search by name** prompt above the **Available Filters** list, then type a name. The list updates as you type to display matching filters.

After you are done selecting filters, use the **Available Applications** list to add those filters to the rule; see Matching Traffic from Individual Applications, page 17-10.

Matching Traffic from Individual Applications

License: Control

When building an application condition in an SSL rule, use the **Available Applications** list to select the applications whose traffic you want to match.

Browsing the List of Applications

When you first start to build the condition the list is unconstrained, and displays every application the module detects, 100 at a time:

- To page through the applications, click the arrows underneath the list.
- To display a pop-up window with summary information about the application's characteristics, as well as Internet search links that you can follow, click the information icon ( ) next to an application.

Finding Applications to Match

To help you find the applications you want to match, you can constrain the **Available Applications** list in the following ways:

- To search for applications, click the **Search by name** prompt above the list, then type a name. The list updates as you type to display matching applications.

- To constrain the applications by applying a filter, use the **Application Filters** list (see Matching Encrypted Traffic with Application Filters, page 17-9). The **Available Applications** list updates as you apply filters.

Once constrained, an **All apps matching the filter** option appears at the top of the **Available Applications** list. This option allows you to add all the applications in the constrained list to the **Selected Applications and Filters** list, all at once.

Note If you select one or more filters in the Application Filters list and also search the **Available Applications** list, your selections and the search-filtered **Available Applications** list are combined using an AND operation. That is, the **All apps matching the filter** condition includes all the individual conditions currently displayed in the **Available Applications** list as well as the search string entered above the **Available Applications** list.

Selecting Single Applications to Match in a Condition

After you find an application you want to match, click to select it. To select multiple applications, use the Shift and Ctrl keys, or right-click and select **Select All** to select all applications in the current constrained view.

In a single application condition, you can match a maximum of 50 applications by selecting them individually; to add more than 50 you must either create multiple SSL rules or use filters to group applications.

Selecting All Applications Matching a Filter for a Condition

Once constrained by either searching or using the filters in the **Application Filters** list, the **All apps matching the filter** option appears at the top of the **Available Applications** list.

This option allows you to add the entire set of applications in the constrained **Available Applications** list to the **Selected Applications and Filters** list, at once. In contrast to adding applications individually, adding this set of applications counts as only one item against the maximum of 50, regardless of the number of individual application that comprise it.

When you build an application condition this way, the name of the filter you add to the **Selected Applications and Filters** list is a concatenation of the filter types represented in the filter plus the names of up to three filters for each type. More than three filters of the same type are followed by an ellipsis (...). For example, the following filter name includes two filters under the Risks type and four under Business Relevance:

```
Risks: Medium, High Business Relevance: Low, Medium, High,...
```

Filter types that are not represented in a filter you add with **All apps matching the filter** are not included in the name of the filter you add. The instructional text that is displayed when you hover your pointer over the filter name in the **Selected Applications and Filters** list indicates that these filter types are set to *any*; that is, these filter types do not constrain the filter, so any value is allowed for these.

You can add multiple instances of **All apps matching the filter** to an application condition, with each instance counting as a separate item in the **Selected Applications and Filters** list. For example, you could add all high risk applications as one item, clear your selections, then add all low business relevance applications as another item. This application condition matches applications that are high risk OR have low business relevance.

Adding an Application Condition to an SSL Rule

License: Control

For encrypted traffic to match an SSL rule with an application condition, the traffic must match one of the filters or applications that you add to a **Selected Applications and Filters** list.

You can add a maximum of 50 items per condition, and filters added to a condition are listed above and separately from individually added applications. When building an application condition, warning icons indicate invalid configurations. For details, hover your pointer over the icon.

To control encrypted application traffic:

Step 1 In the SSL policy where you want to control traffic by application, create a new SSL rule or edit an existing rule.

For detailed instructions, see Understanding and Creating SSL Rules, page 16-4.

Step 2 In the SSL rule editor, select the Applications tab.

The Applications tab appears.

Step 3 Optionally, use filters to constrain the list of applications displayed in the **Available Applications** list.

Select one or more filters in the **Application Filters** list. For more information, see Matching Encrypted Traffic with Application Filters, page 17-9.

Step 4 Find and select the applications you want to add from the **Available Applications** list.

You can search for and select individual applications, or, when the list is constrained, **All apps matching the filter**. For more information, see Matching Traffic from Individual Applications, page 17-10.

Step 5 Click **Add to Rule** to add the selected applications to the **Selected Applications and Filters** list.

You can also drag and drop selected applications and filters. Filters appear under the heading *Filters*, and applications appear under the heading *Applications*.

Tip Before you add another filter to this application condition, click **Clear All Filters** to clear your existing selections.

Step 6 Save or continue editing 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.

Limitations to Encrypted Application Control

License: Control

Keep the following points in mind when performing application control.

Encrypted Application Identification

The ASA FirePOWER module can identify unencrypted applications that become encrypted using StartTLS. This includes such applications as SMTPS, POPS, FTPS, TelnetS, and IMAPS. In addition, it can identify certain encrypted applications based on the Server Name Indication in the TLS client hello message, or the server certificate subject distinguished name value.

Speed of Application Identification

The ASA FirePOWER module cannot perform application control on encrypted traffic before:

- an encrypted connection is established between a client and server, and
- the module identifies the application in the encrypted session

This identification occurs after the server certificate exchange. If traffic exchanged during the handshake matches all other conditions in an SSL rule containing an application condition but the identification is not complete, the SSL policy allows the packet to pass. This behavior allows the handshake to complete so that applications can be identified. For your convenience, affected rules are marked with an information icon ( ).

After the module completes its identification, it applies the SSL rule action to the remaining session traffic that matches its application condition.

Controlling Encrypted Traffic by URL Category and Reputation

License: URL Filtering

URL conditions in SSL rules allow you to handle and decrypt encrypted website traffic that users on your network can access. The module detects the requested URL based on information passed during the SSL handshake. With a URL Filtering license, you can control access to websites based on the URL's general classification, or *category*, and risk level, or *reputation*.

Note You can handle and decrypt traffic to specific URLs by defining a distinguished name SSL rule condition. The common name attribute in a certificate's subject distinguished name contains the site's URL. For more information, see Controlling Encrypted Traffic by Certificate Distinguished Name, page 17-17.

For more information, see:

- Performing Reputation-Based URL Blocking, page 17-13
- Limitations on URL Detection and Blocking, page 17-16

Performing Reputation-Based URL Blocking

License: URL Filtering

With a URL Filtering license, you can control your users' access to websites based on the category and reputation of requested URLs:

- The URL *category* is a general classification for the URL. For example, ebay.com belongs to the **Auctions** category, and monster.com belongs to the **Job Search** category. A URL can belong to more than one category.
- The URL *reputation* represents how likely the URL is to be used for purposes that might be against your organization's security policy. A URL's risk can range from **High Risk** (level 1) to **Well Known** (level 5).

URL categories and reputations, which the Firepower system obtains from the Cisco cloud, allow you to quickly create URL conditions for SSL rules. For example, you could create an SSL rule that identifies and blocks all **High risk** URLs in the **Abused Drugs** category. If a user attempts to browse to any URL with that category and reputation combination over an encrypted connection, the session is blocked.

Note Before SSL rules with category and reputation-based URL conditions can take effect, you **must** enable communications with the Cisco cloud. This allows the ASA FirePOWER module to retrieve URL data. For more information, see Enabling Cloud Communications, page 44-2.

Using category and reputation data from the Cisco cloud simplifies policy creation and administration. It grants you assurance that the module controls encrypted web traffic as expected. Finally, because the cloud is continually updated with new URLs, as well as new categories and risks for existing URLs, you can ensure that the module uses up-to-date information to filter requested URLs. Malicious sites that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and apply new policies.

For example:

- If a rule blocks all gaming sites, as new domains get registered and classified as **Gaming**, the module can block those sites automatically.
- If a rule blocks all malware, and a blog page gets infected with malware, the cloud can recategorize the URL from **Blog** to **Malware** and the module can block that site.
- If a rule blocks high-risk social networking sites, and somebody posts a link on their profile page that contains links to malicious payloads, the cloud can change the reputation of that page from **Benign sites** to **High risk** so the module can block it.

Note that if the cloud does not know the category or reputation of a URL, or if the ASA FirePOWER module cannot contact the cloud, that URL does **not** trigger SSL rules with category or reputation-based URL conditions. You cannot assign categories or reputations to URLs manually.

The following graphic shows the URL condition for an access control rule that blocks: all malware sites, all high-risk sites, and all non-benign social networking sites.



Tip If you decrypt traffic, then block it with access control, you can give users a chance to bypass the block by clicking through a warning page. See Interactive Blocking Actions: Allowing Users to Bypass Website Blocks, page 6-9 for more information.

You can add a maximum of 50 **Selected Categories** to match in a single URL condition. Each URL category, optionally qualified by reputation, counts as a single item.

The following table summarizes how you build the condition shown above. Note that you cannot qualify a literal URL or URL object with a reputation.

Table 17-1 Example: Building A URL Condition

To block...	Select this Category or URL Object...	And this Reputation...
malware sites, regardless of reputation	Malware Sites	Any
any URL with a high risk (level 1)	Any	1 - High Risk
social networking sites with a risk greater than benign (levels 1 through 3)	Social Network	3 - Benign sites with security risks

When building a URL condition, warning icons indicate invalid configurations. For details, hover your pointer over the icon and see Troubleshooting Access Control Policies and Rules, page 4-12.

To control traffic by requested URL using category and reputation data:

Step 1 In the SSL policy where you want to control encrypted traffic by URL, create a new SSL rule or edit an existing rule.

For detailed instructions, see Understanding and Creating SSL Rules, page 16-4.

Step 2 In the SSL rule editor, select the Categories tab.

The Categories tab appears.

Step 3 Find and select the categories of URL you want to add from the **Categories** list. To match encrypted web traffic regardless of category, select **Any** category.

To search for categories to add, click the **Search by name or value** prompt above the **Categories** list, then type the category name. The list updates as you type to display matching categories.

To select a category, click it. To select multiple categories, use the Shift and Ctrl keys.

Tip Although you can right-click and **Select All** categories, adding all categories this way exceeds the 50-item maximum for an SSL rule. Instead, use **Any**.

Step 4 Optionally, qualify your category selections by clicking a reputation level from the **Reputations** list. If you do not specify a reputation level, the module defaults to **Any**, meaning all levels.

You can only select one reputation level. When you choose a reputation level, the SSL rule behaves differently depending on its purpose:

- If the rule blocks web access or decrypts traffic (the rule action is **Block**, **Block with reset**, **Decrypt - Known Key**, **Decrypt - Resign**, or **Monitor**) selecting a reputation level also selects all reputations more severe than that level. For example, if you configure a rule to block **Suspicious sites** (level 2), it also automatically blocks **High Risk** (level 1) sites.
- If the rule allows web access, subject to access control (the rule action is **Do not decrypt**), selecting a reputation level also selects all reputations less severe than that level. For example, if you configure a rule to allow **Benign sites** (level 4), it also automatically allows **Well known** (level 5) sites.

If you change the rule action for a rule, the module automatically changes the reputation levels in URL conditions according to the above points.

Step 5 Click **Add to Rule** or to add the selected items to the **Selected Categories** list.

You can also drag and drop selected items.

Step 6 Save or continue editing 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.

Limitations on URL Detection and Blocking

License: URL Filtering

Keep the following points in mind when performing URL detection and blocking.

Speed of URL Identification

The module cannot categorize URLs before:

- a monitored connection is established between a client and server
- the module identifies the HTTPS application in the session
- the module identifies the requested URL from either the client hello message or the server certificate

This identification occurs after the server certificate exchange. If traffic exchanged during the handshake matches all other conditions in an SSL rule containing a URL condition but the identification is not complete, the SSL policy allows the packet to pass. This behavior allows the connection to be established so that URLs can be identified. For your convenience, affected rules are marked with an information icon ( ).

After the module completes its identification, it applies the SSL rule action to the remaining session traffic that matches its URL condition.

Search Query Parameters in URLs

The module does not use search query parameters in the URL to match URL conditions. For example, consider a scenario where you block all shopping traffic. In that case, using a web search to search for amazon.com is not blocked, but browsing to amazon.com is.

Controlling Traffic Based on Server Certificate Characteristics

License: Any

You can create SSL rules that handle and decrypt encrypted traffic based on server certificate characteristics. You can detect the protocol version or cipher suite used to encrypt the session, and handle traffic accordingly. You can also detect the server certificate and handle traffic, based on the following server certificate characteristics:

- the server certificate itself
- the certificate issuer, whether an issuing CA or if the certificate is self-signed
- the certificate holder
- various certificate statuses, such as whether the certificate is valid, or revoked by the issuing CA

To detect multiple cipher suites in a rule, the certificate issuer, or the certificate holder, you can create reusable cipher suite list and distinguished name objects and add them to your rule. To detect the server certificate and certain certificate statuses, you must create external certificate and external CA objects for the rule.

For more information, see the following sections:

- Controlling Encrypted Traffic by Certificate Distinguished Name, page 17-17
- Controlling Encrypted Traffic by Certificate, page 17-19
- Controlling Encrypted Traffic by Certificate Status, page 17-20
- Controlling Encrypted Traffic by Cipher Suite, page 17-25
- Controlling Traffic by Encryption Protocol Version, page 17-26

Controlling Encrypted Traffic by Certificate Distinguished Name

License: Any

Distinguished name conditions in SSL rules allow you to handle and inspect encrypted traffic based on the CA that issued a server certificate, or the certificate holder. Based on the issuer distinguished name, you can handle traffic based on the CA that issued a site's server certificate.

When configuring the rule condition, you can manually specify a literal value, reference a distinguished name object, or reference a distinguished name group containing multiple objects.

Note You cannot configure a distinguished name condition if you also select the **Decrypt - Known Key** action. Because that action requires you to select a server certificate to decrypt traffic, the certificate already matches the traffic. See Decrypt Actions: Decrypting Traffic for Further Inspection, page 16-10 for more information.

You can match against multiple subject and issuer distinguished names in a single certificate status rule condition; only one common or distinguished name needs to match to match the rule.

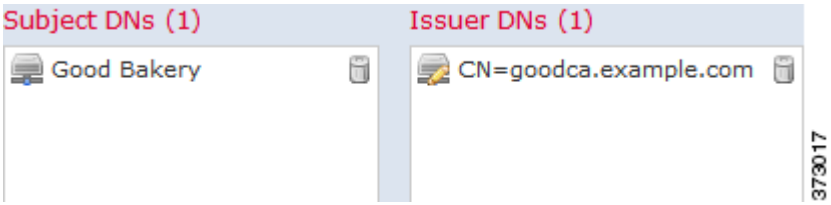
If you add a distinguished name manually, it can contain the common name attribute (**CN**). If you add a common name without `CN=` then the module prepends `CN=` before saving the object.

You can also add a distinguished name with one of each attribute listed in the following table, separated by commas.

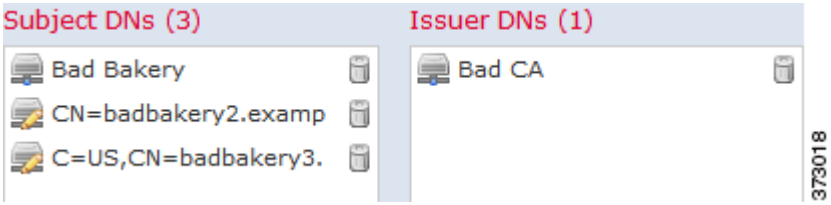
Table 17-2 Distinguished Name Attributes

Attribute	Description	Allowed Values
C	Country Code	two alphabetic characters
CN	Common Name	up to 64 alphanumeric, backslash (\), hyphen (-), quotation ("), asterisk (*), period (.), or space characters
O	Organization	
OU	Organizational Unit	

The following graphic illustrates a distinguished name rule condition searching for certificates issued to goodbakery.example.com or issued by goodca.example.com. Traffic encrypted with these certificates is allowed, subject to access control.



The following graphic illustrates a distinguished name rule condition searching for certificates issued to badbakery.example.com and associated domains, or certificates issued by badca.example.com. Traffic encrypted with these certificates is decrypted using a re-signed certificate.



You can add a maximum of 50 literal values and distinguished name objects to the **Subject DNs**, and 50 literal values and distinguished name objects to the **Issuer DNs**, in a single DN condition.

The ASA FirePOWER module-provided DN object group, Sourcefire Undecryptable Sites, contains websites whose traffic the module cannot decrypt. You can add this group to a DN condition to block or not decrypt traffic to or from these websites, without wasting system resources attempting to decrypt that traffic. You can modify individual entries in the group. You cannot delete the group. System updates can modify the entries on this list, but the module preserves user changes.

The first time the system detects an encrypted session to a new server, DN data is not available for ClientHello processing, which can result in an undecrypted first session. After the initial session, the managed device caches data from the server Certificate message. For subsequent connections from the same client, the system can match the ClientHello message conclusively to rules with DN conditions and process the message to maximize decryption potential.

To inspect encrypted traffic based on certificate subject or issuer distinguished name:

Step 1 In the SSL policy where you want to control encrypted traffic by certificate subject or issuer distinguished name, create a new SSL rule or edit an existing rule.

For detailed instructions, see Understanding and Creating SSL Rules, page 16-4.

Step 2 In the SSL rule editor, select the DN tab.

The DN tab appears.

Step 3 Find and select the distinguished names you want to add from the **Available DNs**, as follows:

- To add a distinguished name object on the fly, which you can then add to the condition, click the add icon ( ) above the **Available DNs** list; see Working with Distinguished Name Objects, page 3-33.

- To search for distinguished name objects and groups to add, click the **Search by name or value** prompt above the **Available DNs** list, then type either the name of the object, or a value in the object. The list updates as you type to display matching objects.

To select an object, click it. To select multiple objects, use the Shift and Ctrl keys, or right-click and then select **Select All**.

Step 4 You have the following options:

- Click **Add to Subject** to add the selected objects to the **Subject DNs** list.
- Click **Add to Issuer** to add the selected objects to the **Issuer DNs** list.

You can also drag and drop selected objects.

Step 5 Add any literal common names or distinguished names that you want to specify manually.

Click the **Enter DN or CN** prompt below the **Subject DNs** or **Issuer DNs** list; then type a common name or distinguished name and click **Add**.

Step 6 Add or continue editing 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.

Controlling Encrypted Traffic by Certificate

License: Any

Certificate conditions in SSL rules allow you to handle and inspect encrypted traffic based on the server certificate used to encrypt that traffic. You can configure a condition with one or more certificates; traffic matches the rule if the certificate matches any of the condition's certificates.

When you build a certificate-based SSL rule condition, you can upload a server certificate; you save the certificate as an external certificate *object*, which is reusable and associates a name with a server certificate. Alternately, you can configure certificate conditions with existing external certificate objects and object groups.

You can search the **Available Certificates** field in the rule condition based for external certificate objects and object groups based on the following certificate distinguished name characteristics:

- subject or issuer common name (CN)
- subject or issuer organization (O)
- subject or issuer organizational unit (OU)

You can choose to match against multiple certificates in a single certificate rule condition; if the certificate used to encrypt the traffic matches any of the uploaded certificates, the encrypted traffic matches the rule.

You can add a maximum of 50 external certificate objects and external certificate object groups to the **Selected Certificates** in a single certificate condition.

Note the following:

- You cannot configure a certificate condition if you also select the **Decrypt - Known Key** action. Because that action requires you to select a server certificate to decrypt traffic, the implication is that the certificate already matches the traffic. See Decrypt Actions: Decrypting Traffic for Further Inspection, page 16-10 for more information.

- If you configure a certificate condition with an external certificate object, any cipher suites you add to a cipher suite condition, or internal CA objects you associate with the **Decrypt - Resign** action, must match the external certificate's signature algorithm type. For example, if your rule's certificate condition references an EC-based server certificate, any cipher suites you add, or CA certificates you associate with the **Decrypt - Resign** action, must also be EC-based. If you mismatch signature algorithm types in this case, the policy editor displays a warning icon next to the rule. For more information, see Controlling Encrypted Traffic by Cipher Suite, page 17-25 and Decrypt Actions: Decrypting Traffic for Further Inspection, page 16-10.
- The first time the system detects an encrypted session to a new server, certificate data is not available for ClientHello processing, which can result in an undecrypted first session. After the initial session, the managed device caches data from the server Certificate message. For subsequent connections from the same client, the system can match the ClientHello message conclusively to rules with certificate conditions and process the message to maximize decryption potential.

To inspect encrypted traffic based on server certificate:

Step 1 In the SSL policy where you want to control encrypted traffic based on server certificate, create a new SSL rule or edit an existing rule.

For detailed instructions, see Understanding and Creating SSL Rules, page 16-4.

Step 2 In the SSL rule editor, select the Certificate tab.

The Certificate tab appears.

Step 3 Find and select the server certificates you want to add from the **Available Certificates**, as follows;

- To add an external certificate object on the fly, which you can then add to the condition, click the add icon ( ) above the **Available Certificates** list; see Working with External Certificate Objects, page 3-41.
- To search for certificate objects and groups to add, click the **Search by name or value** prompt above the **Available Certificates** list, then type either the name of the object, or a value in the object. The list updates as you type to display matching objects.

To select an object, click it. To select multiple objects, use the Shift and Ctrl keys, or right-click and then select **Select All**.

Step 4 Click **Add to Rule** to add the selected objects to the **Subject Certificates** list.

You can also drag and drop selected objects.

Step 5 Add or continue editing 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.

Controlling Encrypted Traffic by Certificate Status

License: Any

Certificate status conditions in SSL rules allow you to handle and inspect encrypted traffic based on the status of the server certificate used to encrypt the traffic, including whether a certificate is valid, revoked, expired, not yet valid, self-signed, or signed by a trusted CA.

Checking whether a CA issued or revoked a certificate requires uploading root and intermediate CA certificates and associated CRLs as objects. You then add these trusted CA objects to an SSL policy's list of trusted CA certificates.

For each certificate status SSL rule condition you configure, you can match traffic against the presence or absence of a given status. You can select several statuses in one rule condition; if the certificate matches any of the selected statuses, the rule matches the traffic.

For more information, see:

- Trusting External Certificate Authorities, page 17-21
- Matching Traffic on Certificate Status, page 17-22

Trusting External Certificate Authorities

License: Any

You can trust CAs by adding root and intermediate CA certificates to your SSL policy, then use these trusted CAs to verify server certificates used to encrypt traffic. Verified server certificates include certificates signed by trusted CAs.

If a trusted CA certificate contains an uploaded certificate revocation list (CRL), you can also verify whether a trusted CA revoked the encryption certificate. See Adding a Certificate Revocation List to a Trusted CA Object, page 3-40 for more information.

After you add trusted CA certificates to the SSL policy, you can configure an SSL rule with various Certificate Status conditions to match against this traffic. See Working with Trusted Certificate Authority Objects, page 3-39 and Controlling Encrypted Traffic by Certificate Status, page 17-20 for more information.

Tip Upload all certificates within a root CA's chain of trust to the list of trusted CA certificates, including the root CA certificate and all intermediate CA certificates. Otherwise, it is more difficult to detect trusted certificates issued by intermediate CAs.

When you create an SSL policy, the ASA FirePOWER module populates the Trusted CA Certificates tab with a default Trusted CA object group, Cisco Trusted Authorities. You can modify individual entries in the group, and choose whether to include this group in your SSL policy. You cannot delete the group. System updates can modify the entries on this list, but user changes are preserved. See Creating a Basic SSL Policy, page 15-2 for more information.

To add trusted CAs to your 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 the **Trusted CA Certificates** tab.

The Trusted CA Certificates page appears.

Step 4 Find and select the trusted CAs you want to add from the **Available Trusted CAs**, as follows:

- To add a trusted CA object on the fly, which you can then add to the condition, click the add icon ( ) above the **Available Trusted CAs** list; see Working with Trusted Certificate Authority Objects, page 3-39.
- To search for trusted CA objects and groups to add, click the **Search by name or value** prompt above the **Available Trusted CAs** list, then type either the name of the object, or a value in the object. The list updates as you type to display matching objects.

To select an object, click it. To select multiple objects, use the Shift and Ctrl keys, or right-click and then select **Select All**.

Step 5 Click **Add to Rule** to add the selected objects to the **Selected Trusted CAs** list.

You can also drag and drop selected objects.

Step 6 Add or continue editing 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.

Matching Traffic on Certificate Status

License: Any

Based on the certificate status rule condition configuration, you can match encrypted traffic based on the status of the server certificate used to encrypt traffic. You can:

- check for a server certificate status
- check that a certificate does not have a status
- skip checking for the presence or absence of a certificate status

You can choose to match against the presence or absence of multiple certificate statuses in a single certificate status rule condition; the certificate needs to only match one of the criteria to match the rule.

The following table describes how the ASA FirePOWER module evaluates encrypted traffic based on the encrypting server certificate's status.

Table 17-3 Certificate Status Rule Condition Criteria

Status Check	Status Set to Yes	Status Set to No
Revoked	The policy trusts the CA that issued the server certificate, and the CA certificate uploaded to the policy contains a CRL that revokes the server certificate.	The policy trusts the CA that issued the server certificate, and the CA certificate uploaded to the policy does not contain a CRL that revokes the certificate.
Self-signed	The detected server certificate contains the same subject and issuer distinguished name.	The detected server certificate contains different subject and issuer distinguished names.

Table 17-3 Certificate Status Rule Condition Criteria (continued)

Status Check	Status Set to Yes	Status Set to No
Valid	All of the following are true: • The policy trusts the CA that issued the certificate • The signature is valid • The issuer is valid • None of the policy's trusted CAs revoked the certificate. • The current date is between the certificate Valid From and Valid To date	At least one of the following is true: • The policy does not trust the CA that issued the certificate • The signature is invalid • The issuer is invalid • A trusted CA in the policy revoked the certificate • The current date is before the certificate Valid From date • The current date is after the certificate Valid To date
Invalid signature	The certificate's signature cannot be properly validated against the certificate's content.	The certificate's signature is properly validated against the certificate's content.
Invalid issuer	The issuer CA certificate is not stored in the policy's list of trusted CA certificates.	The issuer CA certificate is stored in the policy's list of trusted CA certificates.
Expired	The current date is after the certificate Valid To date.	The current date is before or on the certificate Valid To date.
Not yet valid	The current date is before the certificate Valid From date.	The current date is after or on the certificate Valid From date.

Consider the following example. The organization trusts the Verified Authority certificate authority. The organization does not trust the Spammer Authority certificate authority. The system administrator uploads the Verified Authority certificate and an intermediate CA certificate issued by Verified Authority to the module. Because Verified Authority revoked a certificate it previously issued, the system administrator uploads the CRL that Verified Authority distributed.

The following graphic illustrates a certificate status rule condition checking for valid certificates, those issued by Verified Authority, not on the CRL, and still within the Valid From and Valid To date. Because of the configuration, traffic encrypted with these certificates is not decrypted and inspected with access control.



The following graphic illustrates a certificate status rule condition checking for the absence of a status. In this case, because of the configuration, it matches against traffic encrypted with a certificate that has not expired and monitors that traffic.



The following graphic illustrates a certificate status rule condition that matches on the presence or absence of several statuses. Because of the configuration, if the rule matches incoming traffic encrypted with a certificate issued by an invalid user, self-signed, invalid, or expired, it decrypts the traffic with a known key.



Note that even though a certificate may match more than one status, the rule only takes an action on the traffic once.

Note The first time the system detects an encrypted session to a new server, certificate status is not available for ClientHello processing, which can result in an undecrypted first session. After the initial session, the managed device caches data from the server Certificate message. For subsequent connections from the same client, the system can match the ClientHello message conclusively to rules with certificate status conditions and process the message to maximize decryption potential.

To inspect encrypted traffic by server certificate status:

Step 1 In the SSL policy where you want to control encrypted traffic based on server certificate status, create a new SSL rule or edit an existing rule.

For detailed instructions, see Understanding and Creating SSL Rules, page 16-4.

Step 2 In the SSL rule editor, select the Cert Status tab.

The Cert Status tab appears.

Step 3 For each certificate status, you have the following options:

- Select **Yes** to match against the presence of that certificate status.
- Select **No** to match against the absence of that certificate status.
- Select **Do Not Match** to not match that certificate status.

Step 4 Add or continue editing 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.

Controlling Encrypted Traffic by Cipher Suite

License: Any

Cipher suite conditions in SSL rules allow you to handle and inspect encrypted traffic based on the cipher suite used to negotiate the encrypted session. Cisco provides predefined cipher suites you can add to a cipher suite rule condition. You can also add cipher suite list objects containing multiple cipher suites. For more information on cipher suite lists, see Working with Geolocation Objects, page 3-42.

Note You cannot add new cipher suites. You can neither modify nor delete predefined cipher suites.

You can add a maximum of 50 cipher suites and cipher suite lists to the **Selected Cipher Suites** in a single Cipher Suite condition.

Note the following:

- If you add cipher suites not supported for your deployment, you cannot apply the access control policy associated with the SSL policy. For example, passive deployments do not support decrypting traffic with the any of the ephemeral Diffie-Hellman (DHE) or ephemeral elliptic curve Diffie-Hellman (ECDHE) cipher suites. Creating a rule with these cipher suites prevents you from applying your access control policy.
- If you configure a cipher suite condition with a cipher suite, any external certificate objects you add to a certificate condition, or internal CA objects you associate with the **Decrypt - Resign** action, must match the cipher suite's signature algorithm type. For example, if your rule's cipher suite condition references an EC-based cipher suite, any server certificates you add, or CA certificates you associate with the **Decrypt - Resign** action, must also be EC-based. If you mismatch signature algorithm types in this case, the policy editor displays a warning icon next to the rule. For more information, see Controlling Encrypted Traffic by Cipher Suite, page 17-25 and Decrypt Actions: Decrypting Traffic for Further Inspection, page 16-10.
- 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 either the **Decrypt - Resign** or **Decrypt - Known Key** action in the rule, because the system cannot decrypt traffic encrypted with an anonymous cipher suite.

- When specifying a cipher suite as a rule condition, consider that the rule matches on the negotiated cipher suite in the ServerHello message, rather than on the full list of cipher suites specified in the ClientHello message. During ClientHello processing, the managed device strips unsupported cipher suites from the ClientHello message. However, if this results in all specified cipher suites being stripped, the system retains the original list. If the system retains unsupported cipher suites, subsequent evaluation results in an undecrypted session.

To inspect encrypted traffic by cipher suite:

Step 1 In the SSL policy where you want to control encrypted traffic by cipher suite, create a new SSL rule or edit an existing rule.

For detailed instructions, see Understanding and Creating SSL Rules, page 16-4.

Step 2 In the SSL rule editor, select the Cipher Suite tab.

The Cipher Suite tab appears.

Step 3 Find and select the cipher suites you want to add from the **Available Cipher Suites**, as follows;

- To add a cipher suite list on the fly, which you can then add to the condition, click the add icon ( ) above the **Available Cipher Suites** list; see Working with Geolocation Objects, page 3-42.
- To search for cipher suites and lists to add, click the **Search by name or value** prompt above the **Available Cipher Suites** list, then type either the name of the cipher suite, or a value in the cipher suite. The list updates as you type to display matching cipher suites.

To select a cipher suite, click it. To select multiple cipher suites, use the Shift and Ctrl keys, or right-click and then select **Select All**.

Step 4 Click **Add to Rule** to add the selected cipher suites to the **Selected Cipher Suites** list.

You can also drag and drop selected cipher suites.

Step 5 Add or continue editing 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.

Controlling Traffic by Encryption Protocol Version

License: Any

Session conditions in SSL rules allow you to inspect encrypted traffic based on the SSL or TLS version used to encrypt the traffic. You can choose to match against traffic encrypted with SSL version 3.0, or TLS version 1.0, 1.1, or 1.2. By default, all protocol versions are selected when you create a rule; if you select multiple versions, encrypted traffic that matches any of the selected versions matches the rule. You must select at least one protocol version when saving the rule condition.

Note You cannot select SSL v2.0 in a version rule condition; the ASA FirePOWER module does not support decrypting traffic encrypted with SSL version 2.0. You can configure an undecryptable action to allow or block this traffic without further inspection. For more information, see Logging Decryptable Connections with SSL Rules, page 36-14.

To inspect encrypted traffic by SSL or TLS version:

Step 1 In the SSL policy where you want to control encrypted traffic by encryption protocol version, create a new SSL rule or edit an existing rule.

For detailed instructions, see Understanding and Creating SSL Rules, page 16-4.

Step 2 In the SSL rule editor, select the Version tab.

The Version tab appears.

Step 3 Select the protocol versions you want to match against: **SSL v3.0**, **TLS v1.0**, **TLS v1.1**, or **TLS v1.2**.

Step 4 Add or continue editing 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.