CHAPTER 2

Managing Reusable Objects

For increased flexibility and ease-of-use, the ASA FirePOWER module allows you to create named *objects*, which are reusable configurations that associate a name with a value so that when you want to use that value, you can use the named object instead.

You can create the following types of objects:

- network-based objects that represent IP addresses and networks, port/protocol pairs, security zones, and origin/destination country (geolocation)
- objects that help you handle unencrypted and decrypted traffic, including Security Intelligence feeds and lists, application filters, URLs, file lists, and intrusion policy variable sets

You can use these objects in various places in the ASA FirePOWER module, including access control policies, network analysis policies, intrusion policies and rules, reports, dashboards, and so on.

Grouping objects allows you to reference multiple objects with a single configuration. You can group network, port, and URL, and public key infrastructure (PKI) objects.

Note In most cases, editing an object used in a policy requires redeploying your configuration for your changes to take effect.

For more information, see the following sections:

- Using the Object Manager, page 2-2
- Working with Network Objects, page 2-3
- Working with Security Intelligence Lists and Feeds, page 2-4
- Working with Port Objects, page 2-9
- Working with URL Objects, page 2-10
- Working with Application Filters, page 2-10
- Working with Variable Sets, page 2-13
- Working with Sinkhole Objects, page 2-27
- Working with File Lists, page 2-28
- Working with Security Zones, page 2-32
- Working with Cipher Suite Lists, page 2-32
- Working with Distinguished Name Objects, page 2-33
- Working with PKI Objects, page 2-35

- Working with Geolocation Objects, page 2-42
- Working with Security Group Tag Objects, page 2-43

Using the Object Manager

License: Any

Create and manage objects, including application filters, variable sets, and security zones, using the object manager (**Configuration > ASA FirePOWER Configuration > Object Management**). You can group network, port, and URL and PKI objects; you can also sort, filter, and browse the list of objects and object groups.

For more information, see:

- Grouping Objects, page 2-2
- Browsing, Sorting, and Filtering Objects, page 2-3

Grouping Objects

License: Any

You can group network, port, PKI, and URL objects. The system allows you to use objects and object groups interchangeably. For example, anywhere you would use a port object, you can also use a port object group. Objects and object groups of the same type cannot have the same name.

When you edit an object group used in a policy (for example, a network object group used in an access control policy), you must redeploy the configuration for your changes to take effect; see Deploying Configuration Changes, page 4-12.

Deleting a group does not delete the objects in the group, just their association with each other. Additionally, you cannot delete a group that is in use. For example, you cannot delete a URL group that you are using in a URL condition in a saved access control policy.

To group reusable objects:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Under the type of **Network**, **Port**, **URL**, **PKI,** or **Distinguished Name** object you want to group, choose **Object Groups**.

Step 3 Click the **Add** button that corresponds with the object you want to group.

Step 4 Enter a **Name** for the group. You can use any printable standard ASCII characters except curly braces (`{}`).

Step 5 Choose one or more objects and click **Add**.

- Use Shift and Ctrl to choose multiple objects, or right-click and **Select All**.
- Use the filter field (🔍) to search for existing objects to include, which updates as you type to display matching items. Click the reload icon (↻) above the search field or click the clear icon (✖) in the search field to clear the search string.
- Click the add icon (⊕) to create objects on the fly if no existing objects meet your needs.

Step 6 Click **Store ASA FirePOWER Changes**.

Browsing, Sorting, and Filtering Objects

License: Any

The object manager displays 20 objects or groups per page. If you have more than 20 of any type of object or group, use the navigation links at the bottom of the page to view additional pages. You can also go to a specific page or click the refresh icon (↻) to refresh your view.

By default, the page lists objects and groups alphabetically by name. However, you can sort each type of object or group by any column in the display. An up (▲) or down (▸) arrow next to a column heading indicates that the page is sorted by that column in that direction. You can also filter the objects on the page by name or value.

To sort objects or groups:

Step 1 Click a column heading. To sort in the opposite direction, click the heading again.

To filter objects or groups:

Step 1 Enter your filter criteria in the **Filter** field.

The page updates as you type to display matching items. The field accepts one or more asterisks (*) as wild cards.

Working with Network Objects

License: Any

A network object represents one or more IP addresses that you can specify either individually or as address blocks. You can use network objects and groups (see Grouping Objects, page 2-2) in various places in the ASA FirePOWER module, including access control policies, network variables, intrusion rules, reports, and so on.

You also cannot delete a network object that is in use. Additionally, after you edit a network object used in an access control or intrusion policy, you must redeploy policies for your changes to take effect.

To create a network object:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Under **Network**, choose **Individual Objects**.

Step 3 Click **Add Network**.

Step 4 Enter a **Name** for the network object. You can use any printable standard ASCII characters except curly braces (`{}`).

Step 5 For each IP address or address block you want to add to the network object, enter its value and click **Add**.

Step 6 Click **Store ASA FirePOWER Changes**.

Step 7 If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes, page 4-12.

Working with Security Intelligence Lists and Feeds

License: Protection

The Security Intelligence feature allows you to, per access control policy, specify the traffic that can traverse your network based on the source or destination IP address. This is especially useful if you want to blacklist — deny traffic to and from — specific IP addresses, before the traffic is subjected to analysis by access control rules. Similarly, you can add IP addresses to the whitelist to force the system to handle their connections using access control.

If you are not sure whether you want to blacklist a particular IP address, you can use a “monitor-only” setting, which allows the system to handle the connection using access control, but also logs the connection’s match to the blacklist.

A *global whitelist* and *global blacklist* are included by default in every access control policy, and apply to any zone. Additionally, within each access control policy, you can build a separate whitelist and blacklist using a combination of network objects and groups as well as Security Intelligence lists and feeds, all of which you can constrain by security zone.

Comparing Feeds and Lists

A Security Intelligence *feed* is a dynamic collection of IP addresses that the system downloads from an HTTP or HTTPS server at the interval you configure. Because feeds are regularly updated, the system can use up-to-date information to filter your network traffic. To help you build blacklists, the ASA FirePOWER module provides the *Intelligence Feed*, which represents IP addresses determined by the VRT to have a poor reputation.

Although it may take a few minutes for a feed update to take effect, you do not have to deploy policies after you create or modify a feed, or after a scheduled feed update.

Note If you want strict control over when the system downloads a feed from the Internet, you can disable automatic updates for that feed. However, Cisco recommends that you allow automatic updates. Although you can manually perform on-demand updates, allowing the system to download feeds on a regular basis provides you with the most up-to-date, relevant data.

In contrast with a feed, a Security Intelligence *list* is a simple static list of IP addresses that you manually upload to the system. Use custom lists to augment and fine-tune feeds and the global whitelist and blacklist. Note that editing custom lists (as well as editing network objects and removing IP addresses from the global whitelist or blacklist) require you to redeploy the configuration for your changes to take effect.

Formatting and Corrupt Feed Data

Feed and list source must be a simple text file no larger than 500MB, with one IP address or address block per line. Comment lines must start with the `#` character. List source files must use the `.txt` extension.

If the system downloads a corrupt feed or a feed with no recognizable IP addresses, the system continues using the old feed data (unless it is the first download). However, if the system can recognize even one IP address in the feed, it updates the addresses it can recognize.

Internet Access and High Availability

The system uses port 443/HTTPS to download the Intelligence Feed, and either 443/HTTP or 80/HTTP to download custom or third-party feeds. To update feeds, you must open the appropriate port, both inbound and outbound, on the device. If your system does not have direct access to the feed site, it can use a proxy server.

Note The system does **not** perform peer SSL certificate verification when downloading custom feeds, nor does the system support the use of certificate bundles or self-signed certificates to verify the remote peer.

Managing Feeds and Lists

You create and manage Security Intelligence lists and feeds, collectively called Security Intelligence objects, using the object manager's Security Intelligence page.

Note that you cannot delete a custom list or feed that is currently being used in a saved or applied access control policy. You also cannot delete a global list, although you can remove individual IP addresses. Similarly, although you cannot delete the Intelligence Feed, editing it allows you to disable or change the frequency of its updates.

Security Intelligence Object Quick Reference

The following table provides a quick reference to the objects you can use to perform Security Intelligence filtering.

Table 2-1 Security Intelligence Object Capabilities

Capability	Global Whitelist or Blacklist	Intelligence Feed	Custom Feed	Custom List	Network Object
method of use	in access control policies by default	in any access control policy as either a whitelist or blacklist object			
can be constrained by security zone?	no	yes	yes	yes	yes
can be deleted?	no	no	yes, unless currently being used in a saved or applied access control policy		
object manager edit capabilities	delete IP addresses only	disable or change update frequency	fully modify	upload a modified list only	fully modify
requires configuration redeployment when modified?	yes when deleting (adding IP addresses does not require redeploy)	no	no	yes	yes

For more information on creating, managing, and using Security Intelligence lists and feeds, see:

- Working with the Global Whitelist and Blacklist, page 2-6
- Working with the Intelligence Feed, page 2-6
- Working with Custom Security Intelligence Feeds, page 2-7
- Manually Updating Security Intelligence Feeds, page 2-7
- Working with Custom Security Intelligence Lists, page 2-8
- Blacklisting Using Security Intelligence IP Address Reputation, page 5-1

Working with the Global Whitelist and Blacklist

License: Protection

The system's global whitelist and blacklist are included by default in every access control policy, and apply to any zone. You can opt not to use these global lists on a per-policy basis.

You do not have to redeploy your configuration after adding an IP address to a global list. Conversely, after you delete IP addresses from the global whitelist or blacklist, you must redeploy your configuration for your changes to take effect.

Note that although you can add network objects with a netmask of /0 to the whitelist or blacklist, address blocks using a `/0` netmask in those objects are ignored and whitelist and blacklist filtering does not occur based on those addresses. Address blocks with a `/0` netmask from security intelligence feeds is also ignored. If you want to monitor or block all traffic targeted by a policy, instead of security intelligence filtering, use an access control rule with the **Monitor** or **Block** rule action, respectively, and a default value of **any** for the **Source Networks** and **Destination Networks**.

To remove IP addresses from the global whitelist or blacklist:

Step 1 On the object manager's Security Intelligence page, next to the global whitelist or blacklist, click the edit icon (✏).

Step 2 Next to the IP addresses you want to remove from the list, click the delete icon (🗑).

To delete multiple IP addresses at once, use the Shift and Ctrl keys to choose them, then right-click and choose **Delete**.

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

Step 4 If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes, page 4-12.

Working with the Intelligence Feed

License: Protection

To help you build blacklists, the ASA FirePOWER module provides the Intelligence Feed, which is comprised of several regularly updated lists of IP addresses determined by the VRT to have a poor reputation. Each list in the feed represents a specific category: open relays, known attackers, bogus IP addresses (bogon), and so on. In an access control policy, you can blacklist any or all of the categories.

Because the intelligence feed is regularly updated, the system can use up-to-date information to filter your network traffic. Malicious IP addresses that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and deploy new policies.

Although you cannot delete the Intelligence Feed, editing it allows you to change the frequency of its updates. By default, the feed updates every two hours.

To modify the intelligence feed's update frequency:

Step 1 On the object manager's Security Intelligence page, next to the Intelligence Feed, click the edit icon (✏).

Step 2 Edit the **Update Frequency**.

You can choose various intervals from two hours to one week. You can also disable feed updates.

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

Working with Custom Security Intelligence Feeds

License: Protection

Custom or third-party Security Intelligence feeds allow you to augment the Intelligence Feed with other regularly-updated reputable whitelists and blacklists on the Internet. You can also set up an internal feed.

When you configure a feed, you specify its location using a URL; the URL cannot be Punycode-encoded. By default, the system downloads the entire feed source on the interval you configure.

Optionally, you can configure the system to use an md5 checksum to determine whether to download an updated feed. If the checksum has not changed since the last time the module downloaded the feed, the system does not need to re-download it. You may want to use md5 checksums for internal feeds, especially if they are large. The md5 checksum must be stored in a simple text file with only the checksum. Comments are not supported.

To configure a Security Intelligence feed:

Step 1 On the object manager's Security Intelligence page, click **Add Security Intelligence**.

Step 2 Enter a **Name** for the feed. You can use any printable standard ASCII characters except curly braces (`{}`).

Step 3 From the **Type** drop-down list, specify that you want to configure a **Feed**.

Step 4 Specify a **Feed URL** and optionally, an **MD5 URL**.

Step 5 Specify an **Update Frequency**.

You can choose various intervals from two hours to one week. You can also disable feed updates.

Step 6 Click **Store ASA FirePOWER Changes**.

The Security Intelligence feed object is created. Unless you disabled feed updates, the system attempts to download and verify the feed. You can now use the feed object in access control policies.

Manually Updating Security Intelligence Feeds

License: Protection

Manually updating Security Intelligence feeds updates all feeds, including the Intelligence Feed.

To update all Security Intelligence feeds:

Step 1 On the object manager's Security Intelligence page, click **Update Feeds**.

Step 2 Confirm that you want to update all feeds.

The system warns that it can take several minutes for the update to take effect.

Step 3 Click **OK**.

After the system downloads and verifies the feed updates, it begins filtering traffic using the updated feeds.

Working with Custom Security Intelligence Lists

License: Protection

A Security Intelligence list is a simple static list of IP addresses and address blocks that you manually upload. Custom lists are useful if you want to augment and fine-tune feeds or one of the global lists.

Note that netmasks for address blocks can be integers from `0` to `32` or `0` to `128,` for IPv4 and IPv6, respectively.

For example, if a reputable feed improperly blocks your access to vital resources but is overall useful to your organization, you can create a custom whitelist that contains only the improperly classified IP addresses, rather than removing the Security Intelligence feed object from the access control policy's blacklist.

Note that to modify a Security Intelligence list, you must make your changes to the source file and upload a new copy. For more information, see Updating a Security Intelligence List, page 2-8.

To upload a new Security Intelligence list:

Step 1 On the object manager's Security Intelligence page, click **Add Security Intelligence**.

Step 2 Enter a **Name** for the list. You can use any printable standard ASCII characters except curly braces (`{}`).

Step 3 From the **Type** drop-down list, specify that you want to upload a **List**.

Step 4 Click **Browse** to browse to the list`.txt` file, then click **Upload**.

The list is uploaded. The pop-up window displays the total number of IP addresses and address blocks that the system found in the list.

If the number is not what you expected, check the formatting of the file and try again.

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

Updating a Security Intelligence List

License: Protection

To edit a Security Intelligence list, you must make your changes to the source file and upload a new copy. You cannot modify the file's contents using ASDM. If you do not have access to the source file, you can download a copy using the ASDM interface.

To modify a Security Intelligence list:

Step 1 On the object manager's Security Intelligence page, next to the list you want to update, click the edit icon (✎).

Step 2 If you need a copy of the list to edit, click **Download**, then follow the prompts to save the list as a text file.

Step 3 Make changes to the list as necessary.

Step 4 On the Security Intelligence pop-up window, click **Browse** to browse to the modified list, then click **Upload**.

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

Step 6 If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes, page 4-12.

Working with Port Objects

License: Any

Port objects represent different protocols in slightly different ways:

- For TCP and UDP, a port object represents the transport layer protocol, with the protocol number in parentheses, plus an optional associated port or port range. For example: `TCP(6)/22`.
- For ICMP and ICMPv6 (IPv6-ICMP), the port object represents the internet layer protocol plus an optional type and code. For example: `ICMP(1):3:3`.
- A port object can also represent other protocols that do not use ports.

Note that the system provides default port objects for well-known ports. You can modify or delete these objects, but Cisco recommends that you create custom port objects instead.

You can use port objects and groups (see Grouping Objects, page 2-2) in various places in the ASA FirePOWER module, including access control policies and port variables.

You cannot delete a port object that is in use. Additionally, after you edit or delete a port object, if an active policy references the object, you must redeploy your configuration for the changes to take effect; see Deploying Configuration Changes, page 4-12.

Note that you cannot add any protocol other than TCP or UDP for source port conditions in access control rules. Also, you cannot mix transport protocols when setting both source and destination port conditions in a rule.

If you add an unsupported protocol to a port object group used in a source port condition, the rule where it is used does not apply on policy deploy. Additionally, if you create a port object containing both TCP and UDP ports, then add it as a source port condition in a rule, you cannot add a destination port, and vice versa.

To create a port object:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Under **Port**, choose **Individual Objects**.

Step 3 Click **Add Port**.

Step 4 Enter a **Name** for the port object. You can use any printable standard ASCII characters except curly braces (`{}`).

Step 5 Choose a **Protocol**.

You can quickly choose **TCP**, **UDP**, **IP**, **ICMP**, or **IPv6-ICMP**, or you can use the **Other** drop-down list to choose either a different protocol or **All** protocols.

Step 6 Optionally, restrict a TCP or UDP port object using a **Port** or port range.

You can specify any port from 1 to 65535 or `any` to match all ports. Use a hyphen to specify a range of ports.

Step 7 Optionally, restrict an ICMP or IPV6-ICMP port object using a **Type** and, if appropriate, a related **Code**.

When you create an ICMP or IPv6-ICMP object, you can specify the type and, if applicable, the code. For more information on ICMP types and codes, see http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml and http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml. You can set the type to any to match any type or set the code to any to match any code for the specified type.

Step 8 Optionally, choose **Other** and a protocol from the drop-down list. If you choose **All** protocols, enter a port number in the **Port** field.

Step 9 Click **Store ASA FirePOWER Changes**.

Working with URL Objects

License: Any

Each URL object you configure represents a single URL or IP address. You can use URL objects and groups (see Grouping Objects, page 2-2) in access control policies. For example, you could write an access control rule that blocks a specific URL.

Note that to block HTTPS traffic, you can enter the URL from the Secure Sockets Layer (SSL) certificate for the traffic. When entering a URL from a certificate, enter the domain name and omit subdomain information. (For example, type `example.com` rather than `www.example.com`.) If you block traffic based on the certificate URL, both HTTP and HTTPS traffic to that website are blocked.

You cannot delete a URL object that is in use. Additionally, after you edit or delete a URL object, if an active policy references the object, you must redeploy your configuration for the changes to take effect; see Deploying Configuration Changes, page 4-12.

To create a URL object:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Under **URL**, choose **Individual Objects**.

Step 3 Click **Add URL**.

Step 4 Enter a **Name** for the URL object. You can use any printable standard ASCII characters except curly braces (`{}`).

Step 5 Enter the **URL** or IP address for the URL object.

Step 6 Click **Store ASA FirePOWER Changes**.

Working with Application Filters

License: Any

When the ASA FirePOWER module analyzes IP traffic, it attempts to identify the commonly used applications on your network. Application awareness is crucial to performing application-based access control. The system is delivered with detectors for many applications, and Cisco frequently updates and adds additional detectors via system and vulnerability database (VDB) updates.

Application filters group applications according to criteria associated with the applications' risk, business relevance, type, categories, and tags. Using application filters allows you to quickly create application conditions for access control rules because you do not have to search for and add applications individually; for more information, see Matching Traffic with Application Filters, page 8-3.

Another advantage to using application filters is that you do not have to update access control rules that use filters when you modify or add new applications. For example, if you configure your access control policy to block all social networking applications, and a VDB update includes a new social networking application detector, the policy is updated when you update the VDB. Although you must redeploy the changed configuration before the system can block the new application, you do not have to update the access control rule that blocks the application.

If the system-provided application filters do not group applications according to your needs, you can create your own filters. User-defined filters can group and combine system-provided filters. For example, you could create a filter that would allow you to block all very high risk, low business relevance applications. You can also create a filter by manually specifying individual applications, although you should keep in mind those filters do **not** automatically update when you update the module software or the VDB.

As with system-provided application filters, you can use user-defined application filters in access control rules.

You use the object manager (**Configuration > ASA FirePOWER Configuration > Object Management**) to create and manage application filters. Note that you can also create an application filter on the fly while adding an application condition to an access control rule.

The Application Filters list contains the system-provided application filters that you can choose to build your own filter. You can constrain the filters that appear by using a search string; this is especially useful for categories and tags.

The Available Applications list contains the individual applications in the filters you select. You can also constrain the applications that appear by using a search string.

The system links multiple filters of the same filter type with an OR operation. Consider a scenario where the medium risk filter contains 100 applications and the high risk filter contains 50 applications. If you choose both filters, the system would display 150 available applications.

The system links different types of filters with an AND operation. For example, if you choose the medium and high risk filters and the medium and high business relevance filters, the system displays the applications that have medium or high risk, and also have medium or high business relevance.

Tip Click an information icon (ℹ) for more information about the associated application. To display additional information, click any of the Internet search links in the information pop-up.

After you determine the applications you want to add to the filter, you can add them either individually, or, if you chose an application filter, **All apps matching the filter**. You can add multiple filters and multiple applications, in any combination, as long as the total number of items in the Selected Applications and Filters list does not exceed 50.

After you create the application filter, it is listed on the Application Filters page of the object manager. The page displays the total number of conditions that comprise each filter.

For information on sorting and filtering the application filters that appear, see Using the Object Manager, page 2-2. Note that you cannot delete an application filter that is in use. Additionally, after you edit or delete an application filter object, if an active policy references the object, you must redeploy your configuration for the changes to take effect; see Deploying Configuration Changes, page 4-12.

To create an application filter:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Click **Application Filters**.

Step 3 Click **Add Application Filter**.

Step 4 Enter a **Name**. You can use any printable standard ASCII characters except curly braces (`{}`).

Step 5 Optionally, use system-provided filters in the **Application Filters** list to narrow the list of applications you want to add to the filter:

- Click the arrow next to each filter type to expand and collapse the list.
- Right-click a filter type and click **Check All** or **Uncheck All**. Note that the list indicates how many filters you have selected of each type.
- To narrow the filters that appear, enter a search string in the **Search by name** field; this is especially useful for categories and tags. To clear the search, click the clear icon (✖).
- To refresh the filters list and clear any selected filters, click the reload icon (↻).
- To clear all filters and search fields, click **Clear All Filters**.

The applications that match the filters you select appear in the Available Applications list. The list displays 100 applications at a time.

Step 6 Choose the applications that you want to add to the filter from the **Available Applications** list:

- Choose **All apps matching the filter** to add all the applications that meet the constraints you specified in the previous step.
- To narrow the individual applications that appear, enter a search string in the **Search by name** field. To clear the search, click the clear icon (✖).
- Use the paging icons at the bottom of the list to browse the list of individual available applications.
- Use Shift and Ctrl keys to choose multiple individual applications. Right-click to **Select All** currently displayed individual applications.
- To refresh the applications list and clear any selected applications, click the reload icon (↻).

You cannot choose individual applications and **All apps matching the filter** at the same time.

Step 7 Add the selected applications to the filter. You can click and drag, or you can click **Add to Rule**.

The result is the combination of:

- the selected Application Filters
- either the selected individual Available Applications, or **All apps matching the filter**

You can add up to 50 applications and filters to the filter. To delete an application or filter from the selected applications, click the appropriate delete icon (🗑). You can also select one or more applications and filters, or right click to **Select All**, then right-click to **Delete Selected**.

Step 8 Click **Store ASA FirePOWER Changes**.

Working with Variable Sets

License: Protection

Variables represent values commonly used in intrusion rules to identify source and destination IP addresses and ports. You can also use variables in intrusion policies to represent IP addresses in rule suppressions, adaptive profiles, and dynamic rule states.

Tip Preprocessor rules can trigger events regardless of the hosts defined by network variables used in intrusion rules.

You use variable sets to manage, customize, and group your variables. You can use the default variable set provided by the ASA FirePOWER module or create your own custom sets. Within any set you can modify predefined default variables and add and modify user-defined variables.

Most of the shared object rules and standard text rules that the ASA FirePOWER module provides use predefined default variables to define networks and port numbers. For example, the majority of the rules use the variable `$HOME_NET` to specify the protected network and the variable `$EXTERNAL_NET` to specify the unprotected (or outside) network. In addition, specialized rules often use other predefined variables. For example, rules that detect exploits against web servers use the `$HTTP_SERVERS` and `$HTTP_PORTS` variables.

Rules are more effective when variables more accurately reflect your network environment. At a minimum, you should modify default variables in the default set as described in Optimizing Predefined Default Variables, page 2-13. By ensuring that a variable such as `$HOME_NET` correctly defines your network and `$HTTP_SERVERS` includes all web servers on your network, processing is optimized and all relevant systems are monitored for suspicious activity.

To use your variables, you link variable sets to intrusion policies associated with access control rules or with the default action of an access control policy. By default, the default variable set is linked to all intrusion policies used by access control policies.

See the following sections for more information:

- Optimizing Predefined Default Variables, page 2-13
- Understanding Variable Sets, page 2-15
- Managing Variable Sets, page 2-17
- Managing Variables, page 2-18
- Adding and Editing Variables, page 2-20
- Resetting Variables, page 2-25
- Linking Variable Sets to Intrusion Policies, page 2-26
- Understanding Advanced Variables, page 2-27

Optimizing Predefined Default Variables

License: Protection

By default, the ASA FirePOWER module provides a single default variable set, which is comprised of predefined default variables. The Vulnerability Research Team (VRT) uses rule updates to provide new and updated intrusion rules and other intrusion policy elements, including default variables. See Importing Rule Updates and Local Rule Files, page 46-9 for more information.

Because many intrusion rules provided by the ASA FirePOWER module use predefined default variables, you should set appropriate values for these variables. Depending on how you use variable sets to identify traffic on your network, you can modify the values for these default variables in any or all variable sets. See Adding and Editing Variables, page 2-20 for more information.

Caution Importing an access control or an intrusion policy overwrites existing default variables in the default variable set with the imported default variables. If your existing default variable set contains a custom variable not present in the imported default variable set, the unique variable is preserved. For more information, see Importing Configurations, page B-3.

The following table describes the variables provided by the ASA FirePOWER module and indicates which variables you typically would modify. For assistance determining how to tailor variables to your network, contact Professional Services or Support.

Table 2-2 Variables Provided by the ASA FirePower Module

Variable Name	Description	Modify?
`$AIM_SERVERS`	Defines known AOL Instant Messenger (AIM) servers, and is used in chat-based rules and rules that look for AIM exploits.	Not required.
`$DNS_SERVERS`	Defines Domain Name Service (DNS) servers. If you create a rule that affects DNS servers specifically, you can use the `$DNS_SERVERS` variable as a destination or source IP address.	Not required in current rule set.
`$EXTERNAL_NET`	Defines the network that the ASA FirePOWER module views as the unprotected network, and is used in many rules to define the external network.	Yes, you should adequately define `$HOME_NET` and then exclude `$HOME_NET` as the value for `$EXTERNAL_NET`.
`$FILE_DATA_PORTS`	Defines non-encrypted ports used in intrusion rules that detect files in a network stream.	Not required.
`$FTP_PORTS`	Defines the ports of FTP servers on your network, and is used for FTP server exploit rules.	Yes, if your FTP servers use ports other than the default ports (you can view the default ports in the module interface).
`$GTP_PORTS`	Defines the data channel ports where the packet decoder extracts the payload inside a GTP (General Packet Radio Service [GPRS] Tunneling Protocol) PDU.	Not required.
`$HOME_NET`	Defines the network that the associated intrusion policy monitors, and is used in many rules to define the internal network.	Yes, to include the IP addresses for your internal network.
`$HTTP_PORTS`	Defines the ports of web servers on your network, and is used for web server exploit rules.	Yes, if your web servers use ports other than the default ports (you can view the default ports in the module interface).
`$HTTP_SERVERS`	Defines the web servers on your network. Used in web server exploit rules.	Yes, if you run HTTP servers.
`$ORACLE_PORTS`	Defines Oracle database server ports on your network, and is used in rules that scan for attacks on Oracle databases.	Yes, if you run Oracle servers.
`$SHELLCODE_PORTS`	Defines the ports you want the system to scan for shell code exploits, and is used in rules that detect exploits that use shell code.	Not required.

Table 2-2 Variables Provided by the ASA FirePower Module (continued)

Variable Name	Description	Modify?
`$SIP_PORTS`	Defines the ports of SIP servers on your network, and is used for SIP exploit rules.	Not required.
`$SIP_SERVERS`	Defines SIP servers on your network, and is used in rules that address SIP-targeted exploits.	Yes, if you run SIP servers, you should adequately define `$HOME_NET` and then include `$HOME_NET` as the value for `$SIP_SERVERS`.
`$SMTP_SERVERS`	Defines SMTP servers on your network, and is used in rules that address exploits that target mail servers.	Yes, if you run SMTP servers.
`$SNMP_SERVERS`	Defines SNMP servers on your network, and is used in rules that scan for attacks on SNMP servers.	Yes, if you run SNMP servers.
`$SNORT_BPF`	Identifies a legacy advanced variable that appears only when it existed on your system in a ASA FirePOWER module software release before Version 5.3.0 that you subsequently upgraded to Version 5.3.0 or greater. See Understanding Advanced Variables, page 2-27.	No, you can only view or delete this variable. You cannot edit it or recover it after deleting it.
`$SQL_SERVERS`	Defines database servers on your network, and is used in rules that address database-targeted exploits.	Yes, if you run SQL servers.
`$SSH_PORTS`	Defines the ports of SSH servers on your network, and is used for SSH server exploit rules.	Yes, if your SSH servers use ports other than the default port (you can view the default ports in the module interface).
`$SSH_SERVERS`	Defines SSH servers on your network, and is used in rules that address SSH-targeted exploits.	Yes, if you run SSH servers, you should adequately define `$HOME_NET` and then include `$HOME_NET` as the value for `$SSH_SERVERS`.
`$TELNET_SERVERS`	Defines known Telnet servers on your network, and is used in rules that address Telnet server-targeted exploits.	Yes, if you run Telnet servers.
`$USER_CONF`	Provides a general tool that allows you to configure one or more features not otherwise available via the module interface. See Understanding Advanced Variables, page 2-27. ⚠ **Caution** Conflicting or duplicate `$USER_CONF` configurations will halt the system. See Understanding Advanced Variables, page 2-27.	No, only as instructed in a feature description or with the guidance of Support.

Understanding Variable Sets

License: Protection

Adding a variable to any set adds it to all sets; that is, each variable set is a collection of all variables currently configured on your system. Within any variable set, you can add user-defined variables and customize the value of any variable.

Initially, the ASA FirePOWER module provides a single, default variable set comprised of predefined default values. Each variable in the default set is initially set to its default value, which for a predefined variable is the value set by the VRT and provided in rule updates.

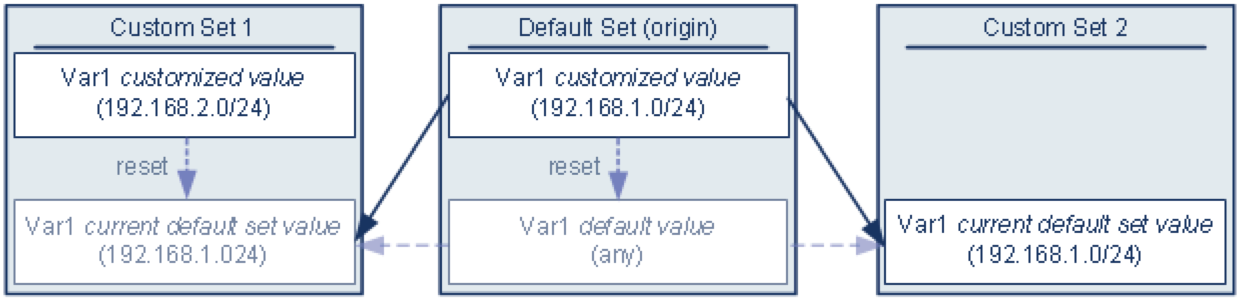
Although you can leave predefined default variables configured to their default values, Cisco recommends that you modify a subset of predefined variables as described in Optimizing Predefined Default Variables, page 2-13.

You could work with variables only in the default set, but in many cases you can benefit most by adding one or more custom sets, configuring different variable values in different sets, and perhaps even adding new variables.

When using multiple sets, it is important to remember that the *current value* of any variable in the default set determines the *default value* of the variable in all other sets.

Example: Adding a User-Defined Variable to the Default Set

The following diagram illustrates set interactions when you add the user-defined variable `Var1` to the default set with the value `192.168.1.0/24`.



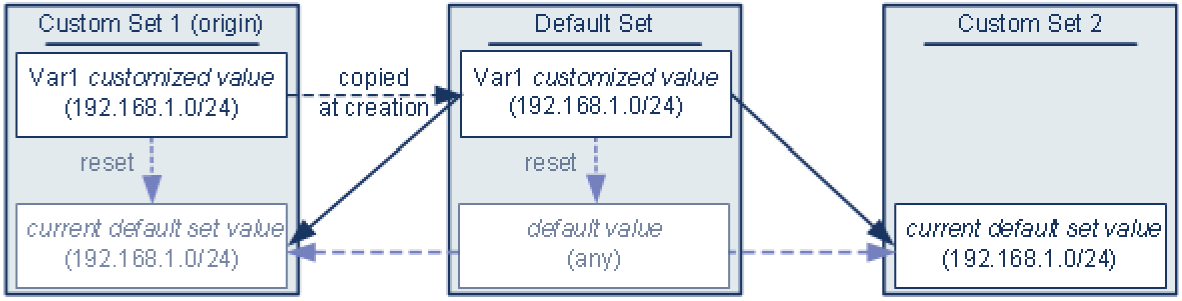
Optionally, you can customize the value of `Var1` in any set. In Custom Set 2 where `Var1` has not been customized, its value is `192.168.1.0/24`. In Custom Set 1 the customized value `192.168.2.0/24` of `Var1` overrides the default value. Resetting a user-defined variable in the default set resets its default value to `any` in all sets.

It is important to note in this example that, if you do not update `Var1` in Custom Set 2, further customizing or resetting `Var1` in the default set consequently updates the current, default value of `Var1` in Custom Set 2, thereby affecting any intrusion policy linked to the variable set.

Although not shown in the example, note that interactions between sets are the same for user-defined variables and default variables except that resetting a default variable in the default set resets it to the value configured by the system in the current rule update.

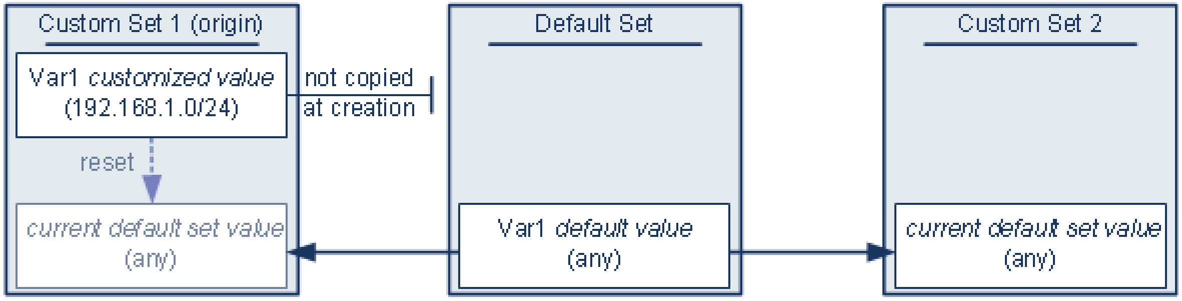
Examples: Adding a User-Defined Variable to a Custom Set

The next two examples illustrate variable set interactions when you add a user-defined variable to a custom set. When you save the new variable, you are prompted whether to use the configured value as the default value for other sets. In the following example, you elect **to use** the configured value.



Note that, except for the origin of `Var1` from Custom Set 1, this example is identical to the example above where you added `Var1` to the default set. Adding the customized value `192.168.1.0/24` for `Var1` to Custom Set 1 copies the value to the default set as a customized value with a default value of `any`. Thereafter, `Var1` values and interactions are the same as if you had added `Var1` to the default set. As with the previous example, keep in mind that further customizing or resetting `Var1` in the default set consequently updates the current, default value of `Var1` in Custom Set 2, thereby affecting any intrusion policy linked to the variable set.

In the next example, you add `Var1` with the value 192.168.1.0/24 to Custom Set 1 as in the previous example, but you elect **not to use** the configured value of `Var1` as the default value in other sets.



This approach adds `Var1` to all sets with a default value of `any`. After adding `Var1`, you can customize its value in any set. An advantage of this approach is that, by not initially customizing `Var1` in the default set, you decrease your risk of customizing the value in the default set and thus inadvertently changing the current value in a set such as Custom Set 2 where you have not customized `Var1`.

Managing Variable Sets

License: Protection

When you choose **Variable Sets** on the Object Manager page (**Configuration > ASA FirePOWER Configuration > Object Management**), the object manager lists the default variable set and any custom sets you created.

On a freshly installed system, the default variable set is comprised only of the default system-provided variables.

Each variable set includes the system-provided default variables and all custom variables you have added from any variable set. Note that you can edit the default set, but you cannot rename or delete the default set.

The following table summarizes the actions you can take to manage your variable sets.

Table 2-3 Variable Set Management Actions

To...	You can...
display your variable sets	choose **Configuration > ASA FirePOWER Configuration > Object Management**, then choose **Variable Set**.
filter variable sets by name	begin entering a name; as you type, the page refreshes to display matching names.
clear name filtering	click the clear icon (✖) in the filter field.
add a custom variable set	click **Add Variable Set**. For your convenience, new variable sets contain all currently defined default and customized variables.
edit a variable set	click the edit icon (✏) next to the variable set you want to edit. **Tip** You can also right-click within the row for a variable set, then choose **Edit**.
delete a custom variable set	click the delete icon (🗑) next to the variable set, then click **Yes**. You cannot delete the default variable set. Note that variables created in a variable set you delete are not deleted or otherwise affected in other sets. **Tip** You can also right-click within the row for a variable set, choose **Delete**, then click **Yes**. Use the Ctrl and Shift keys to choose multiple sets.

After you configure variable sets, you can link them to intrusion policies.

To create or edit a variable set:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Choose **Variable Set**.

Step 3 Create a variable set or edit an existing set:

- To create a variable set, click **Add Variable Set**.
- To create a variable set, click the edit icon (✏) next to the variable set.

See Adding and Editing Variables, page 2-20 for information on adding and editing variables within a variable set.

Step 4 If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes, page 4-12.

Managing Variables

License: Protection

You manage variables on the new or edit variables page within a variable set. The variables page for all variable sets separates variables into Customized Variables and Default Variables page areas.

A *default variable* is a variable provided by the ASA FirePOWER module. You can customize the value of a default variable. You cannot rename or delete a default variable, and you cannot change its default value.

A *customized variable* is one of the following:

- customized default variables

When you edit the value for a default variable, the system moves the variable from the Default Variables area to the Customized Variables area. Because variable values in the default set determine the default values of variables in custom sets, customizing a default variable in the default set modifies the default value of the variable in all other sets.

- user-defined variables

  You can add and delete your own variables, customize their values within different variable sets, and reset customized variables to their default values. When you reset a user-defined variable, it remains in the Customized Variables area.

The following table summarizes the actions you can take to create or edit variables.

Table 2-4 Variable Management Actions

To...	You can...
display the variables page	on the variable sets page, click **Add Variable Set** to create a new variable set, or click the edit icon (✏) next to the variable set you want to edit.
name and, optionally, describe your variable set	enter an alphanumeric string including spaces and special characters in the **Name** and **Description** fields.
add a variable	click **Add**. See Adding and Editing Variables, page 2-20 for more information.
edit a variable	click the edit icon (✏) next to the variable you want to edit. See Adding and Editing Variables, page 2-20 for more information.
reset a modified variable to its default value	click the reset icon (↩) next to a modified variable. A shaded reset icon indicates that the current value is already the default value.
delete a user-defined customized variable	click the delete icon (🗑) next to the variable set; if you have saved the variable set since adding the variable, then click **Yes** to confirm that you want to delete the variable. You cannot delete default variables, and you cannot delete user-defined variables that are used by intrusion rules or other variables.
save changes to a variable set	click **Store ASA FirePOWER Changes**, then click **Yes** if the variable set is in use by an access control policy to confirm that you want to save your changes. Because the current value in the default set determines the default value in all other sets, modifying or resetting a variable in the default set changes the current value in other sets where you have not customized the default value.

To view the variables in a variable set:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Choose **Variable Set**.

Step 3 Create a variable set or edit an existing set:

- To create a variable set, click **Add Variable Set**.
- To create a variable set, click the edit icon (✏) next to the variable set.

Step 4 Create a variable or edit an existing variable:

- To create a variable, click **Add**.
- To edit a variable, click the edit icon (✏) next to the variable.

See Adding and Editing Variables, page 2-20 for information on adding and editing variables within a variable set.

Adding and Editing Variables

License: Protection

You can modify variables in any custom set.

If you create custom standard text rules, you might also want to create your own user-defined variables to more accurately reflect your traffic or as shortcuts to simplify the rule creation process. For example, if you create a rule that you want to inspect traffic in the "demilitarized zone" (or DMZ) only, you can create a variable named `$DMZ` whose value lists the server IP addresses that are exposed. You can then use the `$DMZ` variable in any rule written for this zone.

Adding a variable to a variable set adds it to all other sets. With one exception as explained below, the variable is added to other sets as the default value, which you can then customize.

When you add a variable from a custom set, you must choose whether to use the configured value as the customized value in the default set.

- If you **do use** the configured value (for example, 192.168.0.0/16), the variable is added to the default set using the configured value as a customized value with a default value of `any`. Because the current value in the default set determines the default value in other sets, the initial, default value in other custom sets is the configured value (which in the example is 192.168.0.0/16).
- If you **do not use** the configured value, the variable is added to the default set using only the default value `any` and, consequently, the initial, default value in other custom sets is `any`.

See Understanding Variable Sets, page 2-15 for more information.

You add variables within a variable set on the New Variable page and edit existing variables on the Edit Variable page. You use the two pages identically except that when you edit an existing variable you cannot change the variable name or variable type.

Each page consists mainly of three windows:

- available items, including existing network or port variables, objects, and network object groups
- networks or ports to include in the variable definition
- networks or ports to exclude from the variable definition

You can create or edit two types of variables:

- *network* variables specify the IP addresses of hosts in your network traffic. See Working with Network Variables, page 2-23.
- *port* variables specify TCP or UDP ports in network traffic, including the value `any` for either type. See Working with Port Variables, page 2-24.

When you specify whether you want to add a network or port variable type, the page refreshes to list available items. A search field above the list allows you to constrain the list, which updates as you type.

You can select and drag available items the list of items to include or exclude. You can also select items and click the **Include** or **Exclude** button. Use the Ctrl and Shift keys to choose multiple items. You can use the configuration field below the list of included or excluded items to specify literal IP addresses and address blocks for network variables, and ports and port ranges for port variables.

A list of items to include or exclude can be comprised of any combination of literal strings and existing variables, objects, and network object groups in the case of network variables.

The following table summarizes the actions you can take to create or edit your variables.

Table 2-5 Variable Edit Actions

To...	You can...
display the variables page	on the variable sets page, click **Add** to add a new variable, or click the edit icon (✎) next to an existing variable.
name your variable	in the **Name** field, enter a unique, case-sensitive alphanumeric string that includes no special characters other than the underscore character (_). Note that variable names are case-sensitive; for example, `var` and `Var` are each unique.
specify a network or port variable	choose **Network** or **Port** from the **Type** drop-down list. See Working with Network Variables, page 2-23 and Working with Port Variables, page 2-24 for detailed information on how you can use and configure network and port variables.
add an individual network object so you can then choose it from the list of available networks	choose **Network** from the **Type** drop-down list, then click the add icon (⊕). See Working with Network Objects, page 2-3 for information on adding network objects using the object manager.
add an individual port object so you can then choose it from the list of available ports	choose **Port** from the **Type** drop-down list, then click the add icon (⊕). Although you can add any port type, only TCP and UDP ports, including the value `any` for either type, are valid variable values, and the list of available ports only displays variables that use these value types. See Working with Port Objects, page 2-9 for information on adding port objects using the object manager.
search for available port or network items by name	begin entering a name in the search field above the list of available items; as you type, the page refreshes to display matching names.
clear name searching	click the reload icon (↻) above the search field or the clear icon (✕) in the search field.
differentiate between available items	look for items next to the variables icon ($), network object icon (🖥), port icon (🔧), and object group icon (❐). Note that only network groups, not port groups, are available.
choose objects to include or exclude in the variable definition	click the object in the list of available networks or ports; use the Ctrl and Shift keys to choose multiple objects.
add selected items to the list of included or excluded networks or ports	drag and drop selected items. Alternately, click **Include** or **Exclude**. You can add network and port variables and objects from the list of available items. You can also add network object groups.
add a literal network or port to the list of networks or ports to include or exclude	click to remove the prompt from the literal **Network** or **Port** field, enter the literal IP address or address block for network variables, or the literal port or port range for port variables, then click **Add**. Note that you cannot enter domain names or lists; to add multiple items, add each individually.
add a variable with the value `any`	name the variable and specify the variable type, then click **Store ASA FirePOWER Changes** without configuring a value.

Table 2-5 Variable Edit Actions (continued)

To...	You can...
delete a variable or object from the included or excluded list	click the delete icon (🗑) next to the variable.
save a new or modified variable	click **Store ASA FirePOWER Changes**; if you are adding a variable from custom set, then click **Yes** to use the configured value as the default value in other sets, or **No** to use a default value of `any`.

After you edit a variable, if an active policy references the object, you must redeploy your configuration for the changes to take effect; see Deploying Configuration Changes, page 4-12.

See the following sections for more information:

- Working with Network Variables, page 2-23
- Working with Port Variables, page 2-24

To create or edit a variable:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Choose **Variable Set**.

Step 3 Create a variable set or edit an existing set:

- To create a variable set, click **Add Variable Set**.
- To edit an existing variable set, click the edit icon (✏) next to the variable set.

Step 4 Create a new variable or edit an existing variable:

- To create a new variable, click **Add**.
- To edit an existing variable, click the edit icon (✏) next to the variable.

Step 5 If you are creating a new variable:

- Enter a unique variable **Name**.

  You can use alphanumeric characters and the underscore (_) character.
- Choose the **Network** or **Port** variable **Type** from the drop-down list.

Step 6 Optionally, move items from the list of available networks or ports to the list of included or excluded items.

You can choose one or more items and then drag and drop, or click **Include** or **Exclude**. Use the Ctrl and Shift keys to choose multiple items.

Tip If addresses or ports in the included and excluded lists for a network or port variable overlap, excluded addresses or ports take precedence.

Step 7 Optionally, enter a single literal value, then click **Add**.

For network variables, you can enter a single IP address or address block. For port variables you can add a single port or port range, separating the upper and lower values with a hyphen (-).

Repeat this step as needed to enter multiple literal values.

Step 8 Click **Store ASA FirePOWER Changes** to save the variable. If you are adding a new variable from a custom set, you have the following options:

- Click **Yes** to add the variable using the configured value as the customized value in the default set and, consequently, the default value in other custom sets.
- Click **No** to add the variable as the default value of `any` in the default set and, consequently, in other custom sets.

Step 9 When you have finished making changes, click **Store ASA FirePOWER Changes** to save the variable set, then click **Yes**.

Step 10 If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes, page 4-12.

Working with Network Variables

License: Protection

Network variables represent IP addresses you can use in intrusion rules that you enable in an intrusion policy and in intrusion policy rule suppressions, dynamic rule states, and adaptive profiles. Network variables differ from network objects and network object groups in that network variables are specific to intrusion policies and intrusion rules, whereas you can use network objects and groups to represent IP addresses in various places in the ASA FirePOWER module, including access control policies, network variables, intrusion rules, reports, and so on. See Working with Network Objects, page 2-3 for more information.

You can use network variables in the following configurations to specify the IP addresses of hosts on your network:

- intrusion rules

  Intrusion rule **Source IPs** and **Destination IPs** header fields allow you to restrict packet inspection to the packets originating from or destined to specific IP addresses. See Specifying IP Addresses In Intrusion Rules, page 30-5.

- suppressions

  The **Network** field in source or destination intrusion rule suppressions allows you to suppress intrusion event notifications when a specific IP address or range of IP addresses triggers an intrusion rule or preprocessor. See Configuring Suppression Per Intrusion Policy, page 27-25.

- dynamic rule states

  The **Network** field in source or destination dynamic rule states allows you to detect when too many matches for an intrusion rule or preprocessor rule occur in a given time period. See Adding Dynamic Rule States, page 27-28.

- adaptive profiles

  The adaptive profiles **Networks** field identifies hosts in the network where you want to improve reassembly of packet fragments and TCP streams in passive deployments. See Tuning Preprocessing in Passive Deployments, page 25-1.

When you use variables in the fields identified in this section, the variable set you link to an intrusion policy determines the variable values in the network traffic handled by an access control policy that uses the intrusion policy.

You can add any combination of the following network configurations to a variable:

- any combination of network variables, network objects, and network object groups that you select from the list of available networks

  See Working with Network Objects, page 2-3 for information on creating individual and group network objects using the object manager.
- individual network objects that you add from the New Variable or Edit Variable page, and can then add to your variable and to other existing and future variables
- literal, single IP addresses or address blocks

  You can list multiple literal IP addresses and address blocks by adding each individually. You can list IPv4 and IPv6 addresses and address blocks alone or in any combination. When specifying IPv6 addresses, you can use any addressing convention defined in RFC 4291.

The default value for included networks in any variable you add is the word `any`, which indicates any IPv4 or IPv6 address. The default value for excluded networks is none, which indicates no network. You can also specify the address `::` in a literal value to indicate any IPv6 address in the list of included networks, or no IPv6 addresses in the list of exclusions.

Adding networks to the excluded list negates the specified addresses and address blocks. That is, you can match any IP address with the exception of the excluded IP address or address blocks.

For example, excluding the literal address `192.168.1.1` specifies any IP address other than 192.168.1.1, and excluding `2001:db8:ca2e::fa4c` specifies any IP address other than 2001:db8:ca2e::fa4c.

You can exclude any combination of networks using literal or available networks. For example, excluding the literal values `192.168.1.1` and `192.168.1.5` *includes* any IP address other than 192.168.1.1 or 192.168.1.5. That is, the system interprets this as "**not** 192.168.1.1 **and not** 192.168.1.5," which matches any IP address other than those listed between brackets.

Note the following points when adding or editing network variables:

- You cannot logically exclude the value `any` which, if excluded, would indicate no address. For example, you cannot add a variable with the value `any` to the list of excluded networks.
- Network variables identify traffic for the specified intrusion rule and intrusion policy features. Note that preprocessor rules can trigger events regardless of the hosts defined by network variables used in intrusion rules.
- Excluded values must resolve to a subset of included values. For example, you cannot include the address block 192.168.5.0/24 and exclude 192.168.6.0/24. An error message warns you and identifies the offending variable, and you cannot save your variable set when you exclude a value outside the range of included values.

For information on adding and editing network variables, see Adding and Editing Variables, page 2-20.

Working with Port Variables

License: Protection

Port variables represent TCP and UDP ports you can use in the **Source Port** and **Destination Port** header fields in intrusion rules that you enable in an intrusion policy. Port variables differ from port objects and port object groups in that port variables are specific to intrusion rules. You can create port objects for protocols other than TCP and UDP, and you can use port objects in port variables and access control policies. See Working with Port Objects, page 2-9 for more information.

You can use port variables in the intrusion rule **Source Port** and **Destination Port** header fields to restrict packet inspection to packets originating from or destined to specific TCP or UDP ports.

When you use variables in these fields, the variable set you link to the intrusion policy associated with an access control rule or policy determines the values for these variables in the network traffic where the system applies the access control policy.

You can add any combination of the following port configurations to a variable:

- any combination of port variables and port objects that you cboose from the list of available ports

  Note that the list of available ports does not display port object groups, and you cannot add these to variables. See Working with Port Objects, page 2-9 for information on creating port objects using the object manager.

- individual port objects that you add from the New Variable or Edit Variable page, and can then add to your variable and to other existing and future variables

  Only TCP and UDP ports, including the value `any` for either type, are valid variable values. If you use the new or edit variables page to add a valid port object that is not a valid variable value, the object is added to the system but is not displayed in the list of available objects. When you use the object manager to edit a port object that is used in a variable, you can only change its value to a valid variable value.

- single, literal port values and port ranges

  You must separate port ranges with a dash (-). Port ranges indicated with a colon (:) are supported for backward compatibility, but you cannot use a colon in port variables that you create.

  You can list multiple literal port values and ranges by adding each individually in any combination.

Note the following points when adding or editing port variables:

- The default value for included ports in any variable you add is the word `any`, which indicates any port or port range. The default value for excluded ports is `none`, which indicates no ports.

Tip To create a variable with the value `any`, name and save the variable without adding a specific value.

- You cannot logically exclude the value `any` which, if excluded, would indicate no ports. For example, you cannot save a variable set when you add a variable with the value `any` to the list of excluded ports.
- Adding ports to the excluded list negates the specified ports and port ranges. That is, you can match any port with the exception of the excluded ports or port ranges.
- Excluded values must resolve to a subset of included values. For example, you cannot include the port range 10-50 and exclude port 60. An error message warns you and identifies the offending variable, and you cannot save your variable set when you exclude a value outside the range of included values.

For information on adding and editing port variables, see Adding and Editing Variables, page 2-20.

Resetting Variables

License: Protection

You can reset a variable to its default value on the variable set new or edit variables page. The following table summarizes the basic principles of resetting variables.

Table 2-6 Variable Reset Values

Resetting this variable type...	In this set type...	Resets it to...
default	default	the rule update value
user-defined	default	`any`
default or user-defined	custom	the current default set value (modified or unmodified)

Resetting a variable in a custom set simply resets it to the current value for that variable in the default set.

Conversely, resetting or modifying the value of a variable in the default set always updates the default value of that variable in all custom sets. When the reset icon is grayed out, indicating that you cannot reset the variable, this means that the variable has no customized value in that set. Unless you have customized the value for a variable in a custom set, a change to the variable in the default set updates the value used in any intrusion policy where you have linked the variable set.

Note It is good practice when you modify a variable in the default set to assess how the change affects any intrusion policy that uses the variable in a linked custom set, especially when you have not customized the variable value in the custom set.

When the customized value and the reset value are the same, this indicates one of the following:

- you are in the custom or default set where you added the variable with the value `any`
- you are in the custom set where you added the variable with an explicit value and elected to use the configured value as the default value

Linking Variable Sets to Intrusion Policies

License: Control

By default, the ASA FirePOWER module links the default variable set to all intrusion policies used in an access control policy. When you deploy an access control policy that uses an intrusion policy, intrusion rules that you have enabled in the intrusion policy use the variable values in the linked variable set.

When you modify a custom variable set used by an intrusion policy in an access control policy, the system reflects the status for that policy as out-of-date on the Access Control page. You must deploy the configuration to implement changes in your variable set. When you modify the default set, the system reflects the status of all access control policies that use intrusion policies as out-of-date, and you must redeploy the configuration to implement your changes.

See the following sections for information:

- To link a variable set other than the default set to an access control rule, see the procedure in Configuring an Access Control Rule to Perform Intrusion Prevention, page 11-4.
- To link a variable set other than the default set to the default action of an access control policy, see Setting Default Handling and Inspection for Network Traffic, page 4-4.
- To deploy access control policies, including policies that link variable sets to intrusion policies, see Deploying Configuration Changes, page 4-12.

Understanding Advanced Variables

License: Protection

Advanced variables allow you to configure features that you cannot otherwise configure via the module interface. The ASA FirePOWER module currently provides only two advanced variables, and you can only edit the USER_CONF advanced variable.

USER_CONF

USER_CONF provides a general tool that allows you to configure one or more features not otherwise available via the module interface.

Caution Do **not** use the advanced variable USER_CONF to configure an intrusion policy feature unless you are instructed to do so in the feature description or by Support. Conflicting or duplicate configurations will halt the system.

When editing USER_CONF, you can type up to 4096 total characters on a single line; the line wraps automatically. You can include any number of valid instructions or lines until you reach the 8192 maximum character length for a variable or a physical limit such as disk space. Use the backslash (\) line continuation character after any complete argument in a command directive.

Resetting USER_CONF empties it.

Working with Sinkhole Objects

License: Protection

A sinkhole object represents either a DNS server that gives non-routeable addresses for all domain names within the sinkhole, or an IP address that does not resolve to a server. You can reference the sinkhole object within a DNS policy rule to redirect matching traffic to the sinkhole. You must assign the object both an IPv4 address and an IPv6 address.

You cannot delete a sinkhole object that is in use. Additionally, after you edit a sinkhole object used in a DNS policy, you must redeploy the configuration for your changes to take effect; see Deploying Configuration Changes, page 4-12.

To create a sinkhole object:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Choose **Sinkhole** from the list of object types.

Step 3 Click **Add Sinkhole**.

Step 4 Enter a **Name**.

Step 5 Enter the **IPv4 Address** and **IPv6 Address** of your sinkhole.

Step 6 You have the following options:

- If you want to redirect traffic to a sinkhole server, choose **Log Connections to Sinkhole**.
- If you want to redirect traffic to a non-resolving IP address, choose **Block and Log Connections to Sinkhole**.

Step 7 If you want to assign an Indication of Compromise (IoC) type to your sinkhole, choose one from the **Type** drop-down.

Step 8 Click **Store ASA FirePOWER Changes**.

Working with File Lists

License: Malware

If you use network-based advanced malware protection (AMP), and the Collective Security Intelligence Cloud incorrectly identifies a file's disposition, you can add the file to a *file list* using a SHA-256 hash value to better detect the file in the future. Depending on the type of file list, you can do the following:

- To treat a file as if the cloud assigned a clean disposition, add the file to the *clean list*.
- To treat a file as if the cloud assigned a malware disposition, add the file to the *custom detection list*.

Because you manually specify the blocking behavior for these files, the system does not perform malware cloud lookups, even if the files are otherwise identified as malware by the cloud. Note that you must configure a rule in the file policy with either a **Malware Cloud Lookup** or **Block Malware** action and a matching file type to calculate a file's SHA value. For more information, see Working with File Rules, page 35-9.

The system's clean list and custom detection list are included by default in every file policy. You can opt not to use either or both lists on a per-policy basis.

Caution Do **not** include files on this list that are actually malware. The system does not block them, even if the cloud assigned the file's a Malware disposition, or if you added the file to the custom detection list.

Each file list can contain up to 10000 unique SHA-256 values. To add files to the file list, you can:

- upload a file so the system calculates and adds the file's SHA-256 value.
- enter a file's SHA-256 value directly.
- create and upload a comma-separated value (CSV) source file containing multiple SHA-256 values. All non-duplicate SHA-256 values are added to the file list.

When you add a file to a file list, edit a SHA-256 value in the file list, or delete SHA-256 values from the file list, you must redeploy the configuration for your changes to take effect; see Deploying Configuration Changes, page 4-12.

For more information on using file lists, see the following topics:

- Uploading Multiple SHA-256 Values to a File List, page 2-28
- Uploading an Individual File to a File List, page 2-30
- Adding a SHA-256 Value to the File List, page 2-30
- Modifying Files on a File List, page 2-31
- Downloading a Source File from a File List, page 2-31

Uploading Multiple SHA-256 Values to a File List

License: Malware

You can add multiple SHA-256 values to a file list by uploading a comma-separated value (CSV) source file containing a list of SHA-256 values and descriptions. The system validates the contents and populates the file list with valid SHA-256 values.

The source file must be a simple text file with a .csv file name extension. Any header must start with a pound sign (`#`); it is treated as a comment and not uploaded. Each entry should contain a single SHA-256 value followed by a description of up to 256 alphanumeric or special characters and end with either the `LF` or `CR+LF` Newline character. The system ignores any additional information in the entry.

Note the following:

- Deleting a source file from the file list also removes all associated SHA-256 hashes from the file list.
- You cannot upload multiple files to a file list if the successful source file upload results in the file list containing more than 10000 distinct SHA-256 values.
- The system truncates descriptions exceeding 256 characters to the first 256 characters on upload. If the description contains commas, you must use an escape character (`\,`). If no description is included, the source file name is used instead.
- If a file list contains a SHA-256 value, and you upload a source file containing that value, the newly uploaded value does not modify the existing SHA-256 value. When viewing captured files, file events, or malware events related to the SHA-256 value, any threat name or description is derived from the individual SHA-256 value.
- The system does not upload invalid SHA-256 values in a source file.
- If multiple uploaded source files contain an entry for the same SHA-256 value, the system uses the most recent value.
- If a source file contains multiple entries for the same SHA-256 value, the system uses the last one.
- You cannot directly edit a source file within the object manager. To make changes, you must first modify your source file directly, delete the copy on the system, then upload the modified source file. See Downloading a Source File from a File List, page 2-31 for more information.

To upload a source file to a file list:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Click **File List**.

Step 3 Click the edit icon (✏) next to the file list where you want to add values from a source file.

Step 4 Choose `List of SHAs` from the **Add by** field.

Step 5 Optionally, enter a description of the source file in the **Description** field.

If you do not enter a description, the system uses the file name.

Step 6 Click **Browse** to browse to the source file, then click **Upload and Add List** to add the list.

The source file is added to the file list. The SHA-256 column lists how many SHA-256 values the file contains.

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

Step 8 If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes, page 4-12.

After configuration deployment, the system no longer performs malware cloud lookups on files in the file list.

Uploading an Individual File to a File List

License: Malware

If you have a copy of the file you want to add to a file list, you can upload the file to the system for analysis; the system calculates the file's SHA-256 value and adds the file to the list. The system does not enforce a limit on the size of files for SHA-256 calculation.

To add a file by having the system calculate its SHA-256 value:

Step 1 On the object manager's File List page, click the edit icon (✏) next to the clean list or custom detection list where you want to add a file.

Step 2 Choose **Calculate SHA** from the **Add by** field.

Step 3 Optionally, enter a description of the file in the **Description** field.

If you do not enter a description, the file name is used for the description on upload.

Step 4 Click **Browse** to browse to the source file, then click **Calculate and Add SHA** to add the list.

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

Step 6 If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes, page 4-12.

After configuration deployment, the system no longer performs malware cloud lookups on files in the file list.

Adding a SHA-256 Value to the File List

License: Malware

You can submit a file's SHA-256 value to add it to a file list. You cannot add duplicate SHA-256 values.

To add a file by manually entering the file's SHA-256 value:

Step 1 On the object manager's File List page, click the edit icon (✏) next to the clean list or custom detection list where you want to add a file.

Step 2 Choose `Enter SHA Value` from the **Add by** field.

Step 3 Enter a description of the source file in the **Description** field.

Step 4 Enter or paste the file's entire **SHA-256** value. The system does not support matching partial values.

Step 5 Click **Add** to add the file.

Step 6 Click **Store ASA FirePOWER Changes**.

Step 7 If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes, page 4-12.

After configuration deployment, the system no longer performs malware cloud lookups on files in the file list.

Modifying Files on a File List

License: Malware

You can edit or delete individual SHA-256 values on a file list. Note that you cannot directly edit a source file within the object manager. To make changes, you must first modify your source file directly, delete the copy on the system, then upload the modified source file. See Downloading a Source File from a File List, page 2-31 for more information. To edit a file on a file list:

Step 1 On the object manager’s File List page, click the edit icon (✏) next to the clean list or custom detection list where you want to modify a file.

Step 2 Next to the SHA-256 value you want to edit, click the edit icon (✏).

Tip You can also delete files from the list. Next to the file you want to remove, click the delete icon (🗑).

Step 3 Update the **SHA-256** value or **Description**.

Step 4 Click **Save**.

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

Step 6 If an active policy references your object, deploy configuration changes; see Deploying Configuration Changes, page 4-12.

After configuration deployment, the system no longer performs malware cloud lookups on files in the file list.

Downloading a Source File from a File List

License: Malware

You can view, download, or delete existing source file entries on a file list. Note that you cannot edit a source file once uploaded. You must first delete the source file from the file list, then upload an updated file. For more information on uploading a source file, see Uploading Multiple SHA-256 Values to a File List, page 2-28.

The number of entries associated with a source file refers to the number of distinct SHA-256 values. If you delete a source file from a file list, the total number of SHA-256 entries the file list contains decreases by the number of valid entries in the source file.

To download a source file:

Step 1 On the object manager’s File List page, click the edit icon (✏) next to the clean list or custom detection list where you want to download a source file.

Step 2 Next to the source file you want to download, click the view icon (🔍).

Step 3 Click **Download SHA List** and follow the prompts to save the source file.

Step 4 Click **Close**.

Working with Security Zones

License: Any

Supported Devices: Any

A *security zone* is a grouping of one or more ASA interfaces that you can use to manage and classify traffic flow in various policies and configurations. You can configure multiple zones on a single device. This allows you to divide the network into segments where the system can apply various policies. You must assign at least one interface to a security zone to match traffic against that security zone, and each interface can belong to only one zone.

In addition to using security zones to group interfaces, you can use zones in access control policies. For example, you could write an access control rule that applies only to a specific source or destination zone.

The Security Zones page of the object manager lists the zones configured on your ASA FirePOWER module.

You cannot delete a security zone that is in use. After you add or remove interfaces from a zone, if an active policy references your object, you must deploy the configuration to see your changes take effect; see Deploying Configuration Changes, page 4-12.

To create a security zone:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Choose **Security Zones**.

Step 3 Click **Add Security Zone**.

Step 4 Enter a **Name** for the zone. You can use any printable standard ASCII characters except curly braces ({}) and pound signs (#).

Step 5 Choose an interface **Type** for the zone.

After you create a security zone, you cannot change its type.

Step 6 Choose one or more interfaces.

Use the Shift and Ctrl keys to choose multiple objects. If you have not yet configured interfaces, you can create an empty zone and add interfaces to it later; skip to step 9.

Step 7 Click **Add**.

Step 8 Repeat steps 6 through 8 to add interfaces on other devices to the zone.

Step 9 Click **Store ASA FirePOWER Changes**.

Working with Cipher Suite Lists

License: Any

A cipher suite list is an object comprised of several cipher suites. Each pre-defined cipher suite value represents a cipher suite used to negotiate an SSL- or TLS-encrypted session. You can use cipher suites and cipher suite lists in SSL rules to control encrypted traffic based on whether the client and server negotiated the SSL session using that cipher suite. If you add a cipher suite list to an SSL rule, SSL sessions negotiated with any of the cipher suites in the list match the rule.

Note Although you can use cipher suites in the ASDM interface in the same places as cipher suite lists, you cannot add, modify, or delete cipher suites.

You cannot delete a cipher suite list that is in use. Additionally, after you edit a cipher suite list, if an active policy references your object, you must redeploy the configuration for your changes to take effect; see Deploying Configuration Changes, page 4-12.

To create a cipher suite list:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Choose **Cipher Suite List**.

Step 3 Click **Add Cipher Suites**.

Step 4 Enter a **Name** for the cipher suite list. You can use any printable standard ASCII characters except a pipe (`|`) or curly braces (`{}`).

Step 5 Choose one or more cipher suites and click **Add**.

- Use Shift and Ctrl to choose multiple cipher suites, or right-click and **Select All**.
- Use the filter field (🔍) to search for existing cipher suites to include, which updates as you type to display matching items. Click the reload icon (↻) above the search field or click the clear icon (✖) in the search field to clear the search string.

Step 6 Click **Store ASA FirePOWER Changes**.

Working with Distinguished Name Objects

License: Any

Each distinguished name object represents the distinguished name listed for a public key certificate's subject or issuer. You can use distinguished name objects and groups (see Grouping Objects, page 2-2) in SSL rules to control encrypted traffic based on whether the client and server negotiated the SSL session using a server certificate with the distinguished name as subject or issuer.

Your distinguished name object can contain the common name attribute (**CN**). If you add a common name without "`CN=`" then the system 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 2-7 Distinguished Name Attributes

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

You can define one or more asterisks (*****) as wild cards in an attribute. In a common name attribute, you can define one or more asterisks per domain name label. Wild cards match only within that label, though you can define multiple labels with wild cards. See the following table for examples.

Table 2-8 Common Name Attribute Wild Card Examples

Attribute	Matches	Does Not Match
CN=”*ample.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”exam*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*xamp*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*.example.com”	mail.example.com	example.com example.text.com ampleexam.com
CN=”*.com”	example.com ampleexam.com	mail.example.com example.text.com
CN=”*.*.com”	mail.example.com example.text.com	example.com ampleexam.com

You cannot delete a distinguished name object that is in use. Additionally, after you edit a distinguished name object, if an active policy references your object, you must deploy the configuration for your changes to take effect; see Deploying Configuration Changes, page 4-12.

To create a distinguished name object:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Under **Distinguished Name**, choose **Individual Objects**.

Step 3 Click **Add Distinguished Name**.

Step 4 Enter a **Name** for the distinguished name object. You can use any printable standard ASCII characters except a pipe (`|`) or curly braces (`{}`).

Step 5 In the **DN** field, enter a value for the distinguished name or common name. You have the following options:

- If you add a distinguished name, you can include one of each attribute listed in Table 2-7 on page 2-33 separated by commas.
- If you add a common name, you can include multiple labels and wild cards.

Step 6 Click **Store ASA FirePOWER Changes**.

Working with PKI Objects

License: Any

PKI objects represent the public key certificates and paired private keys required to support your SSL inspection deployment. Internal and trusted CA objects consist of certificate authority (CA) certificates; internal CA objects also contain the private key paired with the certificate. Internal and external certificate objects consist of server certificates; internal certificate objects also contain the private key paired with the certificate. Using these objects in SSL rules, you can decrypt:

- outgoing traffic by re-signing the server certificate with an internal CA object
- incoming traffic using the known private key in an internal certificate object

You can also create SSL rules and match traffic encrypted with:

- the certificate in an external certificate object
- a certificate either signed by the CA in a trusted CA object, or within the CA's chain of trust

You can manually input certificate and key information, upload a file containing that information, or in some cases, generate a new CA certificate and private key.

When you view a list of PKI objects in the object manager, the system displays the certificate's Subject distinguished name as the object value. Hover your pointer over the value to view the full certificate Subject distinguished name. To view other certificate details, edit the PKI object.

Note The ASA FirePOWER module encrypts all private keys stored in internal CA objects and internal certificate objects with a randomly generated key before saving them. If you upload private keys that are password protected, the appliance decrypts the key using the user-supplied password, then reencrypts it with the randomly generated key before saving it.

For more information, see the following sections:

- Working with Internal Certificate Authority Objects, page 2-35
- Working with Trusted Certificate Authority Objects, page 2-39
- Working with External Certificate Objects, page 2-41
- Working with Internal Certificate Objects, page 2-41

Working with Internal Certificate Authority Objects

License: Any

Each internal certificate authority (CA) object you configure represents the CA public key certificate of a CA your organization controls. The object consists of the object name, CA certificate, and paired private key. You can use internal CA objects and groups (see Grouping Objects, page 2-2) in SSL rules to decrypt outgoing encrypted traffic by re-signing the server certificate with the internal CA.

Note If you reference an internal CA object in a **Decrypt - Resign** SSL rule and the rule matches an encrypted session, the user's browser may warn that the certificate is not trusted while negotiating the SSL handshake. To avoid this, add the internal CA object certificate to either the client or domain list of trusted root certificates.

You can create an internal CA object in the following ways:

- import an existing RSA-based or elliptic curve-based CA certificate and private key
- generate a new self-signed RSA-based CA certificate and private key
- generate an unsigned RSA-based CA certificate and private key. You must submit a certificate signing request (CSR) to another CA to sign the certificate before using the internal CA object.

After you create an internal CA object containing a signed certificate, you can download the CA certificate and private key. The system encrypts downloaded certificates and private keys with a user-provided password.

Whether system-generated or user-created, you can modify the internal CA object name, but cannot modify other object properties.

You cannot delete an internal CA object that is in use. Additionally, after you edit an internal CA object, if an active policy references your object, you must deploy the configuration for your changes to take effect; see Deploying Configuration Changes, page 4-12.

For more information, see the following sections:

- Importing a CA Certificate and Private Key, page 2-36
- Generating a New CA Certificate and Private Key, page 2-37
- Obtaining and Uploading a New Signed Certificate, page 2-37
- Downloading a CA Certificate and Private Key, page 2-38

Importing a CA Certificate and Private Key

License: Any

You can configure an internal CA object by importing an X.509 v3 CA certificate and private key. You can upload files encoded in one of the following supported formats:

- Distinguished Encoding Rules (DER)
- Privacy-enhanced Electronic Mail (PEM)

If the private key file is password-protected, you can supply the decryption password. If the certificate and key are encoded in the PEM format, you can also copy and paste the information.

You can upload only files that contain proper certificate or key information, and that are paired with each other. The system validates the pair before saving the object.

Note If you configure a rule with the **Decrypt - Resign** action, the rule matches traffic based on the referenced internal CA certificate's encryption algorithm type, in addition to any configured rule conditions. You must upload an elliptic curve-based CA certificate to decrypt outgoing traffic encrypted with an elliptic curve-based algorithm, for example. For more information, see Decrypt Actions: Decrypting Traffic for Further Inspection, page 16-9.

To import an internal CA certificate and private key:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Under **PKI**, choose **Internal CAs**.

Step 3 Click **Import CA**.

Step 4 Enter a **Name** for the internal CA object. You can use any printable standard ASCII characters except a pipe (`|`) or curly braces (`{}`).

Step 5 Above the **Certificate Data** field, click **Browse** to upload a DER or PEM-encoded X.509 v3 CA certificate file.

Step 6 Above the **Key** field, click **Browse** to upload a DER or PEM-encoded paired private key file.

Step 7 If the uploaded file is password-protected, check the **Encrypted, and the password is:** check box and enter the password.

Step 8 Click **Store ASA FirePOWER Changes**.

The internal CA object is added.

Generating a New CA Certificate and Private Key

License: Any

You can configure an internal CA object by providing identification information to generate a self-signed RSA-based CA certificate and private key. The following table describes the identification information you provide to generate the certificate.

Table 2-9 Generated Internal CA Attributes

Field	Allowed Values	Required
Country Name (two-letter code)	two alphabetic characters	yes
State or Province	up to 64 alphanumeric, backslash (/), hyphen (-), quotation ("), asterisk (*), period (.), or space characters	no
Locality or City		
Organization		
Organizational Unit		
Common Name		

The generated CA certificate is valid for ten years. The Valid From date is a week before generation.

To generate a self-signed CA certificate:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Under **PKI**, choose **Internal CAs**.

Step 3 Click **Generate CA**.

Step 4 Enter a **Name** for the internal CA object. You can use any printable standard ASCII characters except a pipe (|) or curly braces ({}).

Step 5 Enter the identification attributes, as described in Table 2-9 on page 2-37.

Step 6 Click **Generate self-signed CA**.

Obtaining and Uploading a New Signed Certificate

License: Any

You can configure an internal CA object by obtaining a signed certificate from a CA. This involves two steps:

- Provide identification information to configure the internal CA object. This generates an unsigned certificate and paired private key, and creates a certificate signing request (CSR) to a CA you specify.
- After the CA issues the signed certificate, upload it to the internal CA object, replacing the unsigned certificate.

You can only reference an internal CA object in an SSL rule if it contains a signed certificate.

To create an unsigned CA certificate and CSR:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Under **PKI**, choose **Internal CAs**.

Step 3 Click **Generate CA**.

Step 4 Enter a **Name** for the internal CA object. You can use any printable standard ASCII characters except a pipe (`|`) or curly braces (`{}`).

Step 5 Enter the identification attributes, as described in Table 2-9 on page 2-37.

Step 6 Click **Generate CSR**.

Step 7 Copy the CSR to submit to a CA.

Step 8 Click **Store ASA FirePOWER Changes**.

Note that before you can use the CA, you must upload a signed certificate issued by a CA.

To upload a signed certificate issued in response to a CSR:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Under **PKI**, choose **Internal CAs**.

Step 3 Click the edit icon (✎) next to the CA object containing the unsigned certificate awaiting the CSR.

Step 4 Click **Install Certificate**.

Step 5 Above the **Certificate Data** field, click **Browse** to upload a DER or PEM-encoded X.509 v3 CA certificate file.

Step 6 If the uploaded file is password protected, check the **Encrypted, and the password is:** check box and enter the password.

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

The CA object contains a signed certificate, and can be referenced in SSL rules.

Downloading a CA Certificate and Private Key

License: Any

You can back up or transfer a CA certificate and paired private key by downloading a file containing the certificate and key information from an internal CA object.

Caution Always store downloaded key information in a secure location.

The system encrypts the private key stored in an internal CA object with a randomly generated key before saving it to disk. If you download a certificate and private key from an internal CA object, the system first decrypts the information before creating a file containing the certificate and private key information. You must then provide a password the system uses to encrypt the downloaded file.

Caution Private keys downloaded as part of a system backup are decrypted, then stored in the unencrypted backup file. For more information, see Creating Backup Files, page 48-1.

To download an internal CA certificate and private key:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Under **PKI**, choose **Internal CAs**.

Step 3 Click the edit icon (✎) next to the internal CA object whose certificate and private key you want to download.

Step 4 Click **Download**.

Step 5 Enter an encryption password in the **Password** and **Confirm Password** fields.

Step 6 Click **Store ASA FirePOWER Changes**.

The system prompts you to save the file.

Working with Trusted Certificate Authority Objects

License: Any

Each trusted certificate authority (CA) object you configure represents a CA public key certificate belonging to a trusted CA outside your organization. The object consists of the object name and CA public key certificate. You can use external CA objects and groups (see Grouping Objects, page 2-2) in the SSL policy to control traffic encrypted with a certificate signed either by the trusted CA, or any CA within the chain of trust.

After you create the trusted CA object, you can modify the name and add certificate revocation lists (CRL), but cannot modify other object properties. There is no limit on the number of CRLs you can add to an object. If you want to modify a CRL you have uploaded to an object, you must delete the object and recreate it.

You cannot delete a trusted CA object that is in use. Additionally, after you edit a trusted CA object, if an active policy references your object, you must deploy the configuration for your changes to take effect; see Deploying Configuration Changes, page 4-12.

For more information, see the following sections:

- Working with Geolocation Objects, page 2-42
- Adding a Certificate Revocation List to a Trusted CA Object, page 2-40

Adding a Trusted CA Object

License: Any

You can configure an external CA object by uploading an X.509 v3 CA certificate. You can upload a file encoded in one of the following supported formats:

- Distinguished Encoding Rules (DER)
- Privacy-enhanced Electronic Mail (PEM)

If the file is password-protected, you must supply the decryption password. If the certificate is encoded in the PEM format, you can also copy and paste the information.

You can upload a CA certificate only if the file contains proper certificate information; the system validates the certificate before saving the object.

To import a trusted CA certificate:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Under **PKI**, choose **Trusted CAs**.

Step 3 Click **Add Trusted CAs**.

Step 4 Enter a **Name** for the trusted CA object. You can use any printable standard ASCII characters except a pipe (`|`) or curly braces (`{}`).

Step 5 Above the **Certificate Data** field, click **Browse** to upload a DER or PEM-encoded X.509 v3 CA certificate file.

Step 6 If the file is password-protected, check the **Encrypted, and the password is:** check box and enter the password.

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

Adding a Certificate Revocation List to a Trusted CA Object

License: Any

You can upload CRLs to a trusted CA object. If you reference that trusted CA object in an SSL policy, you can control encrypted traffic based on whether the CA that issued the session encryption certificate subsequently revoked the certificate. You can upload files encoded in one of the following supported formats:

- Distinguished Encoding Rules (DER)
- Privacy-enhanced Electronic Mail (PEM)

After you add the CRL, you can view the list of revoked certificates. If you want to modify a CRL you have uploaded to an object, you must delete the object and recreate it.

You can upload only files that contain a proper CRL. There is no limit to the number of CRLs you can add to a trusted CA object. However, you must save the object each time you upload a CRL, before adding another CRL.

To upload a CRL:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Under **PKI**, choose **Trusted CAs**.

Step 3 Click the edit icon (✎) next to a trusted CA object.

Step 4 Click **Add CRL** to upload a DER or PEM-encoded CRL file.

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

Working with External Certificate Objects

License: Any

Each external certificate object you configure represents a server public key certificate that does not belong to your organization. The object consists of the object name and certificate. You can use external certificate objects and groups (see Grouping Objects, page 2-2) in SSL rules to control traffic encrypted with the server certificate. For example, you can upload a self-signed server certificate that you trust, but cannot verify with a trusted CA certificate.

You can configure an external certificate object by uploading an X.509 v3 server certificate. You can upload a file in one of the following supported formats:

- Distinguished Encoding Rules (DER)
- Privacy-enhanced Electronic Mail (PEM)

You can upload only files that contains proper server certificate information; the system validates the file before saving the object. If the certificate is encoded in the PEM format, you can also copy and paste the information.

After you create the external certificate object, you can modify the name, but cannot modify other object properties.

You cannot delete an external certificate object that is in use. Additionally, after you edit an external certificate object, if an active policy references your object, you must deploy the configuration for your changes to take effect; see Deploying Configuration Changes, page 4-12.

To create an external certificate object:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Under **PKI**, choose **External Certs**.

Step 3 Click **Add External Cert**.

Step 4 Enter a **Name** for the external certificate object. You can use any printable standard ASCII characters except a pipe (`|`) or curly braces (`{}`).

Step 5 Above the **Certificate Data** field, click **Browse** to upload a DER or PEM-encoded X.509 v3 server certificate file.

Step 6 Click **Store ASA FirePOWER Changes**.

Working with Internal Certificate Objects

License: Any

Each internal certificate object you configure represents a server public key certificate belonging to your organization. The object consists of the object name, public key certificate, and paired private key. You can use internal certificate objects and groups (see Grouping Objects, page 2-2) in SSL rules to decrypt traffic incoming to one of your organization's servers using the known private key.

You can configure an internal certificate object by uploading an X.509 v3 RSA-based or elliptic curve-based server certificate and paired private key. You can upload a file in one of the following supported formats:

- Distinguished Encoding Rules (DER)
- Privacy-enhanced Electronic Mail (PEM)

If the file is password-protected, you must supply the decryption password. If the certificate and key are encoded in the PEM format, you can also copy and paste the information.

You can upload only files that contain proper certificate or key information, and that are paired with each other. The system validates the pair before saving the object.

After you create the internal certificate object, you can modify the name, but cannot modify other object properties.

You cannot delete an internal certificate object that is in use. Additionally, after you edit an internal certificate object, if an active policy references your object, you must deploy the configuration for your changes to take effect; see Deploying Configuration Changes, page 4-12.

To create an internal certificate object:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Under **PKI**, choose **Internal Certs**.

Step 3 Click **Add Internal Cert**.

Step 4 Enter a **Name** for the internal certificate object. You can use any printable standard ASCII characters except a pipe (`|`) or curly braces (`{}`).

Step 5 Above the **Certificate Data** field, click **Browse** to upload a DER or PEM-encoded X.509 v3 server certificate file.

Step 6 Above the **Key** field, or click **Browse** to upload a DER or PEM-encoded paired private key file.

Step 7 If the uploaded private key file is password-protected, check the **Encrypted, and the password is:** check box and enter the password.

Step 8 Click **Store ASA FirePOWER Changes**.

Working with Geolocation Objects

License: Any

Each geolocation object you configure represents one or more countries or continents that the system has identified as the source or destination of traffic on your monitored network. You can use geolocation objects in access control policies or SSL policies. For example, you could write an access control rule that blocks traffic to or from certain countries. For information on filtering traffic by geographical location, see Controlling Traffic by Network or Geographical Location, page 7-3.

To ensure that you are using up-to-date information to filter your network traffic, Cisco strongly recommends that you regularly update your Geolocation Database (GeoDB). For information on downloading and installing GeoDB updates, see Updating the Geolocation Database, page 46-19.

You cannot delete a geolocation object that is in use. Additionally, after you edit a geolocation object used in an access control policy or SSL policy, you must redeploy policies for your changes to take effect.

To create a geolocation object:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Choose **Geolocation**.

Step 3 Click **Add Geolocation**.

Step 4 Enter a **Name** for the geolocation object. You can use any printable standard ASCII characters except curly braces (`{}`).

Step 5 Check the check boxes for the countries and continents you want to include in your geolocation object.

Selecting a continent selects all countries within that continent, as well as any countries that GeoDB updates may add under that continent in the future. Deselecting any country under a continent deselects the continent. You can select any combination of countries and continents.

Step 6 Click **Store ASA FirePOWER Changes**.

Working with Security Group Tag Objects

License: Any

A Security Group Tag (SGT) object specifies a single SGT value, which you can use as a custom SGT condition in access control rules. You cannot group SGT objects.

If you configure ISE as an identity source, the system automatically disables the Security Group Tag option in the Object Manager. You cannot add new SGT objects, edit existing SGT objects, or use SGT objects as rule conditions unless you disable the ISE connection. For more information on the difference between custom SGTs and ISE SGTs, see ISE SGT v. Custom SGT Rule Conditions, page 10-1.

If you edit or delete an SGT object, if an active policy references the object, you must redeploy your configuration for the changes to take effect; see Deploying Configuration Changes, page 4-12.

To create an SGT object:

Step 1 Choose **Configuration > ASA FirePOWER Configuration > Object Management**.

Step 2 Choose **Security Group Tag**.

Step 3 Click **Add Security Group Tag**.

Step 4 Enter a **Name**.

Step 5 Optionally, enter a **Description**.

Step 6 In the **Tag** field, enter a single SGT.

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