

ASA FirePOWER Module

The following topics describe how to configure the ASA FirePOWER module that runs on the ASA.

- About the ASA FirePOWER Module, on page 1
- Licensing Requirements for the ASA FirePOWER Module, on page 5
- Guidelines for ASA FirePOWER, on page 5
- Defaults for ASA FirePOWER, on page 7
- Perform Initial ASA FirePOWER Setup, on page 7
- Configure the ASA FirePOWER Module, on page 15
- Managing the ASA FirePOWER Module, on page 18
- Monitoring the ASA FirePOWER Module, on page 25
- History for the ASA FirePOWER Module, on page 27

About the ASA FirePOWER Module

The ASA FirePOWER module supplies next-generation firewall services, including Next-Generation Intrusion Prevention System (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP).

The ASA FirePOWER module runs a separate application from the ASA.

How the ASA FirePOWER Module Works with the ASA

You can configure your ASA FirePOWER module using one of the following deployment models:

- Inline mode—In an inline deployment, the actual traffic is sent to the ASA FirePOWER module, and the module's policy affects what happens to the traffic. After dropping undesired traffic and taking any other actions applied by policy, the traffic is returned to the ASA for further processing and ultimate transmission.
- Inline tap monitor-only mode (ASA inline)—In an inline tap monitor-only deployment, a copy of the traffic is sent to the ASA FirePOWER module, but it is not returned to the ASA. Inline tap mode lets you see what the ASA FirePOWER module would have done to traffic, and lets you evaluate the content of the traffic, without impacting the network. However, in this mode, the ASA does apply its policies to the traffic, so traffic can be dropped due to access rules, TCP normalization, and so forth.
- Passive monitor-only (traffic forwarding) mode—If you want to prevent any possibility of the ASA with FirePOWER Services device impacting traffic, you can configure a traffic-forwarding interface and

connect it to a SPAN port on a switch. In this mode, traffic is sent directly to the ASA FirePOWER module without ASA processing. The traffic is dropped, and nothing is returned from the module, nor does the ASA send the traffic out any interface. You must operate the ASA in single context transparent mode to configure traffic forwarding.

Be sure to configure consistent policies on the ASA and the ASA FirePOWER. Both policies should reflect the inline or monitor-only mode of the traffic.

The following sections explain these modes in more detail.

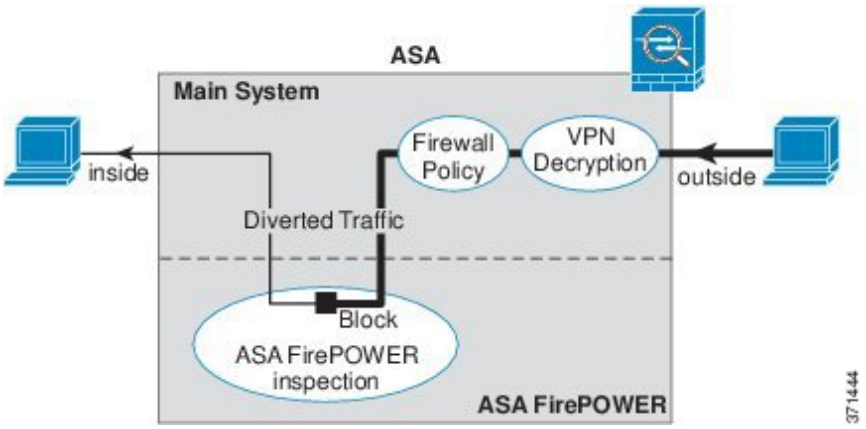
ASA FirePOWER Inline Mode

In inline mode, traffic goes through the firewall checks before being forwarded to the ASA FirePOWER module. When you identify traffic for ASA FirePOWER inspection on the ASA, traffic flows through the ASA and the module as follows:

1. Traffic enters the ASA.
2. Incoming VPN traffic is decrypted.
3. Firewall policies are applied.
4. Traffic is sent to the ASA FirePOWER module.
5. The ASA FirePOWER module applies its security policy to the traffic, and takes appropriate actions.
6. Valid traffic is sent back to the ASA; the ASA FirePOWER module might block some traffic according to its security policy, and that traffic is not passed on.
7. Outgoing VPN traffic is encrypted.
8. Traffic exits the ASA.

The following figure shows the traffic flow when using the ASA FirePOWER module in inline mode. In this example, the module blocks traffic that is not allowed for a certain application. All other traffic is forwarded through the ASA.

Figure 1: ASA FirePOWER Module Traffic Flow in the ASA



Note If you have a connection between hosts on two ASA interfaces, and the ASA FirePOWER service policy is only configured for one of the interfaces, then all traffic between these hosts is sent to the ASA FirePOWER module, including traffic originating on the non-ASA FirePOWER interface (because the feature is bidirectional).

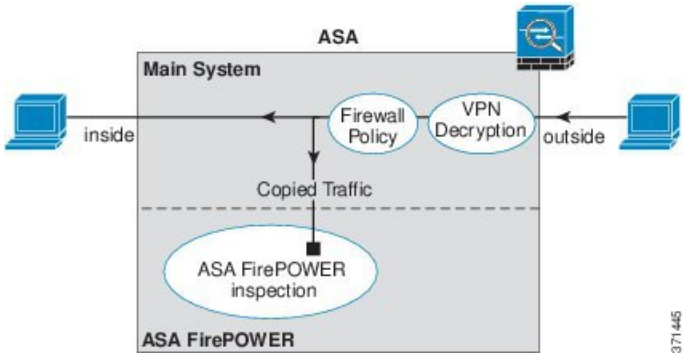
ASA FirePOWER Inline Tap Monitor-Only Mode

This mode sends a duplicate stream of traffic to the ASA FirePOWER module for monitoring purposes only. The module applies the security policy to the traffic and lets you know what it would have done if it were operating in inline mode; for example, traffic might be marked "would have dropped" in events. You can use this information for traffic analysis and to help you decide if inline mode is desirable.

Note You cannot configure both inline tap monitor-only mode and normal inline mode at the same time on the ASA. Only one type of service policy rule is allowed. In multiple context mode, you cannot configure inline tap monitor-only mode for some contexts, and regular inline mode for others.

The following figure shows the traffic flow when operating in inline tap mode.

Figure 2: ASA FirePOWER Inline Tap Monitor-Only Mode



ASA FirePOWER Passive Monitor-Only Traffic Forwarding Mode

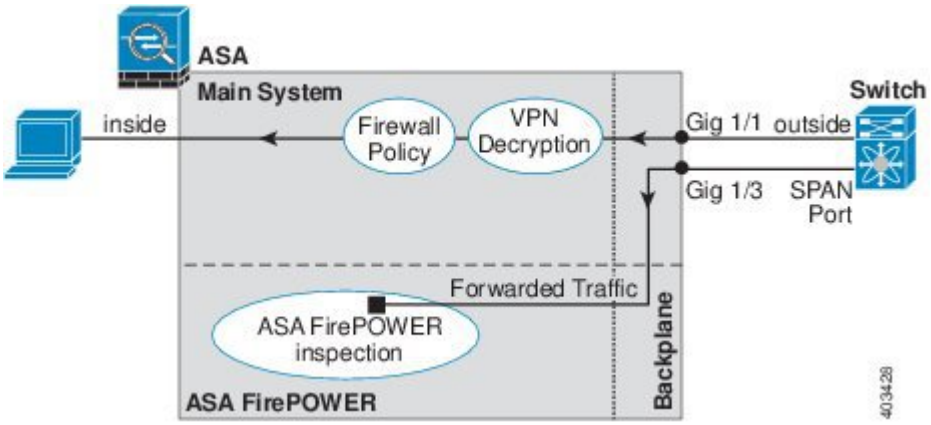
If you want to operate the ASA FirePOWER module as a pure Intrusion Detection System (IDS), where there is no impact on the traffic at all, you can configure a traffic forwarding interface. A traffic forwarding interface sends all received traffic directly to the ASA FirePOWER module without any ASA processing.

The module applies the security policy to the traffic and lets you know what it would have done if it were operating in inline mode; for example, traffic might be marked "would have dropped" in events. You can use this information for traffic analysis and to help you decide if inline mode is desirable.

Traffic in this setup is never forwarded: neither the module nor the ASA sends the traffic on to its ultimate destination. You must operate the ASA in single context and transparent modes to use this configuration.

The following figure shows an interface configured for traffic-forwarding. That interface is connected to a switch SPAN port so the ASA FirePOWER module can inspect all of the network traffic. Another interface sends traffic normally through the firewall.

Figure 3: ASA FirePOWER Passive Monitor-Only, Traffic-Forwarding Mode



ASA FirePOWER Management

The module has a basic command line interface (CLI) for initial configuration and troubleshooting only. You configure the security policy on the ASA FirePOWER module using one of the following methods:

- Firepower/FireSIGHT Management Center—Can be hosted on a separate Management Center appliance or as a virtual appliance. The Management Center application is called Firepower beginning in version 6.0. Previous versions are called FireSIGHT.
- ASDM (check for compatibility with your model/version)—You can manage both the ASA and the module using the on-box ASDM.

Compatibility with ASA Features

The ASA includes many advanced application inspection features, including HTTP inspection. However, the ASA FirePOWER module provides more advanced HTTP inspection than the ASA provides, as well as additional features for other applications, including monitoring and controlling application usage.

You must follow these configuration restrictions on the ASA:

- Do not configure ASA inspection on HTTP traffic that you send to the ASA FirePOWER module.
- Do not enable the Mobile User Security (MUS) server; it is not compatible with the ASA FirePOWER module.

Other application inspections on the ASA are compatible with the ASA FirePOWER module, including the default inspections.

What to Do if the ASA FirePOWER Module Cannot Filter URLs

The ASA FirePOWER module obtains its URL filtering data from the managing Firepower Management Center, over HTTP. The module cannot perform URL filtering if it cannot download this database.

If there is a device between the ASA FirePOWER module and Firepower Management Center that is performing ASA HTTP inspection, the inspections can block the ASA FirePOWER module's HTTP GET requests to the

Firepower Management Center. This problem also occurs if you configure HTTP inspection on the ASA that hosts the ASA FirePOWER module (which is a misconfiguration).

To resolve the issues, do any of the following that apply to your situation:

- If you configured HTTP inspection on the ASA that hosts the ASA FirePOWER module, remove the HTTP inspection configuration. ASA FirePOWER inspection and ASA HTTP inspection are incompatible.
- If there is an intervening device doing ASA HTTP inspection, remove the drop protocol violations action from the HTTP inspection policy map:

```
policy-map type inspect http http_inspection_policy
   parameters
      no protocol-violation action drop-connection
```

Licensing Requirements for the ASA FirePOWER Module

Certain areas of ASA FirePOWER module functionality may require additional licenses.

For an ASA FirePOWER module managed by a Firepower/FireSIGHT Management Center, enable licenses on the module using the Management Center. See the licensing chapter of the *FireSIGHT System User Guide 5.4*, *Firepower Management Center Configuration Guide 6.0*, or the online help on the FireSIGHT Management Center for more information.

For the ASA FirePOWER module managed using ASDM, enable licenses on the module using the FirePOWER module configuration in ASDM. See the licensing chapter of the *ASA FirePOWER Module User Guide 5.4*, *ASA FirePOWER Services Local Management Configuration Guide 6.0*, or the online help for the module in ASDM for more information.

The ASA itself does not require any additional licenses.

Guidelines for ASA FirePOWER

Failover Guidelines

Does not support failover directly; when the ASA fails over, any existing ASA FirePOWER flows are transferred to the new ASA. The ASA FirePOWER module in the new ASA begins inspecting the traffic from that point forward; old inspection states are not transferred.

You are responsible for maintaining consistent policies on the ASA FirePOWER modules in the high-availability ASA pair to ensure consistent failover behavior.



Note Create the failover pair before you configure the ASA FirePOWER modules. If the modules are already configured on both devices, clear the interface configuration on the standby device before creating the high-availability pair. From the CLI on the standby device, enter the **clear configure interface** command.

ASA Clustering Guidelines

Does not support clustering directly, but you can use these modules in a cluster. You are responsible for maintaining consistent policies on the ASA FirePOWER modules in the cluster.

Note Create the cluster before you configure the ASA FirePOWER modules. If the modules are already configured on the data units, clear the interface configuration on the devices before adding them to the cluster. From the CLI, enter the **clear configure interface** command.

Model Guidelines

- For ASA model software and hardware compatibility with the ASA FirePOWER module, see the Cisco ASA Compatibility.
- For the ASA 5515-X through ASA 5555-X, you must install a Cisco solid state drive (SSD). For more information, see the ASA 5500-X hardware guide. (The SSD is standard on the 5508-X, and 5516-X.)

ASDM Guidelines for Managing ASA FirePOWER

- The ASA, ASDM, and ASA FirePOWER versions supported for ASDM management differ by model. For supported combinations, see Cisco ASA Compatibility.
- If you enable command authorization on the ASA that hosts the module, you must log in with a user name that has privilege level 15 to see the **ASA FirePOWER** home, configuration, and monitoring pages. Read-only or monitor-only access to **ASA FirePOWER** pages other than the status page is not supported.
- If you are using Java 7 update 51 up to Java 8, you need to configure identity certificates for both the ASA and the ASA FirePOWER module. See Install an Identity Certificate for ASDM.
- You can never use both ASDM and Firepower Management Center, you must choose one or the other.

Additional Guidelines and Limitations

- See Compatibility with ASA Features, on page 4.
- You cannot configure both normal inline mode and inline tap monitor-only mode at the same time on the ASA. Only one type of service policy rule is allowed. In multiple context mode, you cannot configure inline tap monitor-only mode for some contexts, and regular inline mode for others.
- If you configure NetFlow on the ASA and include the **flow-export delay flow-create** command, even if your ASA FirePOWER access control policy blocks the connection with reset, the connection will remain on the ASA until the connection timeout is reached. If you cannot tolerate this behavior, you need to remove the command from the NetFlow configuration.
- If the module is stuck in recover/init mode, you cannot reload the ASA gracefully. Instead, use the **reload quick** command, so the ASA does not wait for the module to shut down gracefully prior to the system reload. If quick reload does not work, you will have to force-crash the ASA to reload it.
- On the ASA 5500-X series, particularly the smaller models, you can see very intermittent latency, 30-60ms, on .02% of the traffic. If you have applications that cannot tolerate this small latency, ensure

that you configure your redirection service policy so that these latency-sensitive applications are not redirected to the ASA FirePOWER module.

Defaults for ASA FirePOWER

The following table lists the default settings for the ASA FirePOWER module.

Table 1: ASA FirePOWER Default Network Parameters

Parameters	Default
Management IP address	System software image: 192.168.45.45/24 Boot image: 192.168.8.8/24
Gateway	System software image: none Boot image: 192.168.8.1/24
SSH or session Username	admin
Password	System software image: • ISA 3000 only on a new factory default image in Release 7.0.1: **Adm!n123** • Release 6.0 and following: **Admin123** • Releases prior to 6.0: **Sourcefire** Boot image: **Admin123**

Perform Initial ASA FirePOWER Setup

Deploy the ASA FirePOWER module in your network, and then choose your management method.

Deploy the ASA FirePOWER Module in Your Network

See the section for your firewall mode and ASA model to determine how to connect the ASA FirePOWER module management interface to your network.

Routed Mode

ASA 5508-X through ASA 5555-X (Software Module) in Routed Mode

These models run the ASA FirePOWER module as a software module, and the ASA FirePOWER module shares the Management 0/0 or Management 1/1 interface (depending on your model) with the ASA.

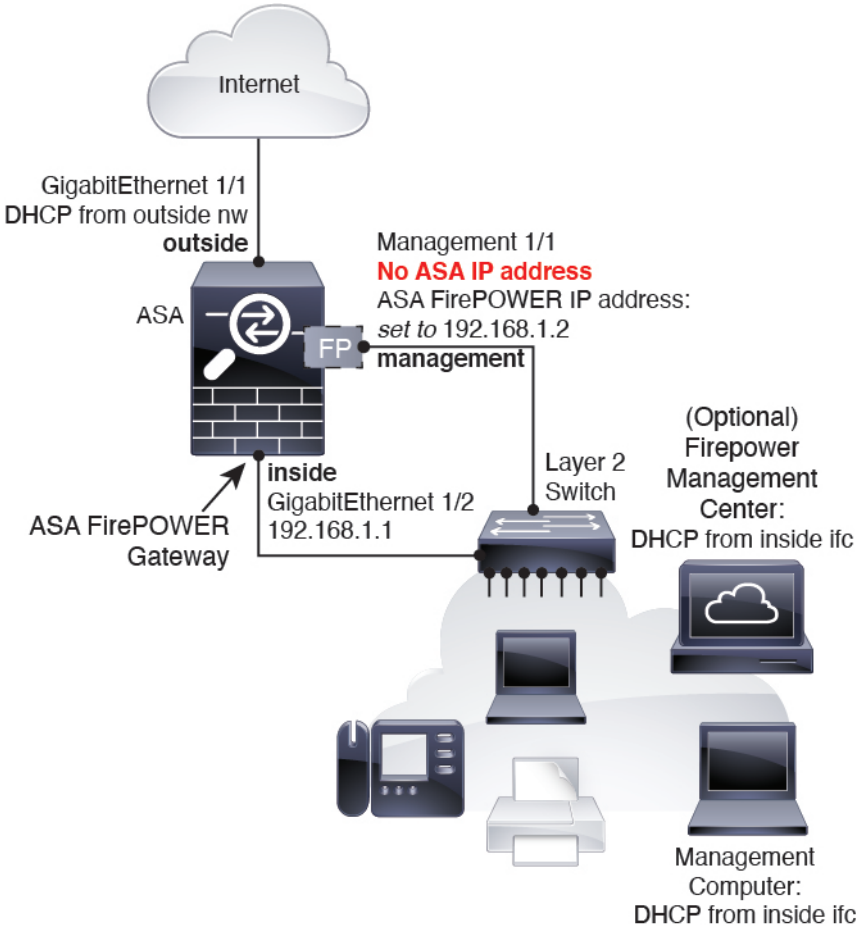
All management traffic to and from the ASA FirePOWER module must enter and exit the Management interface. The ASA FirePOWER module also needs Internet access. Management traffic cannot pass through

the ASA over the backplane; therefore you need to physically cable the management interface to an ASA interface to reach the Internet.

If you do not configure a name and IP address in the ASA configuration for Management, then the interface belongs exclusively to the module. In this case, the Management interface is not a regular ASA interface, and you can:

1. Configure the ASA FirePOWER IP address to be on the same network as a regular ASA data interface.
2. Specify the data interface as the ASA FirePOWER gateway.
3. Directly connect the Management interface to the data interface (using a Layer2 switch).

See the following typical cabling setup to allow ASA FirePOWER access to the Internet through the ASA inside interface.



For the ASA 5508-X, and 5516-X, the default configuration enables the above network deployment; the only change you need to make is to set the module IP address to be on the same network as the ASA inside interface and to configure the module gateway IP address.

For other models, you must remove the ASA-configured name and IP address for Management 0/0 or 1/1, and then configure the other interfaces as indicated above.

Note You can avoid using an external switch if you have extra interfaces that you can assign to an inside bridge group to configure a "soft switch". Be sure to set all bridge group interfaces to the same security level, allow same security communication, and configure NAT for each bridge group member. See the ASA interfaces configuration guide chapter for more information.

Note If you want to deploy a separate router on the inside network, then you can route between management and inside. In this case, you can manage both the ASA and ASA FirePOWER module on the Management interface with the appropriate configuration changes, including configuring the ASA name and IP address for the Management interface (on the same network as the ASA FirePOWER module address).

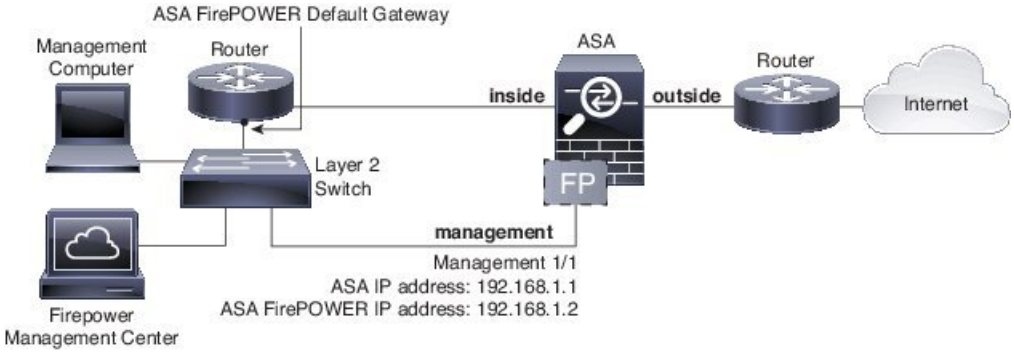
Transparent Mode

ASA 5508-X through ASA 5555-X, ISA 3000 (Software Module) in Transparent Mode

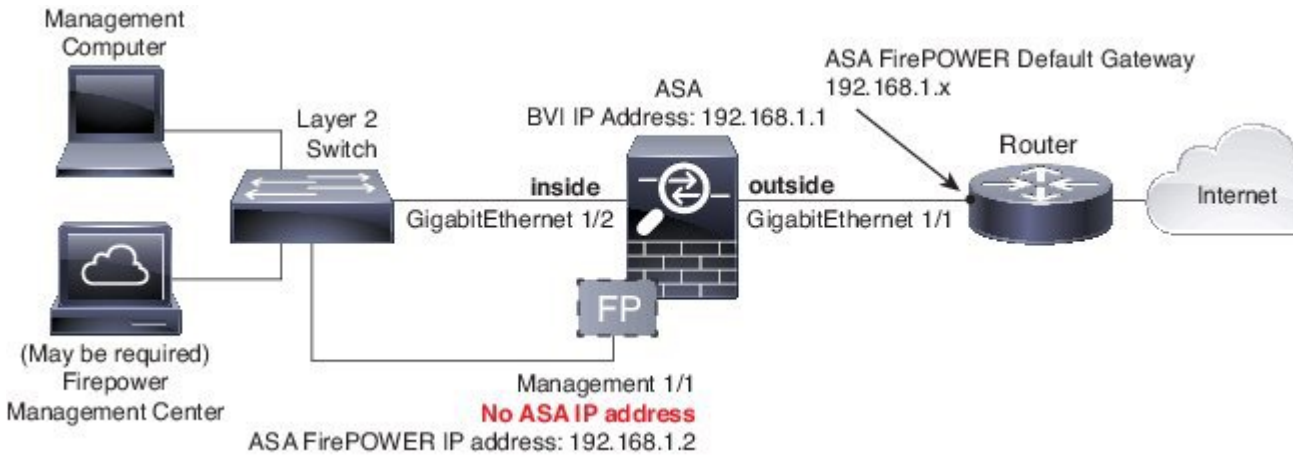
These models run the ASA FirePOWER module as a software module, and the ASA FirePOWER module shares the Management 0/0 or Management 1/1 interface (depending on your model) with the ASA.

All management traffic to and from the ASA FirePOWER module must enter and exit the Management interface. The ASA FirePOWER module also needs Internet access.

The following figure shows the recommended network deployment for the ASA 5500-X or ISA 3000 with the ASA FirePOWER module:



If you do not use an inside router, you can manage the ASA over the inside interface (using the BVI IP address) and not use the Management interface for ASA management:



Note You can avoid using an external switch if you have extra interfaces that you can assign to the inside bridge group to configure a "soft switch". Be sure to set all bridge group interfaces to the same security level, allow same security communication, and configure NAT for each bridge group member. See the ASA interfaces configuration guide chapter for more information.

Register the ASA FirePOWER Module with a Management Center

To register the module with a Firepower/FireSIGHT Management Center, you must access the ASA FirePOWER module CLI. The first time you access the CLI, you are prompted for basic configuration parameters. You must also add the module to the Management Center.

Notes:

- If you want to use ASDM to manage the module, skip this section and see Configure the ASA FirePOWER Module for ASDM Management, on page 12.
- If you need to move the module's management from one management center to another, first remove the device from the management center's inventory. Then, use the **configure manager add** command to point to the new management center. You can then complete the registration from the new management center. This process ensures a clean hand-over.

Access the ASA FirePOWER CLI

To access the ASA FirePOWER CLI, you can use one of the following methods.

Procedure

Step 1 Console Port:

- Connect to the ASA console port using the supplied DB-9 to RJ-45 serial cable and/or your own USB serial adapter. The ASA 5508-X/5516-X also has a mini-USB console port. See the hardware guide for instructions on using the USB console port.

At the ASA CLI, session to the ASA FirePOWER module:

session sfr

See also Session to the Software Module From the ASA, on page 24.

Step 2 SSH:

You can connect to the module default IP address (see Defaults for ASA FirePOWER, on page 7) or you can use ASDM on the ASA to change the management IP address, and then connect using SSH:

In ASDM, choose **Wizards > Startup Wizard**, and progress through the wizard to the **ASA FirePOWER Basic Configuration**, where you can set the IP address, mask, and default gateway.

Configure ASA FirePOWER Basic Settings

The first time you access the ASA FirePOWER module CLI, you are prompted for basic configuration parameters. You must also add the module to the Firepower/FireSIGHT Management Center if you are not using ASDM.

Before you begin

Access the module CLI according to Access the ASA FirePOWER CLI, on page 10.

Procedure

Step 1 At the ASA FirePOWER CLI, log in with the username **admin**.

If this is the first time you are logging in, use the default password. See Defaults for ASA FirePOWER, on page 7.

Step 2 Complete the system configuration as prompted.

Use the following network settings for the ASA FirePOWER module for the recommended network deployment (Deploy the ASA FirePOWER Module in Your Network, on page 7):

- Management interface: 192.168.1.2
- Management subnet mask: 255.255.255.0
- Gateway IP: 192.168.1.1

Example:

```
System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <new password>
Confirm new password: <repeat password>
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.86.118.3
```

```
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.252.0
Enter the IPv4 default gateway for the management interface []: 10.86.116.1
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.100.10.15,
10.120.10.14
Enter a comma-separated list of search domains or 'none' [example.net]: example.com
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
(Wait for the system to reconfigure itself.)

This sensor must be managed by a Defense Center.  A unique alphanumeric
registration key is always required.  In most cases, to register a sensor
to a Defense Center, you must provide the hostname or the IP address along
with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Defense Center are separated by a NAT device,
you must enter a unique NAT ID, along with the unique registration key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Defense Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Defense Center.
```

Step 3 Register the ASA FirePOWER module to a Management Center:

> **configure manager add** {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

where:

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} specifies either the fully qualified host name or IP address of the Management Center. If the Management Center is not directly addressable, use DONTRESOLVE.
- *reg_key* is the unique alphanumeric registration key required to register a ASA FirePOWER module to the Management Center.
- *nat_id* is an optional alphanumeric string used during the registration process between the Management Center and the ASA FirePOWER module. It is required if the hostname is set to DONTRESOLVE.

Step 4 Close the console connection. For the software module, enter:

> **exit**

Configure the ASA FirePOWER Module for ASDM Management

Not supported for all version/model combinations; check for compatibility with your model and version.

ASDM can change the ASA FirePOWER module IP address over the ASA backplane, but all further management requires network access between the ASDM interface and the Management interface, where the module is reachable.

To use ASDM to manage the module, launch ASDM and run the Startup Wizard.

Procedure

Step 1 On the computer connected to the ASA, launch a web browser.

Step 2 In the Address field, enter the following URL: **https://192.168.1.1/admin**. The Cisco ASDM web page appears.

Step 3 Click one of the available options: **Install ASDM Launcher**, **Run ASDM**, or **Run Startup Wizard**.

Step 4 Follow the onscreen instructions to launch ASDM according to the option you chose. The Cisco ASDM-IDM Launcher appears.

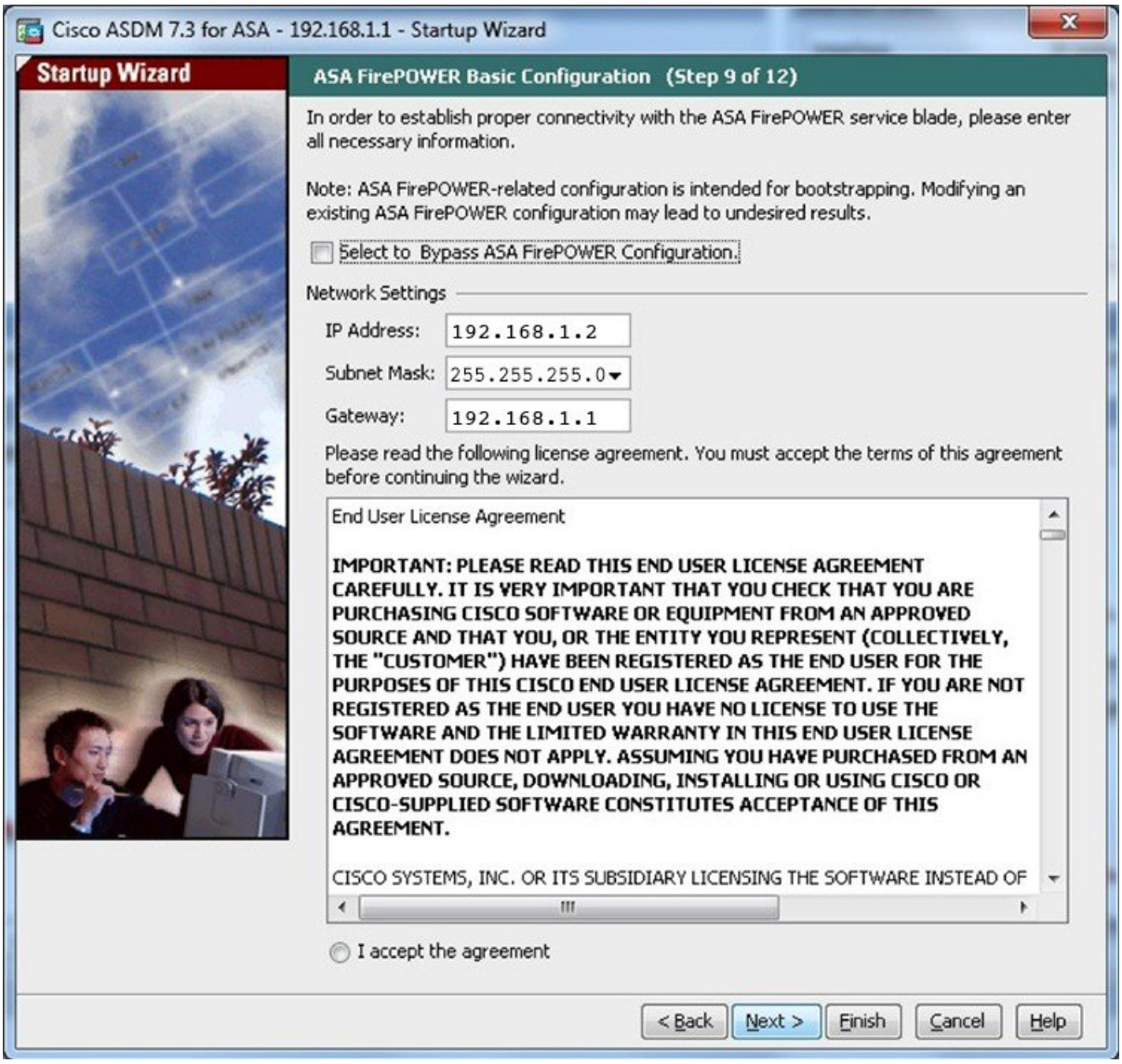
Note
If you click Install ASDM Launcher, in some cases you need to install an identity certificate for the ASA and a separate certificate for the ASA FirePOWER module according to Install an Identity Certificate for ASDM.

Step 5 Leave the username and password fields empty, and click **OK**. The main ASDM window appears.

Step 6 If you are prompted to provide the IP address of the installed ASA Firepower module, cancel out of the dialog box. You must first set the module IP address to the correct IP address using the Startup Wizard.

Step 7 Choose **Wizards** > **Startup Wizard**.

Step 8 Configure additional ASA settings as desired, or skip screens until you reach the **ASA Firepower Basic Configuration** screen.



Set the following values to work with the default configuration:

- **IP Address**—192.168.1.2
- **Subnet Mask**—255.255.255.0
- **Gateway**—192.168.1.1

Step 9 Click I accept the agreement, and click **Next** or **Finish** to complete the wizard.

Step 10 Quit ASDM, and then relaunch. You should see **ASA Firepower** tabs on the **Home** page.

Configure the ASA FirePOWER Module

Configure the security policy in the ASA FirePOWER module, and then configure the ASA to send traffic to the module.

Configure the Security Policy on the ASA FirePOWER Module

The security policy controls the services provided by the module, such as Next Generation IPS filtering and application filtering. You configure the security policy on the ASA FirePOWER module using one of the following methods.

FireSIGHT Management Center

Use a web browser to open **https://***DC_address*, where *DC_address* is the DNS name or IP address of the manager you defined in Configure ASA FirePOWER Basic Settings, on page 11. For example, https://dc.example.com.

Alternatively, in ASDM, choose **Home** > **ASA FirePOWER Status** and click the link at the bottom of the dashboard.

For more information about ASA FirePOWER configuration, see the Management Center online help, *FireSIGHT System User Guide 5.4*, or *Firepower Management Center Configuration Guide 6.0* (available at http://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html).

ASDM

In ASDM, choose **Configuration** > **ASA FirePOWER Configuration**.

For more information about ASA FirePOWER configuration, see the module's online help in ASDM, *ASA FirePOWER Module User Guide 5.4*, or *ASA FirePOWER Services Local Management Configuration Guide 6.0* (available at http://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html.

Redirect Traffic to the ASA FirePOWER Module

For inline and inline tap (monitor-only) modes, you configure a service policy to redirect traffic to the module. If you want passive monitor-only mode, you configure a traffic redirection interface, which bypasses ASA policies.

The following topics explain how to configure these modes.

Configure Inline or Inline Tap Monitor-Only Modes

Redirect traffic to the ASA FirePOWER module by creating a service policy that identifies specific traffic that you want to send. In this mode, ASA policies, such as access rules, are applied to the traffic before it is redirected to the module.

Before you begin

- Be sure to configure consistent policies on the ASA and the ASA FirePOWER module. Both policies should reflect the inline or inline tap mode of the traffic.
- In multiple context mode, perform this procedure within each security context.

Procedure

Step 1 Choose **Configuration** > **Firewall** > **Service Policy Rules**.

Step 2 Choose **Add** > **Add Service Policy Rule**.

Step 3 Choose whether to apply the policy to a particular interface or apply it globally and click **Next**.

Step 4 Configure the traffic match. For example, you could match **Any Traffic** so that all traffic that passes your inbound access rules is redirected to the module. Or, you could define stricter criteria based on ports, ACL (source and destination criteria), or an existing traffic class. The other options are less useful for this policy. After you complete the traffic class definition, click **Next**.

Step 5 On the Rule Actions page, click the **ASA FirePOWER Inspection** tab.

Step 6 Check the **Enable ASA FirePOWER for this traffic flow** check box.

Step 7 In the If ASA FirePOWER Card Fails area, click one of the following:

- **Permit traffic**—Sets the ASA to allow all traffic through, uninspected, if the module is unavailable.
- **Close traffic**—Sets the ASA to block all traffic if the module is unavailable.

Step 8 (Optional) Check **Monitor-only** to send a read-only copy of traffic to the module (inline tap mode).

By default, the traffic is sent in inline mode. Be sure to configure consistent policies on the ASA and the ASA FirePOWER. Both policies should reflect the inline or monitor-only of the traffic.

Step 9 Click **Finish** and then **Apply**.

Repeat this procedure to configure additional traffic flows as desired.

Configure Passive Traffic Forwarding

If you want to operate the module in passive monitor-only mode, where the module gets a copy of the traffic and neither it nor the ASA can affect the network, configure a traffic forwarding interface and connect the interface to a SPAN port on a switch. For more details, see ASA FirePOWER Passive Monitor-Only Traffic Forwarding Mode, on page 3.

The following guidelines explain the requirements for this deployment mode:

- The ASA must be in single-context and transparent mode.
- You can configure up to 4 interfaces as traffic-forwarding interfaces. Other ASA interfaces can be used as normal.
- Traffic-forwarding interfaces must be physical interfaces, not VLANs or BVIs. The physical interface also cannot have any VLANs associated with it.

- Traffic-forwarding interfaces cannot be used for ASA traffic; you cannot name them or configure them for ASA features, including failover or management-only.
- You cannot configure both a traffic-forwarding interface and a service policy for ASA FirePOWER traffic.

Procedure

Step 1 Enter interface configuration mode for the physical interface you want to use for traffic-forwarding.

interface physical_interface

Example:

```
hostname(config)# interface gigabitethernet 0/5
```

Step 2 Remove any name configured for the interface. If this interface was used in any ASA configuration, that configuration is removed. You cannot configure traffic-forwarding on a named interface.

no nameif

Step 3 Enable traffic-forwarding.

traffic-forward sfr monitor-only

Note
You can ignore any warnings about traffic forwarding being for demonstration purposes only. This is a supported production mode.

Step 4 Enable the interface.

no shutdown

Repeat for any additional interfaces.

Example

The following example makes GigabitEthernet 0/5 a traffic-forwarding interface:

```
interface gigabitethernet 0/5
  no nameif
  traffic-forward sfr monitor-only
  no shutdown
```

Enable Captive Portal for Active Authentication

ASA FirePOWER includes identity policies that allow you to collect user identification information. By collecting user identity information, you can tailor access control rules to specific users and user groups,

selectively allowing and disallowing access based on the user. You can also analyze traffic based on user identity.

For HTTP/HTTPS connections, you can define identity rules that collect user identification through active authentication. If you want to implement active authentication identity rules, you must enable captive portal on the ASA to act as the authentication proxy port. When a connection matches an identity rule that requests active authentication, the ASA FirePOWER module redirects the authentication request to the ASA interface IP address/captive portal. The default port is 885, which you can change.

If you do not enable captive portal for the authentication proxy, only passive authentication is available.

Before you begin

- This feature is available in routed mode only for ASA FirePOWER 6.0+ only.
- In multiple context mode, perform this procedure within each security context.

Procedure

Step 1 Select **Tools** > **Command Line Tool**.

Step 2 Enable captive portal.

captive-portal {**global** | **interface** *name*} [**port** *number*]

Where:

- **global** enables captive portal globally on all interfaces.
- **interface** *name* enables captive portal on the specified interface only. You can enter the command multiple times to enable it on more than one interface. You can use this approach if you are redirecting traffic for only a subset of interfaces to the ASA FirePOWER module.
- **port** *number* optionally specifies the authentication port. If you do not include the keyword, port 885 is used. If you do include the keyword, the port number must be 1025 or higher.

Example:

For example, to enable captive portal globally on port 885, enter the following:

```
ciscoasa(config)# captive-portal global
ciscoasa(config)#
```

Step 3 In the ASA FirePOWER identity policy, ensure that the active authentication settings specify the same port you configured for captive portal, and configure the other required settings to enable active authentication.

Managing the ASA FirePOWER Module

This section includes procedures that help you manage the module.

Install or Reimage the Module

This section describes how to install or reimage a software module.

Install or Reimage the Software Module

If you purchase the ASA with the ASA FirePOWER module, the module software and required solid state drives (SSDs) come pre-installed and ready to configure. If you want to add the ASA FirePOWER software module to an existing ASA, or need to replace the SSD, you need to install the ASA FirePOWER boot software, partition the SSD, and install the system software according to this procedure.

Reimaging the module is the same procedure, except you should first uninstall the ASA FirePOWER module. You would reimage a system if you replace an SSD.

For information on how to physically install the SSD, see the ASA hardware guide.

Before you begin

- The free space on flash (disk0) should be at least 3GB plus the size of the boot software.
- In multiple context mode, perform this procedure in the system execution space.
- You must shut down any other software module that you might be running; the ASA can run a single software module at a time. You must do this from the ASA CLI.
- When reimaging the ASA FirePOWER module, use the **sw-module module shutdown** and **uninstall** commands to remove the old image. For example:

  sw-module module sfr shutdown
  sw-module module sfr uninstall
  reload

- If you have an active service policy redirecting traffic to an IPS or CX module, you must remove that policy. For example, if the policy is a global one, you could use **no service-policy** *ips_policy* **global**. If the service policy includes other rules you want to maintain, simply remove the redirection command from the relevant policy map, or the entire traffic class if redirection is the only action for the class. You can remove the policies using CLI or ASDM.
- If you have an active service policy redirecting traffic to another module, you must remove that policy. For example, if the policy is a global one, you could use **no service-policy** *module_policy* **global**.
- Obtain both the ASA FirePOWER Boot Image and System Software packages from Cisco.com.

Procedure

Step 1 Download the boot image to the ASA. Do not transfer the system software; it is downloaded later to the SSD. You have the following options:

- ASDM—First, download the boot image to your workstation, or place it on an FTP, TFTP, HTTP, HTTPS, SMB, or SCP server. Then, in ASDM, choose **Tools > File Management**, and then choose the appropriate **File Transfer** command, either **Between Local PC and Flash** or **Between Remote Server and Flash**. Transfer the boot software to disk0 on the ASA.

- ASA CLI—First, place the boot image on a TFTP, FTP, HTTP, or HTTPS server, then use the **copy** command to download it to flash. The following example uses TFTP.

```
ciscoasa# copy tftp://10.1.1.89/asasfr-5500x-boot-5.4.1-58.img
disk0:/asasfr-5500x-boot-5.4.1-58.img
```

Step 2 Download the ASA FirePOWER system software from Cisco.com to an HTTP, HTTPS, or FTP server accessible from the ASA FirePOWER management interface. Do not download it to disk0 on the ASA.

Step 3 Set the ASA FirePOWER module boot image location in ASA disk0 by entering the following command:

sw-module module sfr recover configure image disk0: *file_path*

Example:

```
hostname# sw-module module sfr recover configure image disk0:asasfr-5500x-boot-5.4.1-58.img
```

If you see a message like "ERROR: Another service (cxsc) is running, only one service is allowed to run at any time," it means that you already have a different software module configured. You must shut it down and remove it to install a new module as described in the prerequisites section above.

Step 4 Load the ASA FirePOWER boot image:

sw-module module sfr recover boot

Step 5 Wait approximately 5-15 minutes for the ASA FirePOWER module to boot up, and then open a console session to the now-running ASA FirePOWER boot image. You might need to press enter after opening the session to get to the login prompt. The default username is **admin** and the default password is **Admin123**.

```
hostname# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

If the module boot has not completed, the **session** command will fail with a message about not being able to connect over ttyS1. Wait and try again.

Step 6 Configure the system so that you can install the system software package:

asasfr-boot> **setup**

Example:

```
asasfr-boot> setup


                        Welcome to SFR Setup
                          [hit Ctrl-C to abort]
                      Default values are inside []
```

You are prompted for the following. Note that the management address and gateway, and DNS information, are the key settings to configure.

- Host name—Up to 65 alphanumeric characters, no spaces. Hyphens are allowed.
- Network address—You can set static IPv4 or IPv6 addresses, or use DHCP (for IPv4) or IPv6 stateless autoconfiguration.
- DNS information—You must identify at least one DNS server, and you can also set the domain name and search domain.
- NTP information—You can enable NTP and configure the NTP servers, for setting system time.

Step 7 Install the System Software image:

asasfr-boot> **system install** [**noconfirm**] *url*

Include the **noconfirm** option if you do not want to respond to confirmation messages. Use an HTTP, HTTPS, or FTP URL; if a username and password are required, you will be prompted to supply them.

When installation is complete, the system reboots. The time required for application component installation and for the ASA FirePOWER services to start differs substantially: high-end platforms can take 10 or more minutes, but low-end platforms can take 60-80 minutes or longer. (The **show module sfr** output should show all processes as Up.)

For example:

```
asasfr-boot> system install http://upgrades.example.com/packages/asasfr-sys-5.4.1-58.pkg
Verifying
Downloading
Extracting
Package Detail
        Description:                    Cisco ASA-FirePOWER 5.4.1-58 System Install
        Requires reboot:                Yes

Do you want to continue with upgrade? [y]: y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
(press Enter)
Broadcast message from root (ttyS1) (Mon Feb 17 19:28:38 2014):

The system is going down for reboot NOW!
Console session with module sfr terminated.
```

Step 8 Open a session to the ASA FirePOWER module. You will see a different login prompt because you are logging into the fully functional module.

ciscoasa# **session sfr console**

Example:

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Sourcefire ASA5555 v5.4.1 (build 58)
```

```
Sourcefire3D login:
```

Step 9 See Configure ASA FirePOWER Basic Settings, on page 11 to complete the setup.

Reset the Password

If you forget the password for the admin user, another user with CLI Configuration permissions can log in and change the password.

If there are no other users with the required permissions, you can reset the admin password from the ASA. The default password differs based on software release; see Defaults for ASA FirePOWER, on page 7.

Before you begin

- In multiple context mode, perform this procedure in the system execution space.
- The password-reset option on the ASA hw-module and sw-module commands does not work with ASA FirePOWER.

Procedure

Reset the module password for the user **admin** to the default:

session {1 | sfr} do password-reset

Use **1** for a hardware module, **sfr** for a software module.

Reload or Reset the Module

You can reload, or to reset and then reload, the module from the ASA.

Before you begin

In multiple context mode, perform this procedure in the system execution space.

Procedure

Enter the following command:

- **sw-module module sfr {reload | reset}**

Shut Down the Module

Shutting down the module software prepares the module to be safely powered off without losing configuration data.

Before you begin

- In multiple context mode, perform this procedure in the system execution space.
- If you reload the ASA, the module is not automatically shut down, so we recommend shutting down the module before reloading the ASA.

Procedure

Enter the following command:

- **sw-module module sfr shutdown**

Uninstall a Software Module Image

You can uninstall a software module image and its associated configuration.

Before you begin

In multiple context mode, perform this procedure in the system execution space.

Procedure

Step 1 Uninstall the software module image and associated configuration.

sw-module module sfr uninstall

Example:

```
ciscoasa# sw-module module sfr uninstall

Module sfr will be uninstalled. This will completely remove the disk image
associated with the sw-module including any configuration that existed within it.

Uninstall module sfr? [confirm]
```

Step 2 Reload the ASA.

reload

You must reload the ASA before you can install a new module.

Session to the Software Module From the ASA

Use the ASA FirePOWER CLI to configure basic network settings and to troubleshoot the module.

To access the ASA FirePOWER software module CLI from the ASA, you can session from the ASA.

You can either session to the module (using Telnet) or create a virtual console session. A console session might be useful if the control plane is down and you cannot establish a Telnet session. In multiple context mode, session from the system execution space.

In either a Telnet or a Console session, you are prompted for a username and password. You can log in with any username configured on the ASA FirePOWER. Initially, the **admin** username is the only one configured (and it is always available). The initial default password differs based on the type of image (full image or boot image) and software release; see Defaults for ASA FirePOWER, on page 7.

- Telnet session:

  session sfr

  When in the ASA FirePOWER CLI, to exit back to the ASA CLI, enter any command that would log you out of the module, such as **logout** or **exit**, or press **Ctrl-Shift-6, x**.

- Console session:

  session sfr console

  The only way out of a console session is to press **Ctrl-Shift-6, x**. Logging out of the module leaves you at the module login prompt.



Note Do not use the **session sfr console** command in conjunction with a terminal server where **Ctrl-Shift-6, x** is the escape sequence to return to the terminal server prompt. **Ctrl-Shift-6, x** is also the sequence to escape the ASA FirePOWER console and return to the ASA prompt. Therefore, if you try to exit the ASA FirePOWER console in this situation, you instead exit all the way to the terminal server prompt. If you reconnect the terminal server to the ASA, the ASA FirePOWER console session is still active; you can never exit to the ASA prompt. You must use a direct serial connection to return the console to the ASA prompt. Use the **session sfr** command instead of the console command when facing this situation.

Upgrade the System Software

Before applying an upgrade, ensure that the ASA is running the minimum required release for the new version; you might need to upgrade the ASA prior to upgrading the module. For more information about applying upgrades, see the Management Center online help, *FireSIGHT System User Guide 5.4*, or *Firepower Management Center Configuration Guide 6.0*.

For ASDM management, you can apply upgrades to the system software and components using **Configuration** > **ASA FirePOWER Configuration** > **Updates**. Click **Help** on the Updates page for more information.

Monitoring the ASA FirePOWER Module

The following topics provide guidance on monitoring the module. For ASA FirePOWER-related syslog messages, see the syslog messages guide. ASA FirePOWER syslog messages start with message number 434001.

Use **Tools > Command Line Interface** to use monitoring commands.

Showing Module Status

From the Home page, you can select the **ASA FirePOWER Status** tab to view information about the module. This includes module information, such as the model, serial number, and software version, and module status, such as the application name and status, data plane status, and overall status. If the module is registered to a Management Center, you can click the link to open the application and do further analysis and module configuration.

When managing the module with ASDM, you can also use the **Home > ASA FirePOWER Dashboard** page to view summary information about the software running on the module, product updates, licensing, system load, disk usage, system time, and interface status.

Showing Module Statistics

Use the show service-policy sfr command to display statistics and status for each service policy that includes the **sfr** command. Use **clear service-policy** to clear the counters.

The following example shows the ASA FirePOWER service policy and the current statistics as well as the module status. In monitor-only mode, the input counters remain at zero.

```
ciscoasa# show service-policy sfr

Global policy:
  Service-policy: global_policy
    Class-map: my-sfr-class
      SFR: card status Up, mode fail-close
        packet input 2626422041, packet output 2626877967, drop 0, reset-drop 0, proxied 0
```

Analyzing Operational Behavior (ASDM Management)

When you manage the ASA FirePOWER module using ASDM, you can view operational information for the module using these pages:

- **Home** > **ASA FirePOWER Reporting**—The reporting page provides Top 10 dashboards for a wide variety of module statistics, such as web categories, users, sources, and destinations for the traffic passing through the module.
- **Monitoring** > **ASA FirePOWER Monitoring**—There are several pages for monitoring the module, including syslog, task status, module statistics, and a real-time event viewer.

Monitoring Module Connections

To show connections through the ASA FirePOWER module, enter one of the following commands:

- **show asp table classify domain sfr**

  Shows the NP rules created to send traffic to the ASA FirePOWER module.

- **show asp drop**

  Shows dropped packets. The drop types are explained below.

- **show conn**

  Shows if a connection is being forwarded to a module by displaying the 'X - inspected by service module' flag.

The **show asp drop** command can include the following drop reasons related to the ASA FirePOWER module.

Frame Drops:

- sfr-bad-tlv-received—This occurs when ASA receives a packet from FirePOWER without a Policy ID TLV. This TLV must be present in non-control packets if it does not have the Standby/Active bit set in the actions field.
- sfr-request—The frame was requested to be dropped by FirePOWER due a policy on FirePOWER whereby FirePOWER would set the actions to Deny Source, Deny Destination, or Deny Pkt. If the frame should not have been dropped, review the policies on the module that are denying the flow.
- sfr-fail-close—The packet is dropped because the card is not up and the policy configured was 'fail-close' (rather than 'fail-open' which allows packets through even if the card was down). Check card status and attempt to restart services or reboot it.
- sfr-fail—The FirePOWER configuration was removed for an existing flow and we are not able to process it through FirePOWER it will be dropped. This should be very unlikely.
- sfr-malformed-packet—The packet from FirePOWER contains an invalid header. For instance, the header length may not be correct.
- sfr-ha-request—This counter is incremented when the security appliance receives a FirePOWER HA request packet, but could not process it and the packet is dropped.
- sfr-invalid-encap—This counter is incremented when the security appliance receives a FirePOWER packet with invalid message header, and the packet is dropped.
- sfr-bad-handle-received—Received Bad flow handle in a packet from FirePOWER Module, thus dropping flow. This counter is incremented, flow and packet are dropped on ASA as the handle for FirePOWER flow has changed in flow duration.
- sfr-rx-monitor-only—This counter is incremented when the security appliance receives a FirePOWER packet when in monitor-only mode, and the packet is dropped.

Flow Drops:

- sfr-request—The FirePOWER requested to terminate the flow. The actions bit 0 is set.
- reset-by-sfr—The FirePOWER requested to terminate and reset the flow. The actions bit 1 is set.

• sfr-fail-close—The flow was terminated because the card is down and the configured policy was 'fail-close'.

Example

The following is sample output from the **show asp table classify domain sfr** command. Note that if you configure redirection globally, only the input table will show data, and the output table will be empty. If you configure redirection by interface, both tables should contain data.

```
ciscoasa# show asp table classify domain sfr

Input Table
in  id=0x2aaae04034f0, priority=71, domain=sfr, deny=false
        hits=0, user_data=0x2aaadfdedf40, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=management, output_ifc=any

Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never
```

History for the ASA FirePOWER Module

Feature	Platform Releases	Description
ASA 5585-X (all models) support for the matching ASA FirePOWER SSP hardware module. ASA 5512-X through ASA 5555-X support for the ASA FirePOWER software module.	ASA 9.2(2.4) ASA FirePOWER 5.3.1	The ASA FirePOWER module supplies next-generation firewall services, including Next-Generation IPS (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP).You can use the module in single or multiple context mode, and in routed or transparent mode. We introduced the following screens: Home > ASA FirePOWER Status Wizards > Startup Wizard > ASA FirePOWER Basic Configuration Configuration > Firewall > Service Policy Rules > Add Service Policy Rule > Rule Actions > ASA FirePOWER Inspection
ASA 5506-X support for the ASA FirePOWER software module, including support for configuring the module in ASDM	ASA 9.3(2) ASDM 7.3(3) ASA FirePOWER 5.4.1	You can run the ASA FirePOWER software module on the ASA 5506-X. You can manage the module using FireSIGHT Management Center, or you can use ASDM. We introduced the following screens: Home > ASA FirePOWER Dashboard, Home > ASA FirePOWER Reporting, Configuration > ASA FirePOWER Configuration (including sub-pages), Monitoring > ASA FirePOWER Monitoring (including sub-pages).

Feature	Platform Releases	Description
ASA FirePOWER passive monitor-only mode using traffic redirection interfaces	ASA 9.3(2) ASA FirePOWER 5.4.1	You can now configure a traffic forwarding interface to send traffic to the module instead of using a service policy. In this mode, neither the module nor the ASA affects the traffic. We fully supported the following command: **traffic-forward sfr monitor-only**. You can configure this in CLI only.
Support for managing the module through ASDM for the 5506H-X, 5506W-X, 5508-X, and 5516-X.	ASA 9.4(1) ASDM 7.4(1) ASA FirePOWER 5.4.1	You can manage the module using ASDM instead of using FireSIGHT Management Center. No new screens or commands were added.
Support for managing the module through ASDM for the 5512-X through 5585-X.	ASA 9.5.(1.5) ASDM 7.5(1.112) ASA FirePOWER 6.0	You can manage the module using ASDM instead of using Firepower Management Center (formerly FireSIGHT Management Center). No new screens or commands were added.
Captive portal for active authentication on ASA FirePOWER 6.0.	ASA 9.5.(2) ASA FirePOWER 6.0	The captive portal feature is required to enable active authentication using identity policies starting with ASA FirePOWER 6.0. We introduced or modified the following commands: **captive-portal**, **clear configure captive-portal**, **show running-config captive-portal**.
No support in 9.10(1) for the ASA FirePOWER module on the ASA 5506-X series and the ASA 5512-X	9.10(1)	The ASA 5506-X series and 5512-X no longer support the ASA FirePOWER module in 9.10(1) and later due to memory constraints. You must remain on 9.9(x) or lower to continue using this module. Other module types are still supported. If you upgrade to 9.10(1), the ASA configuration to send traffic to the FirePOWER module will be erased; make sure to back up your configuration before you upgrade. The FirePOWER image and its configuration remains intact on the SSD. If you want to downgrade, you can copy the ASA configuration from the backup to restore functionality.