Cisco ASA FirePOWER Module Quick Start Guide

Last Updated: December 1, 2021

1. 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. The module can be a hardware module (on the ASA 5585-X only) or a software module (all other models).

For ASA model software and hardware compatibility with the ASA FirePOWER module, see Cisco ASA Compatibility.

Note: The ISA 3000 does not support the FirePOWER module in 9.17 and later.

Note: The ASA 5506-X and 5512-X do not support the FirePOWER module in 9.10 and later.

How the ASA FirePOWER Module Works with the ASA

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

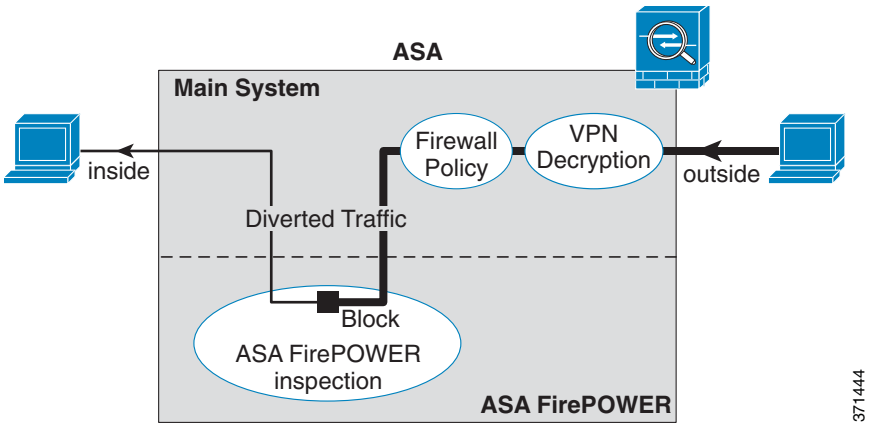
You can configure your ASA FirePOWER module in either an inline or a monitor-only (inline tap or passive) deployment. This guide only describes inline mode. See the ASA firewall configuration guide for information about inline tap and passive monitor-only modes.

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 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 Management Center—Can be hosted on a separate Firepower Management Center appliance or as a virtual appliance. Previous to version 6.0, the management center was called FireSIGHT Management Center.
- Adaptive Security Device Manager (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 configure Cloud Web Security (ScanSafe) inspection on traffic that you send to the ASA FirePOWER module. If traffic matches both your Cloud Web Security and ASA FirePOWER service policies, the traffic is forwarded to the ASA FirePOWER module only. If you want to implement both services, ensure there is no overlap between the traffic matching criteria for each service.
- 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.

Licensing Requirements for the ASA FirePOWER Module

The ASA FirePOWER module uses a separate licensing mechanism from the ASA. No licenses are pre-installed, but the box includes a PAK on a printout that lets you obtain a license activation key for the following licenses:

- **Control and Protection**—Control is also known as “Application Visibility and Control (AVC)” or “Apps”. Protection is also known as “IPS”. In addition to the activation key for these licenses, you also need “right-to-use” subscriptions for automated updates for these features.

  The **Control** (AVC) updates are included with a Cisco support contract.

  The **Protection** (IPS) updates require you to purchase the IPS subscription from http://www.cisco.com/go/ccw. This subscription includes entitlement to Rule, Engine, Vulnerability, and Geolocation updates. **Note:** This right-to-use subscription does not generate or require a PAK/license activation key for the ASA FirePOWER module; it just provides the right to use the updates.

Other licenses that you can purchase include the following:

- **Advanced Malware Protection (AMP)**
- **URL Filtering**

These licenses do generate a PAK/license activation key for the ASA FirePOWER module. See the Cisco ASA with FirePOWER Services Ordering Guide for ordering information. See also the Cisco Firepower System Feature Licenses.

If you are using ASDM for module management, to install the Control and Protection licenses and other optional licenses, see Install the Licenses (ASDM), page 11. For the licensing procedure for the Firepower Management Center, see the Cisco Firepower System Feature Licenses.

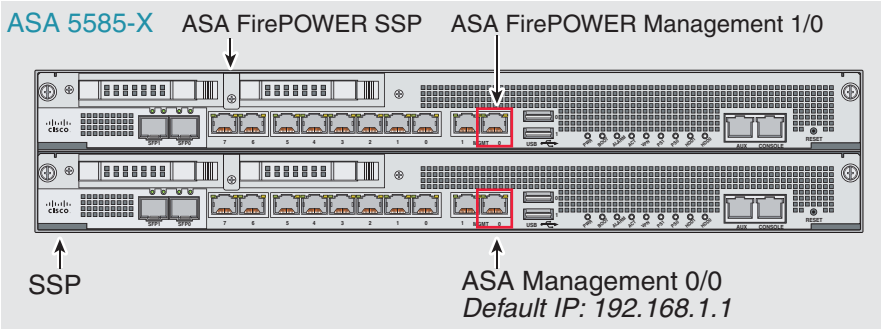
2. Deploy the ASA FirePOWER Module in Your Network

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

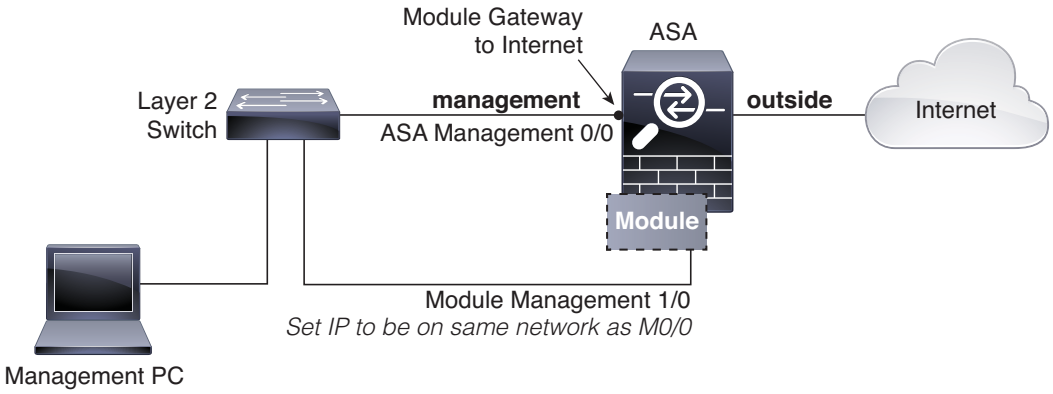
Routed Mode

ASA 5585-X (Hardware Module) in Routed Mode

The ASA FirePOWER module includes separate management interfaces from the ASA.



All management traffic to and from the ASA FirePOWER module must enter and exit the Management 1/0 or 1/1 interface. The ASA FirePOWER module also needs Internet access. Because the Management 1/x interface is not an ASA data interface, traffic cannot pass through the ASA over the backplane; therefore you need to physically cable the management interface to an ASA interface. See the following typical cabling setup to allow ASA FirePOWER access to the Internet through the ASA management interface (or you could use a data interface). Other options are possible, depending on how you want to connect your network; for example, you can make the Management 1/0 interface outside facing; or you can route between it and a different ASA interface if you have an inside router.



ASA 5506-X (Software Module) in Routed Mode (9.7 to 9.9)

Note: The ASA 5506-X does not support the FirePOWER module in 9.10 and later.

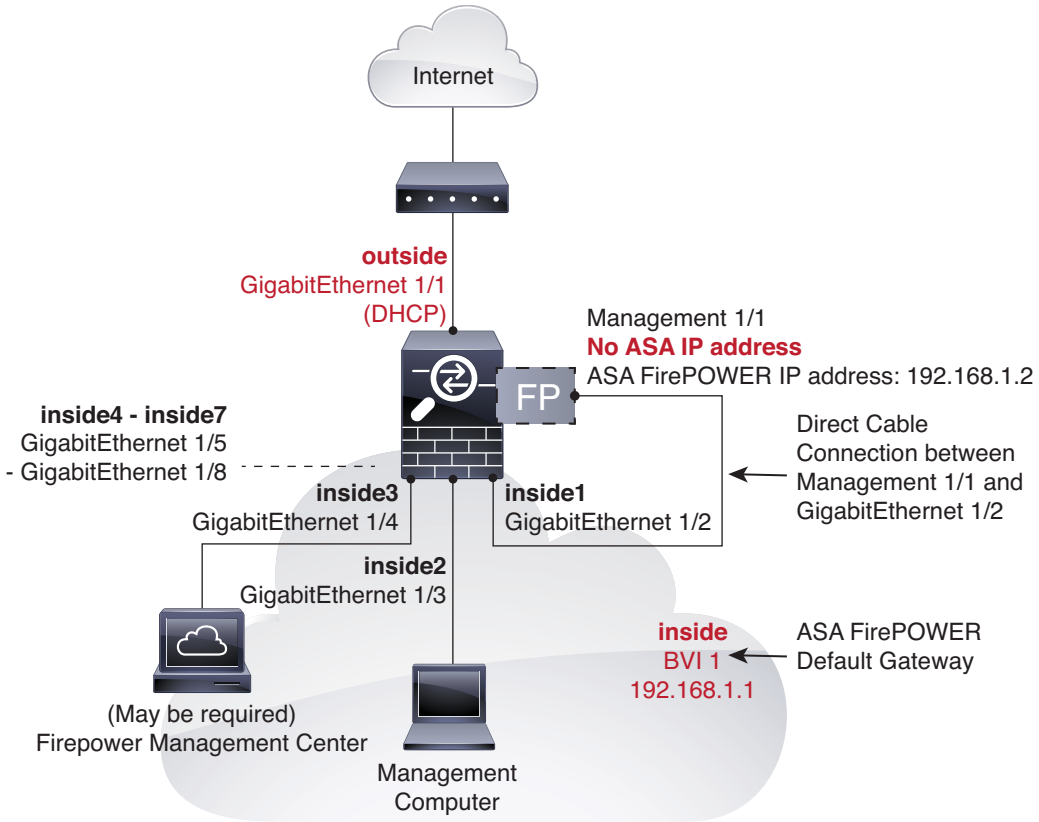
The ASA 5506-X series runs the ASA FirePOWER module as a software module, and the ASA FirePOWER module shares the Management 1/1 interface with the ASA.

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.

The following figure shows the recommended network deployment for the ASA 5506-X with the ASA FirePOWER module. This deployment includes an inside bridge group that includes all but the outside and wifi interfaces so you can use these interfaces as an alternative to an external switch.



For the ASA 5506-X on 9.7 and later, 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.

ASA 5506-X (9.6 and Earlier) through ASA 5555-X (Software Module) in Routed Mode

Note: The ASA 5506-X and 5512-X do not support the FirePOWER module in 9.10 and later.

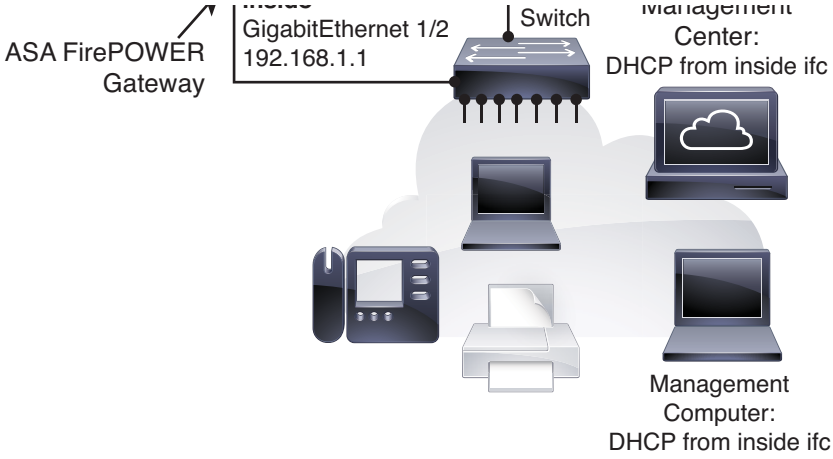
These models run the ASA FirePOWER module as a software module, and the ASA FirePOWER module shares the Management 0/0 or Management 1/1 interface (depending on your model) with the ASA.

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 5506-X on 9.6 and earlier, the ASA 5508-X, and the ASA 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.

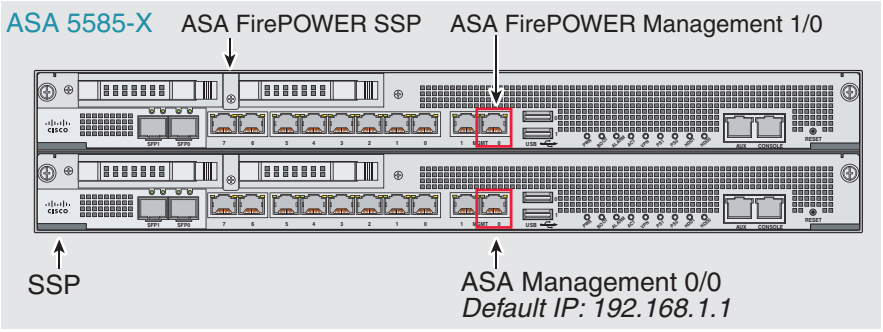
Note: For ASA 9.7 and later, you can avoid using an external switch if you have extra interfaces that you can assign to an inside bridge group. Be sure to set all bridge group interfaces to the same security level, allow same security communication, and configure NAT for each bridge group member. See 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).

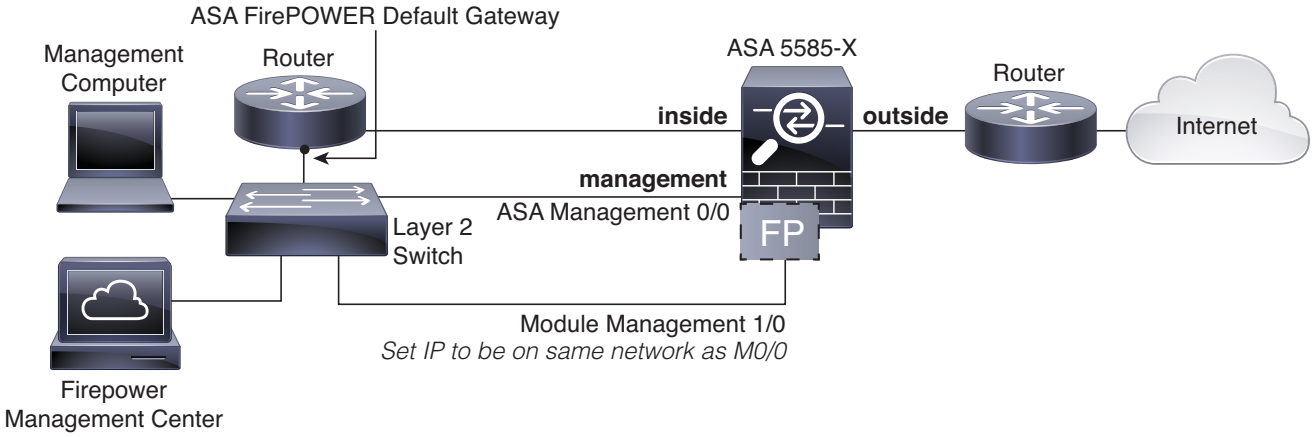
Transparent Mode

ASA 5585-X (Hardware Module) in Transparent Mode

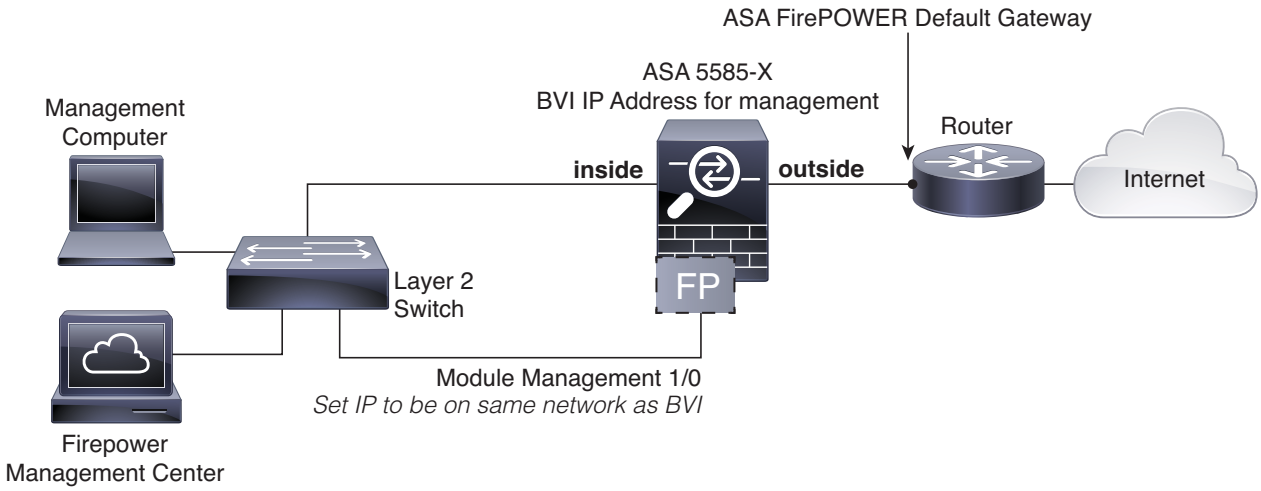
The ASA FirePOWER module includes separate management interfaces from the ASA.



All management traffic to and from the ASA FirePOWER module must enter and exit the Management 1/0 or 1/1 interface. The ASA FirePOWER module also needs Internet access. Because this interface is not an ASA data interface, traffic cannot pass through the ASA over the backplane; therefore you need to physically cable the management interface to an ASA interface. See the following typical cabling setup to allow ASA FirePOWER access to the Internet through the ASA inside interface when using an inside router.



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 0/0 interface:



Note: You can avoid using an external switch if you have extra interfaces that you can assign to the inside bridge group. 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.

ASA 5506-X through ASA 5555-X, ISA 3000 (Software Module) in Transparent Mode

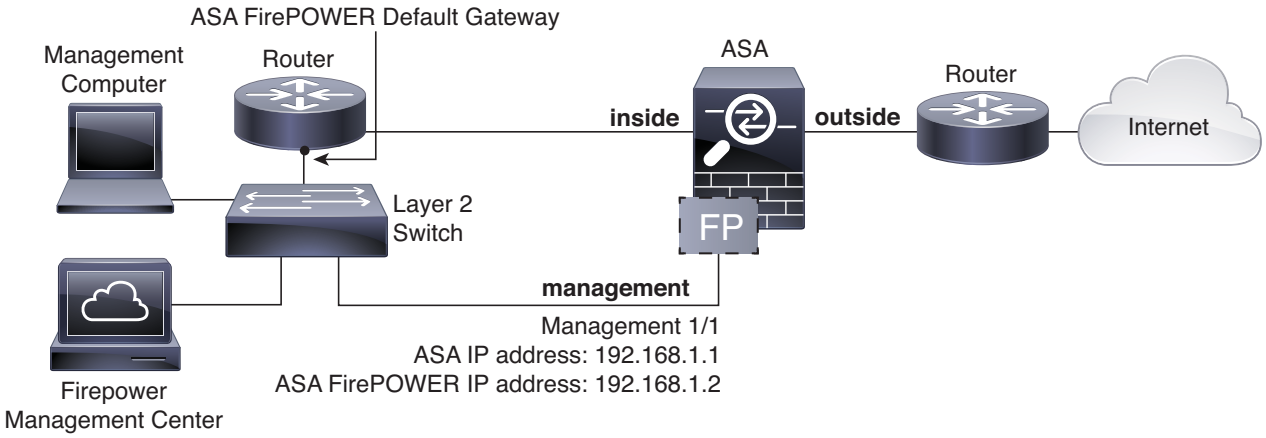
Note: The ISA 3000 does not support the FirePOWER module in 9.17 and later.

Note: The ASA 5506-X and 5512-X do not support the FirePOWER module in 9.10 and later.

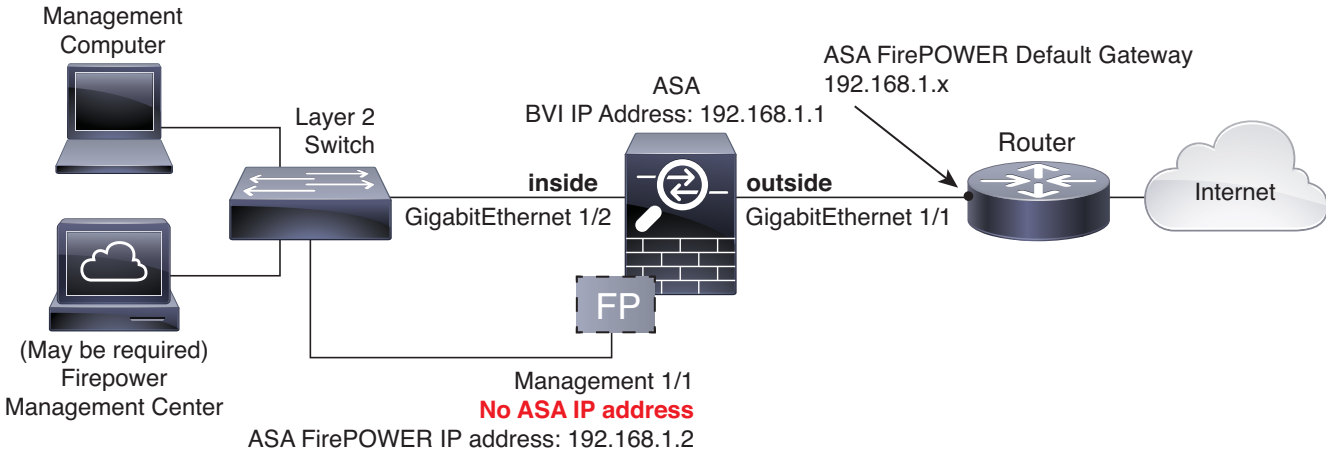
These models run the ASA FirePOWER module as a software module, and the ASA FirePOWER module shares the Management 0/0 or Management 1/1 interface (depending on your model) with the ASA.

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 when you have an inside router:



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. 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.

3. Register the ASA FirePOWER with a Management Center

To register the module with a Firepower 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.

Note: If you want to use ASDM to manage the module, skip this section and see 4. Launch ASDM, page 9.

Procedure

1. Access the ASA FirePOWER console for your model:
   - ASA 5585-X—This model includes a dedicated console port for the ASA FirePOWER module. Use the supplied DB-9 to RJ-45 serial cable and/or your own USB serial adapter.

- All other models—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 5506-X/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
  ```

Note: You can alternatively connect to the ASA FirePOWER module over SSH if you can access the default management IP address of 192.168.45.45.

2. Log in with the username **admin**. The password differs based on software release: **Adm!n123** for 7.0.1 (new device from the factory only), **Admin123** for 6.0 and later, **Sourcefire** for pre-6.0.
3. Complete the system configuration as prompted.

   Use the following network settings for the ASA FirePOWER module for the recommended network deployment (2. Deploy the ASA FirePOWER Module in Your Network, page 3):

   - Management interface: **192.168.1.2**
   - Management subnet mask: **255.255.255.0**
   - Gateway IP: **192.168.1.1**
4. Register the ASA FirePOWER module to a Firepower 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 Firepower Management Center. If the Firepower 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 Firepower Management Center.
   - *nat_id* is an optional alphanumeric string used during the registration process between the Firepower Management Center and the ASA FirePOWER module. It is required if the hostname is set to DONTRESOLVE.
5. Close the console connection. For the software module, enter:

   ```
   > exit
   ```

4. Launch ASDM

See the ASDM release notes on Cisco.com for the requirements to run ASDM.

Procedure

1. On the computer connected to the ASA, launch a web browser.
2. In the Address field, enter the following URL: **https://192.168.1.1/admin**. The **Cisco ASDM** web page appears.
3. Click one of the available options: **Install ASDM Launcher**, **Run ASDM**, or **Run Startup Wizard**.
4. Follow the onscreen instructions to launch ASDM according to the option you chose. The **Cisco ASDM-IDM Launcher** appears.

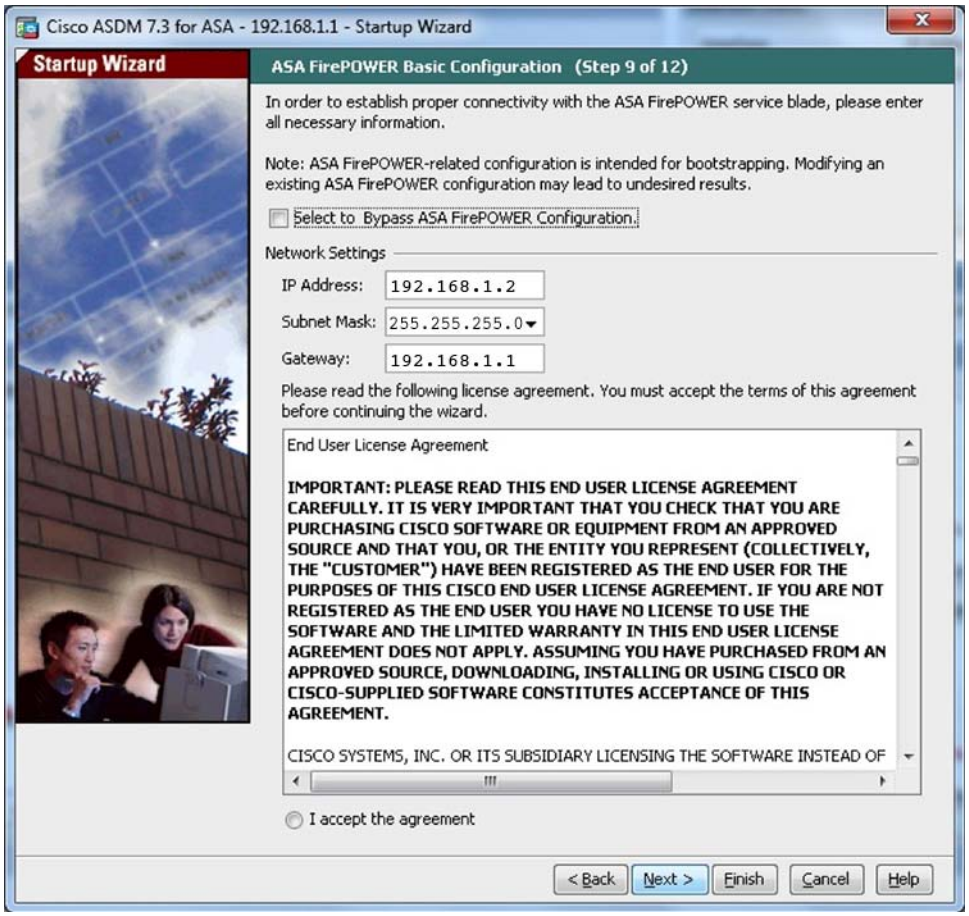
   If you click **Install ASDM Launcher**, in some cases you need to install an identity certificate for the ASA and a separate certificate for the ASA FirePOWER module according to Install an Identity Certificate for ASDM.

5. Leave the username and password fields empty, and click **OK**. The main ASDM window appears.
6. For ASDM module management only:
   a. 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.

      ASDM can change the ASA FirePOWER module IP address settings over the ASA backplane; but for ASDM to then manage the module, ASDM must be able to reach the module (and its new IP address) on the Management 1/1 interface over the network. The recommended deployment allows this access because the module IP address is on the inside network. If ASDM cannot reach the module on the network after you set the IP address, then you will see an error.

   b. Choose **Wizards > Startup Wizard**.

   c. 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

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

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

5. Configure the ASA FirePOWER Module

Install licenses, configure the module security policy, and send ASA traffic to the module.

Install the Licenses (ASDM)

The Control and Protection licenses are provided by default and the Product Authorization Key (PAK) is included on a printout in your box. If you ordered additional licenses, you should have PAKs for those licenses in your email. Use this procedure to install licenses if you are using ASDM to manage your module.

Note: For the licensing procedure for the Firepower Management Center, see the Cisco Firepower System Feature Licenses.

Procedure

1. Obtain the License Key for your chassis by choosing **Configuration > ASA FirePOWER Configuration > Licenses** and clicking **Add New License**.

   The License Key is near the top; for example, 72:78:DA:6E:D9:93:35.
2. Click **Get License** to launch the licensing portal. Alternatively, in your browser go to http://www.cisco.com/go/license.
3. Enter the PAKs separated by commas in the **Get New Licenses** field, and click **Fulfill**.
4. You will be asked for the License Key and email address among other fields.
5. Copy the resulting license activation key from either the website display or from the zip file attached to the licensing email that the system automatically delivers.
6. Return to the ASDM **Configuration > ASA FirePOWER Configuration > Licenses > Add New License** screen.
7. Paste the license activation key into the **License** box.
8. Click **Verify License** to ensure that you copied the text correctly, and then click **Submit License** after verification.
9. Click **Return to License Page**.

Configure the ASA FirePOWER Security Policy

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.

Firepower 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 3. Register the ASA FirePOWER with a Management Center, page 8. 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 online help or theFirepower Management Center configuration guide.

ASDM

Choose **Configuration > ASA FirePOWER Configuration** to configure the ASA FirePOWER security policy.

Use the ASA FirePOWER pages in ASDM for information. You can click **Help** in any page, or choose **Help > ASA FirePOWER Help Topics**, to learn more about how to configure policies.

See also the ASA FirePOWER module configuration guide.

Configure the ASA Security Policy

Redirect traffic to the ASA FirePOWER module by creating a service policy on the ASA that identifies specific traffic that you want to send.

Procedure

1. In ASDM, Choose **Configuration > Firewall > Service Policy Rules**.
2. Choose **Add > Add Service Policy Rule**.
3. Choose whether to apply the policy to a particular interface or apply it globally and click **Next**.
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**.
5. On the **Rule Actions** page, click the **ASA FirePOWER Inspection** tab.
6. Check the **Enable ASA FirePOWER for this traffic flow** check box.
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.
8. (Optional) Check **Monitor-only** to send a read-only copy of traffic to the module, i.e. 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 mode of the traffic.
9. Click **Finish** and then **Apply**.

   Repeat this procedure to configure additional traffic flows as desired.

6. Where to Go Next

- For more information about the ASA FirePOWER module and ASA operation, see the “ASA FirePOWER Module” chapter in the ASA/ASDM firewall configuration guide, or the ASDM online help. You can find links to all ASA/ASDM documentation at Navigating the Cisco ASA Series Documentation.
- For more information about ASA FirePOWER configuration, see the online help or the ASA FirePOWER module configuration guide or the Firepower Management Center configuration guide for your version.