Cisco ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X Quick Start Guide

Last Updated: October 28, 2020

The Cisco ASA 5500-X series is a powerful desktop firewall with the integrated FirePOWER software 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).

Note: ASA 9.14(x) was the final version for the ASA 5525-X, 5545-X, and 5555-X.

Note: ASA 9.12(x) was the final version for the ASA 5512-X and 5515-X.

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

1. License Requirements

ASA Licenses

The ASA 5512-X includes the **Base** or **Security Plus** license, depending on the version you ordered. The ASA 5515-X through 5555-X includes the **Base** license. You can optionally purchase the following licenses:

- **Botnet Traffic Filter**
- **TLS Proxy**
- **Security Contexts**
- **IPS Module**
- **AnyConnect Plus** or **Apex**

They also come pre-installed with the **Strong Encryption (3DES/AES)** license if you qualify for its use. If you need to manually request the Strong Encryption license (which is free), see http://www.cisco.com/go/license.

If you want to upgrade from the Base license to the Security Plus license (ASA 5512-X), or purchase other licenses, see http://www.cisco.com/go/ccw. See also the Cisco AnyConnect Ordering Guide and the AnyConnect Licensing Frequently Asked Questions (FAQ). You will then receive an email with a Product Authorization Key (PAK) so you can obtain the license activation key. For the AnyConnect licenses, you receive a multi-use PAK that you can apply to multiple ASAs that use the same pool of user sessions.

Note: The serial number used for licensing is different from the chassis serial number printed on the outside of your hardware. The chassis serial number is used for technical support, but not for licensing. To view the licensing serial number, enter the **show version | grep Serial** command or see the ASDM **Configuration > Device Management > Licensing Activation Key** page.

ASA FirePOWER Licenses

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 Firepower System Feature Licenses for more information.

To install the Control and Protection licenses and other optional licenses, see Install the Licenses, page 11.

2. Power On the ASA

1. Attach the power cable to the ASA and connect it to an electrical outlet.

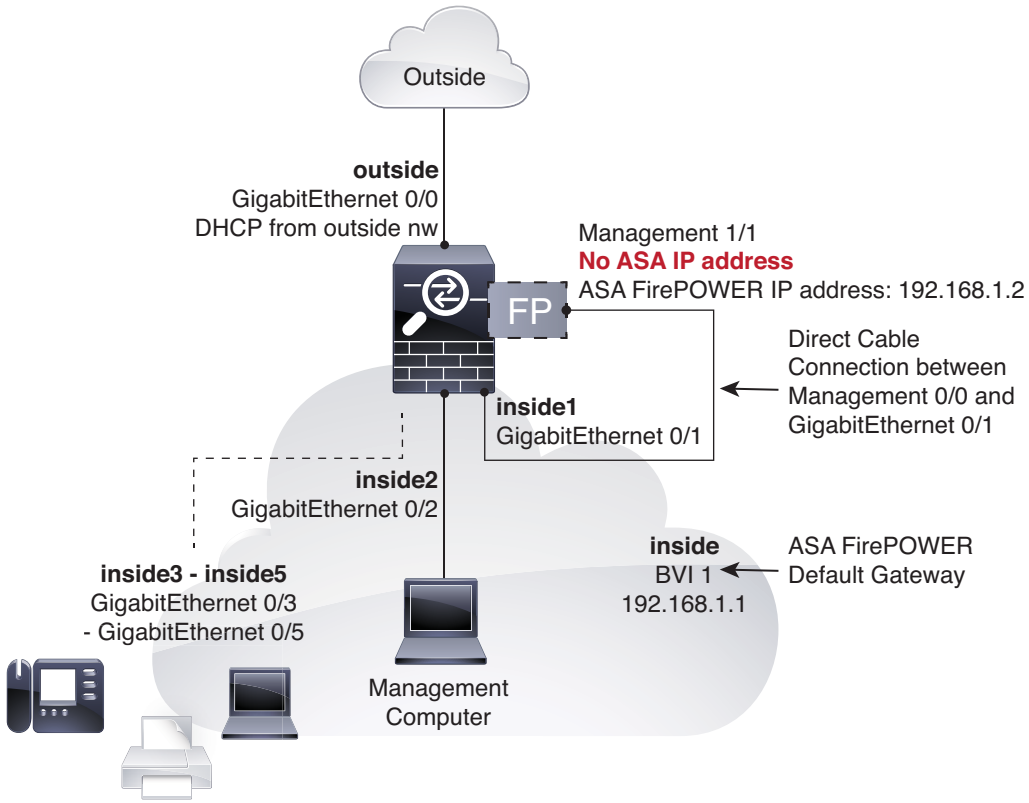
   The power turns on automatically when you plug in the power cable; do not press the power button on the front panel. (For older models, the power does not turn on automatically; check the hardware installation guide for more information).
2. Check the Power LED on the front of the ASA; if it is solid green, the device is powered on.
3. Check the Status LED on the front of the ASA; after it is solid green, the system has passed power-on diagnostics.

3. Modify the Initial Configuration for the ASA FirePOWER Module (Optional)

The ASA ships with a default configuration that enables Adaptive Security Device Manager (ASDM) connectivity to the **Management 0/0** interface. When you use a software module such as the ASA FirePOWER module, we recommend that you do *not* use the default configuration, which can preclude the ASA FirePOWER module from reaching the Internet for updates. This section describes how to apply a new configuration so the ASA FirePOWER can access the Internet. This configuration also enables a basic usable configuration for an inside and outside network.

ASA 9.7 and Later

The following figure shows the recommended network deployment for the ASA 5500-X with the ASA FirePOWER module. This deployment includes an inside bridge group that includes all but the outside interface so you can use these interfaces as an alternative to an external switch.



Note: The ASA 5525-X, 5545-X, and 5555-X include interfaces GigabitEthernet 0/0 through GigabitEthernet **0/7**.

This procedure lets you connect to the ASA console port and paste in a new configuration that configures the following behavior:

- **outside** GigabitEthernet 0/0, IP address from DHCP
- **inside** bridge group with GigabitEthernet 0/1 through 0/5 (or through 0/7 for the ASA 5525-X, 5545-X, and 5555-X) member interfaces, 192.168.1.1
- **inside --> outside** traffic flow
- **inside --> inside** traffic flow for member interfaces
- **DHCP** for clients on **inside**
- **Management 0/0** belongs to the **ASA FirePOWER module**. The interface is Up, *but otherwise unconfigured* on the ASA. The ASA FirePOWER module can then use this interface to **access the ASA inside network** and use the inside interface as the **gateway to the Internet**.

  Note: *Do not* configure an IP address for this interface in the ASA configuration. Only configure an IP address in the FirePOWER configuration. You should **consider this interface as completely separate from the ASA** in terms of routing.
- **ASDM access** on the **inside** interface
- **NAT**: Interface PAT for all traffic from inside and management to outside.

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 Management 0/0 with the appropriate configuration changes.

Procedure

1. Connect your computer to the ASA console port with the supplied console cable. You might need to use a third party serial-to-USB cable to make the connection.
2. Launch a terminal emulator and connect to the ASA.
3. Press the **Enter** key to see the following prompt:

   ```
   ciscoasa>
   ```

4. Access privileged EXEC mode:

   ```
   enable
   ```

   The following prompt appears:

   ```
   Password:
   ```

5. Press **Enter**. By default, the password is blank.
6. Access global configuration mode:

   ```
   configure terminal
   ```

7. Clear the configuration:

   ```
   clear configure all
   ```

8. Copy and paste the following configuration at the prompt. Omit commands with GigabitEthernet0/6 and GigabitEthernet0/7 and inside_6 and inside_7 for the ASA 5512-X and 5515-X.

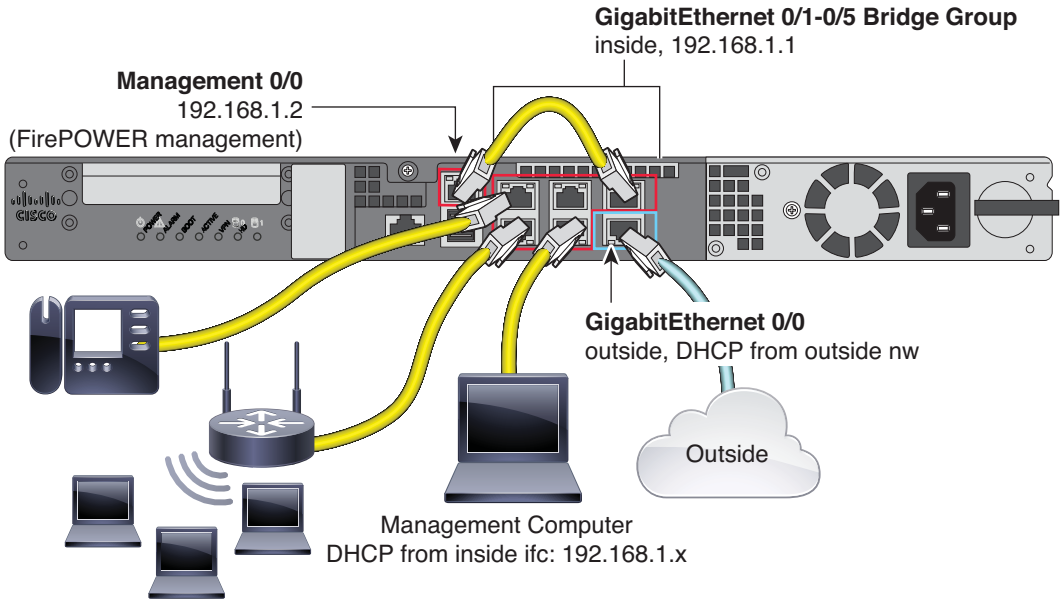
```
interface Management0/0
  no shutdown
interface GigabitEthernet0/0
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
interface bvi 1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
interface GigabitEthernet0/1
  nameif inside_1
  security-level 100
  bridge-group 1
  no shutdown
interface GigabitEthernet0/2
  nameif inside_2
  security-level 100
  no shutdown
bridge-group 1
  interface GigabitEthernet0/3
  nameif inside_3
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet0/4
  nameif inside_4
  security-level 100
  no shutdown
  bridge-group 1
```

```
interface GigabitEthernet0/5
  nameif inside_5
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet0/6
  nameif inside_6
  security-level 100
  no shutdown
  bridge-group 1
interface GigabitEthernet0/7
  nameif inside_7
  security-level 100
  no shutdown
  bridge-group 1
!
object network obj_any1
  subnet 0.0.0.0 0.0.0.0
  nat (inside_1,outside) dynamic interface
object network obj_any2
  subnet 0.0.0.0 0.0.0.0
  nat (inside_2,outside) dynamic interface
object network obj_any3
  subnet 0.0.0.0 0.0.0.0
  nat (inside_3,outside) dynamic interface
object network obj_any4
  subnet 0.0.0.0 0.0.0.0
  nat (inside_4,outside) dynamic interface
object network obj_any5
  subnet 0.0.0.0 0.0.0.0
  nat (inside_5,outside) dynamic interface
object network obj_any6
  subnet 0.0.0.0 0.0.0.0
  nat (inside_6,outside) dynamic interface
object network obj_any7
  subnet 0.0.0.0 0.0.0.0
  nat (inside_7,outside) dynamic interface
!
same-security-traffic permit inter-interface
!
http server enable
http 192.168.1.0 255.255.255.0 inside_1
http 192.168.1.0 255.255.255.0 inside_2
http 192.168.1.0 255.255.255.0 inside_3
http 192.168.1.0 255.255.255.0 inside_4
http 192.168.1.0 255.255.255.0 inside_5
http 192.168.1.0 255.255.255.0 inside_6
http 192.168.1.0 255.255.255.0 inside_7
!
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
!
logging asdm informational
```

9. Save the new configuration:

```
write memory
```

10. Cable the following:



a. Cable Management 0/0 (for the ASA FirePOWER module) directly to one of: GigabitEthernet 0/1 through GigabitEthernet 0/5 (through 0/7 for the ASA 5525-X, 5545-X, and 5555-X).

Note: You can connect inside and management on the same network because the management interface acts like a separate device that belongs only to the ASA FirePOWER module.

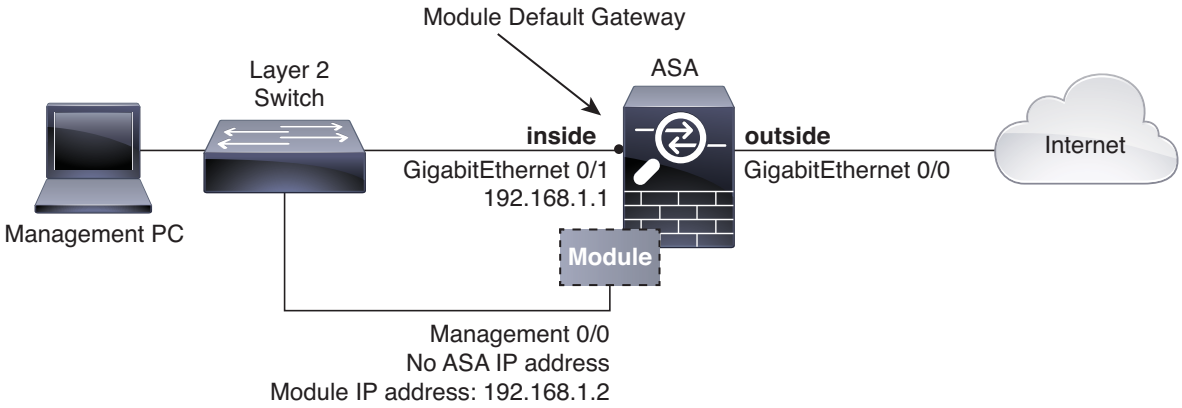
b. Cable your computer to one of: GigabitEthernet 0/1 through GigabitEthernet 0/5 (through 0/7 for the ASA 5525-X, 5545-X, and 5555-X).

c. Cable GigabitEthernet 0/0 (outside) to your WAN device, for example, your cable modem.

Note: If the cable modem supplies an outside IP address that is on 192.168.1.0/24 or 192.168.10.0/24, then you must change the ASA configuration to use a different IP address. Interface IP addresses, HTTPS (ASDM) access, and DHCP server settings can all be changed using the Startup Wizard. If you change the IP address to which you are connected to ASDM, you will be disconnected when you finish the wizard. You must reconnect to the new IP address.

ASA 9.6 and Earlier

The following figure shows the suggested network deployment for the ASA 5500-X with the ASA FirePOWER module:



Note: If you have an inside *router* instead of a switch, you can skip this section and instead configure the ASA to route between management and an inside network. In this case, configure the ASA and the ASA FirePOWER Management 0/0 IP addresses to be on the same network. Be sure to configure appropriate routes on the ASA and on the ASA FirePOWER so the management network can reach the inside network, and vice versa.

This procedure lets you connect to the ASA console port and paste in a new configuration that configures the following behavior:

- **inside** --> **outside** traffic flow
- **outside IP** address from **DHCP**
- **DHCP** for clients on **inside**
- **Management 0/0** belongs to the **ASA FirePOWER module**. The interface is Up, *but otherwise unconfigured* on the ASA. The ASA FirePOWER can then use this interface to **access the ASA inside network** and use the inside interface as the **gateway to the Internet**.

  Note: *Do not* configure an IP address for this interface in the ASA configuration. Only configure an IP address in the module configuration. You should **consider this interface as completely separate from the ASA** in terms of routing.
- **ASDM** access on the **inside** interface

To achieve the above configuration, perform the following steps.

Procedure

1. Connect your computer to the ASA console port with the supplied console cable. You might need to use a third party serial-to-USB cable to make the connection.
2. Launch a terminal emulator and connect to the ASA.
3. Press the **Enter** key to see the following prompt:

   ```
   ciscoasa>
   ```
4. Access privileged EXEC mode:

   ```
   enable
   ```

   The following prompt appears:

   ```
   Password:
   ```
5. Press **Enter**. By default, the password is blank.
6. Access global configuration mode:

   ```
   configure terminal
   ```
7. Clear the configuration:

   ```
   clear configure all
   ```
8. Copy and paste the following configuration at the prompt:

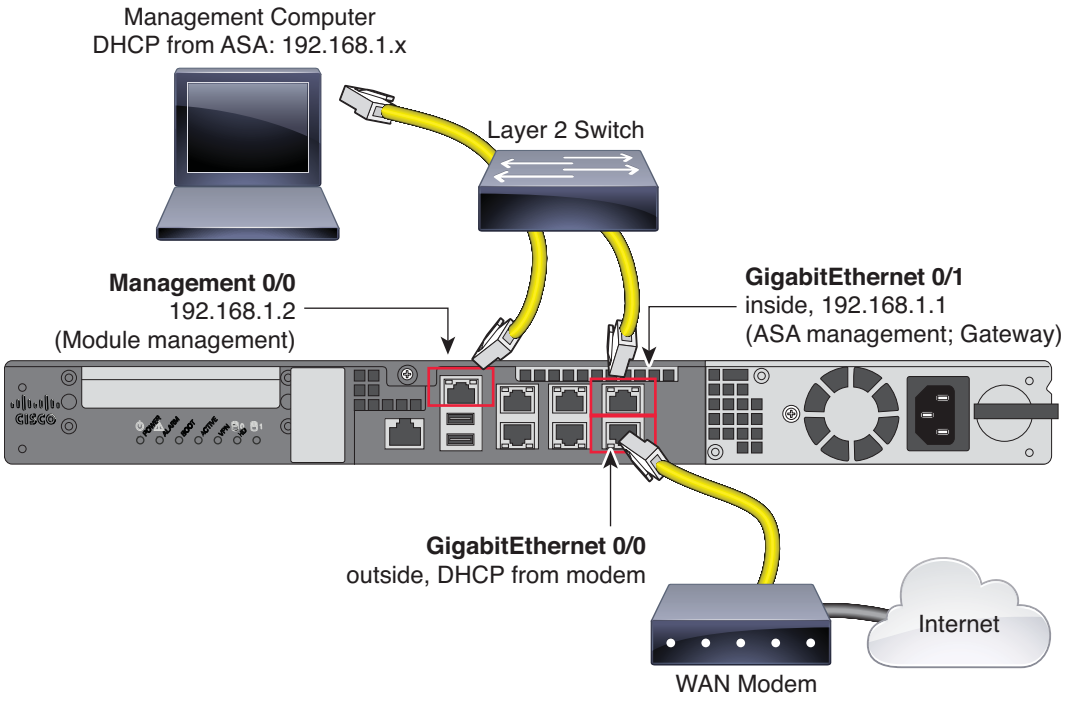
   ```
   interface management0/0
     no shutdown
   interface gigabitethernet0/0
     nameif outside
     ip address dhcp setroute
     no shutdown
   interface gigabitethernet0/1
     nameif inside
     ip address 192.168.1.1 255.255.255.0
     security-level 100
   ```

```
  no shutdown
!
object network obj_any
  subnet 0 0
  nat (any,outside) dynamic interface
!
http server enable
http 192.168.1.0 255.255.255.0 inside
!
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
!
logging asdm informational
```

9. Save the new configuration:

```
write memory
```

1. Cable the following:



a. Cable the following to a Layer 2 Ethernet switch:

- GigabitEthernet 0/1 interface (inside)
- Management 0/0 interface (for the module)
- Your computer

Note: You can connect inside and management on the same network because the management interface acts like a separate device that belongs only to the ASA FirePOWER module.

b. Connect the outside GigabitEthernet 0/0 interface to your upstream router or WAN device.

Note: If the cable modem supplies an outside IP address that is on 192.168.1.0/24 or 192.168.10.0/24, then you must change the ASA configuration to use a different IP address. Interface IP addresses, HTTPS (ASDM) access, and DHCP server settings can all be changed using the Startup Wizard. If you change the IP address to which you are connected to ASDM, you will be disconnected when you finish the wizard. You must reconnect to the new IP address.

5. Launch ASDM

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

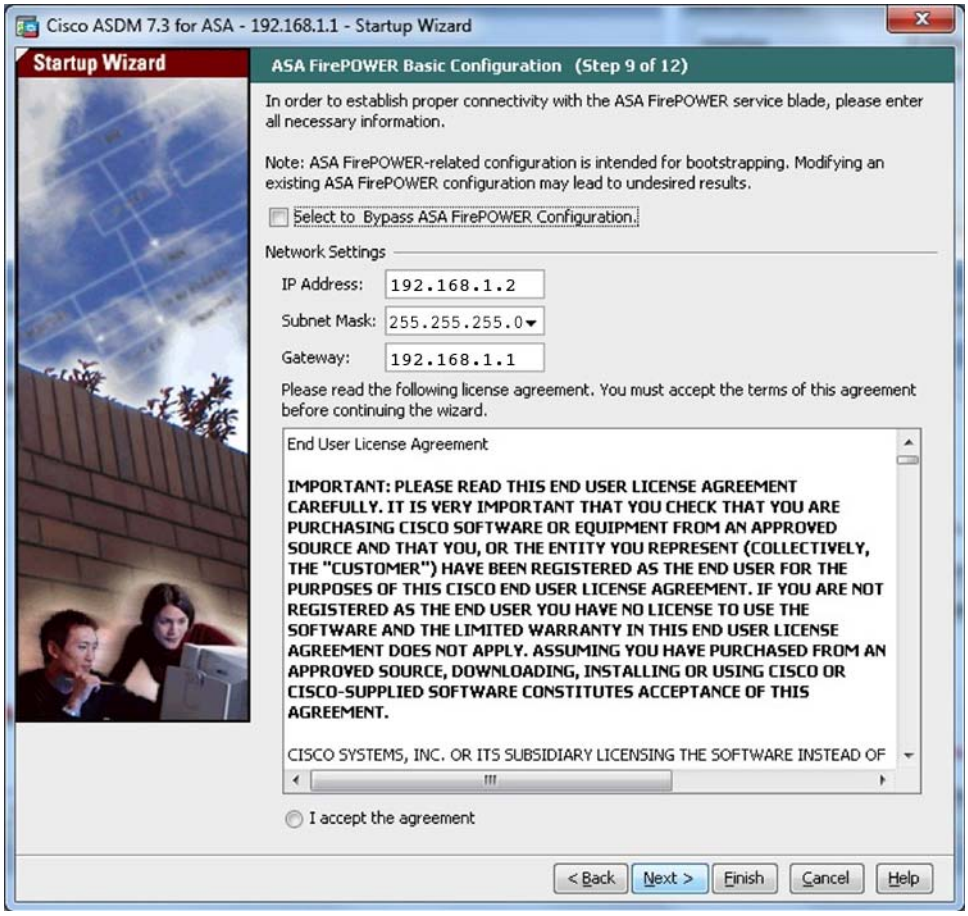
This procedure assumes you want to use ASDM to manage the ASA FirePOWER Module. If you want to use the Firepower Management Center, then you need to connect to the module CLI and run the setup script; see the ASA FirePOWER quick start guide.

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. 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 0/0 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.
7. Choose **Wizards > Startup Wizard**.
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

9. Click **I accept the agreement**, and click **Next** or **Finish** to complete the wizard.
10. Quit ASDM, and then relaunch. You should see **ASA FirePOWER** tabs on the Home page.

6. Run Other ASDM Wizards and Advanced Configuration

ASDM includes many wizards to configure your security policy. See the **Wizards** menu for all available wizards.

To continue configuring your ASA, see the documents available for your software version at Navigating the Cisco ASA Series Documentation.

7.Configure the ASA FirePOWER Module

Use ASDM to install licenses, configure the module security policy, and send traffic to the module.

Note: You can alternatively use the Firepower Management Center to manage the ASA FirePOWER module. See the ASA FirePOWER Module Quick Start Guide for more information.

Install the Licenses

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.

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

Procedure

1. 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 user guide.

Configure the ASA Security Policy

Procedure

1. To send traffic to the module, 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. passive mode.
9. Click **Finish** and then **Apply**.

   Repeat this procedure to configure additional traffic flows as desired.

8. 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.