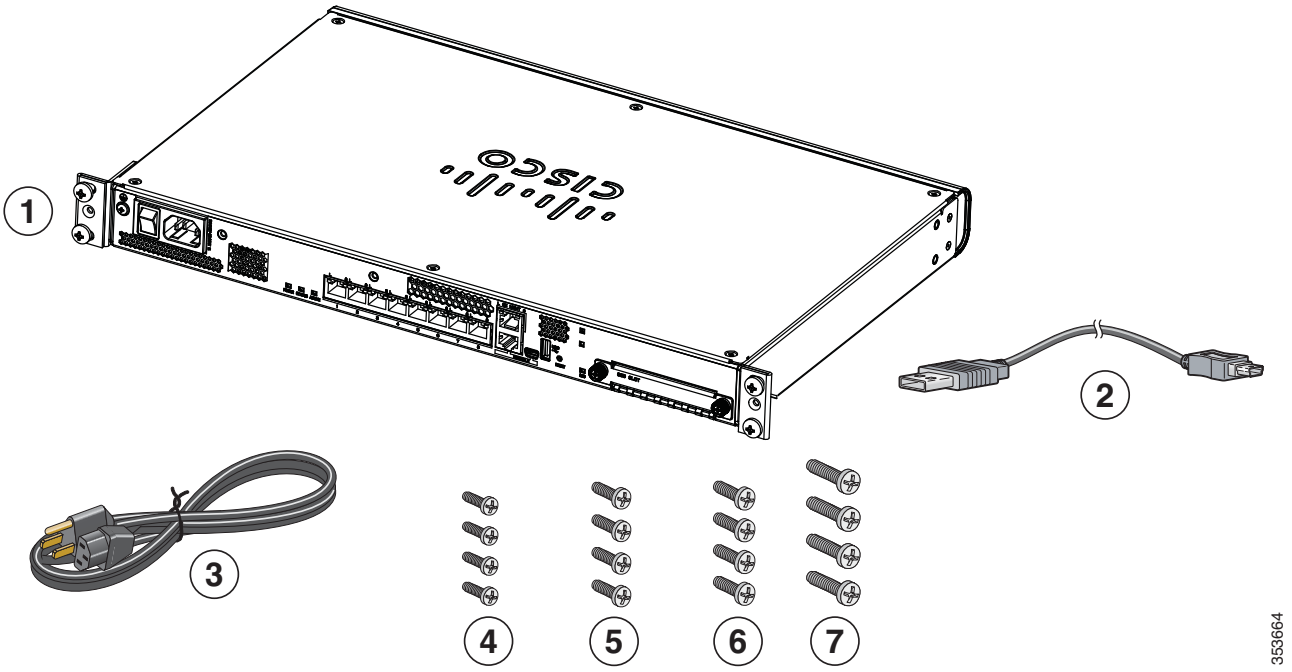
Cisco ASA 5508-X and ASA 5516-X Quick Start Guide

First Published: April 7, 2015
Last Updated: January 23, 2017

1. Package Contents

This section lists the package contents of the chassis. Note that contents are subject to change, and your exact contents might contain additional or fewer items.



1	ASA 5508-X or ASA 5516-X chassis	2	USB Console Cable (Type A to Type B)
3	Power cable	4	4 10-32 Phillips Screws for rack mounting
5	4 12-24 Phillips Screws for rack mounting	6	4 M6 Phillips Screws for rack mounting
7	4 M4 Phillips Screws for rack mounting		

2. License Requirements

ASA Licenses

The ASA 5508-X or ASA 5516-X includes the **Base** license by default, along with the **Strong Encryption (3DES/AES)** license if you qualify for its use. You can also purchase the following licenses:

- **Security Context**
- **AnyConnect Plus** or **Apex**

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, or purchase an AnyConnect license, 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:

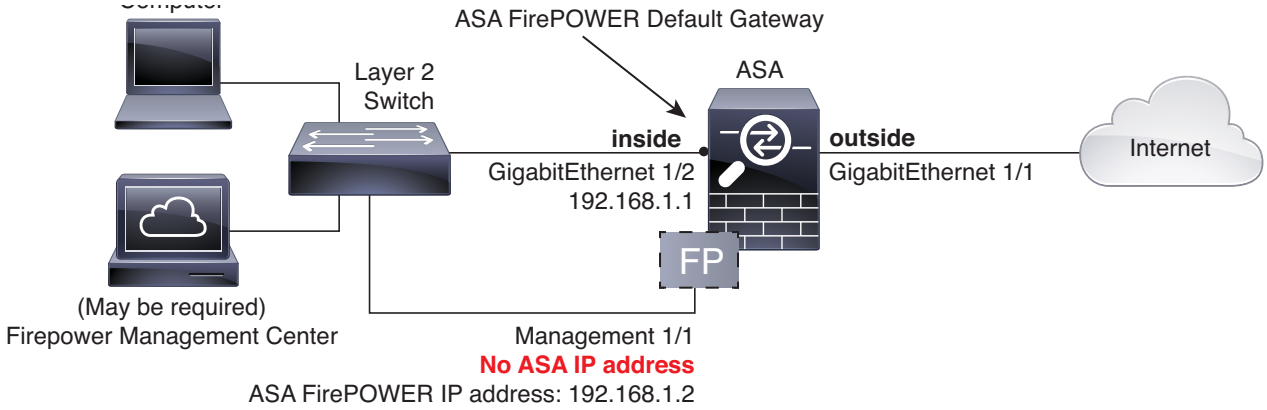
- **Advanced Malware Protection (AMP)**
- **URL Filtering**

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

To install the Control and Protection licenses and other optional licenses, see Install the Licenses, page 6.

3. Deploy the ASA 5508-X or ASA 5516-X in Your Network

The following figure shows the recommended network deployment for the ASA 5508-X or ASA 5516-X with the ASA FirePOWER module:



Note: You must use a separate inside switch in your deployment.

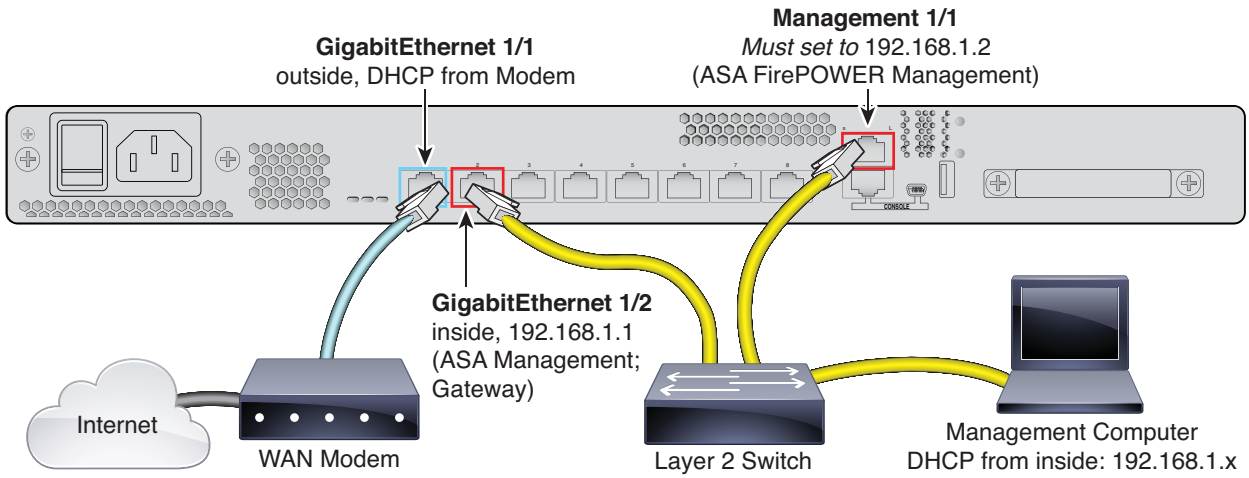
The default configuration enables the above network deployment with the following behavior.

- **inside --> outside** traffic flow
- **outside IP** address from **DHCP**
- **DHCP** for clients on **inside**
- **Management 1/1** 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

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 1/1 with the appropriate configuration changes.

Procedure



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

- GigabitEthernet 1/2 interface (inside)
- Management 1/1 interface (for the ASA FirePOWER 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.

2. Connect the GigabitEthernet 1/1 (outside) interface 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, 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.

4. Power On the ASA

1. Attach the power cable to the ASA and connect it to an electrical outlet.
2. Press the Power button on the back of the ASA.
3. Check the Power LED on the front of the ASA; if it is solid green, the device is powered on.
4. Check the Status LED on the front of the ASA; after it is solid green, the system has passed power-on diagnostics.

5. Launch ASDM

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

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

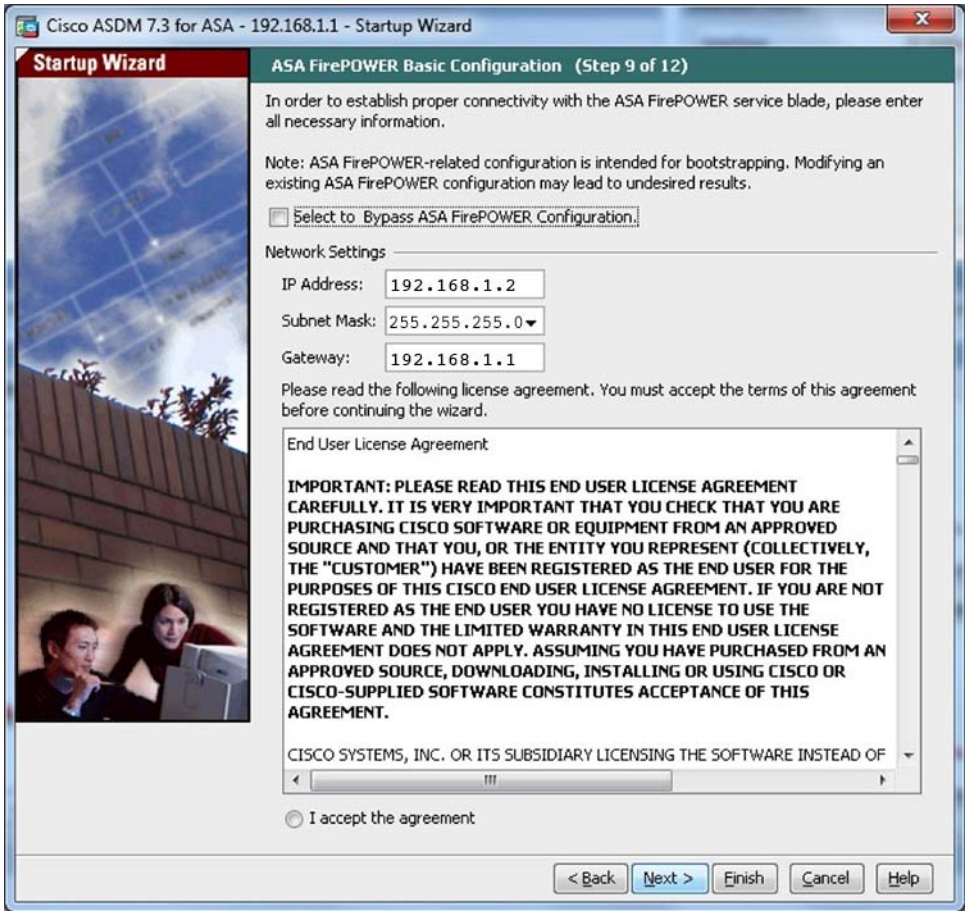
Procedure

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 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.

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 user guide or the FireSIGHT/Firepower Management Center system user guide.