Cisco Firepower Threat Defense for the ASA 5506-X Series Using Firepower Device Manager Quick Start Guide

First Published: August 10, 2016

Last Updated: December 3, 2018

Warning: You cannot install Firepower Threat Defense 6.3 or subsequent releases on the ASA 5506-X, 5506W-X, and 5506H-X. The final supported Firepower Threat Defense release for these platforms is 6.2.3.

1. Is This Guide for You?

This guide explains how to complete the initial configuration of your Firepower Threat Defense device using the Firepower Device Manager web-based device setup wizard included on Firepower Threat Defense devices.

Firepower Device Manager lets you configure the basic features of the software that are most commonly used for small networks. It is especially designed for networks that include a single device or just a few, where you do not want to use a high-powered multiple-device manager to control a large network containing many Firepower Threat Defense devices.

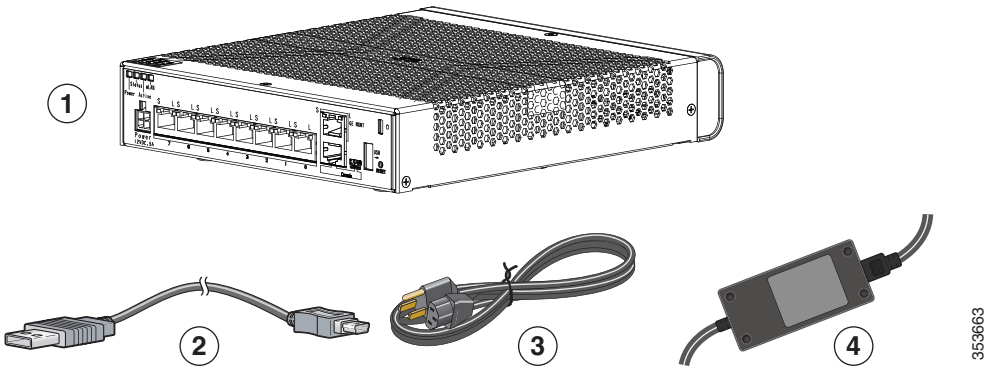
If you are managing large numbers of devices, or if you want to use the more complex features and configurations that Firepower Threat Defense allows, use the Firepower Management Center to configure your devices instead of the integrated Firepower Device Manager.

Use the CLI setup wizard to configure your Firepower Threat Defense device for network connectivity and to register the device to a Firepower Management Center as described in http://www.cisco.com/go/ftd-asa-quick.

2. Package Contents

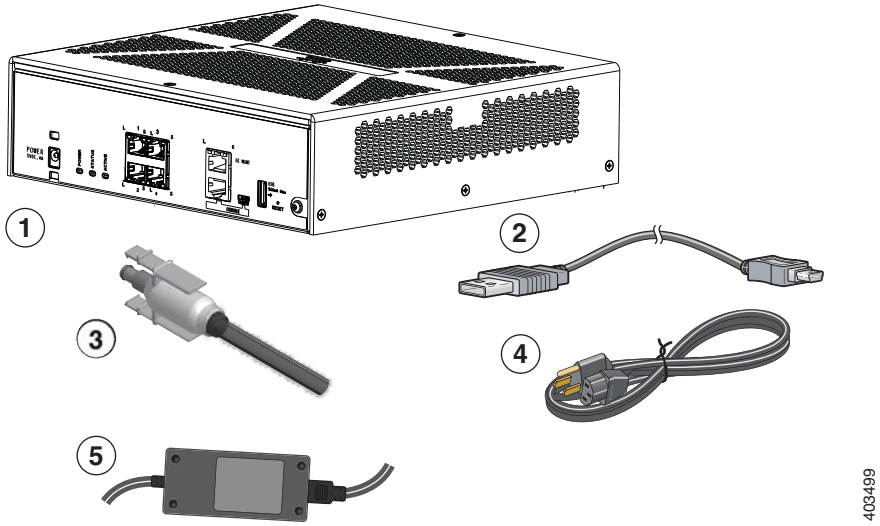
This section lists the package contents of the chassis. Note that contents are subject to change, and your exact contents might contain additional or fewer items.

Figure 1 ASA 5506-X and 5506W-X



1	ASA 5506-X or ASA 5506W-X chassis	2	USB Console Cable (Type A to Type B)
3	Power cable	4	Power supply

Figure 2 ASA 5506H-X



1	ASA 5506H-X chassis	2	Blue Console Cable and Serial PC Terminal Adapter (DB-9 to RJ-45)
3	Power cord retention lock	4	Power cable
5	Power supply		

3. License Requirements

Firepower Threat Defense devices require Cisco Smart Licensing. Smart Licensing lets you purchase and manage a pool of licenses centrally. Unlike product authorization key (PAK) licenses, Smart Licenses are not tied to a specific serial number or license key. Smart Licensing lets you assess your license usage and needs at a glance.

In addition, Smart Licensing does not prevent you from using product features that you have not yet purchased. You can start using a license immediately, as long as you are registered with the Cisco Smart Software Manager, and purchase the license later. This allows you to deploy and use a feature, and avoid delays due to purchase order approval.

When you purchase one or more Smart Licenses for Firepower features, you manage them in the Cisco Smart Software Manager: http://www.cisco.com/web/ordering/smart-software-manager/index.html. The Smart Software Manager lets you create a master account for your organization. For more information about the Cisco Smart Software Manager, see the *Cisco Smart Software Manager User Guide*.

Your purchase of a Firepower Threat Defense device or Firepower Threat Defense Virtual automatically includes a Base license. All additional licenses (Threat, Malware, or URL Filtering) are optional. For more information about Firepower Threat Defense licensing, see the "Licensing the System" chapter of the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*.

4. Deploy the Firepower Threat Defense in Your Network

Note: The default configuration to use Firepower Device Manager to configure a Firepower Threat Defense device, which includes the inside address and management address, changed in Version 6.2. See Figure 3 on page 3 for the default topology for Version 6.2, and Figure 4 on page 4 for the default topology for Version 6.1.

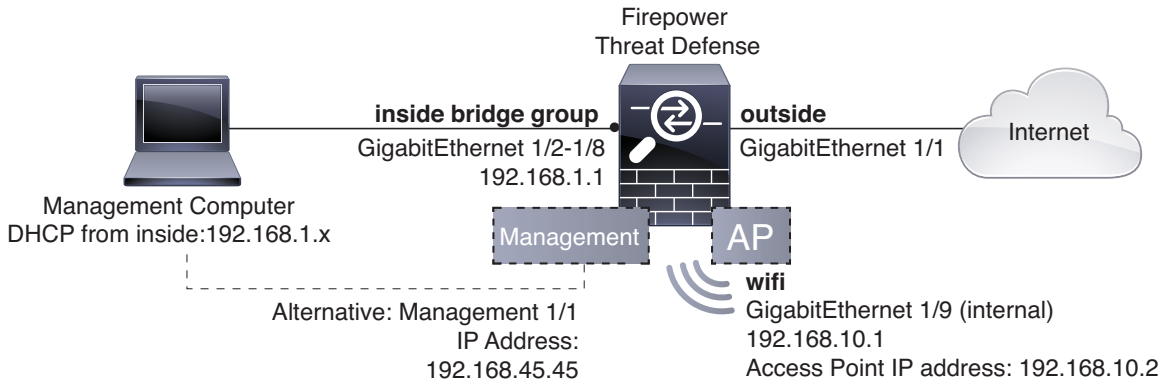
About the Default Configuration (Version 6.2)

Except for the first data interface, and the Wi-Fi interface on an ASA 5506W-X, all other data interfaces on these device models are structured into the "inside" bridge group and enabled. There is a DHCP server on the inside bridge group. You can plug endpoints or switches into any bridged interface and endpoints get addresses on the 192.168.1.0/24 network.

For complete information about the default configuration and the options you have to configure bridged interfaces, see the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*.

The following figure shows the recommended network deployment for Firepower Threat Defense on the ASA 5506-X series of appliances, including the ASA 5506W-X with the built-in wireless access point.

Figure 3 Suggested Network Deployment - Version 6.2



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

- **inside --> outside** traffic flow
- **outside IP** address from **DHCP**
- (ASA 5506W-X) **wifi <--> inside**, **wifi --> outside** traffic flow
- **DHCP** for clients on **inside** and **wifi**. There is a DHCP server on the inside bridge group. You can plug endpoints or switches directly into one of the bridged interfaces and get addresses on the 192.168.1.0/24 network. There is a DHCP server on the wifi interface for the access point itself and all its clients.

  HTTPS access is enabled on the inside bridge group, so you can open Firepower Device Manager through any inside bridge group member interface at the default address, 192.168.1.1.

- Alternatively, you can connect to **Management 1/1** to set up and manage the device using the Firepower Device Manager. There is a DHCP server on the management interface. You can plug your management computer directly into this interface and get an address on the 192.168.45.0/24 network.

  HTTPS access is enabled on the management interface, so you can open Firepower Device Manager through the management interface at the default address, 192.168.45.45.

  The default gateway for the management IP address is to use the data interfaces to route to the Internet. Thus, you do not need to wire the Management physical interface to a network.

  Note: The physical management interface is shared between the Management logical interface and the Diagnostic logical interface; see the "Interfaces" chapter of the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*.

- The Firepower Threat Defense system requires Internet access for licensing and updates. The system can obtain system database updates through the gateway for the outside interface. You do not need to have an explicit route from the management port or network to the Internet. The default is to use internal routes through the data interfaces.

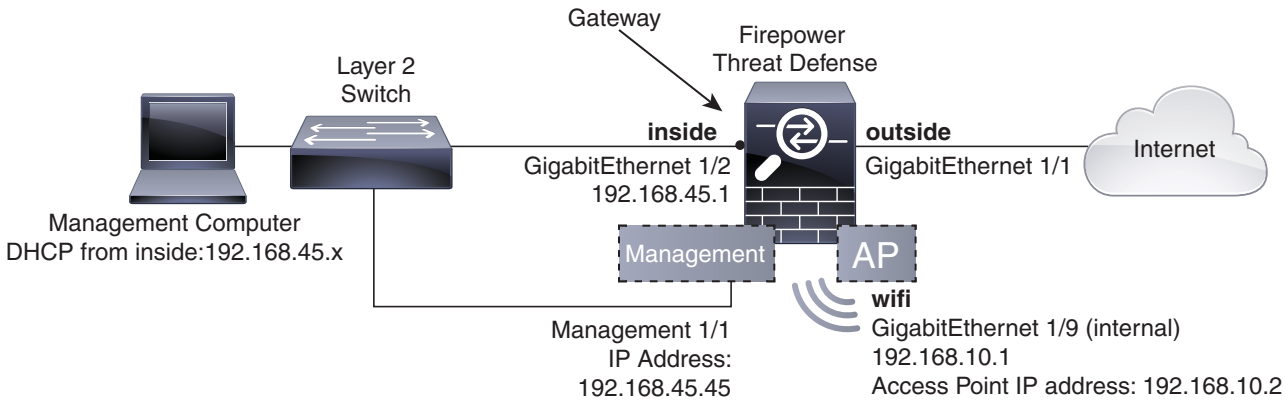
About the Default Configuration (Version 6.1)

The default configuration assumes that you will connect the management and inside interfaces to the same network using a switch. The inside interface is configured as a DHCP server, so you can attach your management workstation to the same switch and get an address through DHCP on the same network. Then you can open the Firepower Device Manager web interface.

For complete information about the default configuration, see the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*.

The following figure shows the recommended network deployment for Firepower Threat Defense on the ASA 5506-X series of appliances, including the ASA 5506W-X with the built-in wireless access point.

Figure 4 Suggested Network Deployment - Version 6.1



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

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

- **inside --> outside** traffic flow
- **outside IP** address from **DHCP**
- (ASA 5506W-X) **wifi <--> inside**, **wifi --> outside** traffic flow
- **DHCP** for clients on **inside** and **wifi**. The access point itself and all its clients use the ASA as the DHCP server.
- **Management 1/1** is used to set up and manage the device using the Firepower Device Manager, a simplified single-device manager included on the box.

The Management interface requires Internet access for updates. When you put Management on the same network as an inside interface, you can deploy the Firepower Threat Defense device with only a switch on the inside and point to the inside interface as its gateway.

The physical management interface is shared between the Management logical interface and the Diagnostic logical interface; see the “Interfaces” chapter of the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*.

Connect the Interfaces

The default configuration assumes that certain interfaces are used for the inside and outside networks. Initial configuration will be easier to complete if you connect network cables to the interfaces based on these expectations. To cable the above scenario on the ASA 5506-X series, see the following illustrations.

Note: The following illustrations show a simple topology using a management computer connected to the inside network. Other topologies can be used and your deployment will vary depending on your basic logical network connectivity, ports, addressing, and configuration requirements.

Version 6.2

Figure 5 ASA 5506W-X (with Wi-Fi), 5506-X (without Wi-Fi) for Version 6.2.

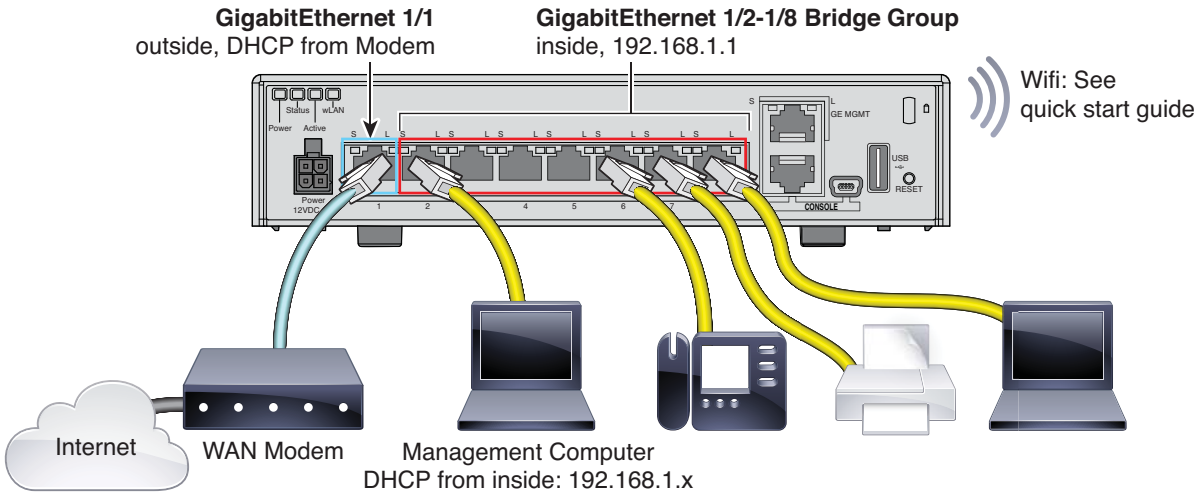
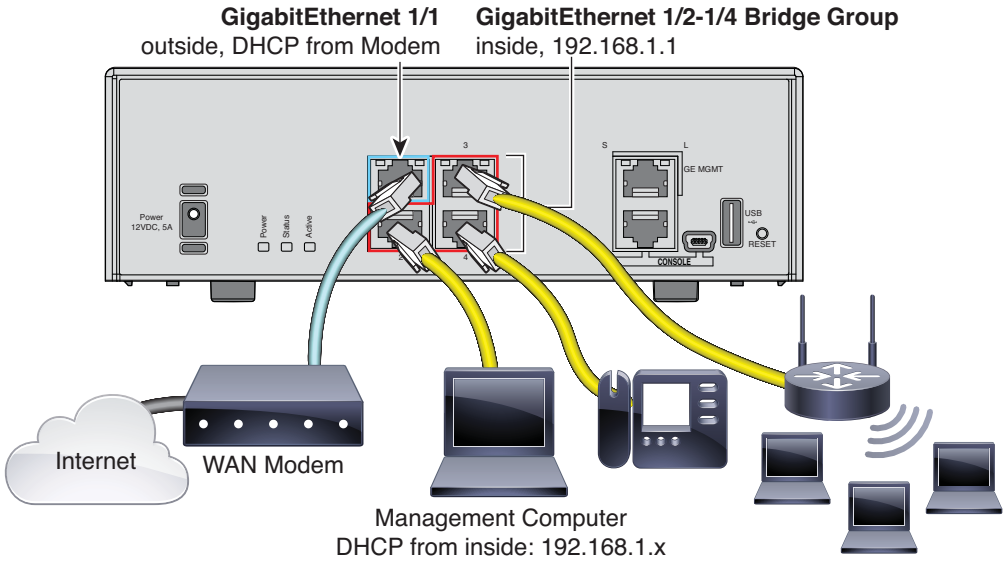


Figure 6 ASA 5506H-X for Version 6.2.



Procedure

1. Connect the GigabitEthernet 1/1 (outside) interface to your ISP/WAN modem or other outside device. By default, the IP address is obtained using DHCP, but you can set a static address during initial configuration.
2. Connect a local management workstation to GigabitEthernet 1/2 (or another of the inside bridge group member interfaces).
3. Configure the workstation to obtain an IP address using DHCP. The workstation gets an address on the 192.168.1.0/24 network.

   Note: You have a couple of other options for connecting the management workstation. You can also directly connect it to the Management port. The workstation gets an address through DHCP on the 192.168.45.0/24 network. Another option is to leave your workstation attached to a switch, and attach that switch to one of the inside ports such as GigabitEthernet1/2. However, you must ensure that no other device on the switch's network is running a DHCP server, because it will conflict with the one running on the inside bridge group, 192.168.1.1.

Version 6.1

Figure 7 ASA 5506W-X (with Wi-Fi), 5506-X (without Wi-Fi) for Version 6.1.

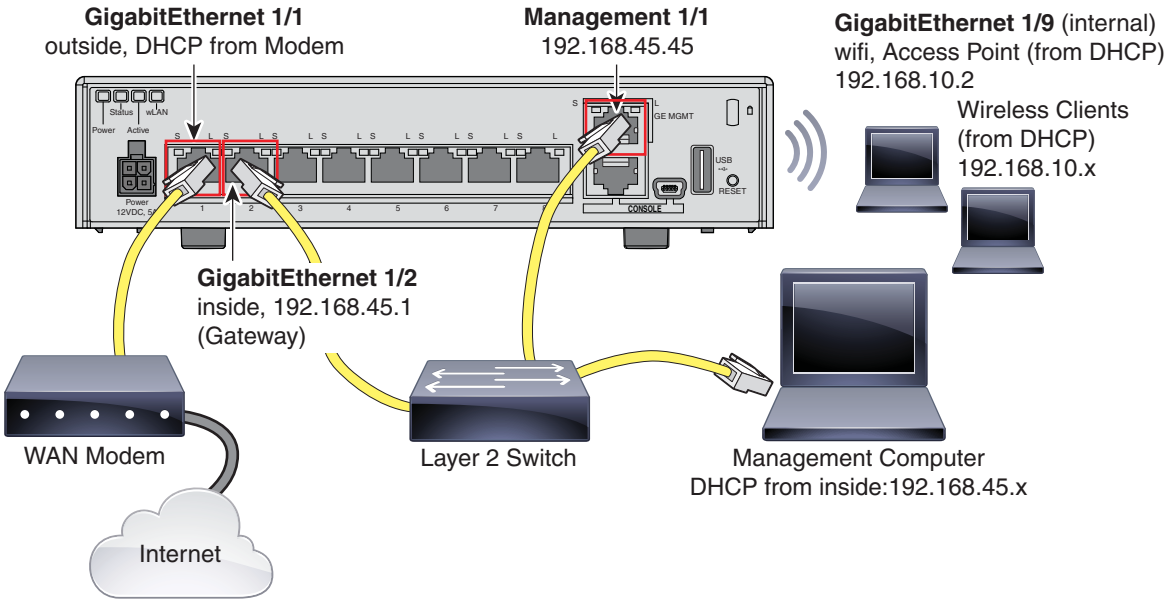
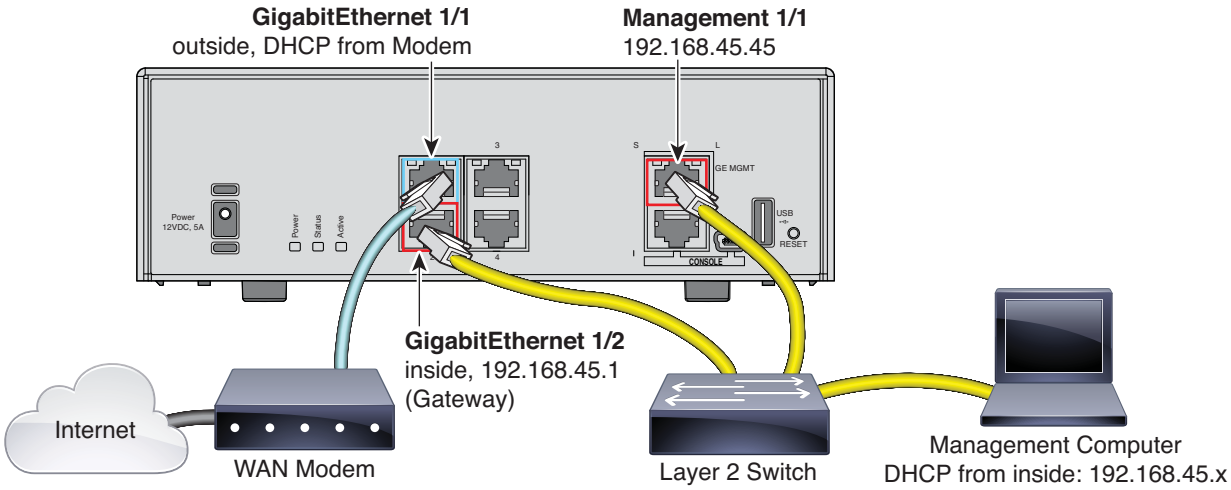


Figure 8 ASA 5506H-X for Version 6.1.



Procedure

1. Cable the following to a Layer 2 Ethernet switch:
   - GigabitEthernet 1/2 interface (inside)
   - Management 1/1 interface (for the Firepower Device Manager)
   - A local management 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 Firepower Device Manager.

2. Connect the GigabitEthernet 1/1 (outside) interface to your ISP/WAN modem or other outside device. By default, the IP address is obtained using DHCP, but you can set a static address during initial configuration.

5. Power on the Firepower Threat Defense Device

Procedure

1. Attach the power cable to the Firepower Threat Defense device and connect it to an electrical outlet.

   The power turns on automatically when you plug in the power cable. There is no power button.
2. Check the Power LED on the back of the Firepower Threat Defense device; if it is solid green, the device is powered on.
3. Check the Status LED on the back of the Firepower Threat Defense device; after it is solid green, the system has passed power-on diagnostics.

6. Launch Firepower Device Manager

When you initially log into Firepower Device Manager, you are taken through the device setup wizard to complete the initial system configuration.

Before You Begin

Ensure that you connect a data interface to your gateway device, for example, a cable modem or router. For edge deployments, this would be your Internet-facing gateway. For data center deployments, this would be a back-bone router. Use the default “outside” interface identified in 4. Deploy the Firepower Threat Defense in Your Network, page 3.

Then, connect your management computer to one of the other data ports, which are part of the inside bridge group. Alternatively, you can connect to the Management physical interface.

The Management physical interface does not need to be connected to a network. By default, the system obtains system licensing and database and other updates through the data interfaces, typically the outside interface, that connect to the Internet. If you instead want to use a separate management network, you can connect the Management interface to a network and configure a separate management gateway after you complete initial setup.

Procedure

1. Open a browser and log into Firepower Device Manager. Assuming you did not go through initial configuration in the CLI, open Firepower Device Manager at **https:**//*ip-address*, where the address is one of the following:
   - (Version 6.2 and greater) If you are connected to an inside bridge group interface: **https://192.168.1.1**.
   - (Version 6.1) If you are connected to the Management physical interface: **https://192.168.45.45**.
2. Log in with the username **admin**, password **Admin123**.
3. If this is the first time logging into the system, and you did not use the CLI setup wizard, you are prompted to read and accept the End User License Agreement and change the admin password. You must complete these steps to continue.
4. Configure the following options for the outside and management interfaces and click **Next**.

   Note: Your settings are deployed to the device when you click **Next**. The interface will be named “outside” and it will be added to the “outside_zone” security zone. Ensure that your settings are correct.

a. **Outside Interface**—This is the data port that you connected to your gateway mode or router. You cannot select an alternative outside interface during initial device setup. The first data interface is the default outside interface.

   Configure IPv4—The IPv4 address for the outside interface. You can use DHCP or manually enter a static IP address, subnet mask, and gateway. You can also select **Off** to not configure an IPv4 address.

   Configure IPv6—The IPv6 address for the outside interface. You can use DHCP or manually enter a static IP address, prefix, and gateway. You can also select **Off** to not configure an IPv6 address.

b. **Management Interface**

   DNS Servers—The DNS server for the system's management address. Enter one or more addresses of DNS servers for name resolution. The default is the OpenDNS public DNS servers. If you edit the fields and want to return to the default, click **Use OpenDNS** to reload the appropriate IP addresses into the fields.

   Firewall Hostname—The hostname for the system's management address.

Note: When you configure the Firepower Threat Defense device using the device setup wizard, the system provides two default access rules for outbound and inbound traffic. You can go back and edit these access rules after initial setup.

5. Configure the system time settings and click **Next**.

   a. **Time Zone**—Select the time zone for the system.

   b. **NTP Time Server**—Select whether to use the default NTP servers or to manually enter the addresses of your NTP servers. You can add multiple servers to provide backups.

6. Configure the smart licenses for the system.

   You must have a smart license account to obtain and apply the licenses that the system requires. Initially, you can use the 90-day evaluation license and set up smart licensing later.

   To register the device now, click the link to log into your Smart Software Manager account, generate a new token, and copy the token into the edit box.

   To use the evaluation license, select **Start 90 day evaluation period without registration**. To later register the device and obtain smart licenses, click the name of the device in the menu to get to the **Device Dashboard**, then click the link in the **Smart Licenses** group.

7. Click **Finish**.

What to Do Next

Once you complete the device setup wizard, a pop-up presents you with your next options to configure the device.

- If you connected other interfaces to networks, select **Configure Interfaces** to configure each of the connected interfaces.
- If you want to modify the default access rules, select **Configure Policy** to configure and manage traffic policies.

You can select either option, or dismiss the pop-up to return to the **Device Dashboard**.

7. How to Configure the Device in Firepower Device Manager

After you complete the setup wizard, you should have a functioning device with a few basic policies in place:

- (Except for ASA 5506-X.) An outside and an inside interface. No other data interfaces are configured.
- (ASA 5506-X only.) An outside interface, and an inside bridge group that includes all other data interfaces.

- Security zones for the inside and outside interfaces.
- An access rule trusting all inside to outside traffic.
- A interface NAT rule that translates all inside to outside traffic to unique ports on the IP address of the outside interface.
- A DHCP server running on the inside interface or bridge group.

The following steps provide an overview of additional features you might want to configure. Please click the help button (**?**) on a page to get detailed information about each step.

Procedure

1. Choose **Device**, then click **View Configuration** in the **Smart License** group.

   Click **Enable** if you want to use the optional Threat license.

   Note: The ISA 3000 supports the Threat license only. It does not support the Malware or URL Filtering licenses. Thus, you cannot configure features that require the Malware or URL Filtering licenses on the ISA 3000.

   If you have not registered, you can do so from this page. Click **Request Register** and follow the instructions. Please register before the evaluation license expires.

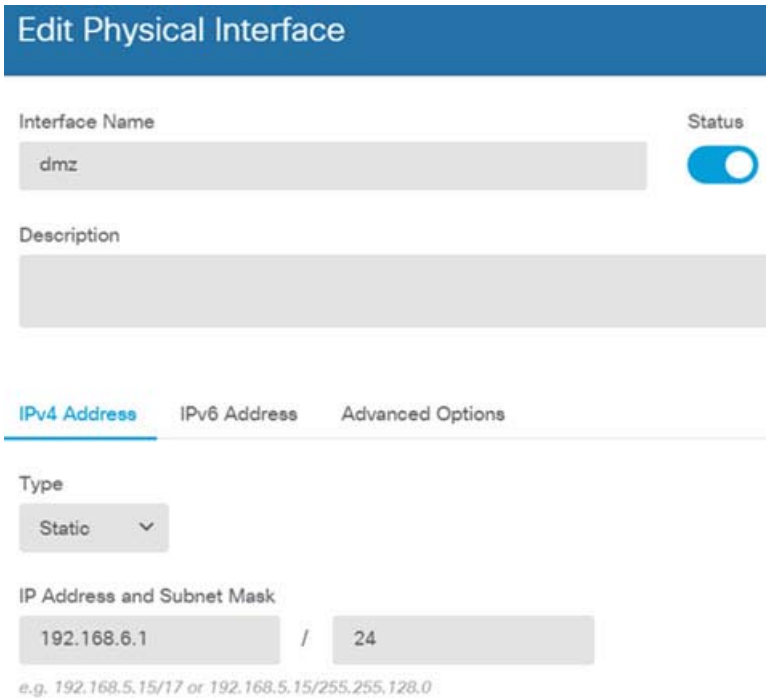
   For example, an enabled Threat license should look like the following:

2. If you wired other interfaces, choose **Device**, then click **View Configuration** in the **Interfaces** group and configure each wired interface.

   The ASA 5506-X comes pre-configured with a bridge group containing all non-outside data interfaces, there is no need to configure these interfaces. However, if you want to break apart the bridge group, you can edit it to remove the interfaces you want to treat separately. Then you can configure those interfaces as hosting separate networks.

   For other models, you can create a bridge group for the other interfaces, or configure separate networks, or some combination of both. Click the edit icon for each interface to define the IP address and other settings.

   The following example configures an interface to be used as a “demilitarized zone” (DMZ), where you place publicly-accessible assets such as your web server. Click **Save** when you are finished.



3. If you configured new interfaces, choose **Objects**, then select **Security Zones** from the table of contents.

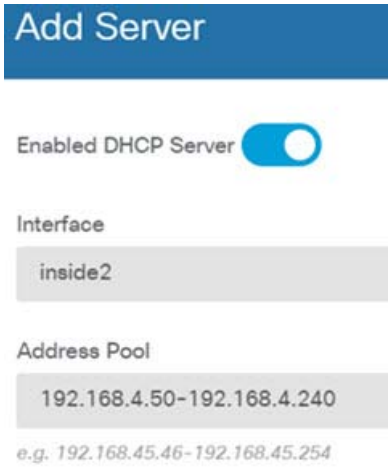
   Edit or create new zones as appropriate. Each interface must belong to a zone, because you configure policies based on security zones, not interfaces. You cannot put the interfaces in zones when configuring them, so you must always edit the zone objects after creating new interfaces or changing the purpose of existing interfaces.

   The following example shows how to create a new dmz-zone for the dmz interface.

4. If you want internal clients to use DHCP to obtain an IP address from the device, choose **Device** > **System Settings** > **DHCP Server**, then select the **DHCP Servers** tab.

   There is already a DHCP server configured for the inside interface, but you can edit the address pool or even delete it. If you configured other inside interfaces, it is very typical to set up a DHCP server on those interfaces. Click + to configure the server and address pool for each inside interface.

You can also fine-tune the WINS and DNS list supplied to clients on the **Configuration** tab. The following example shows how to set up a DHCP server on the inside2 interface with the address pool 192.168.4.50-192.168.4.240.



5. Choose **Device**, then click **View Configuration** (or **Create First Static Route**) in the **Routing** group and configure a default route.

   The default route normally points to the upstream or ISP router that resides off the outside interface. A default IPv4 route is for any-ipv4 (0.0.0.0/0), whereas a default IPv6 route is for any-ipv6 (::0/0). Create routes for each IP version you use. If you use DHCP to obtain an address for the outside interface, you might already have the default routes that you need.

   Note: The routes you define on this page are for the data interfaces only. They do not impact the management interface. Set the management gateway on **Device** > **System Settings** > **Management Interface**.

   The following example shows a default route for IPv4. In this example, isp-gateway is a network object that identifies the IP address of the ISP gateway (you must obtain the address from your ISP). You can create this object by clicking **Create New Network** at the bottom of the **Gateway** drop-down list.

6. Choose **Policies** and configure the security policies for the network.

   The device setup wizard enables traffic flow between the inside-zone and outside-zone, and interface NAT for all interfaces when going to the outside interface. Even if you configure new interfaces, if you add them to the inside-zone object, the access control rule automatically applies to them.

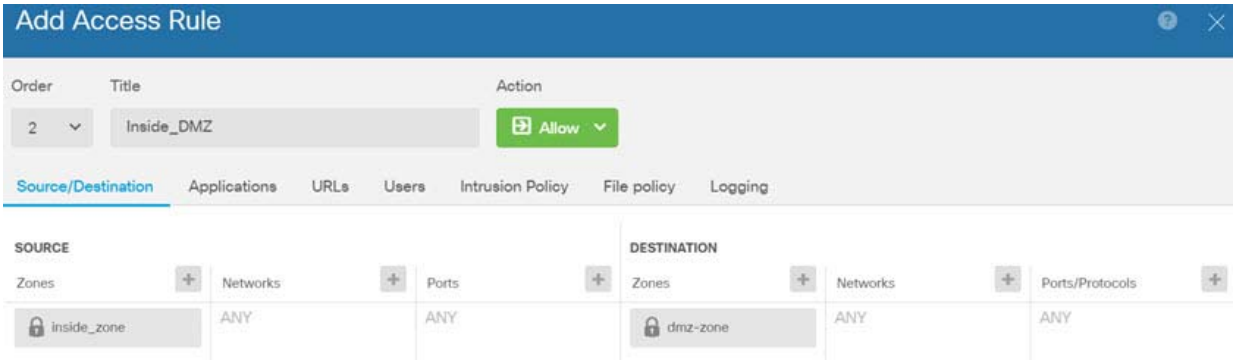
   However, if you have multiple inside interfaces, you need an access control rule to allow traffic flow from inside-zone to inside-zone. If you add other security zones, you need rules to allow traffic to and from those zones. These would be your minimum changes.

   In addition, you can configure other policies to provide additional services, and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies:

   - **SSL Decryption**—If you want to inspect encrypted connections (such as HTTPS) for intrusions, malware, or to enforce compliance with your URL and application usage polices, you must decrypt the connections. Use the SSL decryption policy to determine which connections need to be decrypted. The system re-encrypts the connection after inspecting it.
   - **Identity**—If you want to correlate network activity to individual users, or control network access based on user or user group membership, use the identity policy to determine the user associated with a given source IP address.
   - **Security Intelligence**—Use the Security Intelligence policy to quickly drop connections from or to blacklisted IP addresses or URLs. By blacklisting known bad sites, you do not need to account for them in your access control policy. Cisco provides regularly updated feeds of known bad addresses and URLs so that the Security Intelligence blacklist updates dynamically. Using feeds, you do not need to edit the policy to add or remove items in the blacklist.
   - **NAT** (Network Address Translation)—Use the NAT policy to convert internal IP addresses to externally routeable addresses.
   - **Access Control**—Use the access control policy to determine which connections are allowed on the network. You can filter by security zone, IP address, protocol, port, application, URL, user or user group. You also apply intrusion and file (malware) policies using access control rules. Use this policy to implement URL filtering.

– **Intrusion**—Use the intrusion policies to inspect for known threats. Although you apply intrusion policies using access control rules, you can edit the intrusion policies to selectively enable or disable specific intrusion rules.

The following example shows how to allow traffic between the inside-zone and dmz-zone in the access control policy. In this example, no options are set on any of the other tabs except for **Logging**, where **At End of Connection** is selected.



7. Choose **Device**, then click **View Configuration** in the **Updates** group and configure the update schedules for the system databases.

   If you are using intrusion policies, set up regular updates for the Rules and VDB databases. If you use Security Intelligence feeds, set an update schedule for them. If you use geolocation in any security policies as matching criteria, set an update schedule for that database.

8. Click the **Deploy** button in the menu, then click the Deploy Now button( ), to deploy your changes to the device.

   Changes are not active on the device until you deploy them.

8. Configure the Wireless Access Point (ASA 5506W-X)

The ASA 5506W-X includes a Cisco Aironet 702i wireless access point integrated into the device. The wireless access point is disabled by default. Connect to the access point web interface so that you can enable the wireless radios and configure the SSID and security settings.

The access point connects internally over the GigabitEthernet1/9 interface. All Wi-Fi clients belong to the GigabitEthernet1/9 network. Your security policy determines how the Wi-Fi network can access any networks on other interfaces. The access point does not contain any external interfaces or switch ports.

The following procedure explains how to configure the access point. The procedure assumes that you completed the device setup wizard. If you instead manually configured the device, you might need to adjust the steps based on your configuration.

For more information, see the following manuals:

- For details about using the wireless LAN controller, see the Cisco Wireless LAN Controller Software documentation.
- For details about the wireless access point hardware and software, see the Cisco Aironet 700 Series documentation.

Procedure

1. Configure and enable the wireless interface, GigabitEthernet1/9.

a. Click the device name in the menu to get to the **Device Dashboard**, then click the link in the **Interfaces** group to open the list of interfaces.

b. Click the edit icon ( ) for the GigabitEthernet1/9 interface.

c. Configure the following options.

- **Interface Name**—Enter a name for the interface, for example, **wifi**.
- **Status**—Click the slider to enable the interface.
- **IPv4 Address**—Select **Static** for the address type, then enter an address and subnet mask. For example, 192.168.10.1/24.

d. Click **Save**.

2. Add the Wi-Fi interface to the same security zone as the inside interface.

During device setup, you configured the **inside** interface and placed it in a security zone named **inside_zone**. The Wi-Fi interface needs to be in the same zone so that you can reach the access point web interface.

a. Click **Objects** in the menu, then select **Security Zones** from the table of contents.

b. Click the edit icon ( ) for **inside_zone**.

c. Click + under **Interfaces** and select the **wifi** interface.

3. Configure an access control rule to allow traffic between interfaces in the **inside_zone** security zone.

The device setup wizard creates a rule to allow traffic to flow from the **inside_zone** to the **outside_zone**, which allows inside users to get to the Internet. By adding the **wifi** interface to **inside_zone**, Wi-Fi users are also included in the rule that allows Internet access.

However, the default action is to block all traffic, so you must create a rule to enable traffic between the interfaces in the **inside_zone** security zone.

a. Click **Policies** in the menu.

b. Click + above the **Access Control** table to add a rule.

c. Configure at least the following options in the rule.

- **Title**—Enter a name for the rule. For example, Inside_Inside.
- **Action**—Either Allow or Trust.
- **Source/Destination** > **Source Zones**—Select inside_zone.
- **Source/Destination** > **Destination Zones**—Select inside_zone.

d. Click **OK**.

4. Configure the DHCP server on the wireless interface.

The DHCP server supplies IP addresses to devices that connect to the access point. It also supplies an address to the access point itself.

a. Click the device name in the menu to get to the **Device Dashboard**.

b. Click **System Settings** > **DHCP Server**.

c. Click + above the DHCP server table.

d. Configure the following DHCP server properties.

- **Enable DHCP Server**—Click the slider to enable the DHCP server.
- **Interface**—Select the **wifi** interface.

- **Address Pool**—Enter the address pool for DHCP clients. For example, if you used the example address for the wireless interface, the pool would be 192.168.10.2-192.168.10.254. The pool must be on the same subnet as the IP address for the interface, and it cannot include the address of the interface or the broadcast address.

e. Click **Add**.

5. Click the Deploy button in the menu, then click the Deploy Now button( ), to deploy your changes to the device.

   Wait until the deployment finishes before you continue.

6. Configure the wireless access point.

   The wireless access point obtains its address from the DHCP pool defined for the wireless interface. It should get the first address in the pool. If you used the example addresses, this is 192.168.10.2. (Try the next address in the pool if the first one does not work.)

   a. Use a new browser window to go to the wireless access point IP address, for example, **http://192.168.10.2**. The access point web interface should appear.

      You must be on the inside network, or a network that can route to it, to open this address.

   b. Log in with the username **cisco** and password **Cisco**.

   c. On the left, click **Easy Setup** > **Network Configuration**.

   d. In the **Radio Configuration** area, for each of the **Radio 2.4GHz** and **Radio 5GHz** sections, set at least the following parameters and click **Apply** for each section.

      - **SSID**—The Service Set Identifier. This is the name of the wireless network. Users will see this name when selecting a wireless network for their Wi-Fi connection.
      - **Broadcast SSID in Beacon**—Select this option.
      - **Universal Admin Mode**: **Disable**.
      - **Security**—Select whichever security option you want to use.

7. While in the wireless access point web interface, enable the radios.

   a. On the left, click **Summary**, and then on the main page under **Network Interfaces**, click the link for the 2.4 GHz radio.

   b. Click the **Settings** tab.

   c. For the **Enable Radio** setting, click the **Enable** radio button, and then click **Apply** at the bottom of the page.

   d. Repeat the process for the 5 GHz radio.

Restore the Wireless Access Point Configuration (ASA 5506W-X)

If you are unable to reach the access point, and the Firepower Threat Defense has the suggested configuration and other networking issues are not found, then you may want to restore the access point default configuration. You must access the Firepower Threat Defense CLI (connect to the console port, or configure Telnet or SSH access).

Procedure

1. From the Firepower Threat Defense CLI, navigate to the system support CLI menu:

   ```
   > system support diagnostic-cli
   ```

   Example:

```
> system support diagnostic-cli
Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower>
```

2. Enter the **enable** command to turn on privileged commands:

   ```
   firepower> enable
   ```

   After issuing the **enable** command, the system will prompt you for a password. By default, the password is blank.

   Example:

   ```
   firepower> enable
   Password: <by default, the password is blank>
   firepower#
   ```

3. Enter the command to restore the access point default configuration:

   ```
   firepower# hw-module module wlan recover configuration
   ```

4. See the Cisco IOS Configuration Guide for Autonomous Aironet Access Points for information about the access point CLI.

Access the Wireless Access Point Console (ASA 5506W-X)

You can configure and monitor the wireless access point using the command-line interface (CLI), which you access from the Firepower Threat Defense CLI (connect to the console port, or configure Telnet or SSH access).

Procedure

1. From the Firepower Threat Defense CLI, navigate to the system support CLI menu:

   ```
   > system support diagnostic-cli
   ```

   Example:

   ```
   > system support diagnostic-cli
   Attaching to ASA console ... Press 'Ctrl+a then d' to detach.
   Type help or '?' for a list of available commands.
   firepower>
   ```

2. Enter the **enable** command to turn on privileged commands:

   ```
   firepower> enable
   ```

   After issuing the **enable** command, the system will prompt you for a password. By default, the password is blank.

   Example:

   ```
   firepower> enable
   Password: <by default, the password is blank>
   firepower#
   ```

3. Session to the access point:

   ```
   firepower# session wlan console
   ```

   Example:

   ```
   firepower# session wlan console
   opening console session with module wlan
   connected to module wlan. Escape character sequence is 'CTRL-^X'
   ```

```
ap>
```

4. See the Cisco IOS Configuration Guide for Autonomous Aironet Access Points for information about the access point CLI.

8. Where to Go Next

- For more information about managing the Firepower Threat Defense with the Firepower Device Manager, see the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*, or the Firepower Device Manager online help.