

Firewall Threat Defense Deployment with the Firewall Device Manager

Note Version 7.4 is the final release for the Firepower 2100.

Is This Chapter for You?

To see all available applications and managers, see Which Application and Manager is Right for You?. This chapter applies to the Firewall Threat Defense with the Firewall Device Manager.

About the Firewall

The hardware can run either Firewall Threat Defense software or ASA software. Switching between Firewall Threat Defense and ASA requires you to reimage the device. You should also reimage if you need a different software version than is currently installed. See Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

The firewall runs an underlying operating system called the Secure Firewall eXtensible Operating System (FXOS). The firewall does not support the FXOS Secure Firewall Chassis Manager; only a limited CLI is supported for troubleshooting purposes. See the Cisco FXOS Troubleshooting Guide for the Firewall Threat Defense for more information.

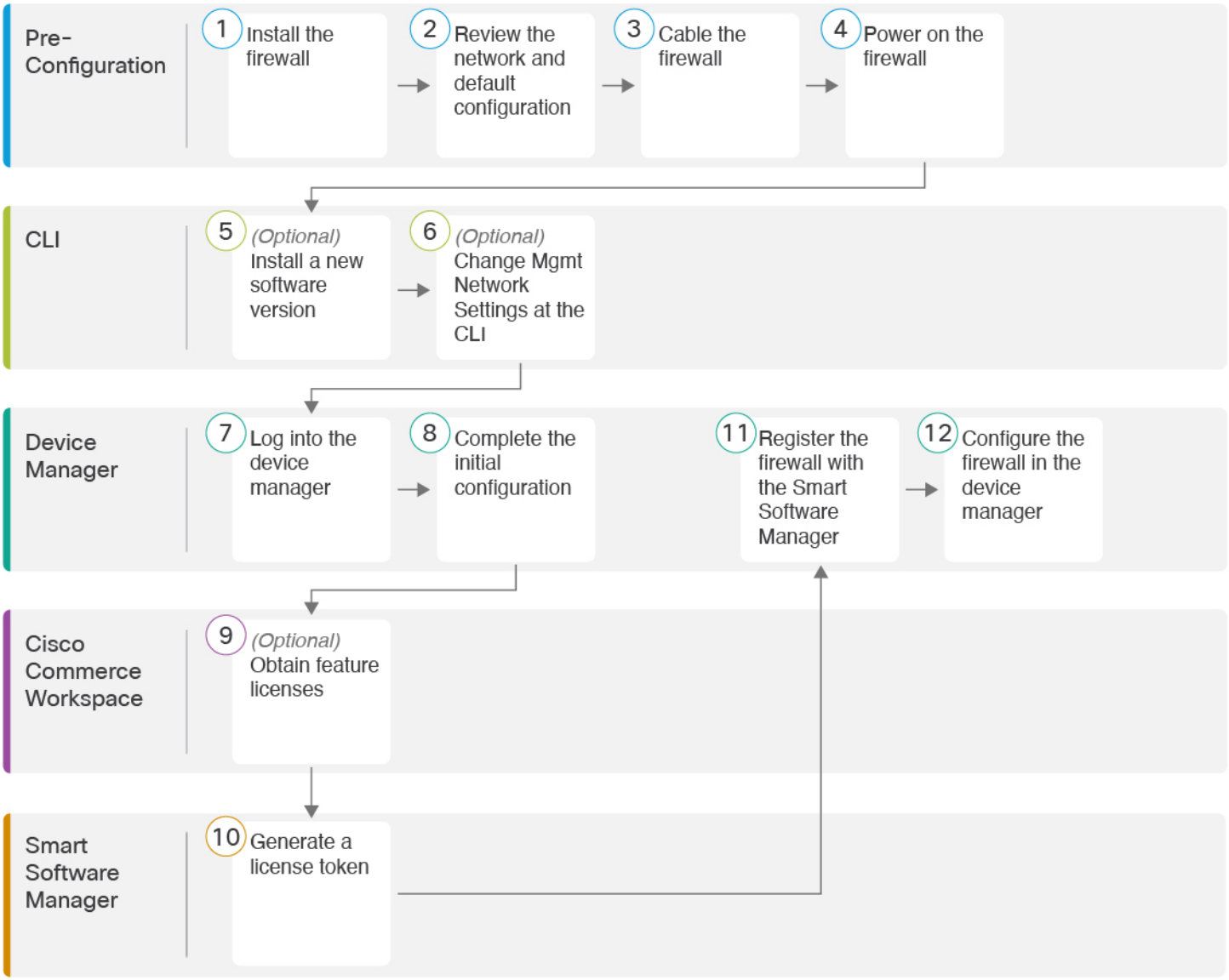
Privacy Collection Statement—The firewall does not require or actively collect personally identifiable information. However, you can use personally identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

- End-to-End Tasks, on page 2
- Review the Network Deployment and Default Configuration, on page 3
- Cable the Device, on page 6
- Power on the Device, on page 7
- (Optional) Check the Software and Install a New Version, on page 8
- (Optional) Change Management Network Settings at the CLI, on page 9
- Log Into the Firewall Device Manager, on page 11
- Complete the Initial Configuration, on page 12
- Configure Licensing, on page 14
- Configure the Firewall in the Firewall Device Manager, on page 20

• Access the Firewall Threat Defense and FXOS CLI, on page 23
• Power Off the Firewall Using the Firewall Device Manager, on page 25
• What's Next?, on page 25

End-to-End Tasks

See the following tasks to deploy the Firewall Threat Defense with the Firewall Device Manager.



1	Pre-Configuration	Install the firewall. See the hardware installation guide.
2	Pre-Configuration	Review the Network Deployment and Default Configuration, on page 3

3	Pre-Configuration	Cable the Device, on page 6.
4	Pre-Configuration	Power on the Device, on page 7.
5	CLI	(Optional) Check the Software and Install a New Version, on page 8
6	CLI	(Optional) Change Management Network Settings at the CLI, on page 9.
7	Firewall Device Manager	Log Into the Firewall Device Manager, on page 11.
8	Firewall Device Manager	Complete the Initial Configuration, on page 12.
9	Cisco Commerce Workspace	(Optional) Obtain feature licenses (Configure Licensing, on page 14).
10	Smart Software Manager	Generate a license token (Configure Licensing, on page 14).
11	Firewall Device Manager	Register the device with the Smart Licensing Server (Configure Licensing, on page 14).
12	Firewall Device Manager	Configure the Firewall in the Firewall Device Manager, on page 20.

Review the Network Deployment and Default Configuration

You can manage the Firewall Threat Defense using the Firewall Device Manager from either the Management 1/1 interface or the inside interface. The dedicated Management interface is a special interface with its own network settings.

The following figure shows the recommended network deployment. If you connect the outside interface directly to a cable modem or DSL modem, we recommend that you put the modem into bridge mode so the Firewall Threat Defense performs all routing and NAT for your inside networks. If you need to configure PPPoE for the outside interface to connect to your ISP, you can do so after you complete initial setup in Firewall Device Manager.

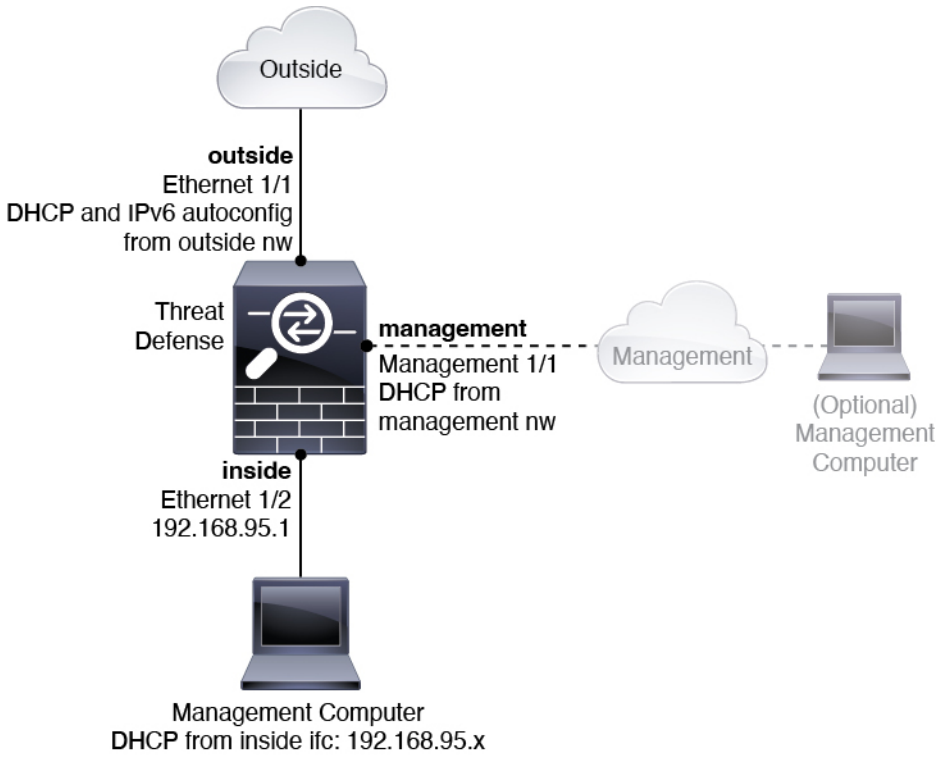
Note If you cannot use the default management IP address (for example, your management network does not include a DHCP server), then you can connect to the console port and perform initial setup at the CLI, including setting the Management IP address, gateway, and other basic networking settings.

If you need to change the inside IP address, you can do so after you complete initial setup in the Firewall Device Manager. For example, you may need to change the inside IP address in the following circumstances:

- (7.0 and later) The inside IP address is 192.168.95.1. (6.7 and earlier) The inside IP address is 192.168.1.1. If the outside interface tries to obtain an IP address on the 192.168.1.0 network, which is a common default network, the DHCP lease will fail, and the outside interface will not obtain an IP address. This problem occurs because the Firewall Threat Defense cannot have two interfaces on the same network. In this case you must change the inside IP address to be on a new network.
- If you add the Firewall Threat Defense to an existing inside network, you will need to change the inside IP address to be on the existing network.

The following figure shows the default network deployment for the Firewall Threat Defense using the Firewall Device Manager with the default configuration.

Figure 1: Suggested Network Deployment



Note For 6.7 and earlier, the Ethernet 1/2 inside IP address is 192.168.1.1.

For 6.5 and earlier, the Management 1/1 default IP address is 192.168.45.45.

Default Configuration

The configuration for the firewall after initial setup includes the following:

- **inside**—Ethernet 1/2, IP address (7.0 and later) 192.168.95.1; (pre-7.0) 192.168.1.1.
- **outside**—Ethernet 1/1, IP address from IPv4 DHCP and IPv6 autoconfiguration
- **inside→outside** traffic flow
- **management**—Management 1/1 (management)
  - (6.6 and later) IP address from DHCP
  - (6.5 and earlier) IP address 192.168.45.45

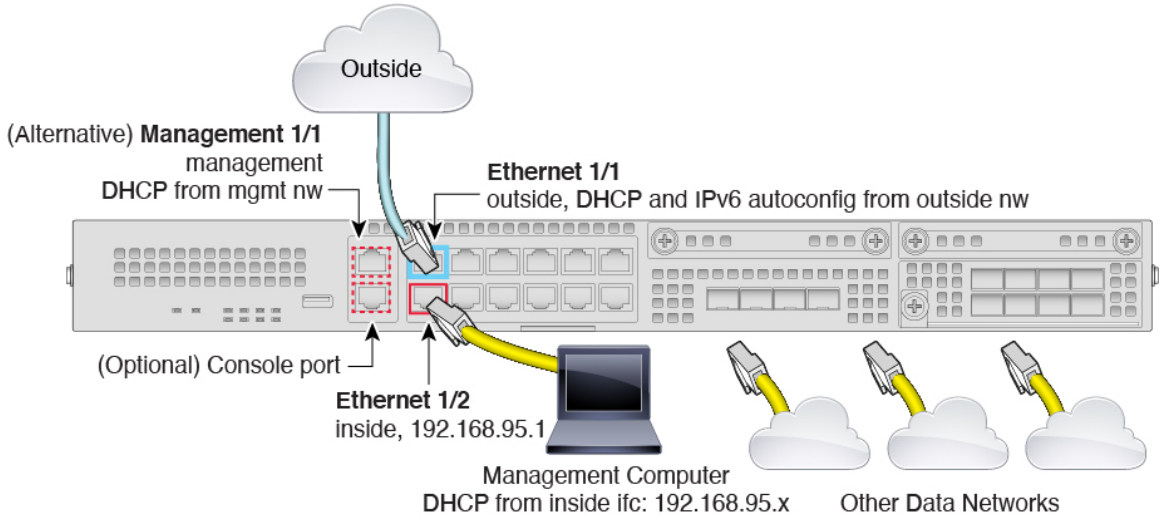


Note The Management 1/1 interface is a special interface separate from data interfaces that is used for management, Smart Licensing, and database updates. (7.4 and later) The Diagnostic interface was merged with the Management interface. (Pre-7.4) The physical interface is shared with a second logical interface, the Diagnostic interface. Diagnostic is a data interface, but is limited to other types of management traffic (to-the-device and from-the-device), such as syslog or SNMP. The Diagnostic interface is not typically used. See the Cisco Secure Firewall Device Manager Configuration Guide for more information.

- **DNS server for management**—OpenDNS: (IPv4) 208.67.222.222, 208.67.220.220; (IPv6) 2620:119:35::35, or servers you specify during setup. DNS servers obtained from DHCP are never used.
- **NTP**—Cisco NTP servers: 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org, or servers you specify during setup
- **Default routes**
  - **Data interfaces**—Obtained from outside DHCP, or a gateway IP address you specify during setup
  - **Management interface**—(6.6 and later) Obtained from management DHCP. If you do not receive a gateway, then the default route is over the backplane and through the data interfaces. (6.5 and earlier) Over the backplane and through the data interfaces

    Note that the Management interface requires internet access for licensing and updates, either over the backplane or using a separate internet gateway. Note that only traffic originating on the Management interface can go over the backplane; otherwise, Management does not allow through traffic for traffic entering Management from the network.
- **DHCP server**—Enabled on the inside interface and (6.5 and earlier only) management interface
- **Firewall Device Manager access**—All hosts allowed on Management and the inside interface.
- **NAT**—Interface PAT for all traffic from inside to outside

Cable the Device



Note For 6.7 and earlier, the Ethernet 1/2 inside IP address is 192.168.1.1.

For 6.5 and earlier, the Management 1/1 default IP address is 192.168.45.45.

Manage the Firepower 2100 on either Management 1/1 or Ethernet 1/2. The default configuration also configures Ethernet1/1 as outside.

Procedure

Step 1 Install the chassis. See the hardware installation guide.

Step 2 Connect your management computer to either of the following interfaces:

- Ethernet 1/2—Connect your management computer directly to Ethernet 1/2 for initial configuration, or connect Ethernet 1/2 to your inside network. Ethernet 1/2 has a default IP address (192.168.95.1) and also runs a DHCP server to provide IP addresses to clients (including the management computer), so make sure these settings do not conflict with any existing inside network settings (see Default Configuration, on page 5).
- Management 1/1 (labeled MGMT)—Connect Management 1/1 to your management network, and make sure your management computer is on—or has access to—the management network. Management 1/1 obtains an IP address from a DHCP server on your management network; if you use this interface, you must determine the IP address assigned to the Firewall Threat Defense so that you can connect to the IP address from your management computer.

  If you need to change the Management 1/1 IP address from the default to configure a static IP address, you must also cable your management computer to the console port. See (Optional) Change Management Network Settings at the CLI, on page 9.

You can later configure the Firewall Device Manager management access from other interfaces; see the FDM configuration guide.

Step 3 Connect the outside network to the Ethernet1/1 interface (labeled WAN).

By default, the IP address is obtained using IPv4 DHCP and IPv6 autoconfiguration, but you can set a static address during initial configuration.

Step 4 Connect other networks to the remaining interfaces.

Power on the Device

The power switch is located to the left of power supply module 1 on the rear of the chassis. It is a toggle switch that controls power to the system. If the power switch is in standby position, only the 3.3-V standby power is enabled from the power supply module and the 12-V main power is OFF. When the switch is in the ON position, the 12-V main power is turned on and the system boots.

Note The first time you boot up the Firewall Threat Defense, initialization can take approximately 15 to 30 minutes.

Before you begin

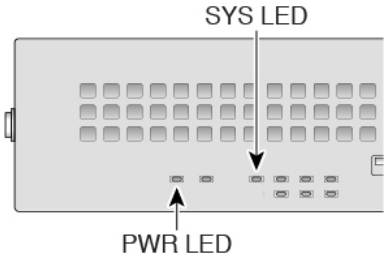
It's important that you provide reliable power for your device (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the graceful shutdown of your system.

Procedure

Step 1 Attach the power cord to the device and connect it to an electrical outlet.

Step 2 Press the power switch on the back of the device.

Step 3 Check the PWR LED on the front of the device; if it is solid green, the device is powered on.



Step 4 Check the SYS LED on the front of the device; after it is solid green, the system has passed power-on diagnostics.

Note

Before you move the power switch to the OFF position, use the shutdown commands so that the system can perform a graceful shutdown. This may take several minutes to complete. After the graceful shutdown is complete, the console displays `It is safe to power off now`. The front panel blue locator beacon LED lights up indicating the system is ready to be powered off. You can now move the switch to the OFF position. The front panel PWR LED flashes momentarily and turns off. Do not remove the power until the PWR LED is completely off.

See the FXOS Configuration Guide for more information on using the shutdown commands.

(Optional) Check the Software and Install a New Version

To check the software version and, if necessary, install a different version, perform these steps. We recommend that you install your target version before you configure the firewall. Alternatively, you can perform an upgrade after you are up and running, but upgrading, which preserves your configuration, may take longer than using this procedure.

What Version Should I Run?

Cisco recommends running a Gold Star release indicated by a gold star next to the release number on the software download page. You can also refer to the release strategy described in https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html; for example, this bulletin describes short-term release numbering (with the latest features), long-term release numbering (maintenance releases and patches for a longer period of time), or extra long-term release numbering (maintenance releases and patches for the longest period of time, for government certification).

Procedure

Step 1 Connect to the CLI. See Access the Firewall Threat Defense and FXOS CLI, on page 23 for more information. This procedure shows using the console port, but you can use SSH instead.

Log in with the **admin** user and the default password, **Admin123**.

You connect to the FXOS CLI. The first time you log in, you are prompted to change the password. This password is also used for the Firewall Threat Defense login for SSH.

Note
If the password was already changed, and you do not know it, you must perform a factory reset to reset the password to the default. See the FXOS troubleshooting guide for the factory reset procedure.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
```

```
Your password was updated successfully.

[...]

firepower#
```

Step 2 At the FXOS CLI, show the running version.

scope ssa

show app-instance

Example:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.6.0.65        7.6.0.65
        Not Applicable
```

Step 3 If you want to install a new version, perform these steps.

a) If you need to set a static IP address for the Management interface, see (Optional) Change Management Network Settings at the CLI, on page 9. By default, the Management interface uses DHCP.

You will need to download the new image from a server accessible from the Management interface.

b) Perform the reimage procedure in the FXOS troubleshooting guide.

After the firewall reboots, you connect to the FXOS CLI again.

c) At the FXOS CLI, you are prompted to set the admin password again.

(Optional) Change Management Network Settings at the CLI

If you cannot use the default management IP address, then you can connect to the console port and perform initial setup at the CLI, including setting the Management IP address, gateway, and other basic networking settings. You can only configure the Management interface settings; you cannot configure inside or outside interfaces, which you can later configure in the GUI.

Note You cannot repeat the CLI setup script unless you clear the configuration; for example, by reimaging. However, all of these settings can be changed later at the CLI using **configure network** commands. See Cisco Secure Firewall Threat Defense Command Reference.

Procedure

Step 1 Connect to the Firewall Threat Defense console port. See Access the Firewall Threat Defense and FXOS CLI, on page 23 for more information.

Log in with the **admin** user and the default password, **Admin123**.

You connect to the FXOS CLI. The first time you log in, you are prompted to change the password. This password is also used for the Firewall Threat Defense login for SSH.

Note
If the password was already changed, and you do not know it, you must reimage the device to reset the password to the default. See the FXOS troubleshooting guide for the reimage procedure.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 2 Connect to the Firewall Threat Defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 3 The first time you log into the Firewall Threat Defense, you are prompted to accept the End User License Agreement (EULA). You are then presented with the CLI setup script.

Defaults or previously-entered values appear in brackets. To accept previously entered values, press **Enter**.

See the following guidelines:

- **Enter the IPv4 default gateway for the management interface**—If you set a manual IP address, enter either **data-interfaces** or the IP address of the gateway router. The **data-interfaces** setting sends outbound management traffic over the backplane to exit a data interface. This setting is useful if you do not have a separate Management network that can access the internet. Traffic originating on the Management interface includes license registration and database updates that require internet access. If you use **data-interfaces**, you can still use the Firewall Device Manager (or SSH) on the Management interface if you are directly-connected to the Management network, but for remote management for specific networks or hosts, you should add a static route using the **configure network static-routes** command.

Note that the Firewall Device Manager management on data interfaces is not affected by this setting. If you use DHCP, the system uses the gateway provided by DHCP and uses the **data-interfaces** as a fallback method if DHCP doesn't provide a gateway.

- **If your networking information has changed, you will need to reconnect**—If you are connected with SSH to the default IP address but you change the IP address at initial setup, you will be disconnected. Reconnect with the new IP address and password. Console connections are not affected.
- **Manage the device locally?**—Enter **yes** to use the Firewall Device Manager. A **no** answer means you intend to use the on-premises or cloud-delivered Firewall Management Center to manage the device.

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

Step 4 Log into the Firewall Device Manager on the new Management IP address.

Log Into the Firewall Device Manager

Log into the Firewall Device Manager to configure your Firewall Threat Defense.

Procedure

Step 1 Enter the following URL in your browser.

- (7.0 and later) Inside (Ethernet 1/2)—**https://192.168.95.1**.
- (6.7 and earlier) Inside (Ethernet 1/2)—**https://192.168.1.1**.

- (6.6 and later) Management—**https://***management_ip*. The Management interface is a DHCP client, so the IP address depends on your DHCP server. If you changed the Management IP address at the CLI setup, then enter that address.
- (6.5 and earlier) Management—**https://192.168.45.45**. If you changed the Management IP address at the CLI setup, then enter that address.

Step 2 Log in with the username **admin**, and thedefault password **Admin123**.

What to do next

- Run through the Firewall Device Manager setup wizard; see Complete the Initial Configuration, on page 12.

Complete the Initial Configuration

Use the setup wizard when you first log into the Firewall Device Manager to complete the initial configuration. After you complete the setup wizard, you should have a functioning device with a few basic policies in place:

- An outside (Ethernet1/1) and an inside interface (Ethernet1/2).
- Security zones for the inside and outside interfaces.
- An access rule trusting all inside to outside traffic.
- An 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.



Note If you performed any initial setup at the CLI, then some of these tasks, specifically changing the admin password and configuring the outside and management interfaces, should have already been completed.

Procedure

Step 1 You are prompted to read and accept the End User License Agreement and change the admin password.

You must complete these steps to continue.

Step 2 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 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. You cannot configure PPPoE using the setup wizard. PPPoE may be required if the interface is connected to a DSL modem, cable modem, or other connection to your ISP, and your ISP uses PPPoE to provide your IP address. You can configure PPPoE after you complete the wizard.

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.

Step 3 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.

Step 4 (Optional) Configure the smart licenses for the system.

Your purchase of the Firewall Threat Defense device automatically includes a Base license. All additional licenses are optional.

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, and see Configure Licensing, on page 14.

To use the evaluation license, select **Start 90 day evaluation period without registration**.

Step 5 Click **Finish**.

What to do next

- Although you can continue using the evaluation license, we recommend that you register and license your device; see Configure Licensing, on page 14.
- You can also choose to configure the device using the Firewall Device Manager; see Configure the Firewall in the Firewall Device Manager, on page 20.

Configure Licensing

The Firewall Threat Defense uses Smart Software Licensing, which lets you purchase and manage a pool of licenses centrally.

When you register the chassis, the Smart Software Manager issues an ID certificate for communication between the chassis and the Smart Software Manager. It also assigns the chassis to the appropriate virtual account.

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

The Essentials license is included automatically. 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 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. See the following licenses:

- Essentials—Required
- IPS
- Malware Defense
- URL Filtering
- Cisco Secure Client

Before you begin

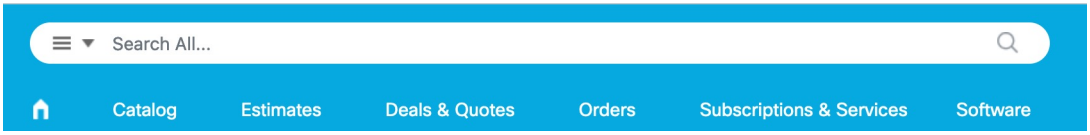
- When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. If you don't have an account on the Smart Software Manager, click the link to set up a new account.
- If you have not already done so, register the Firewall Management Center with the Smart Software Manager. Registering requires you to generate a registration token in the Smart Software Manager. See the Cisco Secure Firewall Management Center Administration Guide for detailed instructions.

Procedure

Step 1 Make sure your Smart Licensing account contains the available licenses you need.

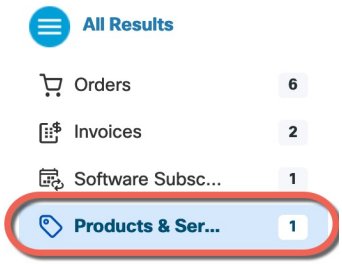
If you need to add licenses yourself, go to Cisco Commerce Workspace and use the **Search All** field.

Figure 2: License Search



Choose **Products & Services** from the results.

Figure 3: Results



Search for the following license PIDs:

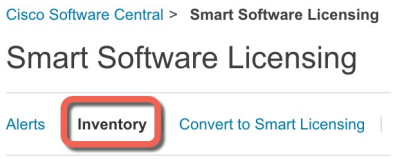
Note
If a PID is not found, you can add the PID manually to your order.

- IPS, Malware Defense, and URL combination:
  - L-FPR2110T-TMC=
  - L-FPR2120T-TMC=
  - L-FPR2130T-TMC=
  - L-FPR2140T-TMC=

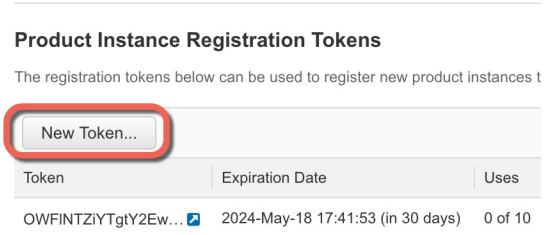
  When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:
  - L-FPR2110T-TMC-1Y
  - L-FPR2110T-TMC-3Y
  - L-FPR2110T-TMC-5Y
  - L-FPR2120T-TMC-1Y
  - L-FPR2120T-TMC-3Y
  - L-FPR2120T-TMC-5Y
  - L-FPR2130T-TMC-1Y
  - L-FPR2130T-TMC-3Y
  - L-FPR2130T-TMC-5Y
  - L-FPR2140T-TMC-1Y
  - L-FPR2140T-TMC-3Y
  - L-FPR2140T-TMC-5Y
- Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

Step 2 In the Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this device.

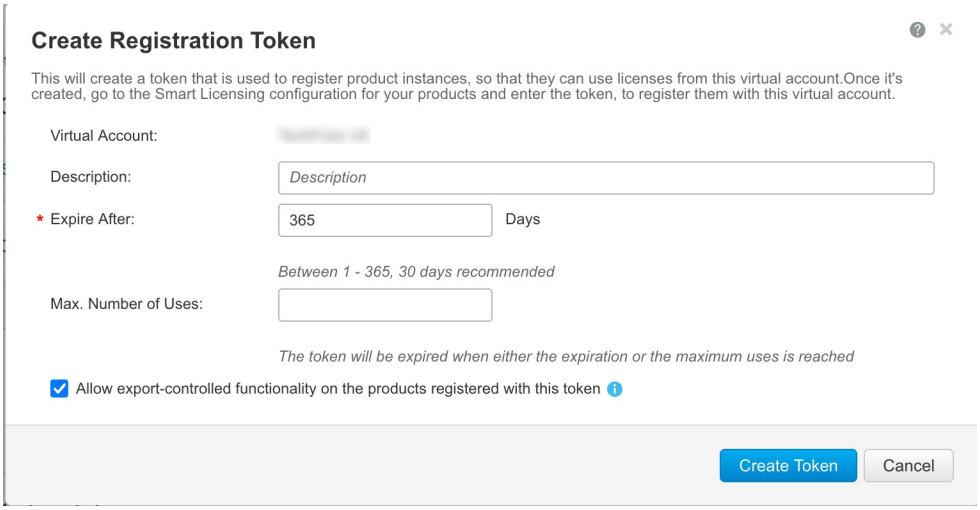
a) Click **Inventory**.



b) On the **General** tab, click **New Token**.



c) On the **Create Registration Token** dialog box enter the following settings, and then click **Create Token**:



- **Description**
- **Expire After**—Cisco recommends 30 days.
- **Max. Number of Uses**
- **Allow export-controlled functionality on the products registered with this token**—Enables the export-compliance flag if you are in a country that allows for strong encryption. You must select this option now if you plan to use this functionality. If you enable this functionality later, you will need to re-register your device with a new product key and reload the device. If you do not see this option, your account does not support export-controlled functionality.

The token is added to your inventory.

d) Click the arrow icon to the right of the token to open the **Token** dialog box so you can copy the token ID to your clipboard. Keep this token ready for later in the procedure when you need to register the Firewall Threat Defense.

Figure 4: View Token

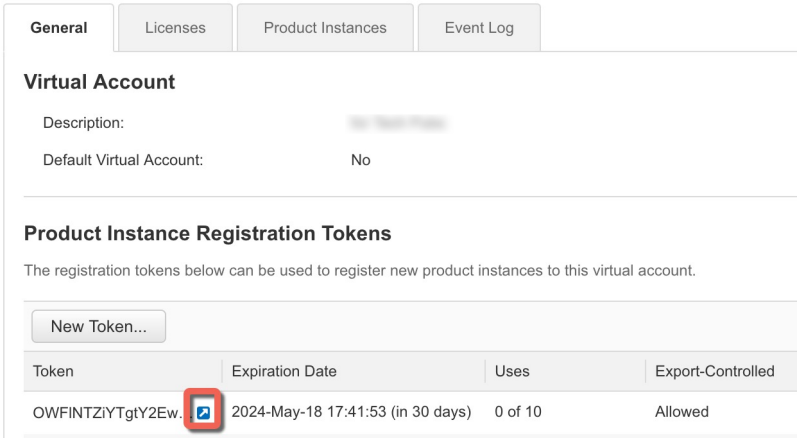
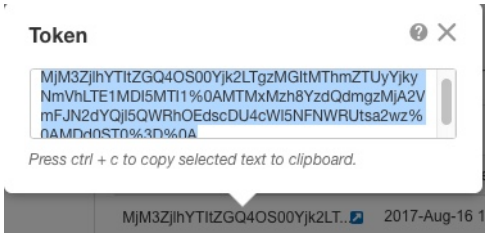


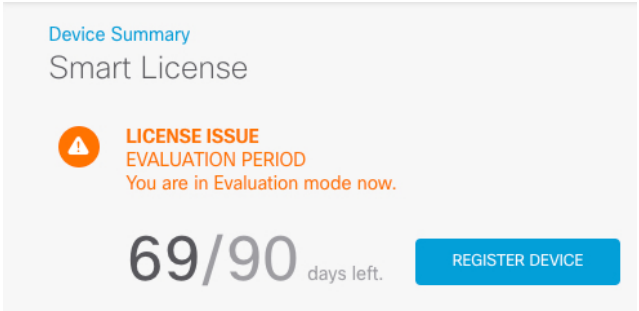
Figure 5: Copy Token



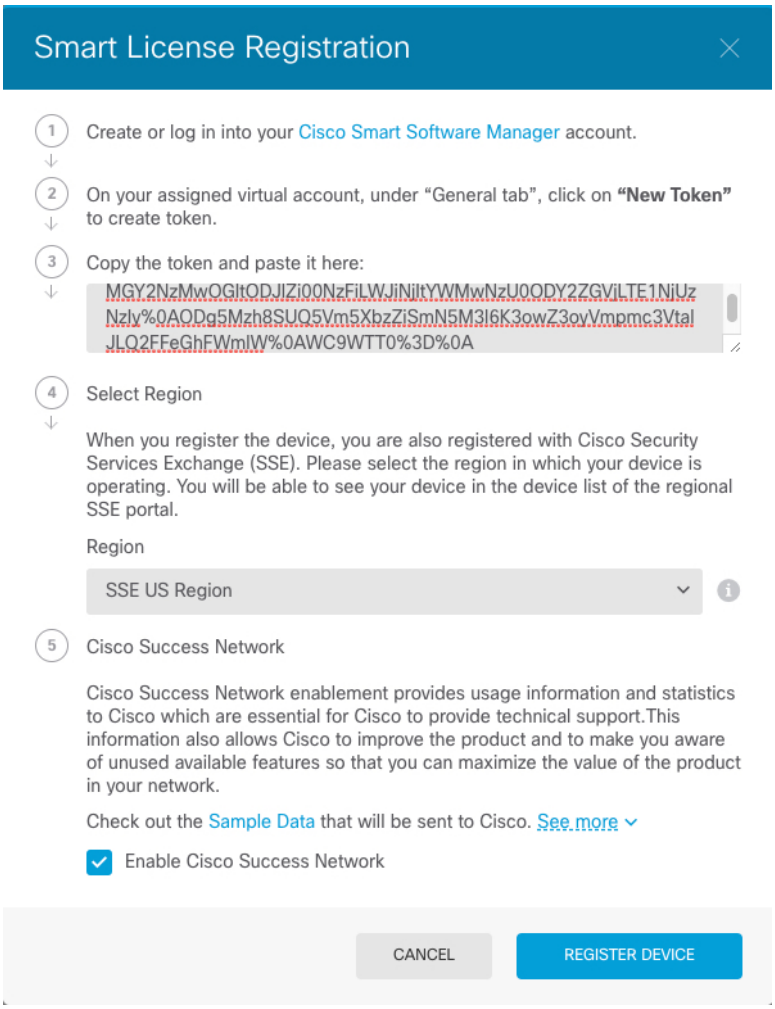
Step 3 In the Firewall Device Manager, click **Device**, and then in the **Smart License** summary, click **View Configuration**.

You see the **Smart License** page.

Step 4 Click **Register Device**.

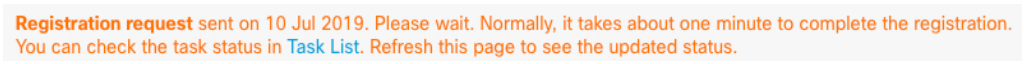


Then follow the instructions on the **Smart License Registration** dialog box to paste in your token:

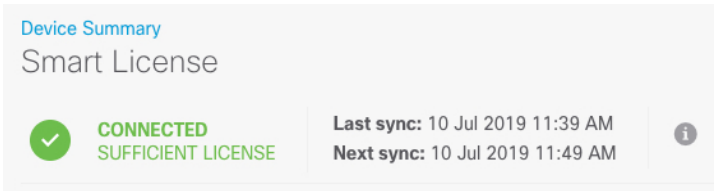


Step 5 Click **Register Device**.

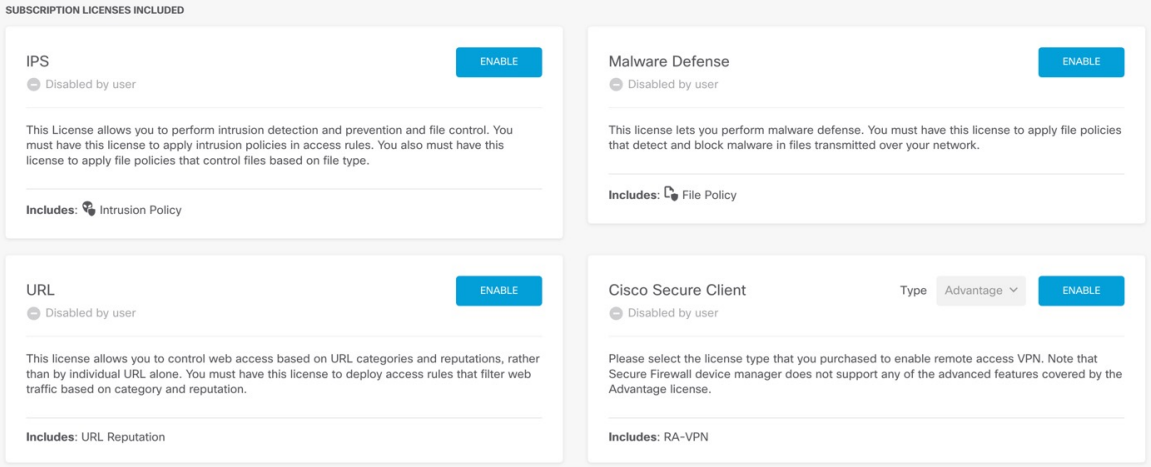
You return to the **Smart License** page. While the device registers, you see the following message:



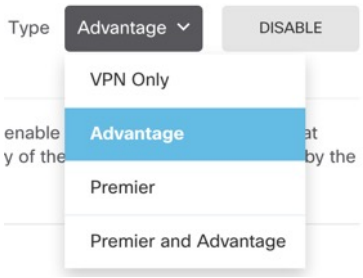
After the device successfully registers and you refresh the page, you see the following:



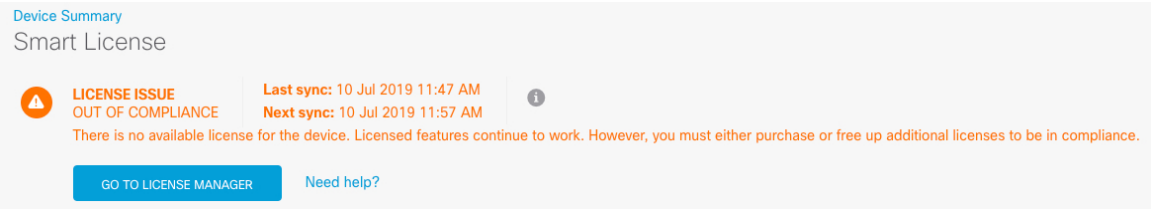
Step 6 Click the **Enable/Disable** control for each optional license as desired.



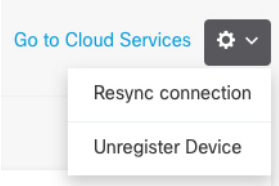
- **Enable**—Registers the license with your Cisco Smart Software Manager account and enables the controlled features. You can now configure and deploy policies controlled by the license.
- **Disable**—Unregisters the license with your Cisco Smart Software Manager account and disables the controlled features. You cannot configure the features in new policies, nor can you deploy policies that use the feature.
- If you enabled the **Cisco Secure Client** license, select the type of license you want to use: **Advantage**, **Premier**, **VPN Only**, or **Premier and Advantage**.



After you enable features, if you do not have the licenses in your account, you will see the following non-compliance message after you refresh the page:



Step 7 Choose **Resync Connection** from the gear drop-down list to synchronize license information with Cisco Smart Software Manager.



Configure the Firewall in the Firewall Device Manager

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.

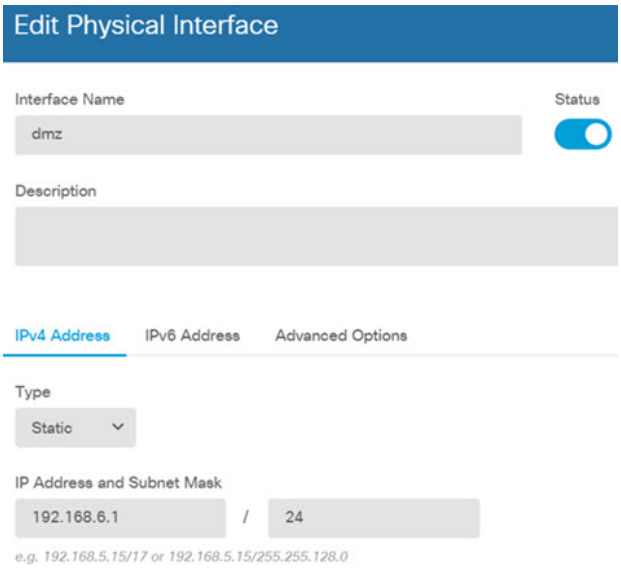
Procedure

Step 1 If you wired other interfaces, choose **Device**, and then click the link in the **Interfaces** summary.

Click the edit icon ( ) for each interface to set the mode and 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.

Figure 6: Edit Interface



Step 2 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.

Figure 7: Security Zone Object

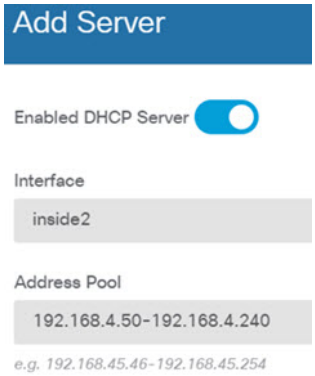


Step 3 If you want internal clients to use DHCP to obtain an IP address from the device, choose **Device** > **System Settings** > **DHCP Server**, then select the **DHCP Servers** tab.

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.

Figure 8: DHCP Server



Step 4 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.

Figure 9: Default Route



Step 5 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.

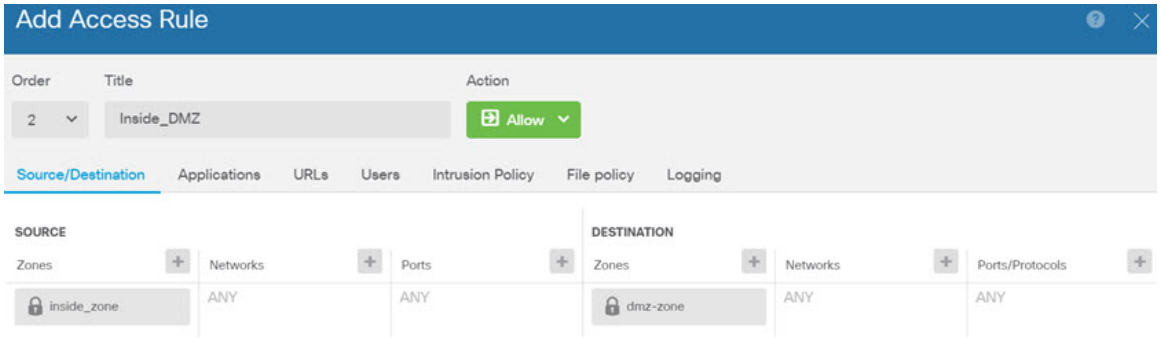
In addition, you can configure other policies to provide additional services, and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies:

- **SSL Decryption**—If you want to inspect encrypted connections (such as HTTPS) for intrusions, malware, and so forth, 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.

Figure 10: Access Control Policy



Step 6 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.

Step 7 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.

Access the Firewall Threat Defense and FXOS CLI

Use the command-line interface (CLI) to set up the system and do basic system troubleshooting. You cannot configure policies through a CLI session. You can access the CLI by connecting to the console port.

You can also access the FXOS CLI for troubleshooting purposes.

Note You can alternatively SSH to the Management interface of the Firewall Threat Defense device. Unlike a console session, the SSH session defaults to the Firewall Threat Defense CLI, from which you can connect to the FXOS CLI using the **connect fxos** command. You can later connect to the address on a data interface if you open the interface for SSH connections. SSH access to data interfaces is disabled by default. This procedure describes console port access, which defaults to the FXOS CLI.

Procedure

Step 1 To log into the CLI, connect your management computer to the console port. The Firepower 2100 ships with a DB-9 to RJ-45 serial cable, so you may need a third party DB-9-to-USB serial cable to make the connection. Be sure to install any necessary USB serial drivers for your operating system. The console port defaults to the FXOS CLI. Use the following serial settings:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

You connect to the FXOS CLI. Log in to the CLI using the **admin** username and the password you set at initial setup (the default is **Admin123**).

Example:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Step 2 Access the Firewall Threat Defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

After logging in, for information on the commands available in the CLI, enter **help** or **?**. For usage information, see Cisco Secure Firewall Threat Defense Command Reference.

Step 3 To exit the Firewall Threat Defense CLI, enter the **exit** or **logout** command.

This command returns you to the FXOS CLI prompt. For information on the commands available in the FXOS CLI, enter **?**.

Example:

```
> exit
firepower#
```

Power Off the Firewall Using the Firewall Device Manager

Shut down your system properly using the Firewall Device Manager.

Procedure

Step 1 Use the Firewall Device Manager to shut down the firewall.

Note
For 6.4 and earlier, enter the **shutdown** command at the Firewall Device Manager CLI.

a) Click **Device**, then click the **System Settings** > **Reboot/Shutdown** link.
b) Click **Shut Down**.

Step 2 If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. You will see the following prompt:

```
System is stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]
```

If you do not have a console connection, wait approximately 3 minutes to ensure the system has shut down.

Step 3 You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

What's Next?

To continue configuring your Firewall Threat Defense, see the documents available for your software version at Navigating the Cisco Firepower Documentation.

For information related to using the Firewall Device Manager, see Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.