Before You Begin

The Secure Firewall 200 offers next-generation firewall capabilities designed for distributed enterprises and small branch locations. It provides robust, cost-effective security and simplified management within a compact form factor, ensuring secure and optimized connectivity at the network edge. The Secure Firewall 200:

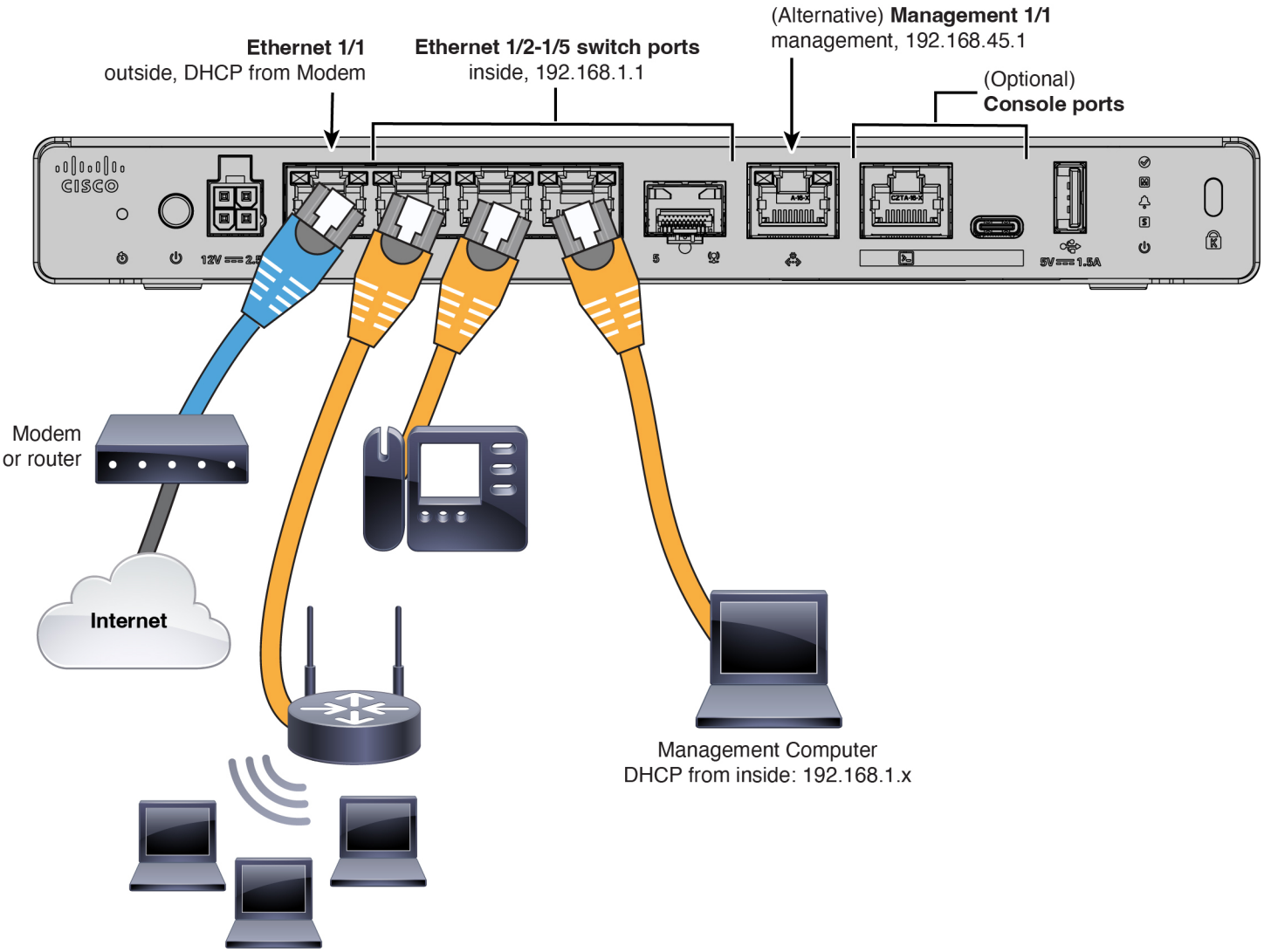
- Extends Cisco's Hybrid Mesh Firewall architecture to branch edges
- Provides AI-powered inspection and consistent security policies
- Integrates SD-WAN capabilities for enhanced application performance and reliable user access
- Delivers application and user control, efficient segmentation, and advanced security features tailored for cost-sensitive environments.

Configure an ASA using ASDM.

- Cable the firewall, on page 1
- Power on the firewall, on page 2
- Which application is installed: Firewall Threat Defense or ASA?, on page 3
- Access the ASA CLI, on page 4
- Obtain licenses, on page 6

Cable the firewall

- Install an SFP into Ethernet 1/5—It is a 1-Gbps SFP port that requires an SFP module.
- See the hardware installation guide for more information.



Power on the firewall

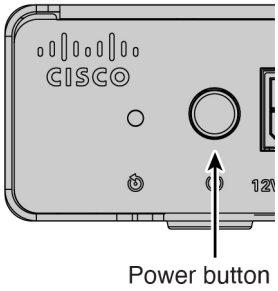
System power is controlled by a power button located on the rear of the firewall. The power button provides a soft notification that supports graceful shutdown of the system to reduce the risk of system software and data corruption.

Procedure

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

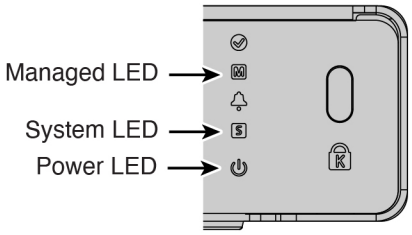
Step 2 Turn the power on using the power button located on the rear of the chassis, adjacent to the power cord.

Figure 1: Power button



Step 3 Check the LEDs for the current status.

Figure 2: LEDs



- Power LED—Solid green means the firewall is powered on.
- System (S) LED—See the following behavior:

Table 1: System (S) LED Behavior

LED Behavior	Description	Time After Device Powered On (minutes:seconds)
Fast flashing green	Booting up	01:00
Fast flashing amber (error condition)	Failed to boot up	01:00
Solid green	Application loaded	15:00 - 30:00
Solid amber (error condition)	Application failed to load	15:00 - 30:00

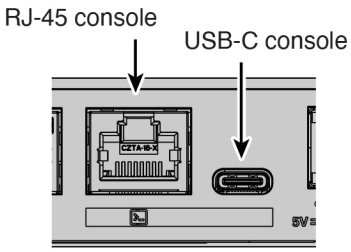
Which application is installed: Firewall Threat Defense or ASA?

Both applications, Firewall Threat Defense or ASA, are supported on the hardware. Connect to the console port and determine which application was installed at the factory.

Procedure

Step 1 Connect to the console port using either port type.

Figure 3: Console port



Step 2 See the CLI prompts to determine if your firewall is running Firewall Threat Defense or ASA.

Firewall Threat Defense

You see the firepower login (FXOS) prompt. You can disconnect without logging in and setting a new password.

```
firepower login:
```

ASA

You see the ASA prompt.

```
ciscoasa>
```

Step 3 If you are running the wrong application, see *Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide*.

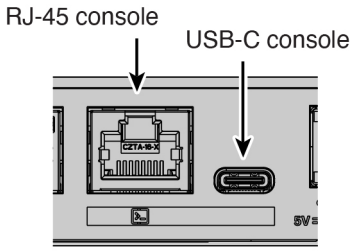
Access the ASA CLI

You might need to access the CLI for configuration or troubleshooting.

Procedure

Step 1 Connect to the console port using either port type.

Figure 4: Console port



Step 2 You connect to the ASA CLI in user EXEC mode. This mode lets you use many **show** commands.

```
ciscoasa>
```

Step 3 Access privileged EXEC mode. This password-protected mode lets you perform many actions, including accessing configuration modes.

enable

You are prompted to change the password the first time you enter the **enable** command.

Example:

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

Step 4 Access global configuration mode.

configure terminal

Example:

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Step 5 Access the FXOS CLI. Use this CLI for troubleshooting at the hardware level.

connect fxos [**admin**]

- **admin**—Provides admin-level access. Without this option, you have read-only access. Note that no configuration commands are available even in admin mode.

You are not prompted for user credentials. The current ASA username is passed through to FXOS, and no additional login is required. To return to the ASA CLI, enter **exit** or type **Ctrl-Shift-6**, **x**.

Example:

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
```

```
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

Obtain licenses

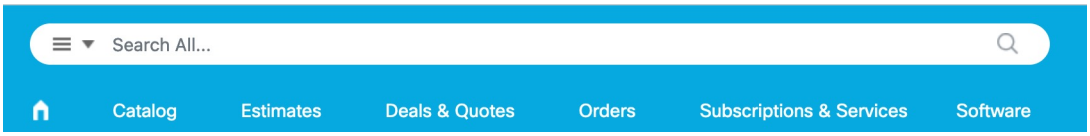
When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. If you don't have an account on the Smart Software Manager, click the link to set up a new account.

The ASA has the following licenses:

- Essentials—Required
- Security Contexts
- Cisco Secure Client

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

   Figure 5: License Search

2. Search for the following license PIDs.

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

   - Essentials—CSF_220_BASE_STD. Required.
   - Cisco Secure Client—See the Cisco Secure Client Ordering Guide. You do not enable this license directly in the ASA.

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

Figure 6: Results