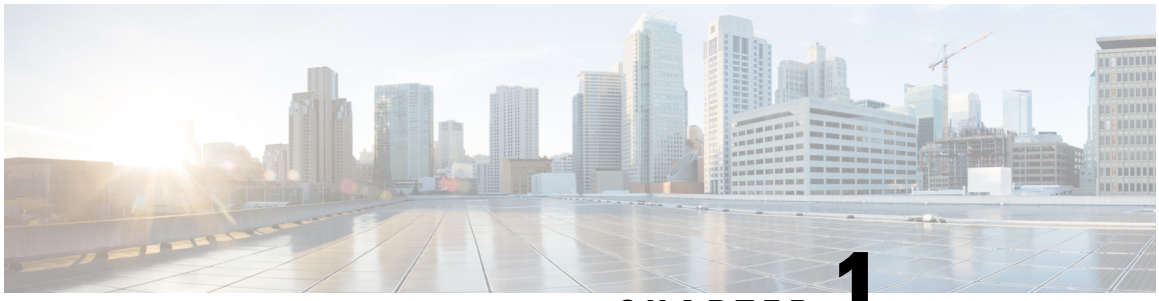


Secure Firewall 1210/20 Threat Defense Getting Started: Firewall Device Manager

First Published: 2024-10-10

Last Modified: 2026-02-05

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

Before You Begin

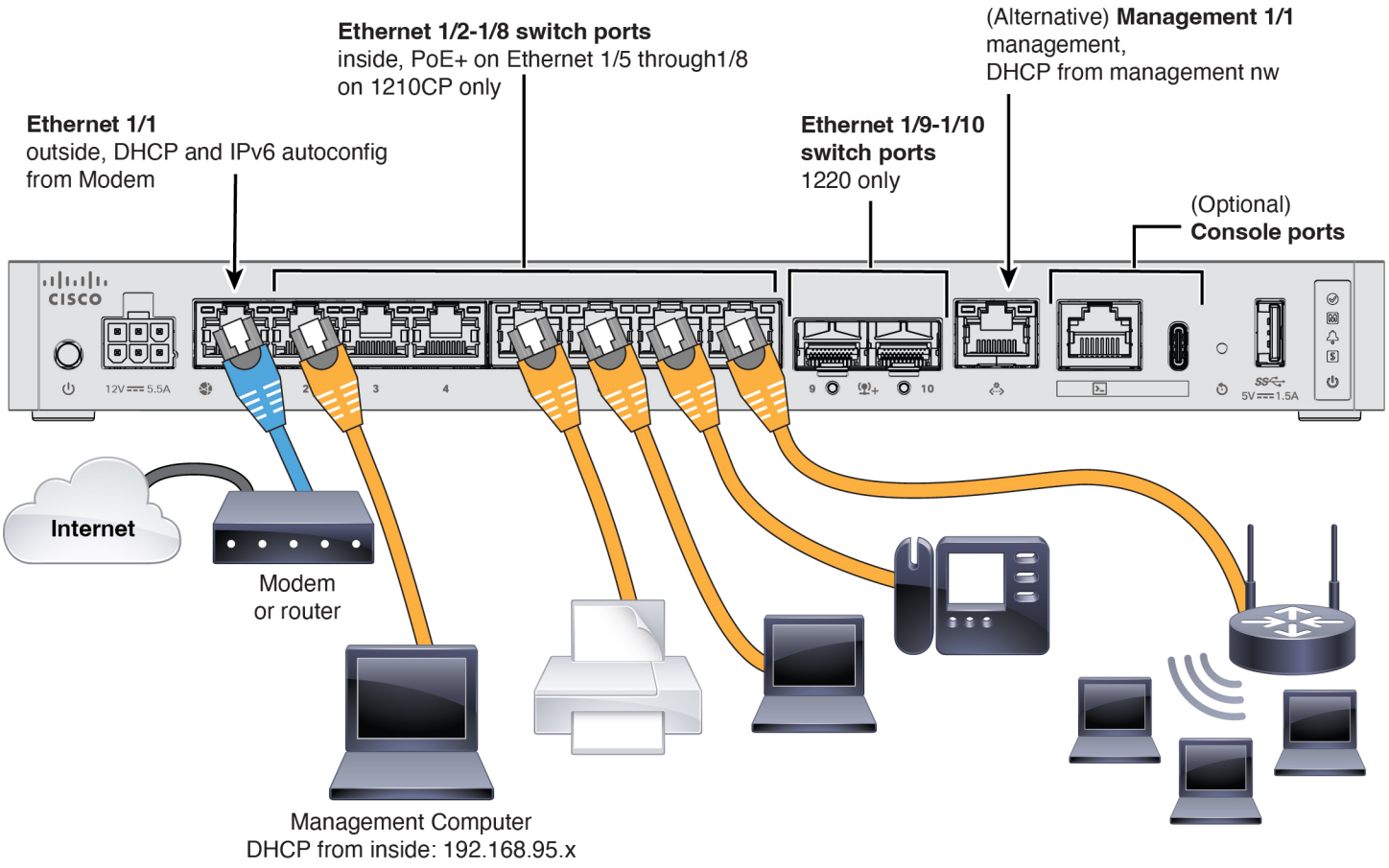
The Secure Firewall 1200 connects and protects the distributed enterprise. It extends Cisco's enterprise security policy and threat inspection to users and devices in branch offices and smaller sites. Powered by an efficient network processor, the Secure Firewall 1200 delivers high levels of security policy and threat defense without compromising user experience.

Manage a firewall using the local Secure Firewall Device Manager.

- Cable the firewall, on page 1
- Power on the firewall, on page 2
- Which application is installed: Firewall Threat Defense or ASA?, on page 4
- Access the Firewall Threat Defense CLI, on page 4
- Check the version and reimage, on page 6
- (Optional) Change management network settings at the CLI, on page 7
- Obtain licenses, on page 8
- (If Needed) Power off the firewall, on page 10

Cable the firewall

- For the Secure Firewall 1220, install SFPs into Ethernet 1/9 and 1/10—They are 1/10-Gb SFP+ ports that require SFP/SFP+ modules.
- 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.

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

Before you begin

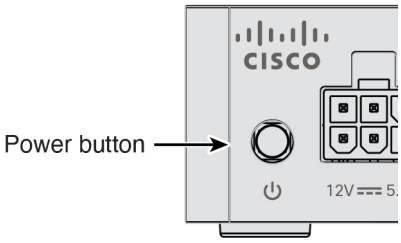
It's important that you provide reliable power for your firewall (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow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

Procedure

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

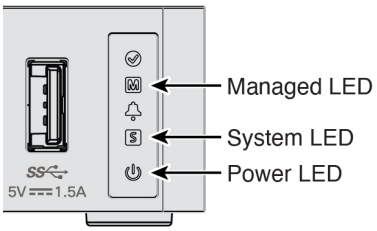
Step 2 Turn the power on using the power button located on the rear of the chassis, adjacent to the power cord.

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

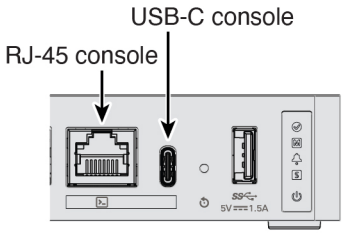
Which application is installed: Firewall Threat Defense or ASA?

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. If you need to log in all the way, see Access the Firewall Threat Defense CLI, on page 4.

```
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*.

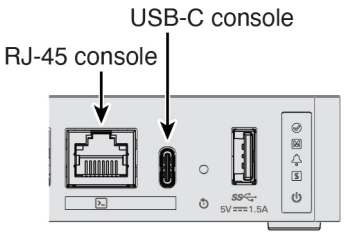
Access the Firewall Threat Defense CLI

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 FXOS. Log in to the CLI using the **admin** username and the password (the default is **Admin123**). The first time you log in, you are prompted to change the password.

```
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 3 Change to the Firewall Threat Defense CLI.

Note
If you want to use the Firewall Device Manager for initial setup, do not access the Firewall Threat Defense CLI, which starts the CLI setup.

connect ftd

The first time you connect to the Firewall Threat Defense CLI, you are prompted to complete initial setup.

Example:

```
firepower# connect ftd
>
```

To exit the Firewall Threat Defense CLI, enter the **exit** or **logout** command. This command returns you to the FXOS prompt.

Example:

```
> exit
firepower#
```

Check the version and reimage

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.

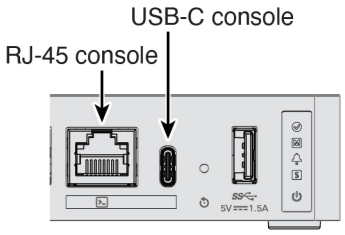
What version should I run?

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.

Procedure

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

Figure 5: Console Port



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) By default, the Management interface uses DHCP. If you need to set a static IP address for the Management interface, enter the following commands.

scope fabric-interconnect a

set out-of-band static ip *ip* **netmask** *netmask* **gw** *gateway*

commit-buffer

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

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

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

By default, you can manage the firewall on either of the following interfaces:

- Ethernet 1/2 and higher—192.168.95.1/24
- Management 1/1—IP address from DHCP

If you can't use the default IP addresses, then you can connect to the console port and perform initial setup at the CLI to set the Management 1/1 IP address to a static address.

Procedure

Step 1 Connect to the console port. See Which application is installed: Firewall Threat Defense or ASA?, on page 4.

Step 2 Connect to the Firewall Threat Defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 3 Complete the CLI setup script for the Management interface settings.

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
[...]

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.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
```

Guidance: Enter **y** for at least one of these types of addresses.

```
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
```

Guidance: Choose **manual** to set a static IP address.

```
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
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
```

Guidance: Set an IP address for the gateway.

```
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com


Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

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

>
```

Guidance: Enter **yes** to use the Firewall Device Manager.

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

Obtain licenses

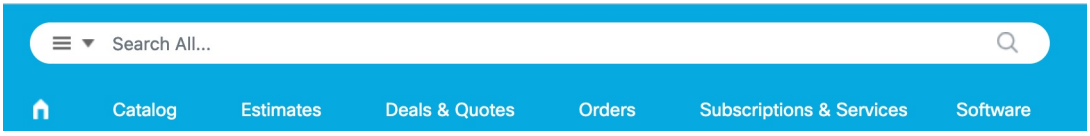
When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. If you don't have an account on the Smart Software Manager, click the link to set up a new account.

The Firewall Threat Defense has the following licenses:

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

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

Figure 6: License Search



2. Search for the following license PIDs.

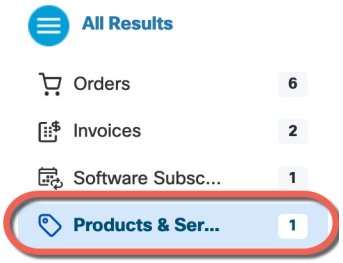
Note If a PID is not found, you can add the PID manually to your order.

- Essentials:
  - *Included automatically*
- IPS, Malware Defense, and URL combination:
  - L-CSF1210CET-TMC=
  - L-CSF1210CPT-TMC=
  - L-CSF1220CXT-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-CSF1210CE-TMC-1Y
  - L-CSF1210CE-TMC-3Y
  - L-CSF1210CE-TMC-5Y
  - L-CSF1210CP-TMC-1Y
  - L-CSF1210CP-TMC-3Y
  - L-CSF1210CP-TMC-5Y
  - L-CSF1220CX-TMC-1Y
  - L-CSF1220CX-TMC-3Y
  - L-CSF1220CX-TMC-5Y
- Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

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

Figure 7: Results



(If Needed) Power off the firewall

It's important that you shut down your system properly. Simply unplugging the power or pressing the power switch can cause serious file system damage. There are many processes running in the background all the time, and unplugging or shutting off the power does not allow the graceful shutdown of your firewall system.

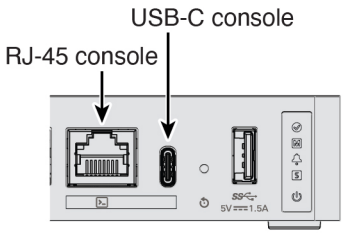
Power off the firewall at the CLI

You can use the FXOS CLI to safely shut down the system and power off the firewall.

Procedure

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

Figure 8: Console Port



Step 2 In the FXOS CLI, connect to local-mgmt mode.

firepower # **connect local-mgmt**

Step 3 Shut down the system.

firepower(local-mgmt) # **shutdown**

Example:

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

Step 4 Monitor the system prompts as the firewall shuts down. When the shutdown is complete, you will see the following prompt.

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Step 5 You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

Power off the firewall using the Firewall Device Manager

Shut down your system properly using the Firewall Device Manager.

Procedure

Step 1 Shut down the firewall.

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

b) Click **Shut Down**.

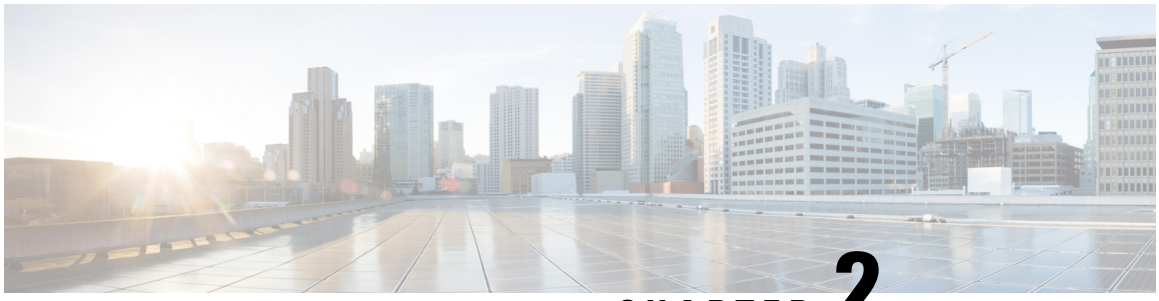
Step 2 If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. When shutdown is complete, you will see the following prompt.

```
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.



CHAPTER 2

Configure a Basic Policy

Complete the initial configuration and then configure additional interfaces and network settings as well as customizing your policy.

- Log Into the Firewall Device Manager, on page 13
- Complete the initial configuration, on page 13
- Configure the network settings and policy, on page 21

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, depending on which interface your computer is connected to.

- Ethernet 1/2 and higher—**https://192.168.95.1**
- Management 1/1—**https://***management_ip* (from DHCP)

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

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 couple of basic policies in place:

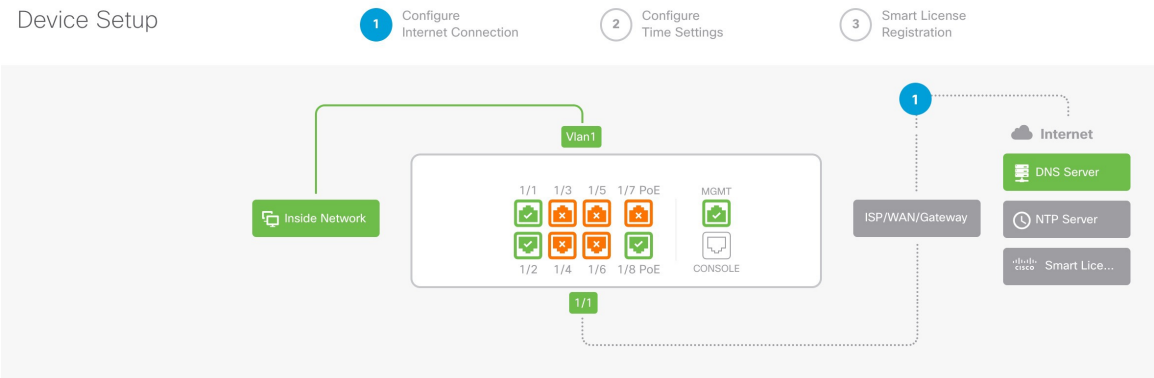
- inside→outside traffic flow
- Interface PAT for all traffic to outside.

Procedure

Step 1 Accept the General Terms and change the admin password.

The **Device Setup** screen appears.

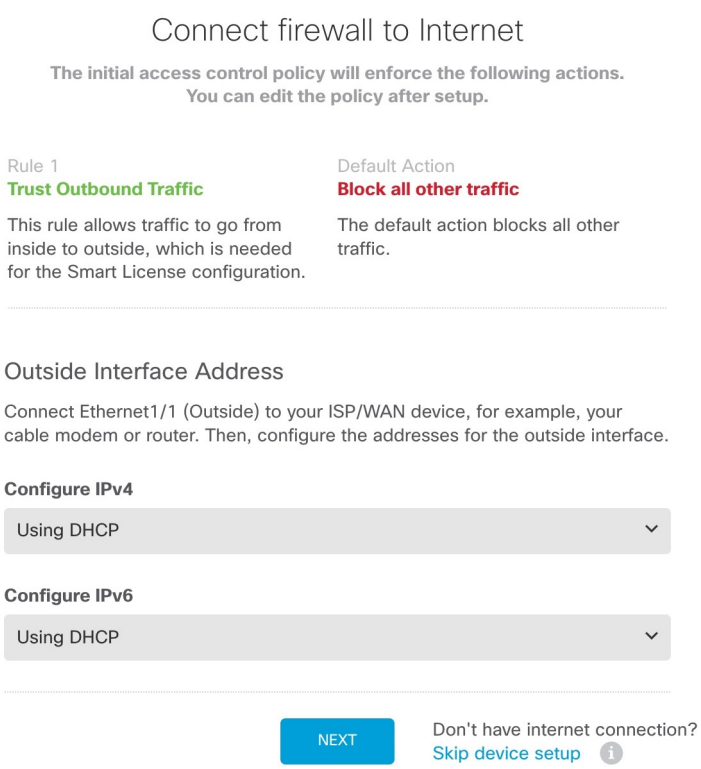
Figure 9: Device Setup



Note
The exact port configuration depends on your model.

Step 2 Configure network settings for the outside and management interfaces.

Figure 10: Connect firewall to internet



a) **Outside Interface**—Ethernet 1/1. You cannot select an alternative outside interface during initial device setup.

Configure IPv4—If you need PPPoE, you can configure it after you complete the wizard.

Configure IPv6

b) **Management Interface**—Sets parameters for the dedicated Management 1/1 interface. If you changed the IP address at the CLI, you will not see these settings because you already configured them.

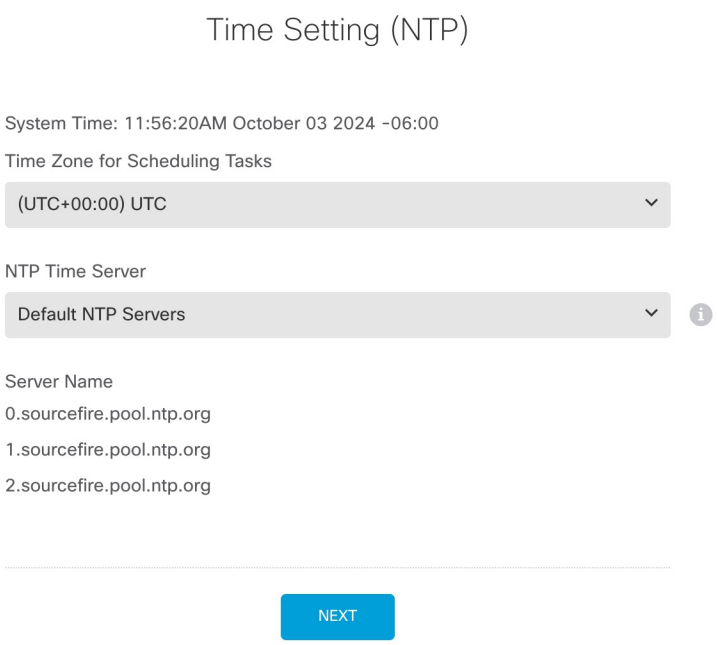
DNS Servers—The default is the OpenDNS public DNS servers.

Firewall Hostname

c) Click **Next**.

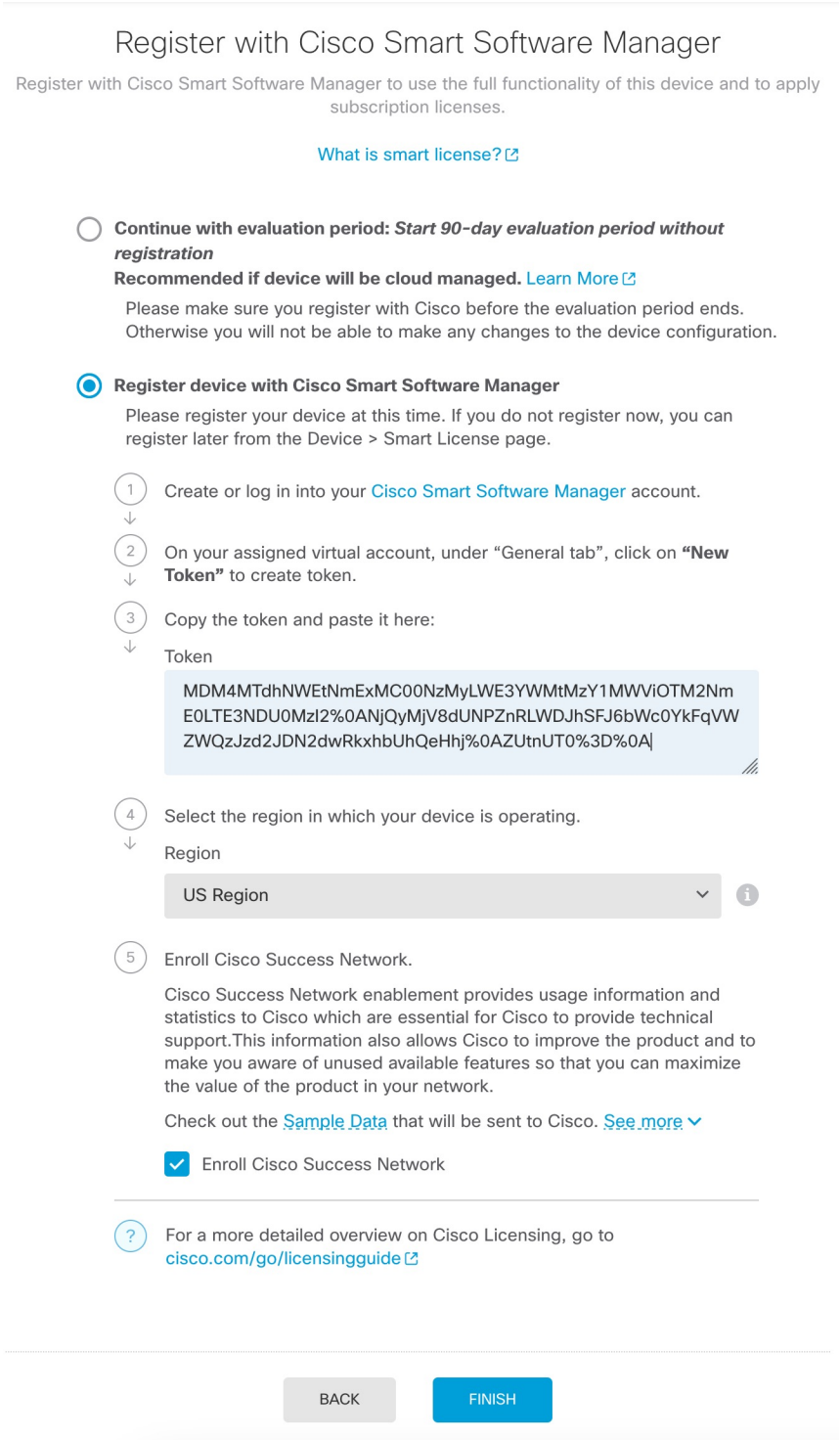
Step 3 Configure the system time settings.

Figure 11: Time Setting (NTP)

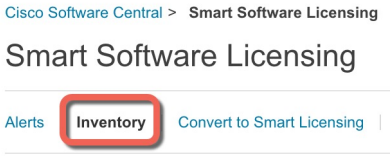


a) **Time Zone**
b) **NTP Time Server**
c) Click **Next**.

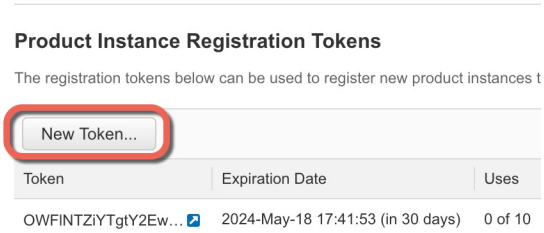
Step 4 Configure Smart Licensing.



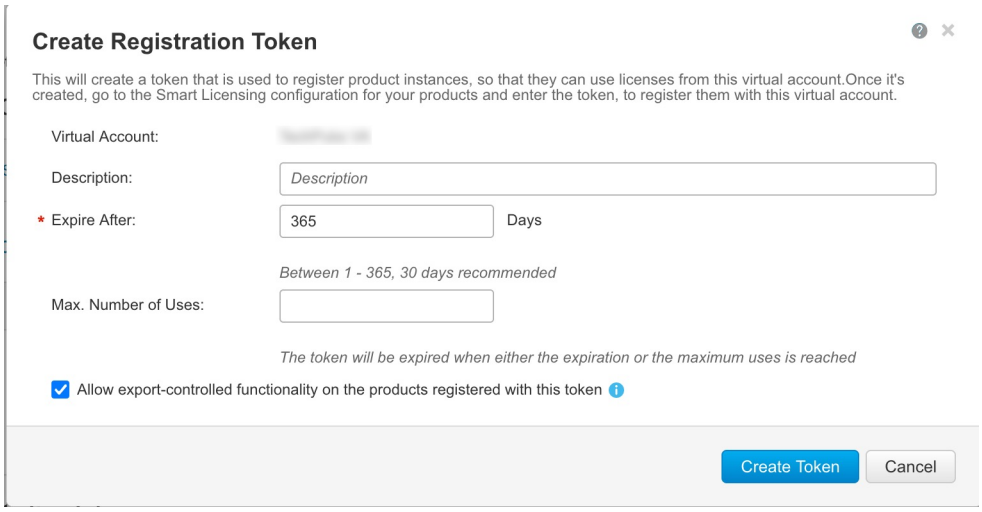
a) Click **Register device with Cisco Smart Software Manager**.
b) Click the Cisco Smart Software Manager link.
c) Click **Inventory**.



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



e) 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.

f) 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 12: View Token

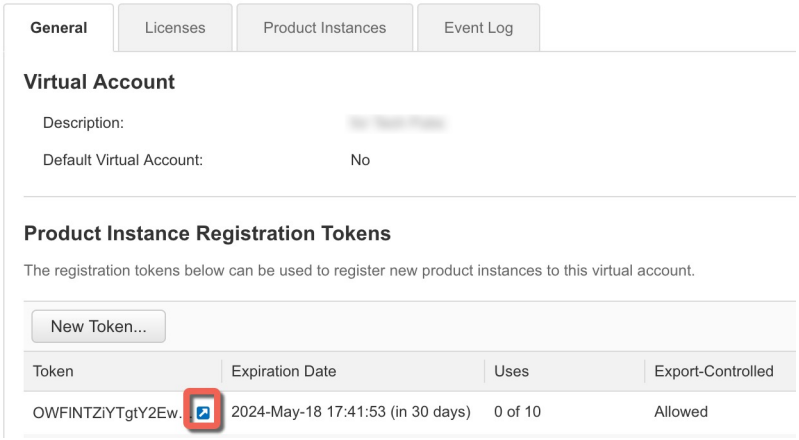
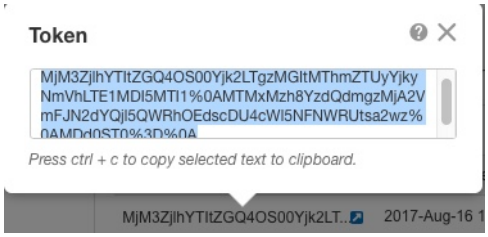


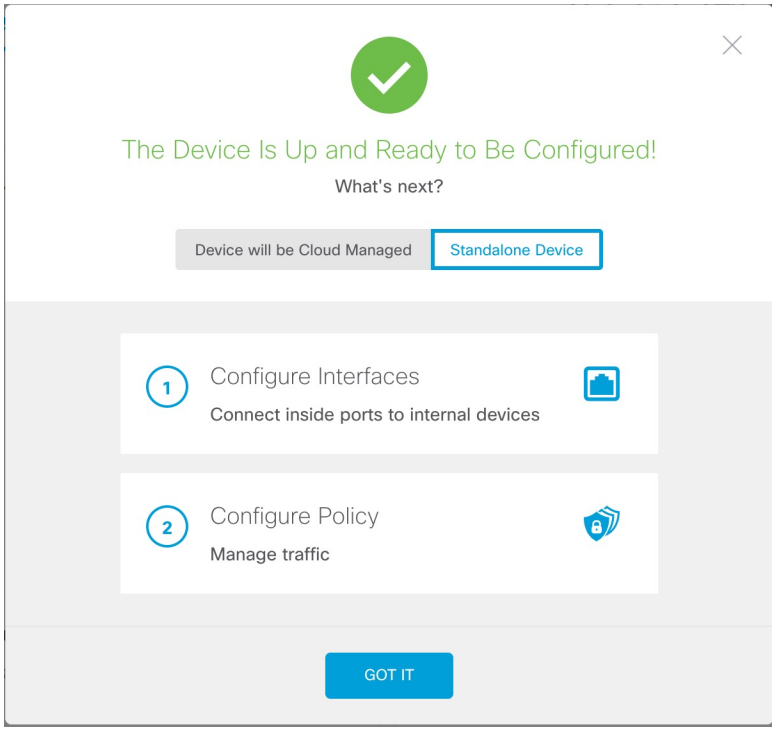
Figure 13: Copy Token



g) In the Firewall Device Manager, paste the token into the token field.
h) Set the other options, and then click **Finish**

Step 5 Finish the setup wizard.

Figure 14: What's Next

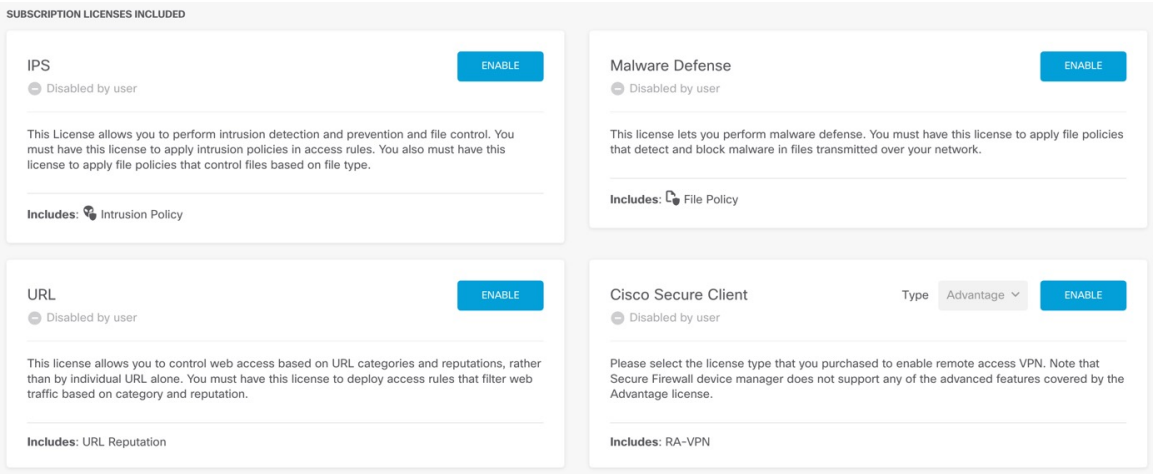


a) Click **Standalone Device** to use the Firewall Device Manager.
b) Click **Configure Interfaces** to go directly to the **Interfaces** page, **Configure Policy** to go to the **Policies** page, or **Got It** to go to the **Device** page.

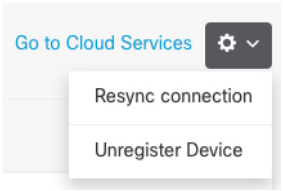
   For interfaces or policy configuration, see Configure the network settings and policy, on page 21.

Step 6 Enable feature licenses.

a) From the **Device** page, click **Smart License** > > **View Configuration**.
b) Click the **Enable/Disable** control for each optional license.



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



Configure the network settings and policy

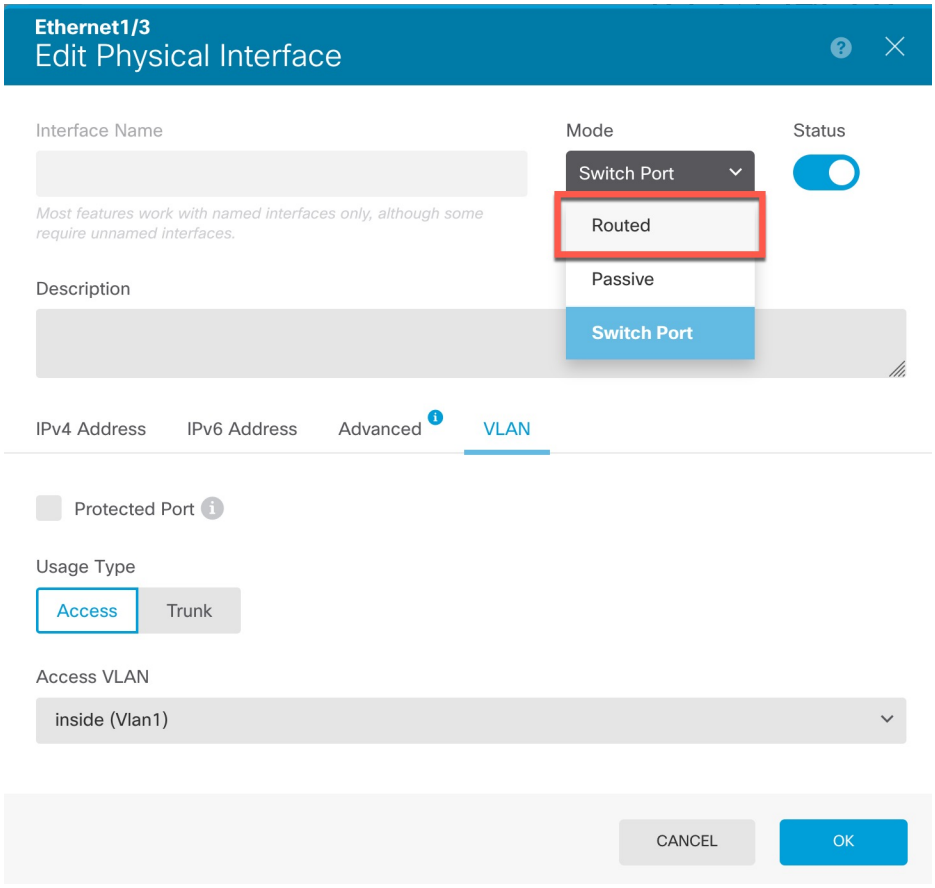
Configure additional interfaces, a DHCP server, and customize the security policy.

Procedure

Step 1 If you want to convert a switch port to a firewall interface, choose **Device**, and then click the link in the **Interfaces** summary.

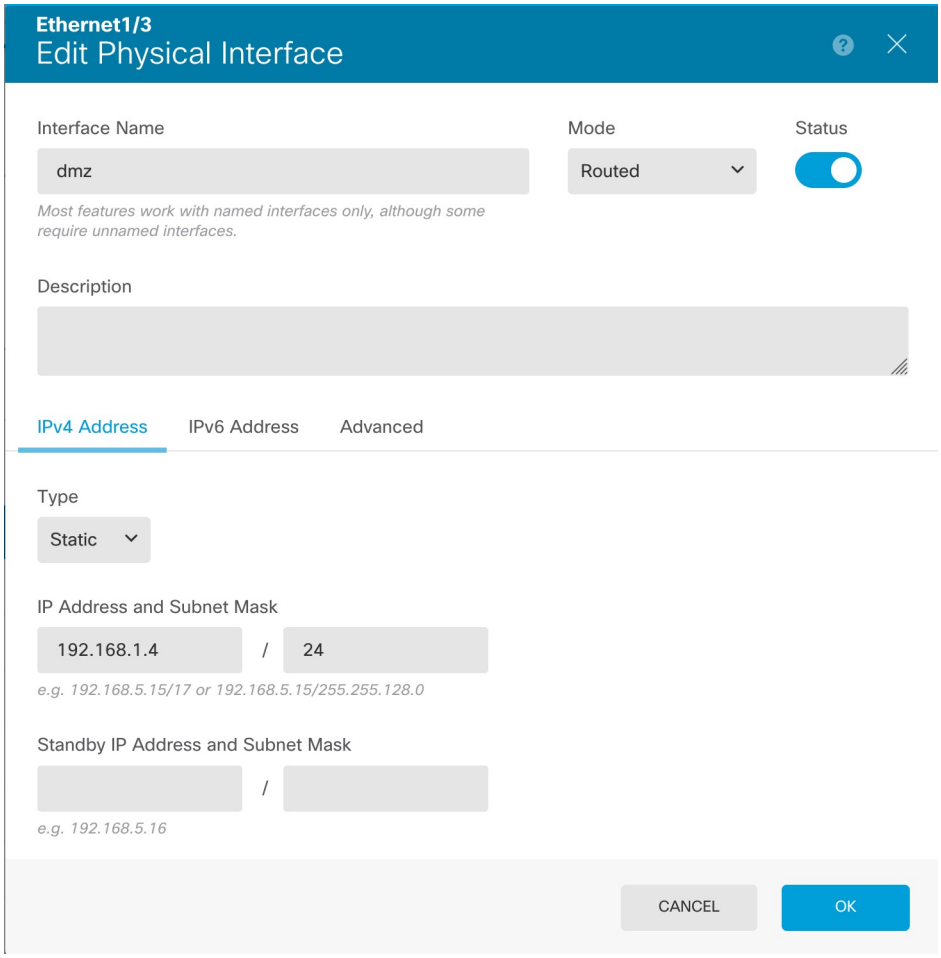
a) Click the edit icon ( ) for the switch port.
b) Change the mode from **Switch Port** to **Routed**.

Figure 15: Change the Mode



c) Set the name and IP address.

Figure 16: Edit Interface



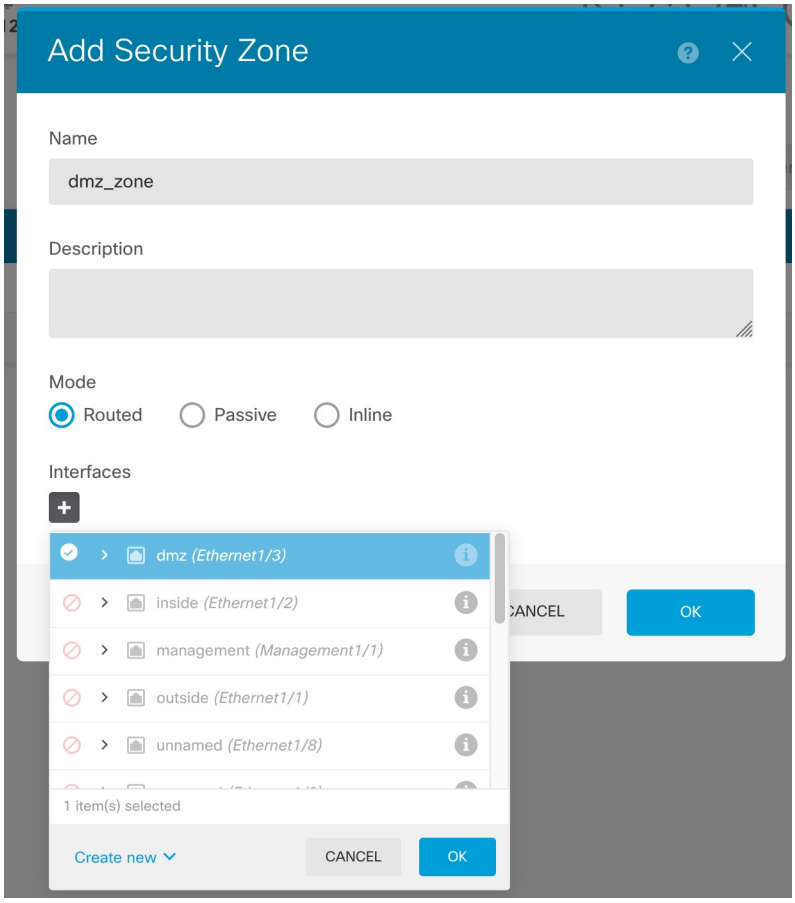
d) Click **OK**.

Step 2 If you configured new firewall interfaces, choose **Objects**, then select **Security Zones**.

Edit or create new zones as appropriate and assign the interface to the zone. Each interface must belong to a zone for which you configure policies.

The following example creates a new dmz_zone and then assigns the dmz interface to it.

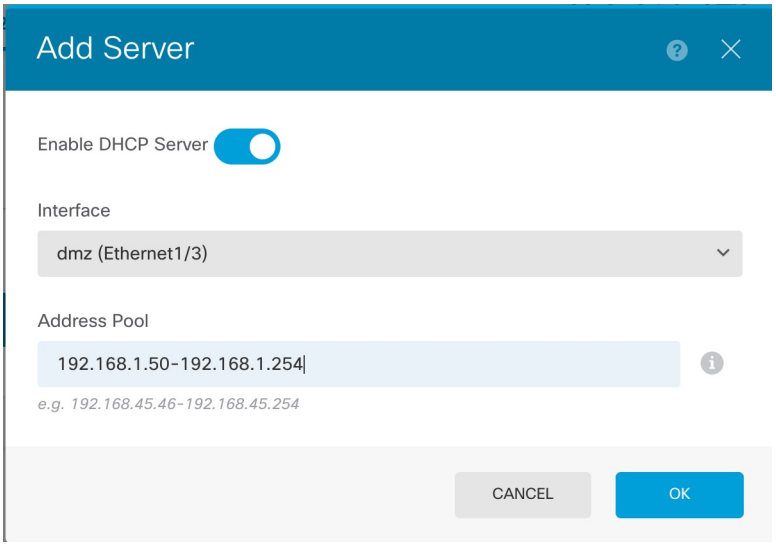
Figure 17: Security Zone Object



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.

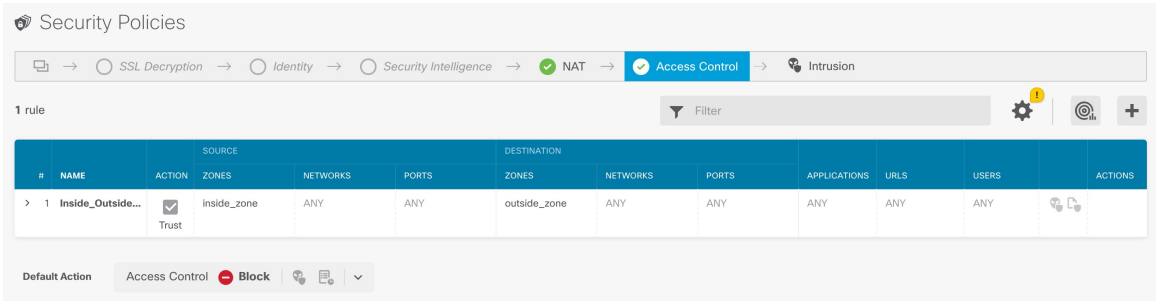
Figure 18: DHCP Server



Step 4 Choose **Policies** and configure the security policies for the network.

The device setup wizard enables traffic flow between the inside_zone and outside_zone using a Trust rule. A Trust rule does not apply an intrusion policy. To use intrusion, specify the Allow action for the rule. The policy also includes interface PAT for all interfaces when going to the outside interface.

Figure 19: Default Security Policies



However, if you have interfaces in different zones, you need access control rules to allow traffic to and from those zones.

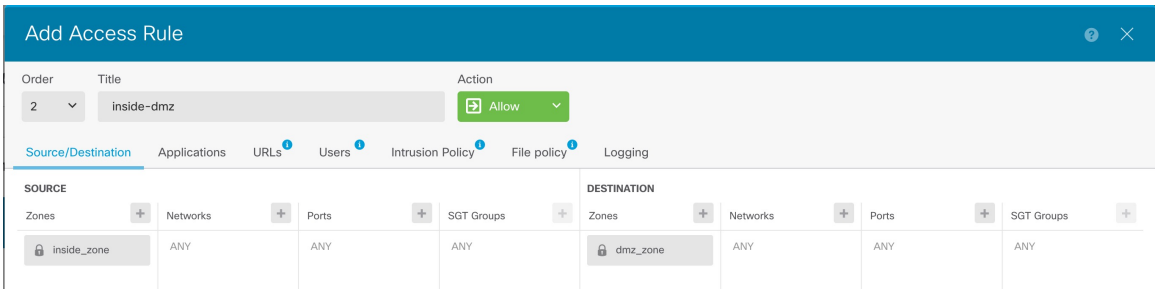
In addition, you can configure other policies to provide additional services and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies by clicking the policy type in the toolbar:

- **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**—(Requires the IPS license) 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 20: Access Control Policy



Step 5 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 6 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.

© 2026 Cisco Systems, Inc. All rights reserved.