cisco.



Secure Firewall 1210/20 Threat Defense Getting Started: Cloud-delivered Firewall Management Center

First Published: 2024-10-10

Last Modified: 2024-10-21

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



Before You Begin

Install the firewall at a branch office and manage it on the outside interface using the Cisco Defense Orchestrator.

Note For high availability, you can use the outside interface with manual registration, but to use zero-touch provisioning, you must use the Management interface. This guide specifically covers outside management, but you can refer to Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator for management using the Management interface.

- Power On the Firewall, on page 1
- Which Application is Installed: Threat Defense or ASA?, on page 2
- Access the Threat Defense CLI, on page 3
- · Check the Version and Reimage, on page 4
- Obtain Licenses, on page 6
- (If Needed) Power Off the Firewall, on page 7

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

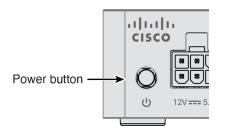
The first time you boot up the firewall, threat defense initialization can take approximately 15 to 30 minutes.

Before you begin

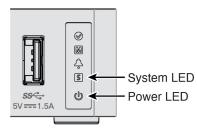
It's important that you provide reliable power for your firewall (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow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

Procedure

- **Step 1** Attach the power cord to the firewall, and connect it to an electrical outlet.
- Step 2Turn the power on using the power button located on the rear of the chassis, adjacent to the power cord.Figure 1: Power Button



Step 3Check the Power LED on the back of the firewall; if it is solid green, the firewall is powered on.Figure 2: System and Power LEDs



Step 4 Check the System LED on the back of the firewall; after it is solid green, the system has passed power-on diagnostics.

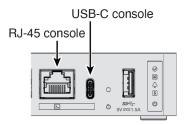
Which Application is Installed: Threat Defense or ASA?

Both applications, 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 threat defense or ASA.

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 Threat Defense CLI, on page 3.

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.

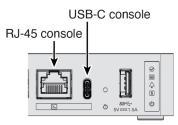
Access the Threat Defense CLI

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 threat defense CLI.
 - Note

If you want to use the device manager for initial setup or use zero-touch provisioning, do not access the threat defense CLI, which starts the CLI setup.

connect ftd

The first time you connect to the threat defense CLI, you are prompted to complete initial setup.

Example:

```
firepower# connect ftd
>
```

To exit the 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

USB-C console RJ-45 console

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

scope ssa

show app-instance

Example:

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

- **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

Note If you encounter the following error, you must disable DHCP before committing the change. Follow the commands below to disable DHCP.

```
firepower /fabric-interconnect* # commit-buffer
Error: Update failed: [Management ipv4 address (IP <ip> / net mask <netmask> ) is not
in the same network of current DHCP server IP range <ip - ip>.
Either disable DHCP server first or config with a different ipv4 address.]
firepower /fabric-interconnect* # exit
firepower* # scope system
firepower /system* # scope services
firepower /system/services* # disable dhcp-server
firepower /system/services* # 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.

For low-touch provisioning, when you onboard the device, for the **Password Reset** area, be sure to choose **No** because you already set the password.

d) Shut down the firewall. See (If Needed) Power Off the Firewall, on page 7.

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.

If you have not already done so, register CDO with the Smart Software Manager. Registering requires you to generate a registration token in the Smart Software Manager. See the CDO documentation for detailed instructions.

The threat defense has the following licenses:

- Essentials—Required
- IPS
- Malware Defense
- URL Filtering
- Cisco Secure Client
- If you need to add licenses yourself, go to Cisco Commerce Workspace and use the Search All field.
 Figure 6: License Search

| ≡▼ | Search All | | | | | Q |
|----|------------|-----------|----------------|--------|--------------------------|----------|
| ń | Catalog | Estimates | Deals & Quotes | Orders | Subscriptions & Services | Software |

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

| | Products & Ser | 1 |
|-------|----------------|---|
| 菎 | Software Subsc | 1 |
| [::\$ | Invoices | 2 |
| Ä | Orders | 6 |
| | All 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

USB-C console RJ-45 console

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 Management Center

Shut down your system properly using the management center.

Procedure

Step 1

Shut down the firewall.

- a) Choose **Devices** > **Device Management**.
- b) Next to the device that you want to restart, click **Edit** (\Diamond).
- c) Click the **Device** tab.

- d) Click **Shut Down Device** (**US**) in the **System** section.
- e) When prompted, confirm that you want to shut down the device.
- **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.

Power Off the Firewall Using the Management Center



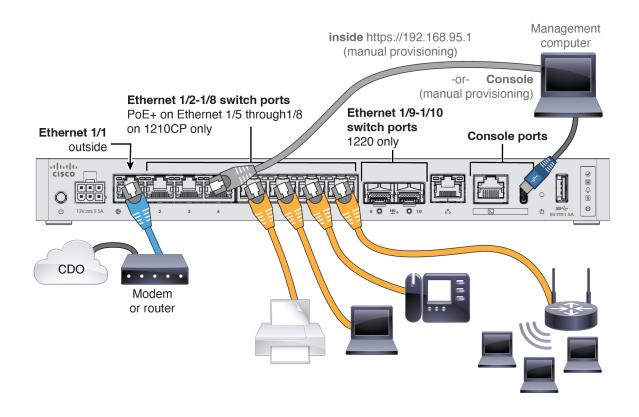
Cable and Onboard the Firewall

Cable and onboard the firewall to CDO.

- Cable the Firewall, on page 11
- Onboard the Firewall to CDO, on page 12
- Perform Initial Configuration (Manual Provisioning), on page 18

Cable the Firewall

- For the Secure Firewall 1220, install SFPs into ports Ethernet 1/9 and 1/10. The ports are 1/10-Gb SFP+ ports that require SFP/SFP+ modules.
- See the hardware installation guide for more information.
- Do not cable the Management interface unless you are using high availability with zero-touch provisioning. In this case, see Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator. This guide covers only the outside interface for zero-touch provisioning.



Onboard the Firewall to CDO

Onboard the firewall using zero-touch provisioning or manual provisioning.

Onboard the Firewall with Zero-Touch Provisioning

Onboard the threat defense using zero-touch provisioning and the device serial number.

Procedure

| Step 1 Step 2 Step 3 | In the CDO navigation pane, click Inventory , then click the blue plus button (+) to Onboard a device. Select the FTD tile. Under Management Mode , be sure FTD is selected. | | | |
|----------------------------|---|--|--|--|
| | At any point after selecting FTD as the management mode, you can click Manage Smart License to enroll in or modify the existing smart licenses available for your device. See Obtain Licenses, on page 6 to see which licenses are available. | | | |
| Step 4 | Select Use Serial Number as the onboarding method. | | | |

Figure 9: Use Serial Number



Step 5 In Select FMC, choose the Cloud-Delivered FMC > Firewall Management Center from the list, and click Next. Figure 10: Select FMC

| 1 Select FMC | Select FMC O For more details, Click Here |
|------------------------|--|
| | Select |
| | Cloud-Delivered FMC |
| | Firepower Management Center (Recommended) |
| 2 Connection | On-Prem FMCs (7.4+) 🕑 |
| 3 Password Reset | FMC-Securex-Onboarding-1654149835633 FMC-Securex-Onboarding-1658238180734 |
| Policy Assignment | FMC-Securex-Onboarding-1681247022490 FMC-Securex-Onboarding-1681762232392 |
| 5 Subscription License | FMC-Securex-Onboarding-1681830086235 |
| 6 Done | Boulder FMC 740-48 1543 + Onboard On-Prem FMC |

Step 6 In the **Connection** area, enter the **Device Serial Number** and the **Device Name** and then click **Next**.

Figure 11: Connection

| 2 Connection | Device Serial Number JAD253802GB | Device Name fp-1010-1 | Enter the serial number of the FTD device you want to onboard, then CDO will attempt to connect to the device. |
|--------------|--|--------------------------|--|
| | Next | | Important: Only FTD 1000, 2100 or 3100 series devices (running on software version 7.4 or later) are supported. |

 Step 7
 In Password Reset, click Yes.... Enter a new password and confirm the new password for the device, then click Next.

For zero-touch provisioning, the device must be brand new or has been reimaged.

Note If you logged into the device and reset the password, and you did not change the configuration in a way that would disable zero-touch provisioning, then you should choose the **No...** option. There are a number of configurations that disable zero-touch provisioning provisioning, so we don't recommend logging into the device unless you need to, for example, to perform a reimage.

Figure 12: Password Reset

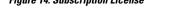
| 3 Password Reset | 1 Please review all the prerequisites for onboarding with a serial number. Learn more ♂ Be 8-128 characters Be 8-128 characters Have at least one lower and one upper case letter |
|------------------|---|
| | 2 Is this a new device that has never been logged into or configured for a manager? Yes, this new device has never been logged into or configured for a manager Enter a new password for devices that have never been configured for a manager. Important: If you select this option and the device's default password has already been changed, onboarding fails. New Password Confirm Password Confirm Password |
| | No, this device has been logged into and configured for a manager Use this option if you already changed the password in the device CLI. Important: If you select this option and the device's default password has not been changed, onboarding fails. |

Step 8 For the **Policy Assignment**, use the drop-down menu to choose an access control policy for the device. If you have no policies configured, choose the **Default Access Control Policy**.

Figure 13: Policy Assignment

| 4 | Policy Assignment | Access Control Policy |
|---|-------------------|-----------------------|
| | | Next |

Step 9For the Subscription License, check each of the feature licenses you want to enable. Click Next.Figure 14: Subscription License



| 6 | Subscription License | | | 0 | Enable subscription licenses. CDO will attempt to |
|---|----------------------|--------------------------|-----------------------------------|---|--|
| | | License Type | Includes | | enable the selected licenses when the device is connected to CDO and registered with the supplied |
| | | Ssentials | Base Firewall Capabilities | | Smart License. Learn more about Cisco Smart Accounts. |
| | | Carrier (7.3+ FTDs only) | GTP/GPRS, Diameter, SCTP, M3UA | | |
| | | V IPS | Intrusion Policy | | |
| | | Malware Defense | C File Policy | | |
| | | URL | URL Reputation | | |
| | | RA VPN VPNOnly - | RA VPN | | |
| | | Next | | | |

Step 10 (Optional) Add labels to your device to help sort and filter the **Inventory** page. Enter a label and select the blue plus

| button (| |). Labels are | applied to the | he device | after it's | onboarded to | OCDO. |
|----------|--|---------------|----------------|-----------|------------|--------------|-------|
|----------|--|---------------|----------------|-----------|------------|--------------|-------|

| Figure 15: Done | |
|-----------------|--|
| 6 Done | Your device is now onboarding. This may take a long time to finish. You can check the status of the device on the Devices and Services page. Add Labels Add Labels Go to Inventory |
| | |

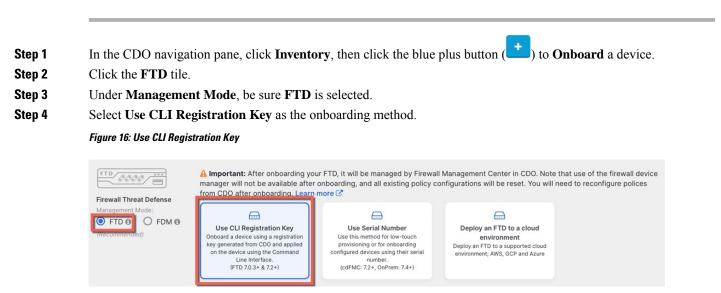
What to do next

From the **Inventory** page, select the device you just onboarded and select any of the option listed under the **Management** pane located to the right.

Onboard the Firewall with Manual Provisioning

Onboard the firewall using a CLI registration key.

Procedure



Step 5 Enter the **Device Name** and click **Next**.

| 1 Device | e Name | Device Name | |
|----------|--------|-------------|--|

Step 6For the Policy Assignment, use the drop-down menu to choose an access control policy for the device. If you have no
policies configured, choose the Default Access Control Policy.

Figure 18: Access Control Policy

| 2 | Policy Assignment | Access Control Policy |
|---|-------------------|---------------------------------|
| | | Default Access Control Policy - |
| | | Next |

Step 7 For the **Subscription License**, click the **Physical FTD Device** radio button, and then check each of the feature licenses you want to enable. Click **Next**.

Figure 19: Subscription License

| 3 Subscription License | Please indicate if this FTD is physical or virtual: Physical FTD Device Virtual FTD Device | | | | |
|------------------------|---|-----------------------------------|--|--|--|
| | License Type | Includes | | | |
| | Ssentials | Base Firewall Capabilities | | | |
| | Carrier (7.3+ FTDs only) | GTP/GPRS, Diameter, SCTP, M3UA | | | |
| | IPS | Intrusion Policy | | | |
| | Malware Defense | C ₆ File Policy | | | |
| | URL | URL Reputation | | | |
| | RA VPN Premier 🕶 | RA VPN | | | |
| | Next | | | | |

Step 8 For the **CLI Registration Key**, CDO generates a command with the registration key and other parameters. You must copy this command and use it in the intial configuration of the threat defense.

Figure 20: CLI Registration Key

| 4 CLI Registration Key | 1 Ensure the device's initial configuration is complete before trying to apply the registration key. Learn more |
|------------------------|--|
| | 2 Copy the CLI Key below and paste it into the CLI of the FTD |
| | configure manager add cisco-security-docs.app.us.cdo.cisco.com BanyI2oaT0ew1JTpC0P2w3xEBnVVkfZv x7R7dwcm43JCMzwGY3ZzCfoFmZhW97my cisco-security- docs.app.us.cdo.cisco.com |
| | Next |

configure manager add *cdo_hostname registration_key nat_id display_name*

Complete initial configuration at the CLI or using the device manager:

- Initial Configuration: CLI, on page 24—Copy this command at the threat defense CLI after you complete the startup script.
- Initial Configuration: Device Manager, on page 18—Copy the cdo_hostname, registration_key, and nat_id parts of the command into the Management Center/CDO Hostname/IP Address, Management Center/CDO Registration Key, and NAT ID fields.

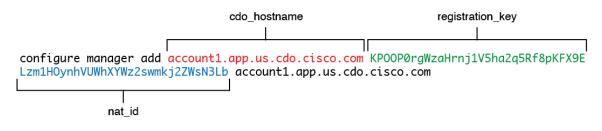
Example:

Sample command for CLI setup:

configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com

Sample command components for GUI setup:

Figure 21: configure manager add command components



- **Step 9** Click **Next** in the onboarding wizard to start registering the device.
- **Step 10** (Optional) Add labels to your device to help sort and filter the **Inventory** page. Enter a label and select the blue plus

button (). Labels are applied to the device after it's onboarded to CDO.

| Done | Your device is now onboarding. | |
|------|--|---------|
| | • This may take a long time to finish. You can check the status of the device on the Devices and Service | es page |
| | Add Labels 🚱 | |
| | Add label groups and labels + | |

Perform Initial Configuration (Manual Provisioning)

For manual provisioning, perfom initial configuration of the firewall using the Secure Firewall device manager or using the CLI.

Initial Configuration: Device Manager

Using this method, after you register the firewall, the following interfaces will be preconfigured in addition to the Management interface:

- Ethernet 1/1-outside, IP address from DHCP, IPv6 autoconfiguration
- VLAN1— inside, 192.168.95.1/24
- Default route-Obtained through DHCP on the outside interface
- Additional interfaces—Any interface configuration from the device manager is preserved.

Other settings, such as the DHCP server on inside, access control policy, or security zones, are not preserved.

Procedure

- **Step 1** Connect your computer to the inside interface (Ethernet 1/2 through 1/8 or for the Secure Firewall 1220, 1/2 through 1/10).
- **Step 2** Log into the device manager.
 - a) Go to https://192.168.95.1.
 - b) Log in with the username admin and the default password Admin123.
 - c) You are prompted to read and accept the General Terms and change the admin password.
- **Step 3** Use the setup wizard.

L

Figure 23: Device Setup Configure Time Settings Smart License **Device Setup** (3) (2) Registration lnternet Vlan 📑 DNS Serve × × **.** × ×

Note

The exact port configuration depends on your model.

a) Configure the outside and management interfaces.

Figure 24: Connect firewall to internet

Connect firewall to Internet

The initial access control policy will enforce the following actions. You can edit the policy after setup.

| Rule 1 Trust Outbound Traffic | Default Action Block all other traffic |
|---|--|
| This rule allows traffic to go from inside to outside, which is needed for the Smart License configuration. | The default action blocks all other traffic. |
| Outside Interface Address | |
| Connect Ethernet1/1 (Outside) to your cable modem or router. Then, configure | |

| Configure IPv4 | | | |
|----------------|------|---|-----|
| Using DHCP | | ~ | |
| Configure IPv6 | | | |
| Using DHCP | | ~ | |
| | | | |
| | NEXT | Don't have internet connections Skip device setup | on? |

- 1. Outside Interface Address—Use a static IP address if you plan for high availability. You cannot configure PPPoE using the setup wizard; you can configure PPPoE after you complete the wizard.
- 2. Management Interface—The Management interface settings are used even though you are using manager access on the outside interface. For example, management traffic that is routed over the backplane through the outside

interface will resolve FQDNs using these Management interface DNS servers, and not the outside interface DNS servers.

DNS Servers—The DNS server for the system's management address. The default is the OpenDNS public DNS servers. These will probably match the outside interface DNS servers you set later since they are both accessed from the outside interface.

Firewall Hostname

b) Configure the Time Setting (NTP) and click Next.

Figure 25: Time Setting (NTP)

| Time Setting (NTP) | | |
|--|---|---|
| System Time: 11:56:20AM October 03 2024 -06:00 | | |
| Time Zone for Scheduling Tasks | | |
| (UTC+00:00) UTC | ~ | |
| | | |
| NTP Time Server | | |
| Default NTP Servers | ~ | 6 |
| | | |
| Server Name | | |
| 0.sourcefire.pool.ntp.org | | |
| 1.sourcefire.pool.ntp.org | | |
| 2.sourcefire.pool.ntp.org | | |
| | | |
| | | |
| NEXT | | |

c) Select Start 90 day evaluation period without registration.



d) Click Finish.

I

Figure 26: What's Next

| | | \times |
|-----|---|----------|
| The | e Device Is Up and Ready to Be Configured! What's next? | |
| | Device will be Cloud Managed Standalone Device | |
| | | |
| (| 1 Configure Interfaces Connect inside ports to internal devices | |
| (| 2 Configure Policy Manage traffic | |
| | | |
| | GOT IT | |

e) Choose Standalone Device, and then Got It.

Step 4 If you want to configure additional interfaces, choose Device, and then click the link in the Interfaces summary.

 Step 5
 Register with the CDO by choosing Device > System Settings > Central Management and clicking Proceed

 Configure the Management Center/CDO Details.

Figure 27: Management Center/CDO Details

Configure Connection to Management Center or CDO

Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

| ● Yes ○ No |
|---|
| Threat Defense Management Center/CDO 10.89.5.16 10.89.5.35 fe80::6a87:c6ff:fea6:4c00/64 10.89.5.35 |
| Management Center/CDO Hostname or IP Address |
| 10.89.5.35 |
| Management Center/CDO Registration Key |
| •••• |
| NAT ID Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address. |
| 11203 |
| Connectivity Configuration Threat Defense Hostname |
| 1120-3 |
| DNS Server Group |
| CustomDNSServerGroup |
| Management Center/CDO Access Interface O Data Interface |
| Please select an interface |
| Management Interface View details |
| CANCEL |

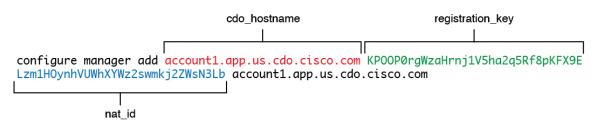
a) For Do you know the Management Center/CDO hostname or IP address, click Yes.

CDO generates the **configure manager add** command. See Onboard the Firewall with Manual Provisioning, on page 15 to generate the command.

configure manager add cdo_hostname registration_key nat_id display_name

Example:

Figure 28: configure manager add command components



b) Copy the *cdo_hostname*, *registration_key*, and *nat_id* parts of the command into the **Management Center/CDO** Hostname/IP Address, Management Center/CDO Registration Key, and NAT ID fields.

Step 6 Configure the **Connectivity Configuration**.

a) Specify the **Threat Defense Hostname**.

This FQDN will be used for the outside interface.

b) Specify the **DNS Server Group**.

Choose an existing group, or create a new one. The default DNS group is called **CiscoUmbrellaDNSServerGroup**, which includes the OpenDNS servers.

To retain the outside DNS server setting after registration, you need to re-configure the DNS Platform Settings in the management center.

c) For the Management Center/CDO Access Interface, click Data Interface, and then choose outside.

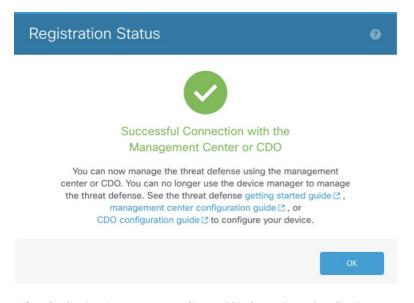
Step 7 (Optional) Click Add a Dynamic DNS (DDNS) method.

DDNS ensures the management center can reach the threat defense at its FQDN if the threat defense's IP address changes.

Step 8 Click Connect.

The Registration Status dialog box shows the current status of the CDO registration.

Figure 29: Successful Connection



Step 9 After the **Saving Management Center/CDO Registration Settings** step on the status screen, go to the CDO and add the firewall. See Onboard the Firewall with Manual Provisioning, on page 15.

Initial Configuration: CLI

Set the dedicated Management IP address, gateway, and other basic networking settings using the CLI setup script.

Procedure

Step 1 Connect to the console port and access the threat defense CLI. See Access the Threat Defense CLI, on page 3.
Step 2 Complete the CLI setup script for the Management interface settings.
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.
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. Although you do not plan to use the Management interface, you must set an IP address, for example, a private address.

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

Guidance: Choose **manual**. DHCP is not supported when using the outside interface for manager access. Make sure this interface is on a different subnet from the manager access interface to prevent routing issues.

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]:

Guidance: Set the gateway to be **data-interfaces**. This setting forwards management traffic over the backplane so it can be routed through the outside interface.

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

Guidance: Set the Management interface DNS servers. These will probably match the outside interface DNS servers you set later, since they are both accessed from the outside interface.

```
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]: no

Guidance: Enter **no** to use the management center.

```
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'
```

Guidance: Enter routed. Outside manager access is only supported in routed firewall mode.

Configuring firewall mode ...

Device is in OffBox mode - disabling/removing port 443 from iptables. Update policy deployment information

- add device configuration
- add network discovery
- add system policy

You can register the sensor to a Firepower Management Center and use the Firepower Management Center to manage it. Note that registering the sensor to a Firepower Management Center disables on-sensor Firepower Services management capabilities.

When registering the sensor to a Firepower Management Center, a unique alphanumeric registration key is always required. In most cases, to register a sensor to a Firepower Management Center, you must provide the hostname or the IP address along with the registration key. 'configure manager add [hostname | ip address] [registration key]' However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key] [NAT ID]'
Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.

Step 3 Configure the outside interface for manager access.

>

6

configure network management-data-interface

You are then prompted to configure basic network settings for the outside interface.

Manual IP Address

> configure network management-data-interface Data interface to use for management: ethernet1/1 Specify a name for the interface [outside]: internet IP address (manual / dhcp) [dhcp]: manual IPv4/IPv6 address: 10.10.6.7 Netmask/IPv6 Prefix: 255.255.255.0 Default Gateway: 10.10.6.1 Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220

Guidance: To retain the outside DNS servers after registration, you need to re-configure the DNS Platform Settings in the management center.

DDNS server update URL [none]: Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to change the manager access network

use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration. Network settings changed.

>

IP Address from DHCP

> configure network management-data-interface Data interface to use for management: ethernet1/1 Specify a name for the interface [outside]: IP address (manual / dhcp) [dhcp]: DDNS server update URL [none]: https://dwinchester:pa\$\$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a> Do you wish to clear all the device configuration before applying ? (y/n) [n]: Configuration done with option to allow manager access from any network, if you wish to change the manager access network use the 'client' option in the command 'configure network management-data-interface'. Setting IPv4 network configuration. Network settings changed.

>

L

Step 4 Identify the CDO that will manage this threat defense using the **configure manager add** command that CDO generated. See Onboard the Firewall with Manual Provisioning, on page 15 to generate the command.

Example:

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
LzmlHOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
```

Step 5 Shut down the threat defense so you can send the device to the remote branch office.

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. Remember that 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 system.

- a) Enter the **shutdown** command.
- b) Observe the Power LED and Status LED to verify that the chassis is powered off (appear unlit).
- c) After the chassis has successfully powered off, you can then unplug the power to physically remove power from the chassis if necessary.



Configure a Basic Policy

Configure a basic security policy with the following settings:

- Inside and outside interfaces—Assign a static IP address to the inside interface, and use DHCP for the outside interface.
- DHCP server—Use a DHCP server on the inside interface for clients.
- Default route—Add a default route through the outside interface.
- NAT—Use interface PAT on the outside interface.
- Access control-Allow traffic from inside to outside.

You can also ccustomize your security policy to include more advanced inspections.

- Configure Interfaces, on page 29
- Configure the DHCP Server, on page 34
- Configure NAT, on page 35
- Configure an Access Control Rule, on page 38
- Enable SSH on the Outside Interface, on page 41
- Deploy the Configuration, on page 42

Configure Interfaces

When you use zero-touch provisioning or the device manager for initial setup instead of using the CLI, the following interfaces are preconfigured:

- Ethernet 1/1—outside, IP address from DHCP, IPv6 autoconfiguration
- VLAN1— inside, 192.168.95.1/24
- Default route—Obtained through DHCP on the outside interface

If you performed additional interface-specific configuration within device manager before registering with the management center, then that configuration is preserved.

If you used the CLI for initial setup, there is no preconfiguration of your device.

In both cases, you need to perform additional interface configuration after you register the device. For CLI initial setup, you must add the VLAN1 interface for the inside switch ports. Additional configuration includes

converting switch ports to firewall interfaces as desired, assigning interfaces to security zones, and changing IP addresses.

The following example configures a routed-mode inside interface (VLAN1) with a static address and a routed-mode outside interface using DHCP (Ethernet1/1). It also adds a DMZ interface for an internal web server.

Procedure

Step 1 Choose **Devices** > **Device Management**, and click **Edit** (\Diamond) for the device.

Step 2 Click Interfaces.

Figure 30: Interfaces

| vice Routing Interfact | es Inline Sets D | HCP VTE | P SNMP | | (| ्रे Search by na | me | Syn | c Device Add II | nterfac |
|------------------------|------------------|----------|----------------|---|---------------|------------------|------------|---------|------------------|---------|
| Interface | Logical Name | Туре | Security Zones | MAC Address (Active/Standby) IP Address | Path Monitori | n: Port Mode | VLAN Usage | SwitchP | o Virtual Router | |
| Management1/1 | management | Physical | | | Disabled | | | | Global | Q |
| Ethernet1/1 | outside | Physical | outside | 10.89.5.29/255.255.255.192(| Disabled | | | | Global | Ø |
| Ethernet1/2 | | Physical | | | Disabled | Access | 1 | | | Ø |
| Ethernet1/3 | | Physical | | | Disabled | Access | 1 | | | Ø |
| Ethernet1/4 | | Physical | | | Disabled | Access | 1 | | | 0 |

- **Step 3** If you used the CLI for initial setup, enable the switch ports.
 - a) Click **Edit** (\Diamond) for the switch port.

Figure 31: Enable Switch Port

| Edit Physical Interface |
|--------------------------------|
| General Hardware Configuration |
| Interface ID: Ethernet1/2 |
| Description: |
| Port Mode: |
| Access ~ |
| VLAN ID: |
| Protected: |

b) Enable the interface by checking the **Enabled** check box.

L

- c) (Optional) Change the VLAN ID; the default is 1. You will next add a VLAN interface to match this ID.
- d) Click OK.
- **Step 4** Add (or edit) the **inside** VLAN interface.
 - a) Click Add Interfaces > VLAN Interface, or if this interface already exists, click Edit (2) for the interface. Figure 32: Add VLAN Interface

| Ceneral IPv4 IPv6 Advanced Name: inside Description: Mode: None Security Zone: inside_zone VII: 1500 (d - 9198) Priority: 0 0 VLAN ID *: 1 (r + 000) Disable Forwarding on Interface Vlan: None Port Mo Korecords to display | Add VLAN Interface | 0 |
|---|---|---|
| inside Image: Construction: Constru | General IPv4 IPv6 Advanced | |
| Priority: 0 (0 - 65535) VLAN ID *: 1 (1 - 4070) Disable Forwarding on Interface Vlan: None ~ Associated Interface Port Mo | inside I Enabled Description: Mode: None Security Zone: inside_zone MTU: 1500 | |
| | Priority: 0 VLAN ID *: 1 (1 ~ 4070) Disable Forwarding on Interface Vlan: None ~ | |
| | | |

- b) From the Security Zone drop-down list, choose an existing inside security zone or add a new one by clicking New.
 For example, add a zone called inside_zone. You apply your security policy based on zones or groups.
 If VLAN1 was preconfigured, the rest of these fields are optional.
- c) Enter a Name up to 48 characters in length.

For example, name the interface inside.

- d) Check the **Enabled** check box.
- e) Leave the Mode set to None.

f) Set the VLAN ID to 1.

By default, all of the switchports are set to VLAN 1; if you choose a different VLAN ID here, you need to also edit each switchport to be on the new VLAN ID.

You cannot change the VLAN ID after you save the interface; the VLAN ID is both the VLAN tag used, and the interface ID in your configuration.

- g) Click the IPv4 and/or IPv6 tab.
 - IPv4—Choose Use Static IP from the drop-down list, and enter an IP address and subnet mask in slash notation.

For example, enter 192.168.1.56/24

Figure 33: Set Inside IP Address

Add VLAN Interface

| General | IPv4 | IPv6 | Advanced |
|---------------|----------|------------|--------------|
| IP Type: | | | |
| Use Stat | ic IP | | ~) |
| IP Address | : | | |
| 192.168.1 | .56/24 | | |
| eg. 192.0.2.1 | /255.255 | 255.128 or | 192.0.2.1/25 |

• IPv6—Check the Autoconfiguration check box for stateless autoconfiguration.

- h) Click **OK**.
- **Step 5** Click Edit (\Diamond) for Ethernet1/1 that you want to use for **outside**.

The General page appears.

Figure 34: General

Edit Physical Interface

| General | IPv4 | IPv6 | Path Monitoring | Harc |
|--|-----------|----------|-----------------|--------|
| Name: | | | _ | |
| | | | | |
| outside | | | | |
| 🔽 Enable | ed | | | |
| Manag | gement O | inly | | |
| Descriptior | า: | | | |
| | | | | |
| Mode: | | | | |
| None | | | ~ | |
| Security Zo | one: | | | |
| outside_: | zone | | ~] | |
| Outside_ | 20110 | | | |
| Interface I | | | | |
| | D: | | | |
| Interface II | D: | | | |
| Interface II | D: | | | |
| Interface II Ethernet | D: | | | |
| Interface II Ethernet MTU: 1500 | D: | | | |
| Interface II Ethernet MTU: 1500 (64 - 9198) | D: | | (0 - | 65535) |
| Interface II Ethernet MTU: 1500 (64 - 9198) Priority: | D: 1/1 | Group Ta | | 65535) |
| Interface II Ethernet MTU: 1500 (64 - 9198) Priority: 0 | D: 1/1 | Group Ta | | 65535) |
| Interface II Ethernet MTU: 1500 (64 - 9198) Priority: 0 Propagate | D: 1/1 | Group Ta | | 65535) |

a) From the Security Zone drop-down list, choose an existing outside security zone or add a new one by clicking New.
 For example, add a zone called outside_zone.

You should not alter any other basic settings because doing so will disrupt the management center management connection.

- b) Click OK.
- **Step 6** Configure a DMZ interface to host a web server, for example.
 - a) Disable switch-port mode for the switch port you want to use for the DMZ by clicking the slider in the **SwitchPort** column so it shows as disabled (.....).
 - b) Click **Edit** (\Diamond) for the interface.
 - c) From the Security Zone drop-down list, choose an existing DMZ security zone or add a new one by clicking New.
 For example, add a zone called dmz_zone.
 - d) Enter a Name up to 48 characters in length.

For example, name the interface **dmz**.

e) Check the **Enabled** check box.

- f) Leave the Mode set to None.
- g) Click the IPv4 and/or IPv6 tab and configure the IP address as desired.
- h) Click **OK**.

```
Step 7 Click Save.
```

Configure the DHCP Server

Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the firewall.

Procedure

| Step | 1 | Choose | e Devices | > Device Management, | and click Edit (\mathcal{O}) for the device. | |
|------|---|-----------|-----------|----------------------|---|--|
| • | • | C1 | DITOD | DILODO | | |

Step 2 Choose **DHCP** > **DHCP Server**.

Figure 35: DHCP Server

| Device Routing | Interfaces | Inline Sets DHC | P VTEP | SNMP | | | | | |
|----------------|------------|-----------------------|-------------|----------|-----------------------|---------------|---|--------------------|-------|
| | | Ping Timeout | | ~ | | | | | |
| DHCP Server | | 50 | | (10 - 1 | 10000 ms) | | | | |
| DHCP Relay | | Lease Length | | | | | | | |
| DDNS | | 3600 | |) (300 · | - 10,48,575 sec) | | | | |
| | | Auto-Configuration | ı | | | | | | |
| | | Interface | | | | | | | |
| | | | ~ | ·] | | | | | |
| | | Override Auto Con | igured Sett | ings: | | | | | |
| | | Domain Name | | _ | | | | | |
| | | | | J | | | | | |
| | | Primary DNS Server | | _ | Primary WINS Server | _ | | | |
| | | | \sim |) + | | ~] | + | | |
| | | Secondary DNS Server | | | Secondary WINS Server | | | | |
| | | | ~ |) + | | $\overline{}$ | + | | |
| | Г | Server Advanced | | | | | | | |
| | | | | | | | | | + Add |
| | | Interface | | | Address Pool | | | Enable DHCP Server | |
| | | No records to display | | | | | | | |

Step 3 In the **Server** area, click **Add** and configure the following options.

Figure 36: Add Server

| Add Server | | ? |
|--------------------------|--------|----|
| Interface* | | |
| inside v | | |
| Address Pool* | | |
| 192.168.1.2-192.168.1.55 | | |
| (2.2.2.10-2.2.2.20) | | |
| Enable DHCP Server | | |
| | | |
| | | |
| | Cancel | ок |

- Interface—Choose the interface name from the drop-down list.
- Address Pool—Set the range of IP addresses. The IP addresses must be on the same subnet as the selected interface and cannot include the IP address of the interface itself.
- Enable DHCP Server—Enable the DHCP server on the selected interface.

Step 4Click OK.Step 5Click Save.

Configure NAT

This procedure creates a NAT rule for internal clients to convert the internal addresses to a port on the outside interface IP address. This type of NAT rule is called *interface Port Address Translation (PAT)*.

Procedure

- **Step 1** Choose **Devices** > **NAT**, and click **New Policy**.
- **Step 2** Name the policy, select the devices that you want to use the policy, and click **Save**.

Figure 37: New Policy

| New Policy | | | ? |
|---|---------------|-------------------------------|--------|
| Name: FTD_policy | | | |
| Description: | | | |
| Targeted Devices Select devices to which you want to apply t | his policy. | | _ |
| Available Devices and Templates |) | Selected Devices and Template | s Ē |
| 192.168.0.124 192.168.0.155 | | | |
| | Add to Policy | | |
| | | | |
| | | | |
| | | | |
| | | Cancel | Save |

The policy is added the management center. You still have to add rules to the policy.

Figure 38: NAT Policy

| FTD_Policy | | | | | | | | Show Warning | s Save | Cancel |
|--------------------------------------|-------------------------------------|-------------------------------------|---------------------|--------------------------|----------------------|-----------------------|----------------------------|------------------------|------------|--------------|
| Enter Description | | | | | | | | | | |
| Rules | | | | | | | N | IAT Exemptions | Policy Ass | ignments (1) |
| Filter by Device | √ Filter Rules | | | | | | | | \otimes | Add Rule |
| | | | | | | | | | | |
| | | | | Original Packet | | | Translated Packet | | | |
| # Direction | Source Type Interface Objects | Destination Interface Objects | Original Sources | Original Destinations | Original Services | Translated Sources | Translated Destinations | Translated Services | Options | |
| NAT Rules Before | | | | | | | | | | |
| | | | | | | | | | | |
| Auto NAT Rules | | | | | | | | | | |
| ✓ NAT Rules After | | | | | | | | | | |

Step 3 Click Add Rule.

Step 4 Configure the basic rule options:

I

Figure 39: Basic Rule Options

| Add NAT Rule | • |
|-------------------|-------------|
| NAT Rule: | |
| Auto NAT Rule | ~ |
| Туре: | |
| Dynamic | ~ |
| Enable | |
| Interface Objects | Translation |

- NAT Rule—Choose Auto NAT Rule.
- Type—Choose Dynamic.
- **Step 5** On the **Interface Objects** page, add the outside zone from the **Available Interface Objects** area to the **Destination Interface Objects** area.

Figure 40: Interface Objects

| Interface Objects | Translation | PAT Pool | Advanced | | | |
|-----------------------------|-------------|---------------|--------------------------|-----|-------------------------------|-----|
| Available Interface Objects | e C' | | Source Interface Objects | (0) | Destination Interface Objects | (1) |
| Q Search by name | | | any | | 3 outside | ō) |
| inside | Ad | d to Source | | | | |
| 1 outside | Add t | o Destination | | | | |
| T | 2 | | | | | |
| | - | | | | | |
| | | | | | | |

Step 6 On the **Translation** page, configure the following options:

Figure 41: Translation

| Interface Objects | Translation | PAT Pool | Advanced | | | | | |
|-------------------------------|-------------|----------|---|--|--|--|--|--|
| Original Packet | | | Translated Packet | | | | | |
| Original Source:* all-ipv4 | ~ + | | Translated Source: Destination Interface IP The values selected for | | | | | |
| Original Port: TCP | ~ | | Destination Interface Objects in 'Interface Objects' tab will be used | | | | | |
| | | | Translated Port: | | | | | |

• Original Source—Click Add (+) to add a network object for all IPv4 traffic (0.0.0.0/0).

Figure 42: New Network Object

| New Network Object | | ? |
|----------------------------|--------|------|
| Name all-ipv4 | | |
| Description | | |
| Network Arge Range Network | O FQDN | |
| 0.0.0.0/0 | | |
| Allow Overrides | | |
| | Cancel | Save |

Note You cannot use the system-defined **any-ipv4** object, because Auto NAT rules add NAT as part of the object definition, and you cannot edit system-defined objects.

- Translated Source—Choose Destination Interface IP.
- **Step 7** Click **Save** to add the rule.

The rule is saved to the **Rules** table.

Step 8 Click **Save** on the **NAT** page to save your changes.

Configure an Access Control Rule

If you created a basic **Block all traffic** access control policy when you registered the device, then you need to add rules to the policy to allow traffic through the device. The access control policy can include multiple rules that are evaluated in order.

This procedure creates an access control rule to allow all traffic from the inside zone to the outside zone.

Procedure

Step 1Choose Policy > Access Policy > Access Policy, and click Edit (?) for the access control policy assigned to the device.Step 2Click Add Rule, and set the following parameters.

L

Figure 43: Source Zone

| 1 | 🇯 Add Rul | e | | | | | | | |
|--------|------------------------------------|---------------------------------------|------------|--------------|---------|---------------|--------------------|---------------------|-----------------|
| Name | inside-to-outsid | e | | | | | | Action 💽 Allow | |
| Insert | into Mandatory | ~ | | | | | | Intrusion Policy | None |
| Q | Zones (1) | Networks | Ports | Applications | 🛕 Users | URLs | Dynamic Attributes | s VLAN Tags | |
| Clea | ar Selections | Search Security Zc | ne Objects | | Showir | ng 2 out of 2 | Selected 1 | Selected Sources: 0 | I |
| 2 | ♣ inside (Route) ♣ outside (Route) | d Security Zone) ed Security Zone) | | | | | | | |
| | | | | | | | | | Any |
| + C | reate Security Zor | ne Object | | | | | | 3 | Add Source Zone |

- 1. Name this rule, for example, inside-to-outside.
- 2. Select the inside zone from Zones

3. Click Add Source Zone.

Figure 44: Destination Zone

| 1 🗘 Add Rule | | |
|---|---|------------------------|
| Name inside-to-outside | Action 💽 Allow 🔍 🖻 Logging OFF 🖪 Time Range None | ∼ Ru |
| Insert into Mandatory V | Intrusion Policy None Variable Set Variable Set | File Policy None |
| Q Zones (2) Networks Ports Applications 🛕 Users URLs | Dynamic Attributes VLAN Tags | |
| Clear Selections Q Search Security Zone Objects Showing 2 out of 2 Search Security Zone Objects | elected 1 Selected Sources: 1 Selected Destination | ns and Applications: 0 |
| inside (Routed Security Zone) | Collapse All Remove All | |
| 4 vutside (Routed Security Zone) | ZONE V 1 Object | |
| | 🚓 inside | |
| | | Any |
| + Create Security Zone Object | Add Source Zone 5 | Add Destination Zone |

4. Select the outside zone from Zones.

5. Click Add Destination Zone.

Leave the other settings as is.

Step 3 (Optional) Customize associated policies by clicking on the policy type in the packet flow diagram.

Prefilter, Decryption, Security Intelligence, and Identity policies are applied before an access control rule. Customizing these policies is not required, but after you know your network's needs, they let you improve network performance by either fastpathing trusted traffic (bypassing processing) or blocking traffic so no further processing is required.

Figure 45: Policies Applied Before Access Control

| <i>□</i> Packets → | 0 | Prefilter Rules | → C | Decryption | → | Ø | Security Intelligence | + | 🔘 Ide | ntity | • | Ø | Access Control | |
|--------------------|---|------------------------|-----|------------|---|---|-----------------------|---|-------|-------|---|---|----------------|--|
|--------------------|---|------------------------|-----|------------|---|---|-----------------------|---|-------|-------|---|---|----------------|--|

• **Prefilter Rules**—The Default Prefilter Policy passes all traffic for the other rules to act on (analyzes). The only change to the default policy you can make is to **block** tunnel traffic. Otherwise, you can create a new prefilter policy to associate with the access control policy that can analyze (pass on), fastpath (bypass further checks) or block.

Prefiltering lets you improve performance by dealing with traffic before it gets any further, by either blocking or fastpathing. In a new policy, you can add *tunnel* rules and *prefilter* rules. A tunnel rule lets you fastpath, block, or rezone plaintext (non-encrypted), passthrough tunnels. A prefilter rule lets you fastpath or block non-tunneled traffic identified by IP address, port, and protocol.

For example, if you know you want to block all FTP traffic on your network, but fastpath SSH traffic from an administrator, you can add a new prefilter policy.

- **Decryption**—Decryption is not applied by default. Decryption is a way to expose network traffic to deep inspection. In most cases, you don't want to decrypt traffic, and can only do so if it is legally allowed. For maximum network protection, a decryption policy might be a good idea for traffic going to critical servers or coming from untrusted network segments.
- Security Intelligence—(Requires the IPS license) Security Intelligence is enabled by default. Security Intelligence is another early defense against malicious activity applied before passing connections to the access control policy for further processing. Security Intelligence uses reputation intelligence to quickly block connections to or from IP addresses, URLs, and domain names provided by Talos, the threat intelligence organization at Cisco. You can add or delete additional IP addresses, URLs, or domains if desired.
- **Note** If you do not have the IPS license, this policy will not be deployed even though it shows in your access control policy as enabled.
- **Identity**—Identity is not applied by default. You can require a user to authenticate before allowing traffic to be processed by the access control policy.
- **Step 4** (Optional) Add an Intrusion policy that is applied after the access control rule.

The Intrusion policy is a defined set of intrusion detection and prevention configurations that inspects traffic for security violations. The management center includes many system-provided policies you can enable as-is or that you can customize. This step enables a system-provided policy.

a) Click the Intrusion Policy drop-down list.

Figure 46: System-Provided Intrusion Policies

| Intr | usion Policy | None ^ |
|---------------------|--------------|-----------------------------|
| ags | | System-Provided Policies |
| Selected Sources: 1 | | Balanced Security and Conne |
| | | Connectivity Over Security |
| ZONE | 🗸 1 Object | Maximum Detection |
| | 📫 inside_ | Security Over Connectivity |
| | | User-Created Policies |

- b) Choose one of the system-provided policies from the list.
- **Step 5** (Optional) Add a File policy that is applied after the access control rule.

a) Click the **File Policy** drop-down list and choose either an existing policy or add one by choosing the **Open File Policy** List.

Figure 47: File Policy

| File Policy | None | ^ |
|-------------------|------------------------------------|---|
| | No options | |
| ns and Applicatio | Open File Policy List [↗] | |

For a new policy, the **Policies** > **Malware & File** page opens in a separate tab.

- b) See the Cisco Secure Firewall Device Manager Configuration Guide for details on creating the policy.
- c) Return to the Add Rule page and select the newly created policy from the drop-down list.

Step 6 Click Apply.

The rule is added to the **Rules** table.

Step 7 Click Save.

Enable SSH on the Outside Interface

This section describes how to enable SSH connections to the outside interface.

By default, you can use the admin user for which you configured the password during initial setup.

Procedure

Step 3

| Step 1 Choose Devices > Platform Settings and create or edit the threat | defense | policy. |
|---|---------|---------|
|---|---------|---------|

- Step 2 Select SSH Access.
 - Identify the outside interface and IP addresses that allow SSH connections.
 - a) Click Add to add a new rule, or click Edit to edit an existing rule.
 - b) Configure the rule properties:
 - **IP** Address—The network object or group that identifies the hosts or networks you are allowing to make SSH connections. Choose an object from the drop-down menu, or click + to add a new network object.
 - Available Zones/Interfaces—Add the outside zone or type the outside interface name into the field below the Selected Zones/Interfaces list and click Add.

| Edit Secure Shell | Configuration | 0 |
|----------------------------|--|------|
| IP Address* any-ipv4 | ~ + | |
| Available Zones/Interfaces | C [™] Selected Zones/Interfaces | |
| Q Search | Add | |
| inside | | |
| outside | | |
| | outside | Add |
| | Canc | е ОК |

c) Click **OK**.

Step 4 Click Save.

You can now go to **Deploy > Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Deploy the Configuration

Deploy the configuration changes to the device; none of your changes are active on the device until you deploy them.

Procedure

Step 1 Click **Deploy** in the upper right.

Figure 49: Deploy



Step 2 For a quick deployment, check specific devices and then click **Deploy**.

Figure 50: Deploy Selected

| Q | Advanced Deploy |
|--------|----------------------|
| 1010-2 | Ready for Deployment |
| 1120-3 | Ready for Deployment |

Or click **Deploy All** to deploy to all devices.

Figure 51: Deploy All

| Q | Advanced Deploy Ignore warnings Deploy All |
|--------------|---|
| 1010-2 | Ready for Deployment |
| 1120-3 | Ready for Deployment |
| 1120-4 | Ready for Deployment |
| ftd-cluster1 | Ready for Deployment |
| ftd1 | Ready for Deployment |
| | |

🟮 5 devices are available for deployment 📴 🕓

Otherwise, for additional deployment options, click Advanced Deploy.

Figure 52: Advanced Deployment

| nding C | hanges Reports | | | | | | | |
|------------|---|----------------------|--|------|-------|--------------------|---------|----------------------|
| | Device | Modified by | Inspect Interru | Туре | Group | Last Deploy Time | Preview | |
| , 🗆 | ftd1 | rboersma, Syster | n | FTD | | Feb 26, 2024 11:09 | đ | Ready for Deployment |
| , | ftd-cluster1 | rboersma, Syster | n | FTD | | Feb 22, 2024 10:36 | đ | Ready for Deployment |
| - 🔽 | 1010-2 | rboersma, Syster | n | FTD | | Feb 22, 2024 11:09 | ٩ | Ready for Deployment |
| x= ⊘ | Access Control Group Access Control Policy: In-out Intrusion Policy: No Rules Active Network Manysis Policy: Balanced Secur Device Configurations Interface Policy Flex Configuration Tempiate Policy: Unassigned NAT Group Manual NAT Rules: interface_PAT Security Updates Rule Uodates (Bcref-20240311-2013) | ity and Connectivity | Q rboersma, System Q System Q rboersma Q rboersma Q rboersma Q rboersma | | | | | |

Step 3 Ensure that the deployment succeeds. Click the icon to the right of the **Deploy** button in the menu bar to see status for deployments.

Figure 53: Deployment Status

| | Q s | earch | | Deploy | @ | ? |
|-------------|----------------------------------|---------------|-----------------|--------------|----------|------------------------|
| Deployments | Upgrades | A Health | Tasks | \checkmark | Show | Pop-up Notifications 🥫 |
| 7 total | 1 running | 6 success | 0 warnings | 0 failures | Q | Filter |
| 😜 1010-2 | Deploy comple | | and object coll | ection | 10% 💻 | <u>11s</u> |
| 1120-3 | Deployment to device successful. | | | | | |
| 1120-4 | Deployment to device successful. | | | | | 2m 43s |
| 3110-1 | Deploy | ment to devic | e successful. | | | 1m 38s |

 $^{\odot}$ 2024 Cisco Systems, Inc. All rights reserved.