Firepower Threat Defense Deployment with FMC

Is This Chapter for You?

This chapter describes how to deploy a standalone FTD logical device with FMC. To deploy a High Availability pair or a cluster, see the FMC configuration guide.

In a typical deployment on a large network, multiple managed devices are installed on network segments, monitor traffic for analysis, and report to a managing FMC, which provides a centralized management console with web interface that you can use to perform administrative, management, analysis, and reporting tasks.

For networks that include only a single device or just a few, where you do not need to use a high-powered multiple-device manager like the FMC, you can use the integrated Firepower Device Manager (FDM). Use the FDM web-based device setup wizard to configure the basic features of the software that are most commonly used for small network deployments.

Privacy Collection Statement—The Firepower 4100 does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

• About Firepower Threat Defense with FMC, on page 2
• Before You Start, on page 2
• End-to-End Procedure, on page 2
• Firepower Chassis Manager: Add a Firepower Threat Defense Logical Device, on page 4
• Log Into the Firepower Management Center, on page 8
• Obtain Licenses for the Firepower Management Center, on page 9
• Register the Firepower Threat Defense with the Firepower Management Center, on page 11
• Configure a Basic Security Policy, on page 13
• Access the Firepower Threat Defense CLI, on page 23
• What’s Next?, on page 25
• History for FTD with FMC, on page 25
About Firepower Threat Defense with FMC

The FTD provides next-generation firewall services, including stateful firewalling, routing, VPN, Next-Generation Intrusion Prevention System (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP).

You can manage the FTD using the Firepower Management Center (FMC), a full-featured, multidevice manager on a separate server.

The FTD registers and communicates with the FMC on the Management interface that you allocated to the FTD logical device.

For troubleshooting purposes, you can access the FTD CLI using SSH on the Management interface, or you can connect to the FTD from the FXOS CLI.

Before You Start

Deploy and perform initial configuration of the FMC. See the FMC getting started guide.

Note

The Firepower device and the FMC both have the same default management IP address: 192.168.45.45. This guide assumes that you will set different IP addresses for your devices during initial setup.

End-to-End Procedure

See the following tasks to deploy and configure the FTD on your chassis.
<table>
<thead>
<tr>
<th>Workspace</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower Chassis Manager</td>
<td>Firepower Chassis Manager: Add a Firepower Threat Defense Logical Device, on page 4.</td>
</tr>
<tr>
<td>FMC</td>
<td>Log Into the Firepower Management Center, on page 8.</td>
</tr>
<tr>
<td>Cisco Commerce Workspace</td>
<td>Obtain Licenses for the Firepower Management Center, on page 9: Buy feature licenses.</td>
</tr>
<tr>
<td>Smart Software Manager</td>
<td>Obtain Licenses for the Firepower Management Center, on page 9: Generate a license token for the FMC.</td>
</tr>
<tr>
<td>FMC</td>
<td>Obtain Licenses for the Firepower Management Center, on page 9: Register the FMC with the Smart Licensing server.</td>
</tr>
<tr>
<td>FMC</td>
<td>Register the Firepower Threat Defense with the Firepower Management Center, on page 11.</td>
</tr>
<tr>
<td>FMC</td>
<td>Configure a Basic Security Policy, on page 13.</td>
</tr>
</tbody>
</table>
Firepower Chassis Manager: Add a Firepower Threat Defense Logical Device

You can deploy an FTD from the Firepower 4100 as either a native or container instance. You can deploy multiple container instances per security engine, but only one native instance. See Logical Device Application Instances: Container or Native for the maximum container instances per model.

To add a High Availability pair or a cluster, see the FMC configuration guide.

This procedure lets you configure the logical device characteristics, including the bootstrap configuration used by the application.

Before you begin

- Configure a Management interface to use with the FTD; see Configure Interfaces. The Management interface is required. Note that this Management interface is not the same as the chassis management port that is used only for chassis management (and that appears at the top of the Interfaces tab as MGMT).
- You must also configure at least one Data interface.
- For container instances, if you do not want to use the default profile, which uses the minimum resources, add a resource profile on Platform Settings > Resource Profiles.
- For container instances, before you can install a container instance for the first time, you may need to reinitialize the security engine so that the disk has the correct formatting. If this action is required, you will not be able to save your logical device. Click Security Engine, and then click the Reinitialize icon (ゴ).
- Gather the following information:
  - Interface IDs for this device
  - Management interface IP address and network mask
  - Gateway IP address
  - FMC IP address and/or NAT ID of your choosing
  - DNS server IP address

Procedure

**Step 1**
In Firepower Chassis Manager, choose Logical Devices.

**Step 2**
Click Add > Standalone, and set the following parameters:
a) Provide a **Device Name**.
   This name is used by the chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the application configuration.

b) For the **Template**, choose **Cisco Firepower Threat Defense**.

c) Choose the **Image Version**.

d) Choose the **Instance Type**: Container or Native.
   A native instance uses all of the resources (CPU, RAM, and disk space) of the security module/engine, so you can only install one native instance. A container instance uses a subset of resources of the security module/engine, so you can install multiple container instances.

e) Click **OK**.
   You see the Provisioning - device name window.

**Step 3**  
Expand the **Data Ports** area, and click each interface that you want to assign to the device.

You can only assign Data and Data-sharing interfaces that you previously enabled on the **Interfaces** page. You will later enable and configure these interfaces in FMC, including setting the IP addresses.
You can only assign up to 10 Data-sharing interfaces to a container instance. Also, each Data-sharing interface can be assigned to at most 14 container instances. A Data-sharing interface is indicated by the sharing icon (🔗).

Hardware Bypass–capable ports are shown with the following icon: ⚪️. For certain interface modules, you can enable the Hardware Bypass feature for Inline Set interfaces only (see the FMC configuration guide for information about Inline Sets). Hardware Bypass ensures that traffic continues to flow between an inline interface pair during a power outage. This feature can be used to maintain network connectivity in the case of software or hardware failures. If you do not assign both interfaces in a Hardware Bypass pair, you see a warning message to make sure your assignment is intentional. You do not need to use the Hardware Bypass feature, so you can assign single interfaces if you prefer.

**Step 4**

Click the device icon in the center of the screen.

A dialog box appears where you can configure initial bootstrap settings. These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

**Step 5**

On the **General Information** page, complete the following:

<table>
<thead>
<tr>
<th>Cisco Firepower Threat Defense - Bootstrap Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Information</strong></td>
</tr>
<tr>
<td>SM 1 - 22 Cores Available</td>
</tr>
<tr>
<td>Resource Profile:</td>
</tr>
</tbody>
</table>

**Interface Information**

| Management Interface: | Ethernet1/8 |
| Address Type: | IPv4 only |
| IPv4 Management IP: | 10.63.58.239 |
| Network Mask: | 255.255.252.0 |
| Network Gateway: | 10.63.56.1 |

a) For a container instance, specify the **Resource Profile**.

If you later assign a different resource profile, then the instance will reload, which can take approximately 5 minutes. Note that for established High Availability pairs or clusters, if you assign a different-sized resource profile, be sure to make all members the same size as soon as possible.

b) Choose the **Management Interface**.

This interface is used to manage the logical device. This interface is separate from the chassis management port.

c) Choose the management interface **Address Type**: IPv4 only, IPv6 only, or IPv4 and IPv6.

d) Configure the **Management IP** address.
Set a unique IP address for this interface.

e) Enter a **Network Mask** or **Prefix Length**.
f) Enter a **Network Gateway** address.

**Step 6**  
On the **Settings** tab, complete the following:

### Cisco Firepower Threat Defense - Bootstrap Configuration

<table>
<thead>
<tr>
<th>General Information</th>
<th>Settings</th>
<th>Agreement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management type of application instance:</td>
<td>FMC</td>
<td></td>
</tr>
<tr>
<td>Firepower Management Center IP:</td>
<td>10.99.5.55</td>
<td></td>
</tr>
<tr>
<td>Search domains:</td>
<td>cisco.com</td>
<td></td>
</tr>
<tr>
<td>Firewall Modes:</td>
<td>Routed</td>
<td></td>
</tr>
<tr>
<td>DNS Servers:</td>
<td>10.99.5.67</td>
<td></td>
</tr>
<tr>
<td>Firepower Management Center NAT ID:</td>
<td>test</td>
<td></td>
</tr>
<tr>
<td>Fully Qualified Hostname:</td>
<td>ftd2.cisco.com</td>
<td></td>
</tr>
<tr>
<td>Registration Key:</td>
<td>****</td>
<td></td>
</tr>
<tr>
<td>Confirm Registration Key:</td>
<td>****</td>
<td></td>
</tr>
<tr>
<td>Password:</td>
<td>********</td>
<td></td>
</tr>
<tr>
<td>Confirm Password:</td>
<td>********</td>
<td></td>
</tr>
<tr>
<td>Egressing Interface:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

a) For a native instance, in the **Management type of application instance** drop-down list, choose **FMC**. Native instances also support FDM as a manager. After you deploy the logical device, you cannot change the manager type.

b) Enter the **Firepower Management Center IP** of the managing FMC. If you do not know the FMC IP address, leave this field blank and enter a passphrase in the **Firepower Management Center NAT ID** field.

c) For a container instance, **Permit Expert mode from FTD SSH sessions**: **Yes** or **No**. Expert Mode provides FTD shell access for advanced troubleshooting.

   If you choose **Yes** for this option, then users who access the container instance directly from an SSH session can enter Expert Mode. If you choose **No**, then only users who access the container instance from the FXOS CLI can enter Expert Mode. We recommend choosing **No** to increase isolation between instances.

   Use Expert Mode only if a documented procedure tells you it is required, or if the Cisco Technical Assistance Center asks you to use it. To enter this mode, use the **expert** command in the FTD CLI.

d) Enter the **Search Domains** as a comma-separated list.

e) Choose the **Firewall Mode**: **Transparent** or **Routed**.

   In routed mode, the FTD is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.
The firewall mode is only set at initial deployment. If you re-apply the bootstrap settings, this setting is not used.

f) Enter the **DNS Servers** as a comma-separated list.

The FTD uses DNS if you specify a hostname for the FMC, for example.

g) Enter the **Fully Qualified Hostname** for the FTD.

h) Enter a **Registration Key** to be shared between the FMC and the device during registration.

You can choose any text string for this key between 1 and 37 characters; you will enter the same key on the FMC when you add the FTD.

i) Enter a **Password** for the FTD admin user for CLI access.

j) Choose the **Eventing Interface** on which Firepower events should be sent. If not specified, the management interface will be used.

This interface must be defined as a Firepower-eventing interface.

k) For a container instance, set the **Hardware Crypto** as **Enabled** or **Disabled**.

This setting enables TLS crypto acceleration in hardware, and improves performance for certain types of traffic. For more information, see the FMC configuration guide. This feature is not supported for native instances. To view the percentage of hardware crypto resources allocated to this instance, enter the **show hw-crypto** command.

---

### Step 7

On the **Agreement** tab, read and accept the end user license agreement (EULA).

### Step 8

Click **OK** to close the configuration dialog box.

### Step 9

Click **Save**.

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for the status of the new logical device. When the logical device shows its **Status** as **online**, you can start configuring the security policy in the application.

---

**Log Into the Firepower Management Center**

Use the FMC to configure and monitor the FTD.
Before you begin

For information on supported browsers, refer to the release notes for the version you are using (see https://www.cisco.com/go/firepower-notes).

Procedure

| Step 1 | Using a supported browser, enter the following URL. |
|        | **https://fmc_ip_address** |
| Step 2 | Enter your username and password. |
| Step 3 | Click **Log In**. |

Obtain Licenses for the Firepower Management Center

All licenses are supplied to the FTD by the FMC. You can optionally purchase the following feature licenses:

- **Threat**—Security Intelligence and Cisco Firepower Next-Generation IPS
- **Malware**—Advanced Malware Protection for Networks (AMP)
- **URL**—URL Filtering
- **RA VPN**—AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only.

In addition to the above licenses, you also need to buy a matching subscription to access updates for 1, 3, or 5 years.

Before you begin

- Have a master account on the Cisco Smart Software Manager.

  If you do not yet have an account, click the link to set up a new account. The Smart Software Manager lets you create a master account for your organization.

- Your Cisco Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

Procedure

Step 1

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

When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. However, if you need to add licenses yourself, use the Find Products and Solutions search field on the Cisco Commerce Workspace. Search for the following license PID:s:
Figure 1: License Search

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

- Threat, Malware, and URL license combination:
  - L-FPR4110T-TMC=
  - L-FPR4120T-TMC=
  - L-FPR4140T-TMC=
  - L-FPR4150T-TMC=

- Threat, Malware, and URL subscription combination:
  - L-FPR4110T-TMC-1Y
  - L-FPR4110T-TMC-3Y
  - L-FPR4110T-TMC-5Y
  - L-FPR4120T-TMC-1Y
  - L-FPR4120T-TMC-3Y
  - L-FPR4120T-TMC-5Y
  - L-FPR4140T-TMC-1Y
  - L-FPR4140T-TMC-3Y
  - L-FPR4140T-TMC-5Y
  - L-FPR4150T-TMC-1Y
  - L-FPR4150T-TMC-3Y
  - L-FPR4150T-TMC-5Y

- RA VPN—See the Cisco AnyConnect Ordering Guide.

Step 2 If you have not already done so, register the FMC with the Smart Licensing server.

Registering requires you to generate a registration token in the Smart Software Manager. See the FMC configuration guide for detailed instructions.
Register the Firepower Threat Defense with the Firepower Management Center

Register each logical device individually to the same FMC.

**Before you begin**

- Make sure the FTD logical device **Status** is **online** on the Firepower Chassis Manager **Logical Devices** page.
- Gather the following information that you set in the FTD initial bootstrap configuration (see Firepower Chassis Manager: Add a Firepower Threat Defense Logical Device, on page 4):
  - FTD management IP address and/or NAT ID
  - FMC registration key

**Procedure**

**Step 1**
In FMC, choose **Devices > Device Management**.

**Step 2**
From the **Add** drop-down list, choose **Add Device**, and enter the following parameters.

**Add Device**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host</strong></td>
<td>192.168.101.10</td>
</tr>
<tr>
<td><strong>Display Name</strong></td>
<td>192.168.101.10</td>
</tr>
<tr>
<td><strong>Registration Key</strong></td>
<td>1e2b3c4d5e</td>
</tr>
<tr>
<td><strong>Group</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Access Control Policy</strong></td>
<td>initial.ac</td>
</tr>
<tr>
<td><strong>Smart Licensing</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Malware</strong></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Threat</strong></td>
<td>✓</td>
</tr>
<tr>
<td><strong>URL Filtering</strong></td>
<td>✓</td>
</tr>
</tbody>
</table>

**Advanced**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unique NAT ID</strong></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Transfer Packets</strong></td>
<td>✓</td>
</tr>
</tbody>
</table>

- **Host**—Enter the IP address of the FTD you want to add. You can leave this field blank if you specified both the FMC IP address and a NAT ID in the FTD initial bootstrap configuration.
Register the Firepower Threat Defense with the Firepower Management Center

- **Display Name**—Enter the name for the FTD as you want it to display in the FMC.
- **Registration Key**—Enter the same registration key that you specified in the FTD initial bootstrap configuration.
- **Domain**—Assign the device to a leaf domain if you have a multidomain environment.
- **Group**—Assign it to a device group if you are using groups.
- **Access Control Policy**—Choose an initial policy. Unless you already have a customized policy you know you need to use, choose **Create new policy**, and choose **Block all traffic**. You can change this later to allow traffic; see **Allow Traffic from Inside to Outside**, on page 21.

![New Policy](image)

- **Smart Licensing**—Assign the Smart Licenses you need for the features you want to deploy: **Malware** (if you intend to use AMP malware inspection), **Threat** (if you intend to use intrusion prevention), and **URL** (if you intend to implement category-based URL filtering).
- **Unique NAT ID**—Specify the NAT ID you specified in the FTD initial bootstrap configuration.
- **Transfer Packets**—Allow the device to transfer packets to the FMC. When events like IPS or Snort are triggered with this option enabled, the device sends event metadata information and packet data to the FMC for inspection. If you disable it, only event information will be sent to the FMC, but packet data is not sent.

**Step 3**

Click **Register**, and confirm a successful registration.

If the registration succeeds, the device is added to the list. If it fails, you will see an error message. If the FTD fails to register, check the following items:

- **Ping**—Access the FTD CLI (Access the Firepower Threat Defense CLI, on page 23), and ping the FMC IP address using the following command:
  
  `ping system ip_address`

  If the ping is not successful, check your network settings using the `show network` command. If you need to change the FTD IP address, use the `configure network {ipv4 | ipv6} manual` command.

- **NTP**—Make sure the Firepower 4100 NTP server matches the FMC server set on the **System > Configuration > Time Synchronization** page.

- **Registration key, NAT ID, and FMC IP address**—Make sure you are using the same registration key, and if used, NAT ID, on both devices. You can set the registration key and NAT ID on the FTD using the `configure manager add` command. This command also lets you change the FMC IP address.
Configure a Basic Security Policy

This section describes how to 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.

To configure a basic security policy, complete the following tasks.

1. Configure Interfaces, on page 13.
2. Configure the DHCP Server, on page 16.
3. Add the Default Route, on page 17.
4. Configure NAT, on page 18.
5. Allow Traffic from Inside to Outside, on page 21.
6. Deploy the Configuration, on page 22.

Configure Interfaces

Enable FTD interfaces, assign them to security zones, and set the IP addresses. Typically, you must configure at least a minimum of two interfaces to have a system that passes meaningful traffic. Normally, you would have an outside interface that faces the upstream router or internet, and one or more inside interfaces for your organization’s networks. Some of these interfaces might be “demilitarized zones” (DMZs), where you place publically-accessible assets such as your web server.

A typical edge-routing situation is to obtain the outside interface address through DHCP from your ISP, while you define static addresses on the inside interfaces.

The following example configures a routed mode inside interface with a static address and a routed mode outside interface using DHCP.

**Procedure**

**Step 1** Choose Devices > Device Management, and click the edit icon (✏️) for the device.
Step 2
Click **Interfaces**.

Step 3
Click the edit icon (📝) for the interface that you want to use for *inside*. The **General** tab appears.

a) Enter a **Name** up to 48 characters in length. For example, name the interface *inside*.

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

c) Leave the **Mode** set to **None**.

d) 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*. Each interface must be assigned to a security zone and/or interface group. An interface can belong to only one security zone, but can also belong to multiple interface groups. You apply your security policy based on zones or groups. For example, you can assign the inside interface to the inside zone; and the outside interface to the outside zone. Then you can configure your access control policy to enable traffic to go from inside to outside, but not from outside to inside. Most
policies only support security zones; you can use zones or interface groups in NAT policies, prefilter policies, and QoS policies.

e) 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 **192.168.1.1/24**

- **IPv6**—Check the **Autoconfiguration** check box for stateless autoconfiguration.

f) Click **OK**.

**Step 4**

Click the edit icon (🔗) for the interface that you want to use for **outside**.

The **General** tab appears.

a) Enter a **Name** up to 48 characters in length.

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

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

c) Leave the **Mode** set to **None**.
d) 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.

e) Click the IPv4 and/or IPv6 tab.

- **IPv4**—Choose Use DHCP, and configure the following optional parameters:
  - **Obtain default route using DHCP**—Obtains the default route from the DHCP server.
  - **DHCP route metric**—Assigns an administrative distance to the learned route, between 1 and 255. The default administrative distance for the learned routes is 1.

- **IPv6**—Check the Autoconfiguration check box for stateless autoconfiguration.

f) Click OK.

**Step 5** Click Save.

---

**Configure the DHCP Server**

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

**Procedure**

**Step 1** Choose Devices > Device Management, and click the edit icon ( dõi for the device.

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

**Step 3** On the Server page, click Add, and configure the following options:

- **Interface**—Choose the interface from the drop-down list.
• **Address Pool**—Set the range of IP addresses from lowest to highest that are used by the DHCP server. The range of 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 4**  
Click OK.

**Step 5**  
Click Save.

---

## Add the Default Route

The default route normally points to the upstream router reachable from the outside interface. If you use DHCP for the outside interface, your device might have already received a default route. If you need to manually add the route, complete this procedure. If you received a default route from the DHCP server, it will show in the IPv4 Routes or IPv6 Routes table on the Devices > Device Management > Routing > Static Route page.

**Procedure**

**Step 1**  
Choose Devices > Device Management, and click the edit icon (✍️) for the device.

**Step 2**  
Choose Routing > Static Route, click Add Route, and set the following:

![Add Static Route Configuration](image)

- **Type**—Click the IPv4 or IPv6 radio button depending on the type of static route that you are adding.
- **Interface**—Choose the egress interface; typically the outside interface.
Configure NAT

- **Available Network**—Choose any-ipv4 for an IPv4 default route, or any-ipv6 for an IPv6 default route and click Add to move it to the Selected Network list.

- **Gateway** or **IPv6 Gateway**—Enter or choose the gateway router that is the next hop for this route. You can provide an IP address or a Networks/Hosts object.

- **Metric**—Enter the number of hops to the destination network. Valid values range from 1 to 255; the default value is 1.

**Step 3**

Click OK.

The route is added to the static route table.

**Step 4**

Click Save.

---

**Configure NAT**

A typical NAT rule converts 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 > Threat Defense NAT.

**Step 2**

Name the policy, select the device(s) that you want to use the policy, and click Save.
The policy is added the FMC. You still have to add rules to the policy.

**Step 3**  
Click **Add Rule**.

The **Add NAT Rule** dialog box appears.

**Step 4**  
Configure the basic rule options:

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

- **Original Source**—Click the add icon (◉) to add a network object for all IPv4 traffic (0.0.0.0/0).

  ![Network Object](image)

  **New Network Object**

  - Name: all-ipv4
  - Network: 0.0.0.0/0

  **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.

## Allow Traffic from Inside to Outside

If you created a basic **Block all traffic** access control policy when you registered the FTD with the FMC, then you need to add rules to the policy to allow traffic through the device. The following procedure adds a rule to allow traffic from the inside zone to the outside zone. If you have other zones, be sure to add rules allowing traffic to the appropriate networks.

See the **FMC configuration guide** to configure more advanced security settings and rules.

### Procedure

**Step 1**  
Choose **Policy > Access Policy > Access Policy**, and click the edit icon (_Edit_ ) for the access control policy assigned to the FTD.

**Step 2**  
Click **Add Rule**, and set the following parameters:

- **Name**—Name this rule, for example, **inside_to_outside**.

- **Source Zones**—Select the inside zone from **Available Zones**, and click **Add to Source**.

- **Destination Zones**—Select the outside zone from **Available Zones**, and click **Add to Destination**.
Leave the other settings as is.

**Step 3**
Click **Add**.

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

**Step 4**
Click **Save**.

---

**Deploy the Configuration**

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

**Procedure**

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

**Step 2**
Select the device in the **Deploy Policies** dialog box, then click **Deploy**.

**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.
Access the Firepower Threat Defense CLI

You can use the FTD CLI to change management interface parameters and for troubleshooting purposes. You can access the CLI using SSH to the Management interface, or by connecting from the FXOS CLI.

**Procedure**

**Step 1**  
(Option 1) SSH directly to the FTD management interface IP address.

You set the management IP address when you deployed the logical device. Log into the FTD with the admin account and the password you set during initial deployment.

If you forgot the password, you can change it by editing the logical device in the Firepower Chassis Manager.

**Step 2**  
(Option 2) From the FXOS CLI, connect to the module CLI using a console connection or a Telnet connection.

a) Connect to the security engine.

```
connect module 1 {console | telnet}
```

The benefits of using a Telnet connection is that you can have multiple sessions to the module at the same time, and the connection speed is faster.

**Example:**

```
Firepower# connect module 1 console
Telnet escape character is '^-'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '^-'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connect to the FTD console.

```
connect ftd name
```
If you have multiple application instances, you must specify the name of the instance. To view the instance names, enter the command without a name.

**Example:**

Firepower-module1> connect ftd FTD_Instance1

```
---------------------------------------------------------- ATTENTION ----------------------------------------------------------
You are connecting to ftd from a serial console. Please avoid executing any commands which may produce large amount of output. Otherwise, data cached along the pipe may take up to 12 minutes to be drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use 'connect module <slot> telnet' to connect to the security module.

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI>
```

**c)** Exit the application console to the FXOS module CLI by entering **exit**.

**Note** For pre-6.3 versions, enter **Ctrl-a, d**.

**d)** Return to the supervisor level of the FXOS CLI.

**To exit the console:**

1. Enter ~
   You exit to the Telnet application.

2. To exit the Telnet application, enter:
   `telnet>quit`

**To exit the Telnet session:**

Enter **Ctrl-[,**.

---

**Example**

The following example connects to an FTD and then exits back to the supervisor level of the FXOS CLI.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1> connect ftd FTD_Instance1
```

```
---------------------------------------------------------- ATTENTION ----------------------------------------------------------
```
You are connecting to ftd from a serial console. Please avoid executing any commands which may produce large amount of output. Otherwise, data cached along the pipe may take up to 12 minutes to be drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use 'connect module <slot> telnet' to connect to the security module.
======================================================================
Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
> ~
telnet> quit
Connection closed.
Firepower#

What's Next?

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

For information related to using FMC, see the Firepower Management Center Configuration Guide.

History for FTD with FMC

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Version</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for ASA and FTD on separate modules of the same Firepower 9300</td>
<td>6.4</td>
<td>You can now deploy ASA and FTD logical devices on the same Firepower 9300. Requires FXOS 2.6.1.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Version</td>
<td>Feature Information</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Multi-instance capability for Firepower Threat Defense on the Firepower 4100/9300 | 6.3.0   | You can now deploy multiple logical devices, each with a Firepower Threat Defense container instance, on a single security engine/module. Formerly, you could only deploy a single native application instance.  
To provide flexible physical interface use, you can create VLAN subinterfaces in FXOS and also share interfaces between multiple instances. Resource management lets you customize performance capabilities for each instance.  
You can use High Availability using a container instance on 2 separate chassis. Clustering is not supported.  
**Note** Multi-instance capability is similar to ASA multiple context mode, although the implementation is different. Multiple context mode is not available on the Firepower Threat Defense.  
New/Modified Firepower Management Center screens:  
• Devices > Device Management > Edit icon > Interfaces tab  
New/Modified Firepower Chassis Manager screens:  
• Overview > Devices  
• Interfaces > All Interfaces > Add New drop-down menu > Subinterface  
• Interfaces > All Interfaces > Type  
• Logical Devices > Add Device  
• Platform Settings > Mac Pool  
• Platform Settings > Resource Profiles |