Threat Defense Deployment with the Management Center

Is This Chapter for You?

This chapter explains how to complete the initial configuration of your threat defense and how to register the device to a management center. 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 management center, 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 management center, you can use the integrated device manager. Use the device manager web-based device setup wizard to configure the basic features of the software that are most commonly used for small network deployments.

The Cisco ISA 3000 can run either the threat defense software or ASA software. Switching between threat defense and ASA requires you to reimage the device. See Reimage the Cisco ASA or Firepower Threat Defense Device.

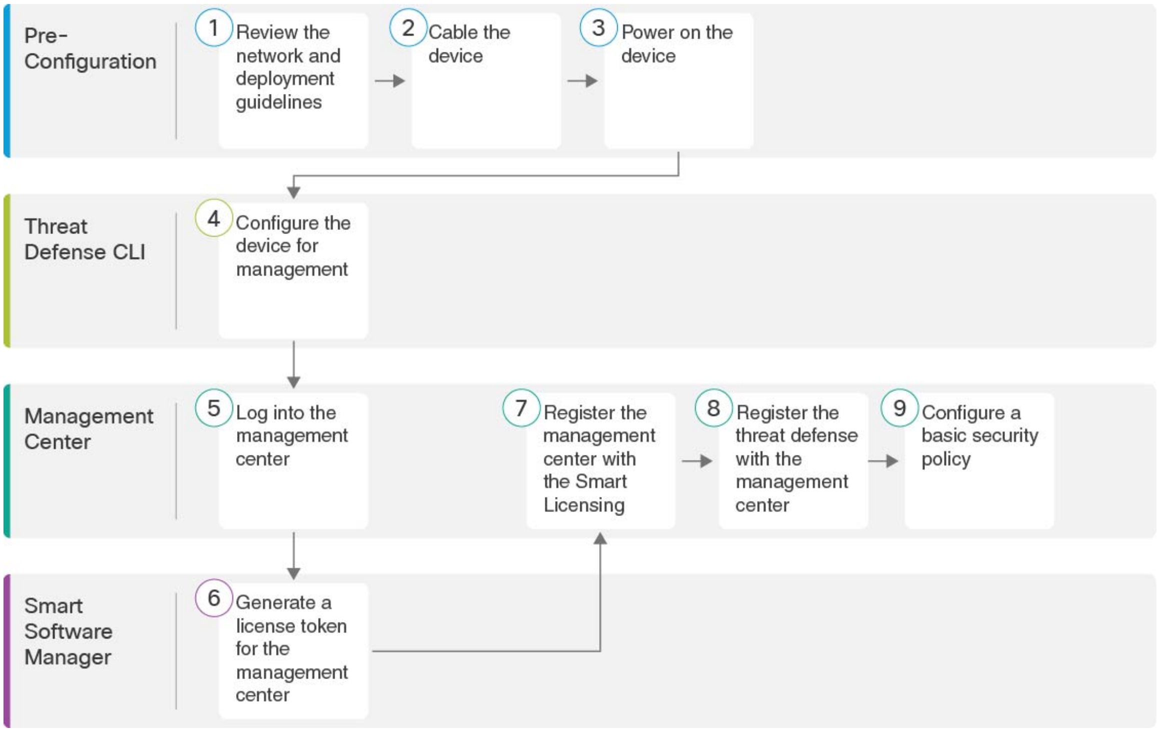
Privacy Collection Statement—The ISA 3000 does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

Before You Start

Deploy and perform initial configuration of the management center. See the Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guide or Cisco Secure Firewall Management Center Virtual Getting Started Guide.

End-to-End Procedure

See the following tasks to deploy the threat defense with management center on your chassis.


Pre-Configuration
1 Review the network and deployment guidelines
2 Cable the device
3 Power on the device
Threat Defense CLI
4 Configure the device for management
Management Center
5 Log into the management center
7 Register the management center with the Smart Licensing
8 Register the threat defense with the management center
9 Configure a basic security policy
Smart Software Manager
6 Generate a license token for the management center

1	Pre-Configuration	Review the Network Deployment, on page 3.
2	Pre-Configuration	Cable the Device, on page 7.
3	Pre-Configuration	Power on the Device, on page 11.
4	Threat Defense CLI	Complete the Threat Defense Initial Configuration Using the CLI, on page 12.
5	Management Center	Log Into the Management Center, on page 17.

6	Smart Software Manager	Obtain Licenses for the Management Center, on page 18: Generate a license token for the management center.
7	Management Center	Obtain Licenses for the Management Center, on page 18: Register the management center with the Smart Licensing server.
8	Management Center	Register the Threat Defense with the Management Center, on page 19.
9	Management Center	Configure a Basic Security Policy, on page 22.

Review the Network Deployment

You can manage the threat defense using management center from the Management 1/1 interface, or in 6.7 and later, a data interface. By default, the Management 1/1 interface is enabled and configured with an IP address (192.168.45.45). This interface also runs a DHCP server initially; after you select the management center as the manager during initial setup, the DHCP server is disabled. You can configure the Management interface and an management center access data interface during initial setup at the console port. You can configure other data interfaces after you connect the threat defense to the management center.

Note Management Center access from a data interface has the following limitations:

- You can only enable manager access on one physical, data interface. You cannot use a subinterface or EtherChannel.
- This interface cannot be management-only.
- Routed firewall mode only, using a routed interface.
- PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the threat defense and the WAN modem.
- The interface must be in the global VRF only.
- You cannot use separate management and event-only interfaces.
- SSH is not enabled by default for data interfaces, so you will have to enable SSH later using the management center. Because the Management interface gateway will be changed to be the data interfaces, you also cannot SSH to the Management interface from a remote network unless you add a static route for the Management interface using the **configure network static-routes** command.

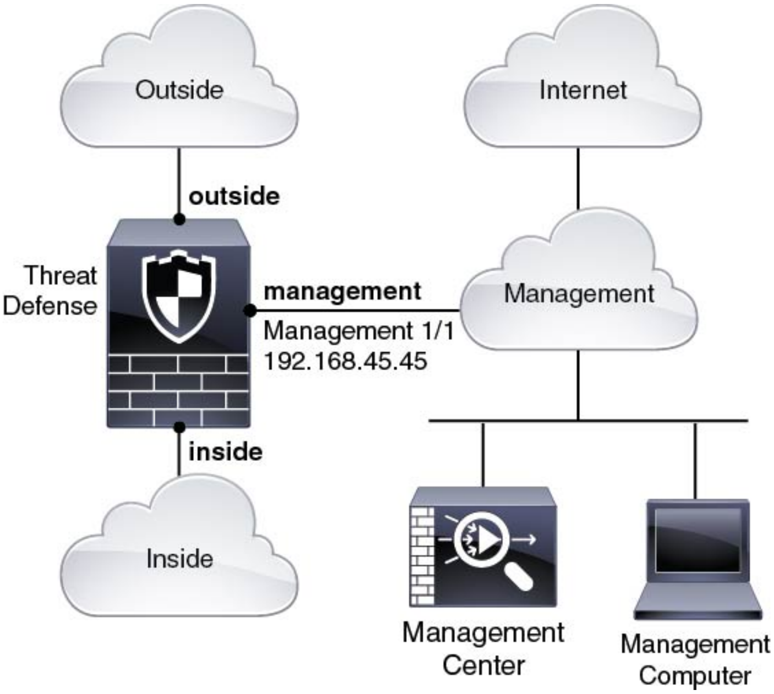
See the following sample network deployments for ideas on how to place your threat defense device in your network.

Separate Management Network

Both the management center and the threat defense require internet access from management for licensing and updates.

The following figure shows a possible network deployment for the ISA 3000 where the management center and management computer connect to the management network. The management network has a path to the internet for licensing and updates.

Figure 1: Separate Management Network



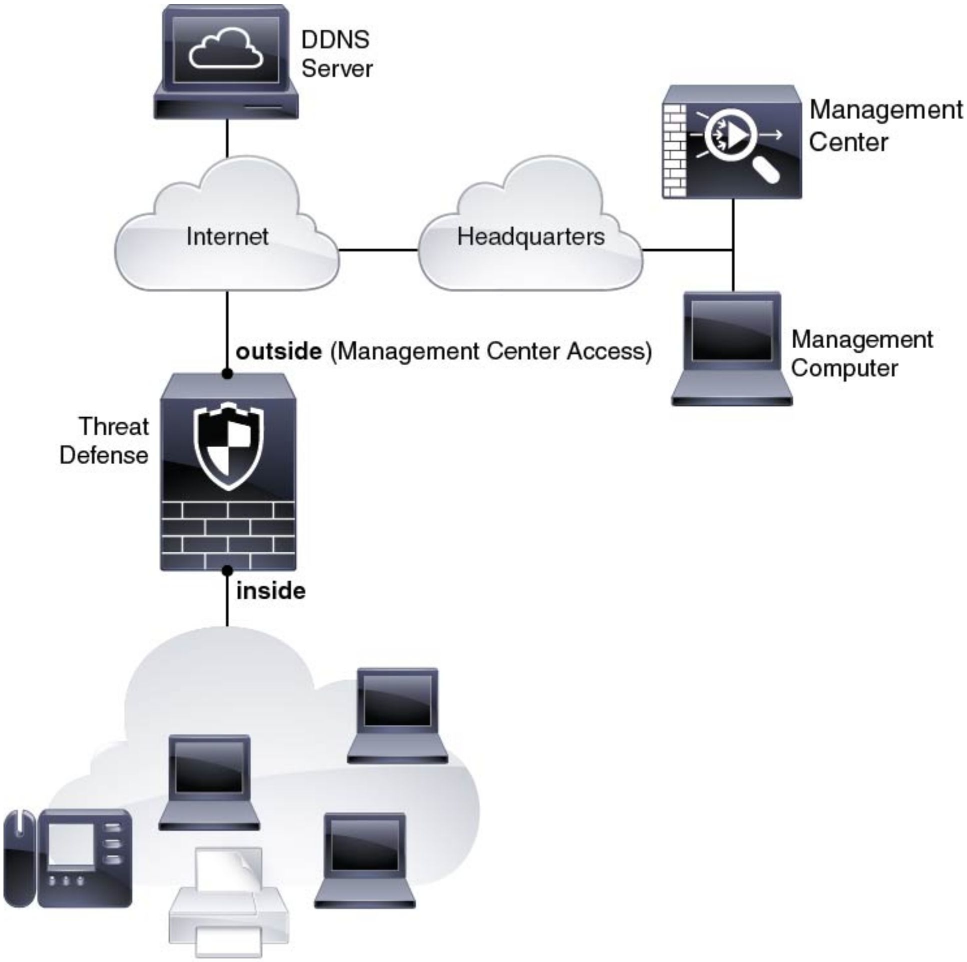
6.7 and Later Remote Management Deployment

Note For a remote branch setup, we recommend that you use the standalone document specific to that deployment.

The following figure shows the recommended network deployment for the ISA 3000 using the outside interface for management. This scenario is ideal for managing branch offices from a central headquarters. You can perform initial setup of the threat defense at headquarters and then send a pre-configured device to a branch location.

Either the threat defense or management center needs a public IP address or hostname. If the threat defense receives a public IP address using DHCP, then you can optionally configure Dynamic DNS (DDNS) for the outside interface. DDNS ensures the management center can reach the threat defense at its Fully-Qualified Domain Name (FQDN) if the threat defense's IP address changes. If the threat defense receives a private IP address, then the management center needs to have a public IP address or hostname.

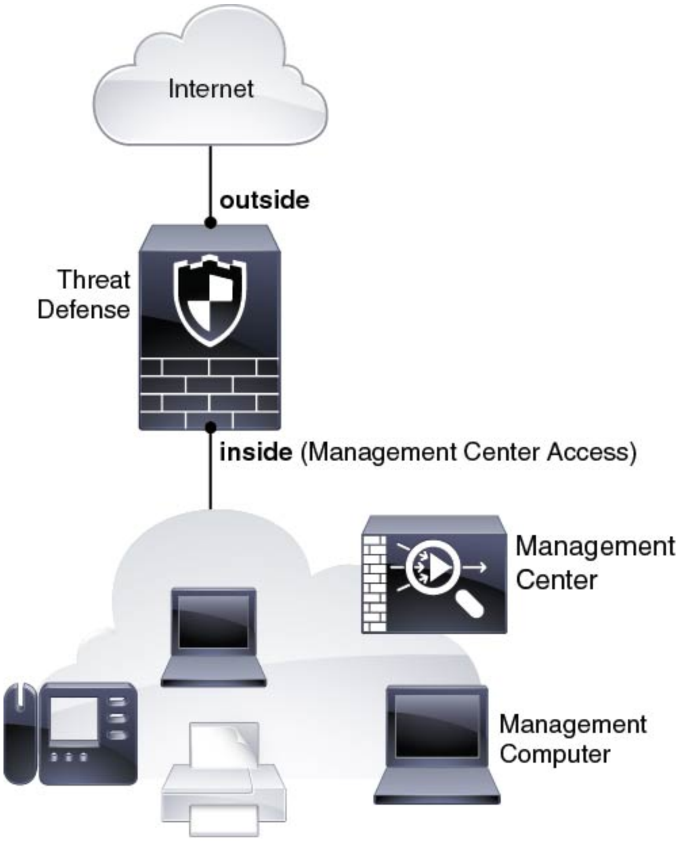
Figure 2: Remote Management Deployment



6.7 and Later Inside Management Deployment

The following figure shows the recommended network deployment for the ISA 3000 using the inside interface for management.

Figure 3: Inside Management Deployment



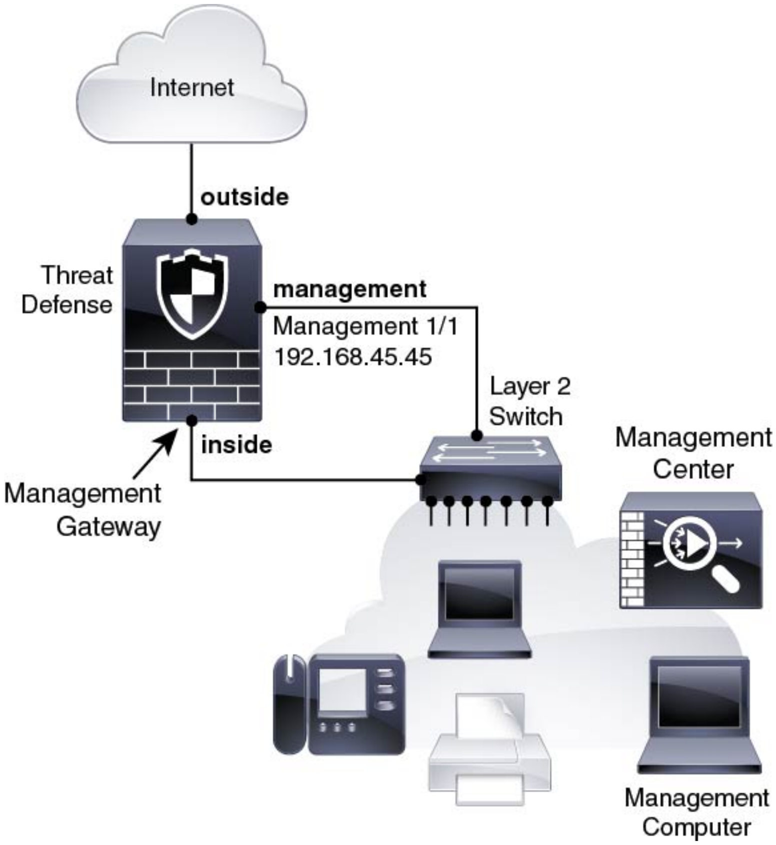
6.6 and Earlier Edge Network Deployment

The management center can only communicate with the threat defense on the management interface in 6.6 and earlier. Moreover, both the management center and threat defense require internet access from management for licensing and updates.

The following figure shows a possible network deployment for the ISA 3000 where the ISA 3000 acts as the internet gateway for the management center and threat defense management.You can also use this scenario in 6.7 and later for a High Availability deployment, for example.

In the following diagram, the ISA 3000 acts as the internet gateway for the management interface and the management center by connecting Management 1/1 to an inside interface through a Layer 2 switch, and by connecting the management center and management computer to the switch. (This direct connection is allowed because the management interface is separate from the other interfaces on the threat defense.)

Figure 4: Edge Network Deployment



Cable the Device

To cable one of the recommended scenarios on the ISA 3000, see the following steps.

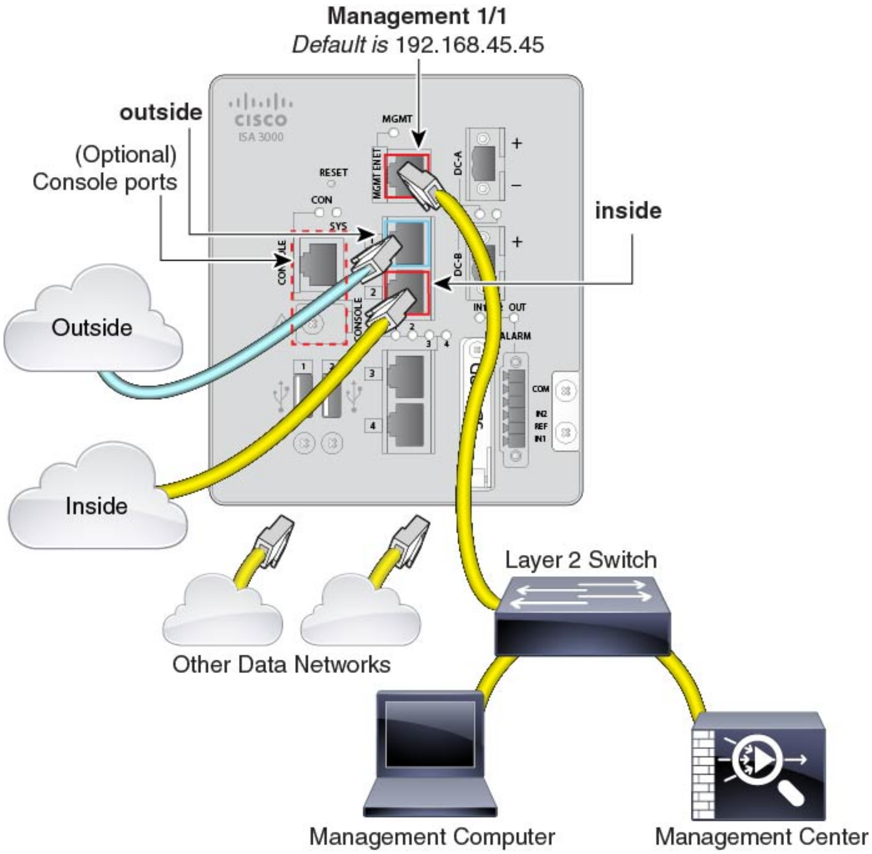
Note The ISA 3000 and the management center both have the same default management IP address: 192.168.45.45. This guide assumes that you will set different IP addresses for your devices during initial setup. Note that the management center on 6.5 and later defaults to a DHCP client for the management interface; however, if there is no DHCP server, it will default to 192.168.45.45.

Note Other topologies can be used, and your deployment will vary depending on your basic logical network connectivity, ports, addressing, and configuration requirements.

Procedure

Step 1 Cable for a separate management network.

Figure 5: Cabling a Separate Management Network



a) Cable the following to your management network:

- Management 1/1 interface
- Management Center
- Management computer

b) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup if you do not use SSH to the Management interface.

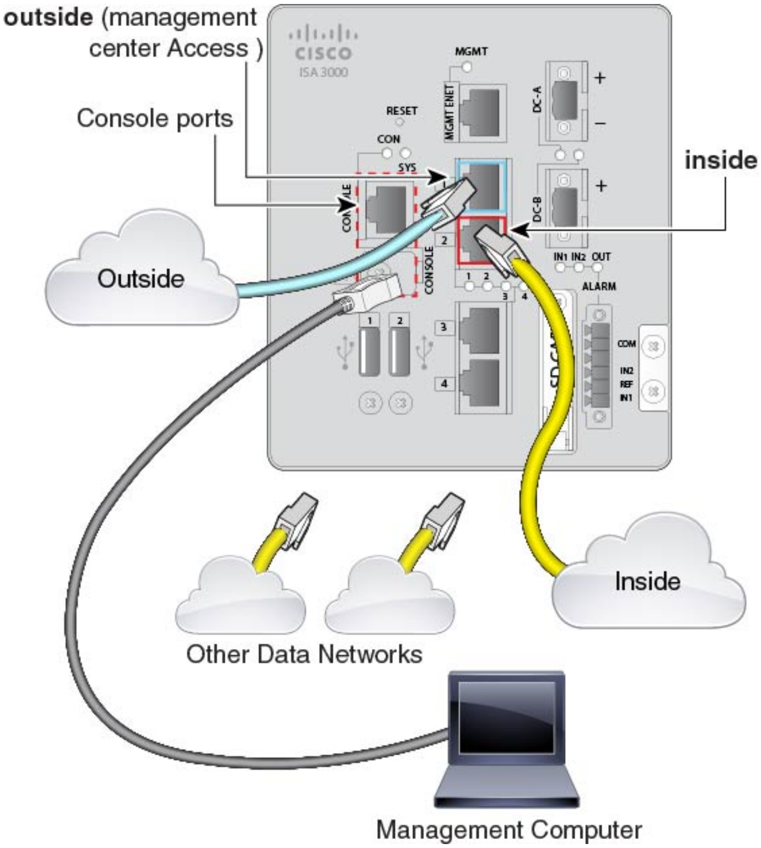
c) Connect the inside interface (for example, GigabitEthernet 1/2) to your inside router.

d) Connect the outside interface (for example, GigabitEthernet 1/1) to your outside router.

e) Connect other networks to the remaining interfaces.

Step 2 (6.7 and later) Cable for a remote management deployment:

Figure 6: Cabling a Remote Management Deployment



The management center and your management computer reside at a remote headquarters, and can reach the threat defense over the internet.

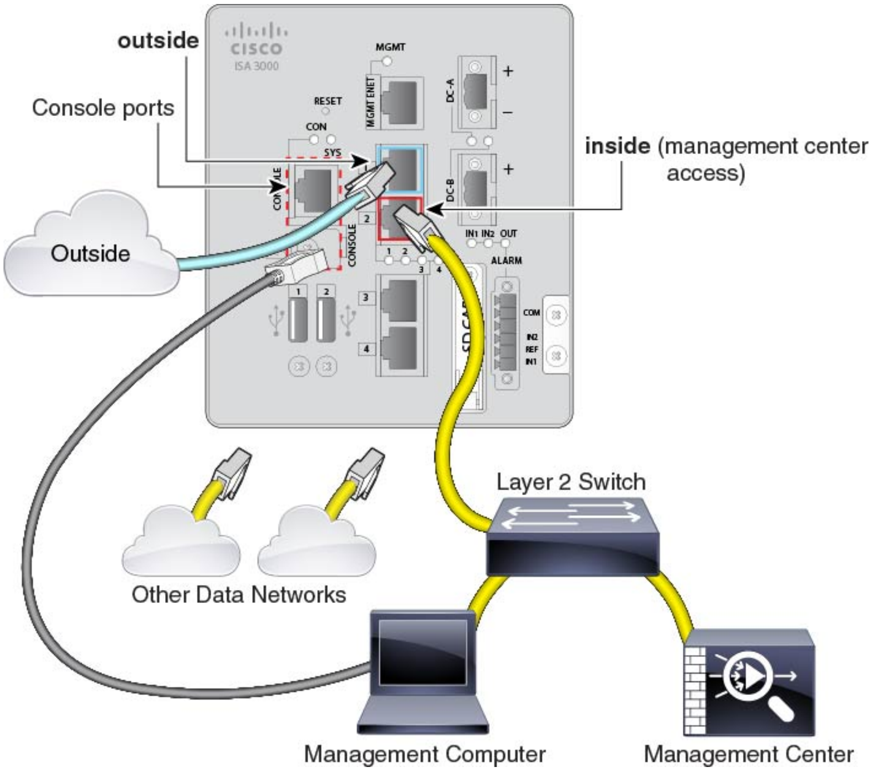
a) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup.

   You can perform initial CLI setup at headquarters, and then send the threat defense to the remote branch office. At the branch office, the console connection is not required for everyday use; it may be required for troubleshooting purposes.

b) Cable your inside network (for example, GigabitEthernet 1/2).
c) Connect the outside interface (for example, GigabitEthernet 1/1) to your outside router.
d) Connect other networks to the remaining interfaces.

Step 3 (6.7 and later) Cable for an inside management deployment:

Figure 7: Cabling an Inside Management Deployment



The management center and your management computer reside on the inside network with your other inside end points.

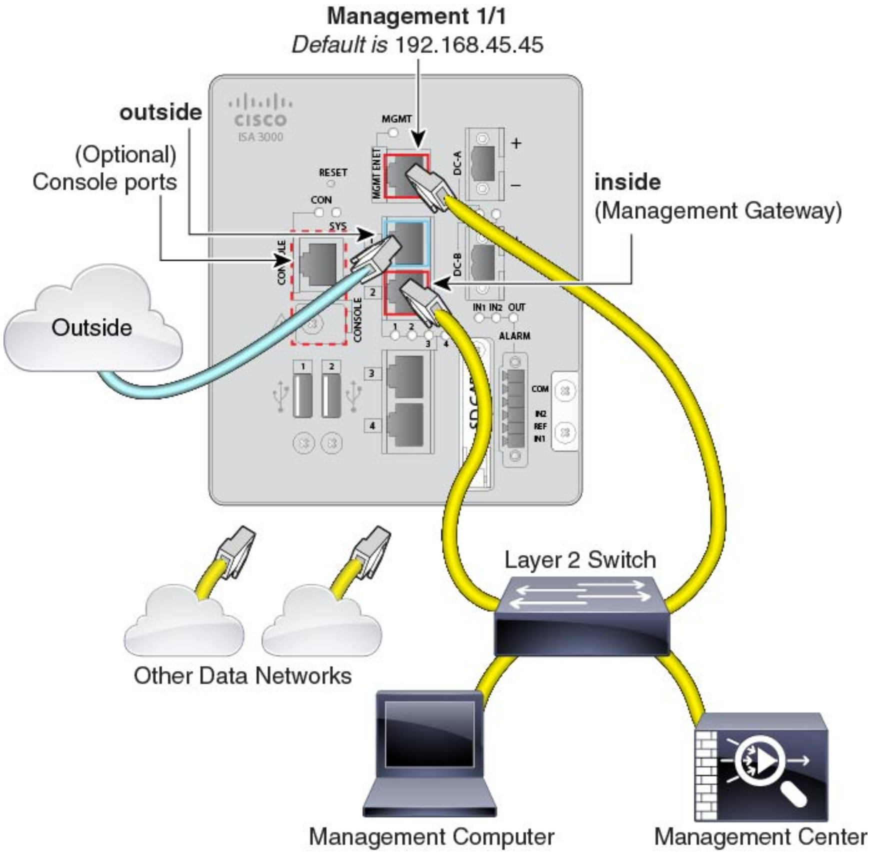
a) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup.
b) Cable the following to the inside network (for example, GigabitEthernet 1/2):

   - Management Center
   - Management computer

c) Connect the outside interface (for example, GigabitEthernet 1/1) to your outside router.
d) Connect other networks to the remaining interfaces.

Step 4 (6.6 and earlier) Cable for an edge deployment.

Figure 8: Cabling an Edge Deployment



a) Cable the following to a Layer 2 Ethernet switch:

   - Inside interface (for example, GigabitEthernet 1/2)
   - Management 1/1 interface
   - Management Center
   - Management computer

b) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup if you do not use SSH to the Management interface.

c) Connect the outside interface (for example, GigabitEthernet 1/1) to your outside router.

d) Connect other networks to the remaining interfaces.

Power on the Device

System power is controlled by DC power; there is no power button.

Before you begin

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

Procedure

Step 1 Attach the power plug to the ISA 3000 after wiring it to the DC power source.

Refer to “Connecting to DC Power” in the hardware installation guide for instructions on proper wiring of the power plug.

Step 2 Check the System LED on the front panel of the ISA 3000 device; if it is steady green, the device is powered on. If it is flashing green, the device is in Boot up phase and POST.

Refer to “Verifying Connections” in the hardware installation guide to verify that all devices are properly connected to the ISA 3000.

Complete the Threat Defense Initial Configuration Using the CLI

Connect to the threat defense CLI to perform initial setup, including setting the Management IP address, gateway, and other basic networking settings using the setup wizard. The dedicated Management interface is a special interface with its own network settings. In 6.7 and later: If you do not want to use the Management interface for the management center access, you can use the CLI to configure a data interface instead. You will also configure management center communication settings.

Procedure

Step 1 Connect to the threat defense CLI, either from the console port or using SSH to the Management interface, which obtains an IP address from a DHCP server by default. If you intend to change the network settings, we recommend using the console port so you do not get disconnected.

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

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

Step 3 The first time you log in to the threat defense, you are prompted to accept the End User License Agreement (EULA) and to change the admin password. You are then presented with the CLI setup script.

Note You cannot repeat the CLI setup wizard 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 the FTD command reference.

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

Note In 6.7 and later: The Management interface settings are used even when you enable the management center access on a data interface. For example, the management traffic that is routed over the backplane through the data interface will resolve FQDNs using the Management interface DNS servers, and not the data interface DNS servers.

See the following guidelines:

- **Configure IPv4 via DHCP or manually?**—In 6.7 and later: If you want to use a data interface for the management center access instead of the management interface, choose **manual**. Although you do not plan to use the Management interface, you must set an IP address, for example, a private address. You cannot configure a data interface for management if the management interface is set to DHCP, because the default route, which must be **data-interfaces** (see the next bullet), might be overwritten with one received from the DHCP server.

- **Enter the IPv4 default gateway for the management interface**—In 6.7 and later: If you want to use a data interface for the management center access instead of the management interface, set the gateway to be **data-interfaces**. This setting forwards management traffic over the backplane so it can be routed through the management center access data interface. If you want to use the Management interface for the management center access, you should set a gateway IP address on the Management 1/1 network.

- **If your networking information has changed, you will need to reconnect**—If you are connected with SSH but you change the IP address at initial setup, you will be disconnected. Reconnect with the new IP address and password. Console connections are not affected.

- **Manage the device locally?**—Enter **no** to use management center. A **yes** answer means you will use the device manager instead.

- **Configure firewall mode?**—We recommend that you set the firewall mode at initial configuration. Changing the firewall mode after initial setup erases your running configuration. Note that data interface management center access is only supported in routed firewall mode.

Example:

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

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

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

```
Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

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 4 Identify the management center that will manage this threat defense.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the management center. If the management center is not directly addressable, use **DONTRESOLVE** and also specify the *nat_id*. At least one of the devices, either the management center or the threat defense, must have a reachable IP address to establish the two-way, SSL-encrypted communication channel between the two devices. If you specify **DONTRESOLVE** in this command, then the threat defense must have a reachable IP address or hostname.
- *reg_key*—Specifies a one-time registration key of your choice that you will also specify on the management center when you register the threat defense. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).
- *nat_id*—Specifies a unique, one-time string of your choice that you will also specify on the management center when you register the threat defense when one side does not specify a reachable IP address or hostname. It is required if you set the management center to **DONTRESOLVE**. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the management center.

  Note If you use a data interface for management, then you must specify the NAT ID on both the threat defense and the management center for registration.

Example:

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

If the management center is behind a NAT device, enter a unique NAT ID along with the registration key, and specify DONTRESOLVE instead of the hostname, for example:

Example:

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

If the threat defense is behind a NAT device, enter a unique NAT ID along with the management center IP address or hostname, for example:

Example:

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

Step 5 (Optional) (6.7 and Later) Configure a data interface for the management center access.

configure network management-data-interface

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

Note You should use the console port when using this command. If you use SSH to the Management interface, you might get disconnected and have to reconnect to the console port. See below for more information about SSH usage.

See the following details for using this command:

- The original Management interface cannot use DHCP if you want to use a data interface for management. If you did not set the IP address manually during initial setup, you can set it now using the **configure network** {**ipv4** | **ipv6**} **manual** command. If you did not already set the Management interface gateway to **data-interfaces**, this command will set it now.
- Management Center access from a data interface has the following limitations:
  - You can only enable manager access on one physical, data interface. You cannot use a subinterface or EtherChannel.
  - This interface cannot be management-only.
  - Routed firewall mode only, using a routed interface.
  - PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the threat defense and the WAN modem.
  - The interface must be in the global VRF only.
  - You cannot use separate management and event-only interfaces.
  - SSH is not enabled by default for data interfaces, so you will have to enable SSH later using the management center. Because the Management interface gateway will be changed to be the data interfaces, you also cannot SSH to the Management interface from a remote network unless you add a static route for the Management interface using the **configure network static-routes** command.
- When you add the threat defense to the management center, the management center discovers and maintains the interface configuration, including the following settings: interface name and IP address, static route to the gateway, DNS servers, and DDNS server. For more information about the DNS server configuration, see below. In management center, you can later make changes to the management center access interface configuration, but make sure you don't make changes that can prevent the threat defense

or management center from re-establishing the management connection. If the management connection is disrupted, the threat defense includes the **configure policy rollback** command to restore the previous deployment.

- If you configure a DDNS server update URL, the threat defense automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the threat defense can validate the DDNS server certificate for the HTTPS connection. The threat defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).
- This command sets the *data* interface DNS server. The Management DNS server that you set with the setup script (or using the **configure network dns servers** command) is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface.

  On the management center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this threat defense. When you add the threat defense to the management center, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the threat defense that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively configure the DNS Platform Settings to match this setting to bring the management center and the threat defense into sync.

  Also, local DNS servers are only retained by the management center if the DNS servers were discovered at initial registration. For example, if you registered the device using the Management interface, but then later configure a data interface using the **configure network management-data-interface** command, then you must manually configure all of these settings in the management center, including the DNS servers, to match the threat defense configuration.
- You can change the management interface after you register the threat defense to the management center, to either the Management interface or another data interface.
- The FQDN that you set in the setup wizard will be used for this interface.
- You can clear the entire device configuration as part of the command; you might use this option in a recovery scenario, but we do not suggest you use it for initial setup or normal operation.
- To disable data managemement, enter the **configure network management-data-interface disable** command.

Example:

```
> 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://jcrichton: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 FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> 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
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 FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Step 6 (Optional) (6.7 and Later) Limit data interface access to an management center on a specific network.

configure network management-data-interface client *ip_address netmask*

By default, all networks are allowed.

What to do next

Register your device to a management center.

Log Into the Management Center

Use the management center to configure and monitor the threat defense.

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 Management Center

All licenses are supplied to the threat defense by the management center. You can purchase the following licenses:

- **Threat**—Security Intelligence and Next-Generation IPS
- **Malware**—Malware defense
- **URL**—URL Filtering
- **RA VPN**—AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only

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

Before you begin

- Have a master account on the 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.

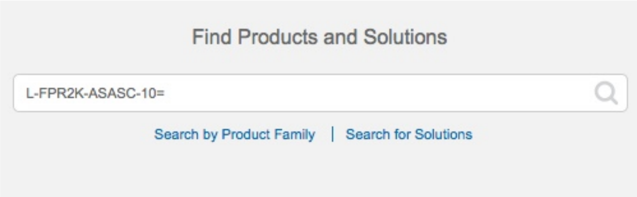
- Your Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

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 PIDs:

Figure 9: License Search



Find Products and Solutions

L-FPR2K-ASASC-10=

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

- Threat, Malware, and URL license combination:
  - L-ISA3000T-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-ISA3000T-TMC-1Y

  - L-ISA3000T-TMC-3Y
  - L-ISA3000T-TMC-5Y

- RA VPN—See the Cisco Secure Client Ordering Guide.

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

Registering requires you to generate a registration token in the Smart Software Manager. See the Cisco Secure Firewall Management Center Administration Guide for detailed instructions.

Register the Threat Defense with the Management Center

Register the threat defense to the management center manually using the device IP address or hostname.

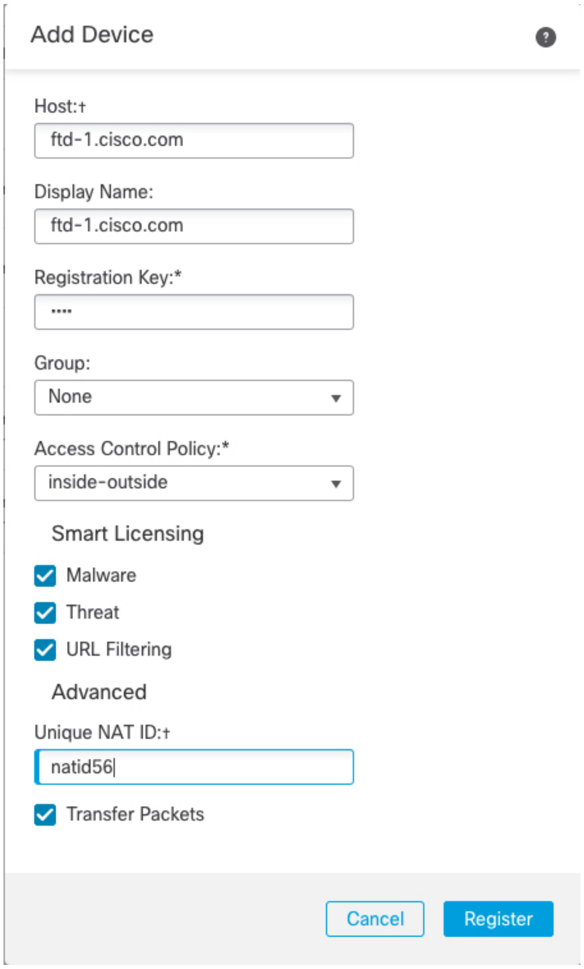
Before you begin

- Gather the following information that you set in the threat defense initial configuration:
  - The threat defense management IP address or hostname, and NAT ID
  - The management center registration key

Procedure

Step 1 In the management center, choose **Devices** > **Device Management**.

Step 2 From the **Add** drop-down list, choose **Add Device**.



Add Device

Host:†
ftd-1.cisco.com

Display Name:
ftd-1.cisco.com

Registration Key:*
••••

Group:
None

Access Control Policy:*
inside-outside

Smart Licensing

☑ Malware

☑ Threat

☑ URL Filtering

Advanced

Unique NAT ID:†
natid56

☑ Transfer Packets

Set the following parameters:

- **Host**—Enter the IP address or hostname of the threat defense you want to add. You can leave this field blank if you specified both the management center IP address and a NAT ID in the threat defense initial configuration.

  Note In an HA environment, when both the management centers are behind a NAT, you can register the threat defense without a host IP or name in the primary management center. However, for registering the threat defense in a secondary management center, you must provide the IP address or hostname for the threat defense.

- **Display Name**—Enter the name for the threat defense as you want it to display in the management center.

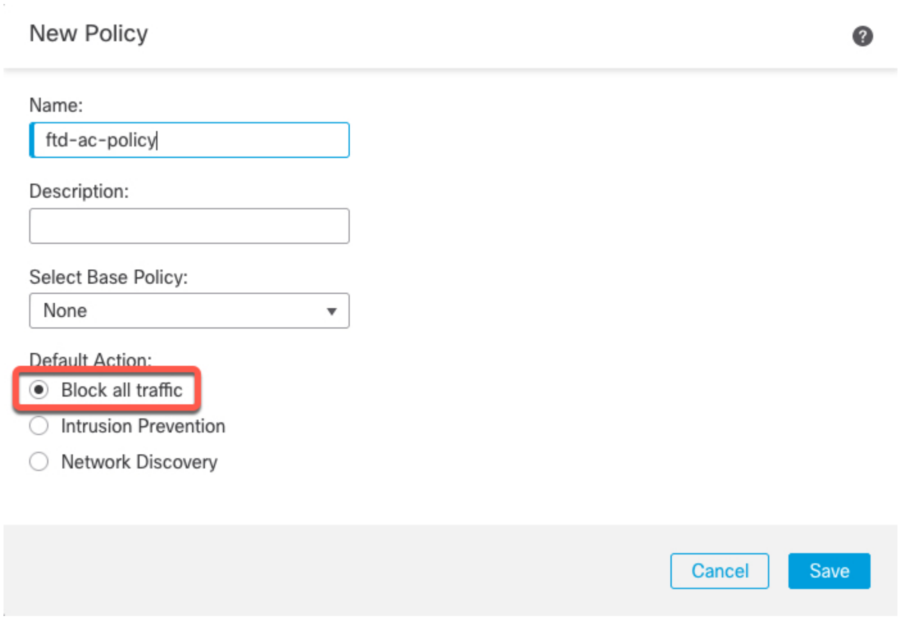
- **Registration Key**—Enter the same registration key that you specified in the threat defense initial configuration.

- **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 30.

Figure 10: New Policy



New Policy

Name: ftd-ac-policy

Description:

Select Base Policy: None

Default Action:

● Block all traffic
○ Intrusion Prevention
○ Network Discovery

- **Smart Licensing**—Assign the Smart Licenses you need for the features you want to deploy: **Malware** (if you intend to use malware inspection), **Threat** (if you intend to use intrusion prevention), and **URL** (if you intend to implement category-based URL filtering). **Note:** You can apply an AnyConnect Client remote access VPN license after you add the device, from the **System** > **Licenses** > **Smart Licenses** page.
- **Unique NAT ID**—Specify the NAT ID that you specified in the threat defense initial configuration.
- **Transfer Packets**—Allow the device to transfer packets to the management center. When events like IPS or Snort are triggered with this option enabled, the device sends event metadata information and packet data to the management center for inspection. If you disable it, only event information will be sent to the management center, but packet data is not sent.

Step 3 Click **Register**, or if you want to add another device, click **Register and Add Another** 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 threat defense fails to register, check the following items:

- Ping—Access the threat defense CLI, and ping the management center 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 threat defense Management IP address, use the **configure network** {**ipv4** | **ipv6**} **manual** command. If you configured a data interface for the management center access, use the **configure network management-data-interface** command.

- Registration key, NAT ID, and the management center 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 management center using the **configure manager add** command.

For more troubleshooting information, see https://cisco.com/go/fmc-reg-error.

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 22.
②	Configure the DHCP Server, on page 25.
③	Add the Default Route, on page 26.
④	Configure NAT, on page 28.
⑤	Allow Traffic from Inside to Outside, on page 30.
⑥	Deploy the Configuration, on page 31.

Configure Interfaces

Enable the threat defense 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.

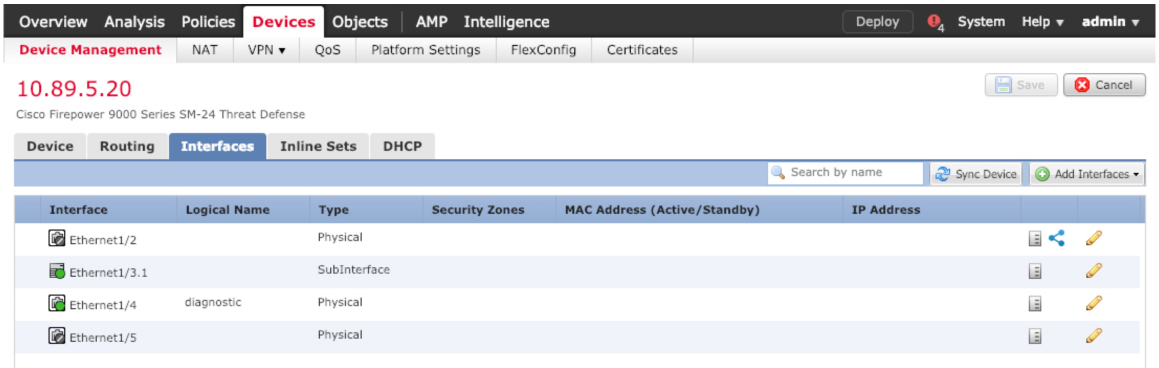
A typical edge-routing situation is to obtain the outside interface address through DHCP from your ISP, while you define static addresses on the inside interfaces.

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** (✎) for the firewall.

Step 2 Click **Interfaces**.



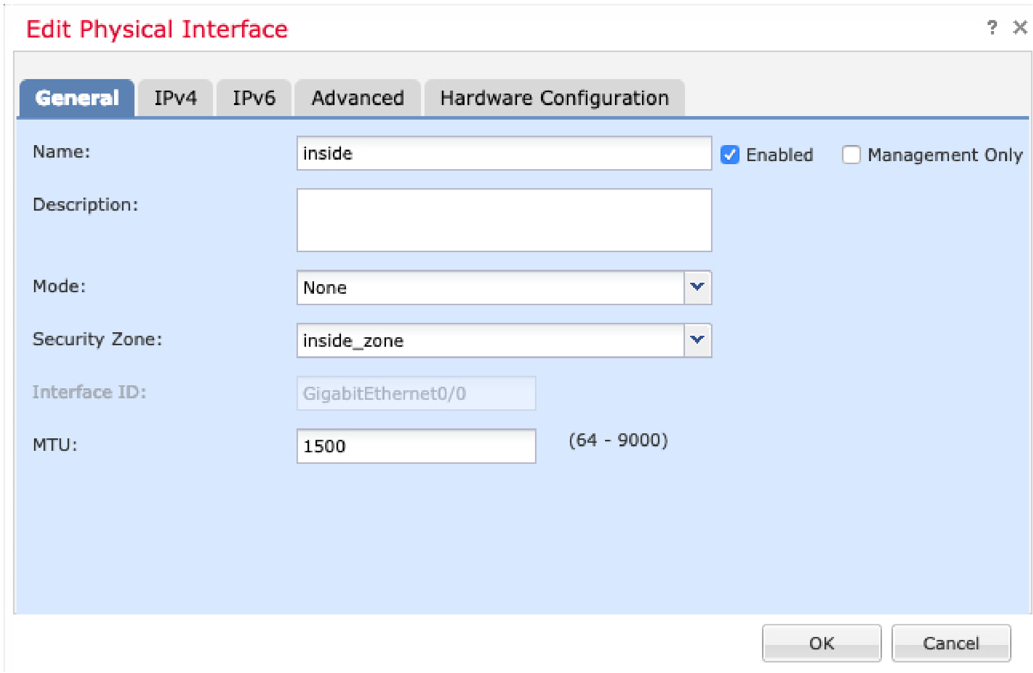
10.89.5.20

Cisco Firepower 9000 Series SM-24 Threat Defense

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Ethernet1/2		Physical			
Ethernet1/3.1		SubInterface			
Ethernet1/4	diagnostic	Physical			
Ethernet1/5		Physical			

Step 3 Click **Edit** (✎) for the interface that you want to use for *inside*.

The **General** tab appears.



Name: inside ☑ Enabled □ Management Only

Description:

Mode: None

Security Zone: inside_zone

Interface ID: GigabitEthernet0/0

MTU: 1500 (64 - 9000)

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**.

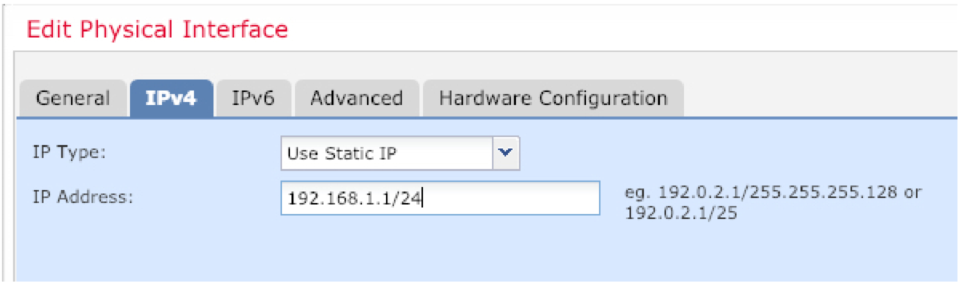
d) From the **Security Zone** drop-down list, choose an existing inside security zone or add a new one by clicking **New**.

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**



IP Type: Use Static IP

IP Address: 192.168.1.1/24

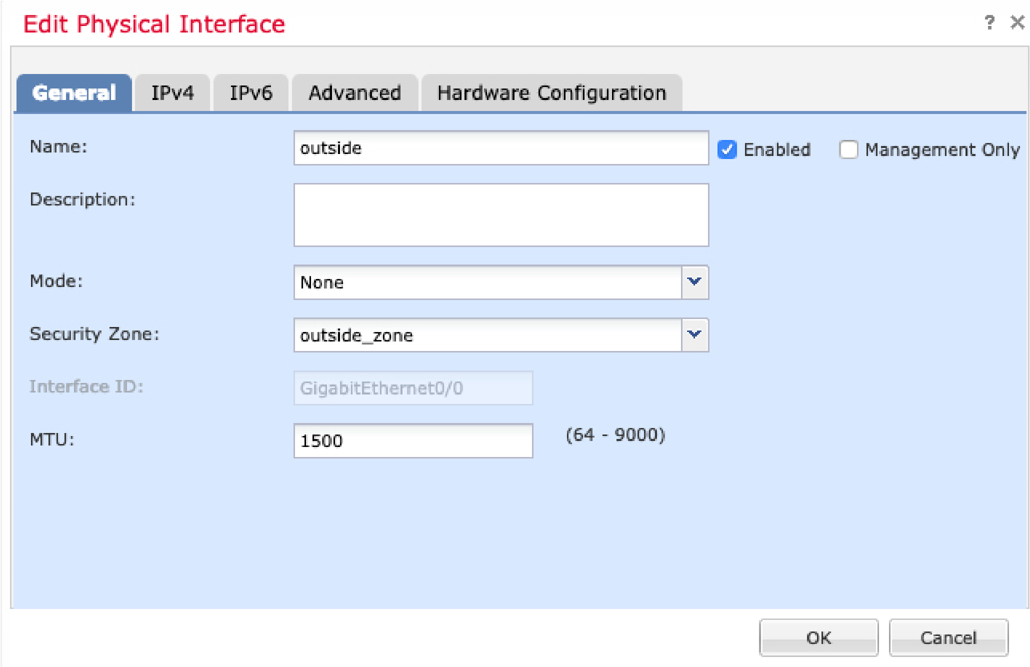
eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

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

f) Click **OK**.

Step 4 Click the **Edit** (✎) for the interface that you want to use for *outside*.

The **General** tab appears.



Name: outside ☑ Enabled ☐ Management Only

Description:

Mode: None

Security Zone: outside_zone

Interface ID: GigabitEthernet0/0

MTU: 1500 (64 - 9000)

Note If you pre-configured this interface for manager access, then the interface will already be named, enabled, and addressed. You should not alter any of these basic settings because doing so will disrupt the management center management connection. You can still configure the Security Zone on this screen for through traffic policies.

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

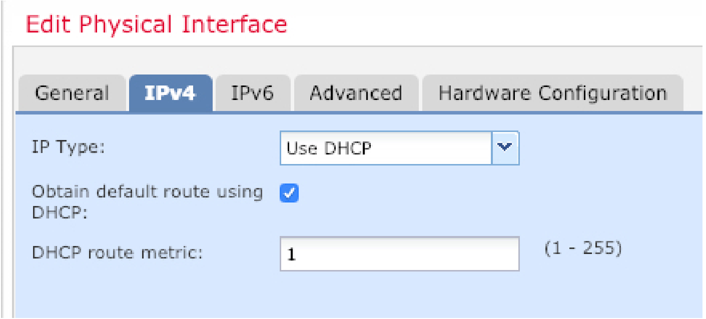
For example, name the interface **outside**.

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.



Edit Physical Interface

IP Type: Use DHCP

Obtain default route using DHCP: ☑

DHCP route metric: 1 (1 - 255)

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

f) Click **OK**.

Step 5 Click **Save**.

Configure the DHCP Server

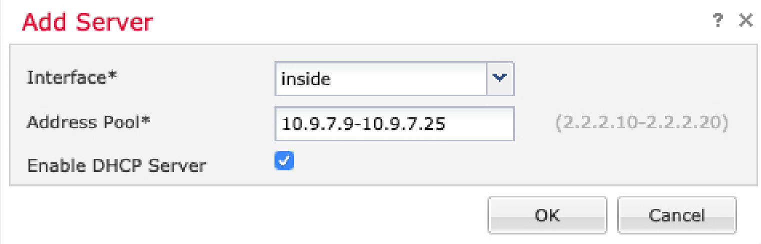
Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the threat defense.

Procedure

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

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

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



Interface* inside

Address Pool* 10.9.7.9-10.9.7.25 (2.2.2.10-2.2.2.20)

Enable DHCP Server ☑

- **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**.

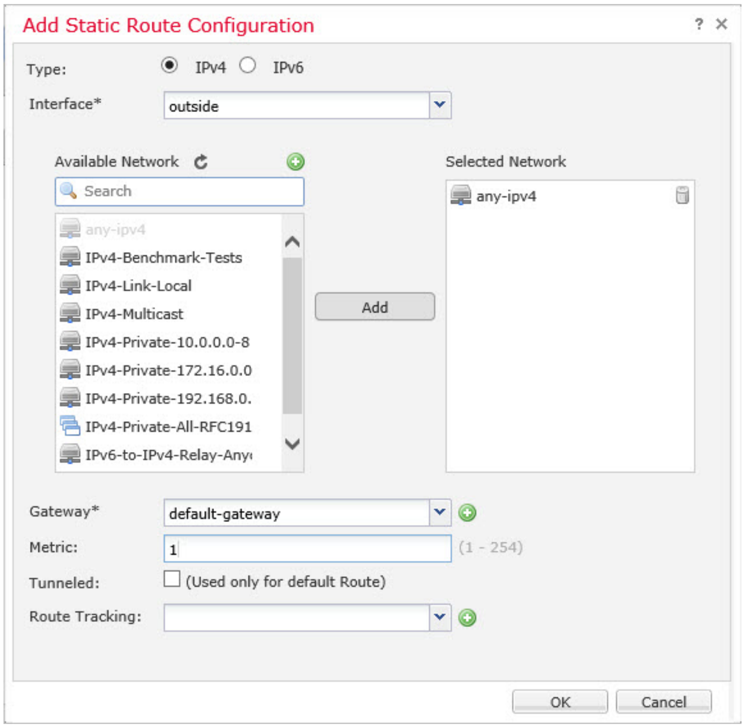
Add the Default Route

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** (✎) for the device.

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



Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*: outside

Available Network

Search

- any-ipv4
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0
- IPv4-Private-192.168.0.
- IPv4-Private-All-RFC191
- IPv6-to-IPv4-Relay-Any

Add

Selected Network

- any-ipv4

Gateway*: default-gateway

Metric: 1 (1 - 254)

Tunneled: □ (Used only for default Route)

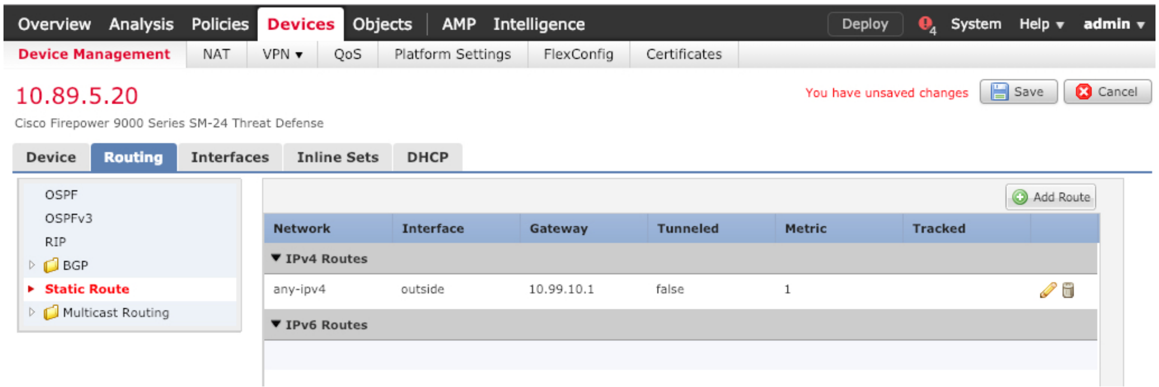
Route Tracking:

OK Cancel

- **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.
- **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.



10.89.5.20

Cisco Firepower 9000 Series SM-24 Threat Defense

You have unsaved changes

Network	Interface	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes					
any-ipv4	outside	10.99.10.1	false	1	
▼ IPv6 Routes					

Step 4 Click **Save**.

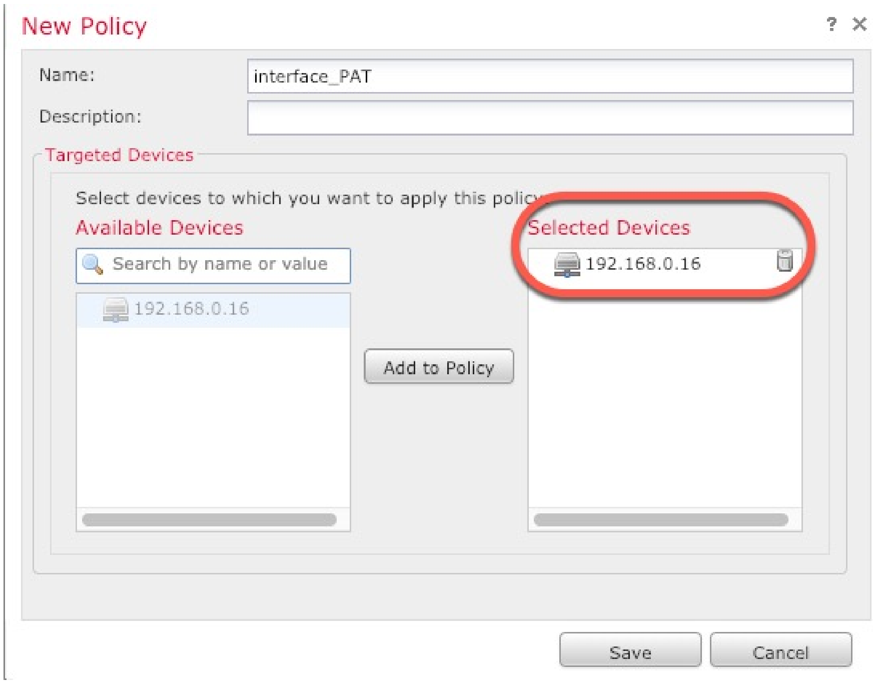
Configure NAT

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**.



New Policy

Name: interface_PAT

Description:

Targeted Devices

Select devices to which you want to apply this policy

Available Devices

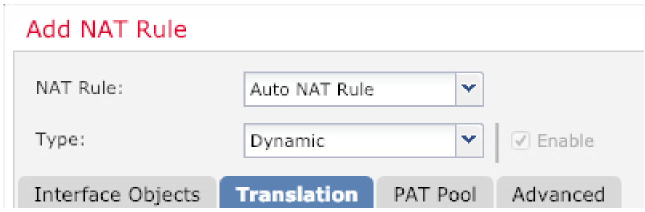
Selected Devices: 192.168.0.16

The policy is added the management center. 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:



Add NAT Rule

NAT Rule: Auto NAT Rule

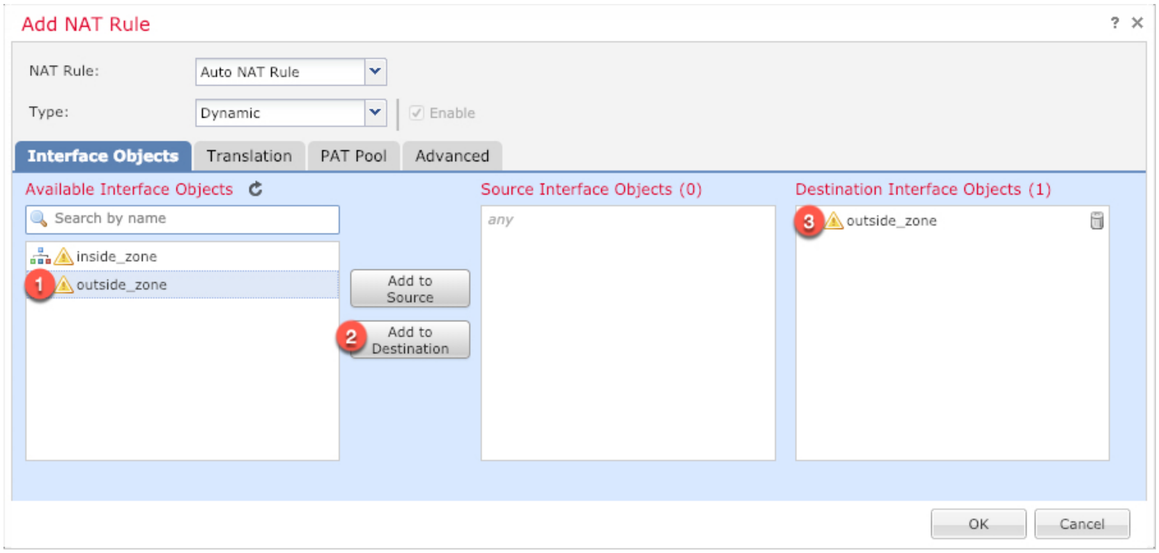
Type: Dynamic

☑ Enable

- **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.

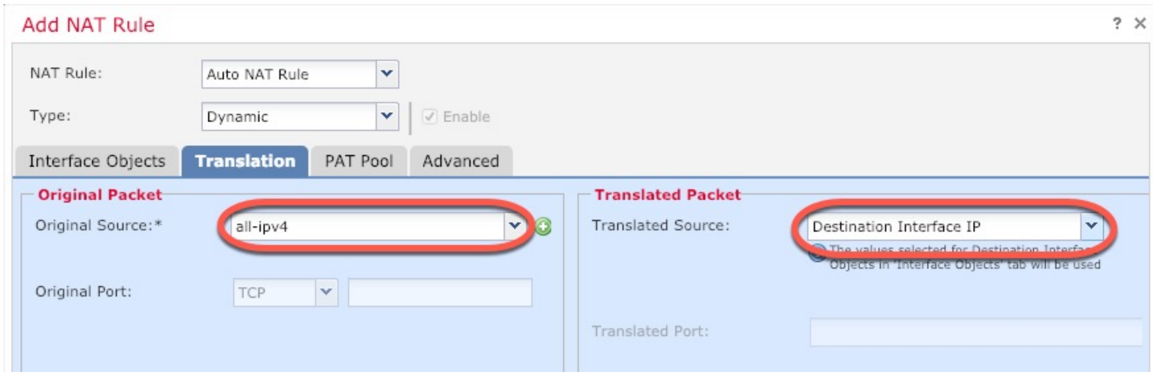


Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic ☑ Enable

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



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic ☑ Enable

Original Packet

Original Source:* all-ipv4

Original Port: TCP

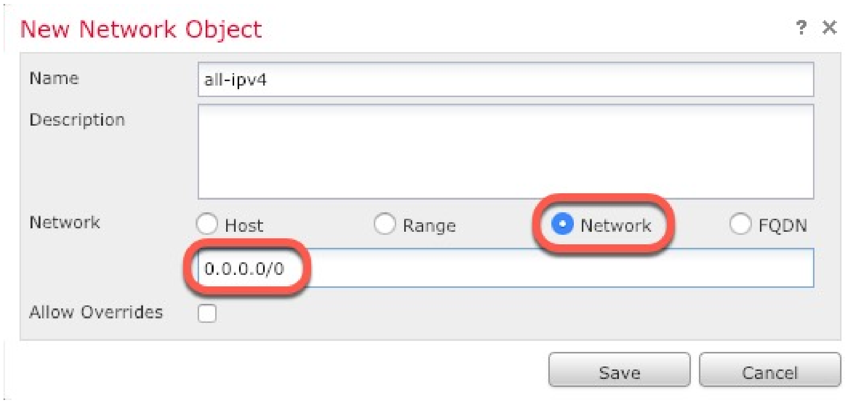
Translated Packet

Translated Source: Destination Interface IP

The values selected for 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).



New Network Object

Name: all-ipv4

Description:

Network: ○ Host ○ Range ● Network ○ FQDN

0.0.0.0/0

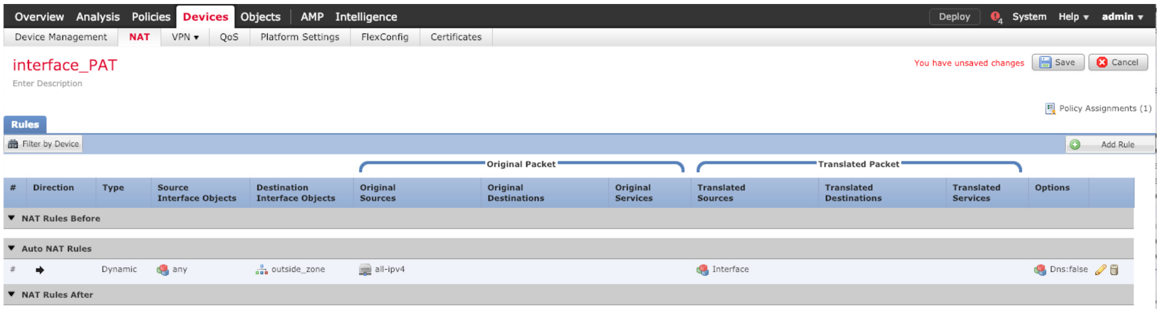
Allow Overrides ☐

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.



interface_PAT

Enter Description

You have unsaved changes

Policy Assignments (1)

					Original Packet			Translated Packet			
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
▼ NAT Rules Before											
▼ Auto NAT Rules											
#	➔	Dynamic	any	outside_zone	all-ipv4			Interface			Dns:false
▼ NAT Rules After											

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

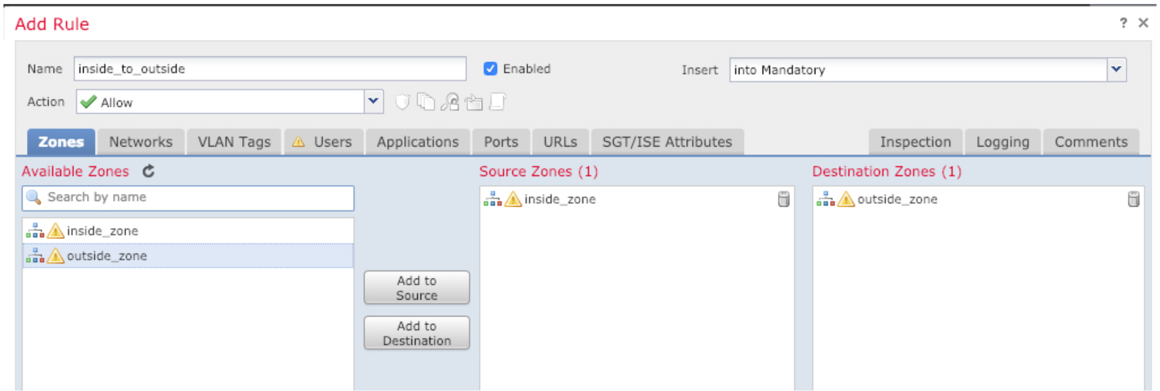
Allow Traffic from Inside to Outside

If you created a basic **Block all traffic** access control policy when you registered the threat defense, 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.

Procedure

Step 1 Choose **Policy** > **Access Policy** > **Access Policy**, and click the **Edit** (✎) for the access control policy assigned to the threat defense.

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



Name: inside_to_outside ☑ Enabled Insert: into Mandatory

Action: ✓ Allow

Source Zones (1): inside_zone

Destination Zones (1): outside_zone

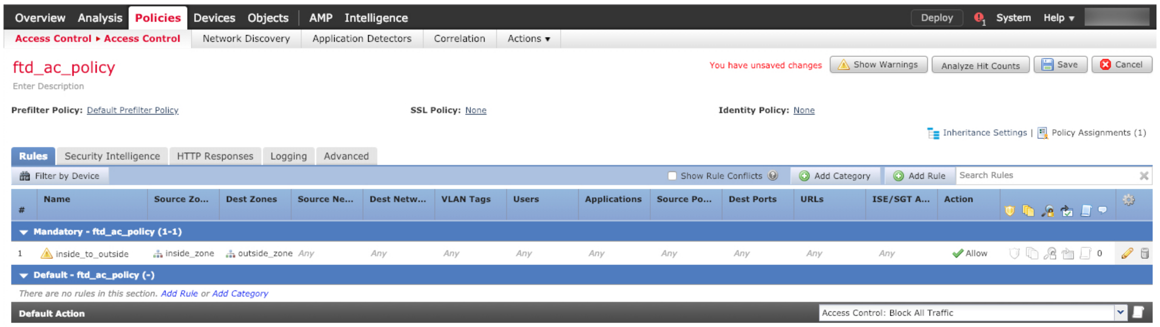
- **Name**—Name this rule, for example, **inside_to_outside**.

- **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.



ftd_ac_policy

Enter Description

Prefilter Policy: Default Prefilter Policy **SSL Policy:** None **Identity Policy:** None

#	Name	Source Zo...	Dest Zones	Source Ne...	Dest Netw...	VLAN Tags	Users	Applications	Source Po...	Dest Ports	URLs	ISE/SGT A...	Action		
Mandatory - ftd_ac_policy (1-1)															
1	⚠ inside_to_outside	inside_zone	outside_zone	Any	Any	Any	Any	Any	Any	Any	Any	Any	✓ Allow	0	
Default - ftd_ac_policy (-)															
There are no rules in this section. Add Rule or Add Category															

Default Action Access Control: Block All Traffic

Step 4 Click **Save**.

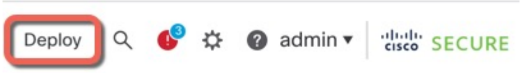
Deploy the Configuration

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

Procedure

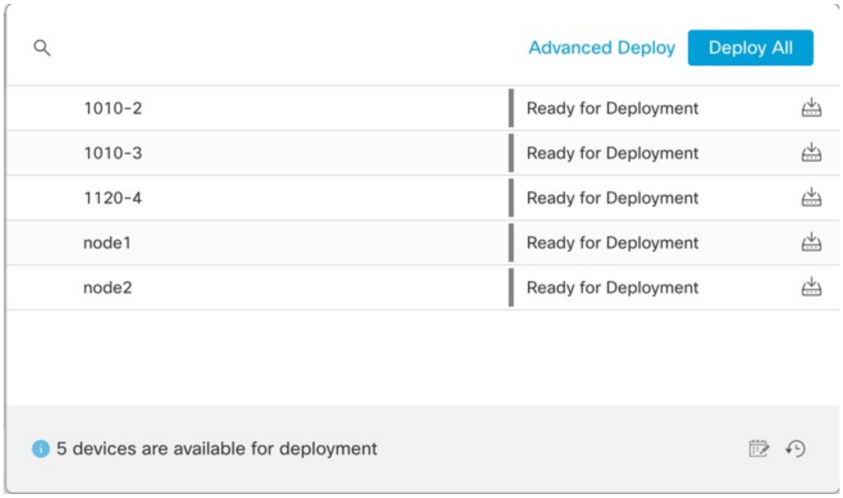
Step 1 Click **Deploy** in the upper right.

Figure 11: Deploy



Step 2 Either click **Deploy All** to deploy to all devices or click **Advanced Deploy** to deploy to selected devices.

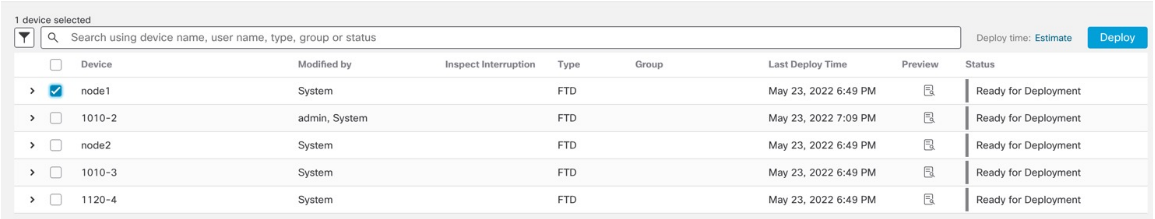
Figure 12: Deploy All



1010-2	Ready for Deployment
1010-3	Ready for Deployment
1120-4	Ready for Deployment
node1	Ready for Deployment
node2	Ready for Deployment

5 devices are available for deployment

Figure 13: Advanced Deploy

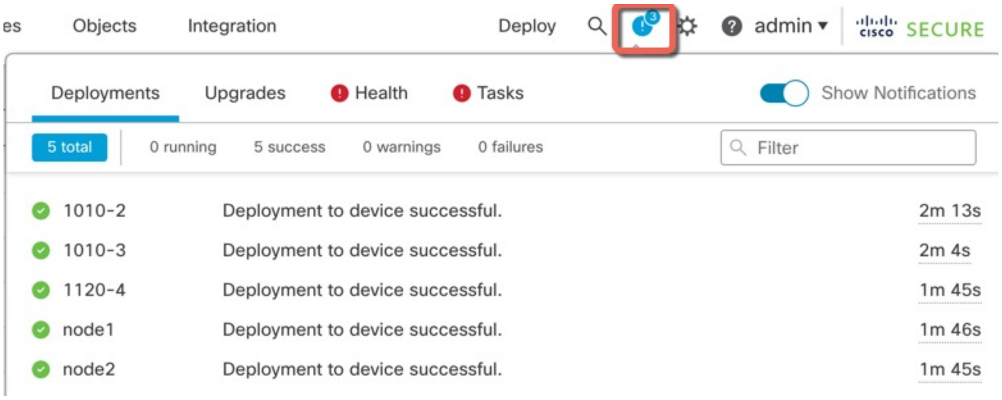


1 device selected

	☐	Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
›	☑	node1	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment
›	☐	1010-2	admin, System		FTD		May 23, 2022 7:09 PM		Ready for Deployment
›	☐	node2	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment
›	☐	1010-3	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment
›	☐	1120-4	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment

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 14: Deployment Status



1010-2	Deployment to device successful.	2m 13s
1010-3	Deployment to device successful.	2m 4s
1120-4	Deployment to device successful.	1m 45s
node1	Deployment to device successful.	1m 46s
node2	Deployment to device successful.	1m 45s

Access the Threat Defense CLI

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

You can SSH to the management interface of the threat defense device. You can also connect to the address on a data interface if you open the interface for SSH connections. SSH access to data interfaces is disabled by default.

Procedure

Step 1 To log into the CLI, connect your management computer to the console port., either the RJ-45 port or the mini-USB port.Be sure to install any necessary USB serial drivers for your operating system. Use the following serial settings:

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

Step 2 Log in to the threat defense CLI using the **admin** username and the password you set at initial setup (the default is **Admin123**).

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

Power Off the Firewall

It's important that you shut down your system properly. Simply unplugging the power 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 firewall system.

The ISA 3000 chassis does not have an external power switch.You can power off the device using the management center device management page, or you can use the CLI.

Power Off the Firewall Using the Management Center

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 firewall.

Note Shutting down is supported in 7.0.2+/7.2+.

You can shut down your system properly using the management center.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device that you want to restart, click the edit icon (✎).

Step 3 Click the **Device** tab.

Step 4 Click the shut down device icon (●) in the **System** section.

Step 5 When prompted, confirm that you want to shut down the device.

Step 6 Monitor the shutdown process. If you cannot monitor the device, wait approximately 3 minutes to ensure the system has shut down.

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

```
Firepower Threat Defense is stopped.
It is safe to power off now.

To restart the device, you must Power cycle to the device.
```

Step 7 You can now unplug the power to physically remove power from the chassis if necessary.

Power Off the Firewall at the CLI

It's important that you shut down your system properly. Simply unplugging the power 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. The ISA 3000 chassis does not have an external power switch.

Note Shutting down is supported in 7.0.2+/7.2+.

Procedure

Step 1 Connect to the console port to access the threat defense CLI, and then shut down the threat defense.

shutdown

Example:

```
> shutdown
```

```
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
Shutting down sfifd...                                                [  OK  ]
Clearing static routes
Unconfiguring default route                                           [  OK  ]
Unconfiguring address on br1                                          [  OK  ]
Unconfiguring IPv6                                                    [  OK  ]
Downing interface                                                     [  OK  ]
Stopping xinetd:
Stopping nscd...                                                      [  OK  ]
Stopping system log daemon...                                         [  OK  ]
Stopping Threat Defense ...
Stopping system message bus: dbus.                                    [  OK  ]
Un-mounting disk partitions ...
device-mapper: remove ioctl on root failed: Device or resource busy
[...]
mdadm: Cannot get exclusive access to /dev/md0:Perhaps a running process, mounted filesystem
 or active volume group?
Stopping OpenBSD Secure Shell server: sshd
stopped /usr/sbin/sshd (pid 3520)
done.
Stopping Advanced Configuration and Power Interface daemon: stopped /usr/sbin/acpid (pid
3525)
acpid.
Stopping system message bus: dbus.
Stopping internet superserver: xinetd.
no /etc/sysconfig/kdump.conf
Deconfiguring network interfaces... ifdown: interface br1 not configured
done.
SSP-Security-Module is shutting down ...
Sending ALL processes the TERM signal ...
acpid: exiting
Sending ALL processes the KILL signal ...
Deactivating swap...
Unmounting local filesystems...

Firepower Threat Defense stopped.
It is safe to power off now.

To restart the device, you must Power cycle to the device.
```

Step 2 After the threat defense shuts down, and the console shows that "It is safe to power off now", you can then unplug the power to physically remove power from the chassis if necessary.

What's Next?

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

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