How to Manage a Device with the Firepower Management Center

First Published: 2018-11-28

Last Modified: 2018-11-28

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CHAPTER 1

About This Guide

This how-to guide explains how to set up a Firepower Management Center Version 6.2.3 device to manage a Firepower Threat Defense Version 6.2.3 device to provide inspection and security for a sample network that includes an inside network and outside network (that is, the internet). If you follow all the steps in this guide, you can configure a system identical to this one.

- What's In This Guide, on page 1
- About the Network Setup, on page 2
- Network Setup Task Overview, on page 4

What's In This Guide

This guide discusses setting up a basic network with the Firepower Version 6.2.3 System (that is, Firepower Management Center and a Firepower Threat Defense device both running Version 6.2.3). This basic setup is required to use the Firepower Management Center for access control, intrusion prevention, and monitoring. You must perform these tasks before you can do anything else with the Firepower System.

Note This guide has sample IP addresses that you can use in your system, provided they do not conflict with addresses in your network. You can either use the same IP addresses described in this guide or you can use IP addresses that are compatible with your network. If you change IP addresses to conform with your network, make sure that the Firepower Threat Defense management interface and the Firepower Management Center interface are on the same subnet.

Setup Tasks Covered in this Guide

This guide uses sample values to tell you step by step how to:

- Configure a Firepower Management Center on the network.
- Configure a Firepower Threat Defense on the network.
- License the Firepower Management Center.
- Manage the Firepower Threat Defense device using Firepower Management Center.
- Configure a NAT policy and a static route.

- Set up an initial access control rule that allows all traffic so you can test internet access from a client connected to the inside network and make sure the managed device is filtering the traffic.

Who Should Use This Guide

Anyone who wants to configure the Firepower System, including administrators and integrators.

What You'll Need

To complete the tasks discussed in this guide, you'll need:

- Firepower Management Center (any model, physical or virtual) running version 6.2.3
- Firepower Threat Defense (any model, physical or virtual) running version 6.2.3

  For information about upgrading a Firepower Management Center or Firepower Threat Defense device, see the Firepower Management Center Upgrade Guide.

  Note You can use another version of the Firepower System software but additional tasks, or different tasks, might be required. Consult the appropriate configuration or quick start guide for the version you're using for details.

- For virtual devices, a hypervisor manager and client.
- A private network so the IP addresses used in this system don't conflict with IP addresses used in your network. For example, you can set up a Virtual LAN (VLAN). Explaining how to isolate this system from the rest of your network is beyond the scope of this guide.
- (Optional.) Cisco Smart License. If you don't have a Smart License, you can use a 90-day evaluation license.

  For more information about Smart Licenses in version 6.2.3, see Smart Licensing for the Firepower System.

Related Topics

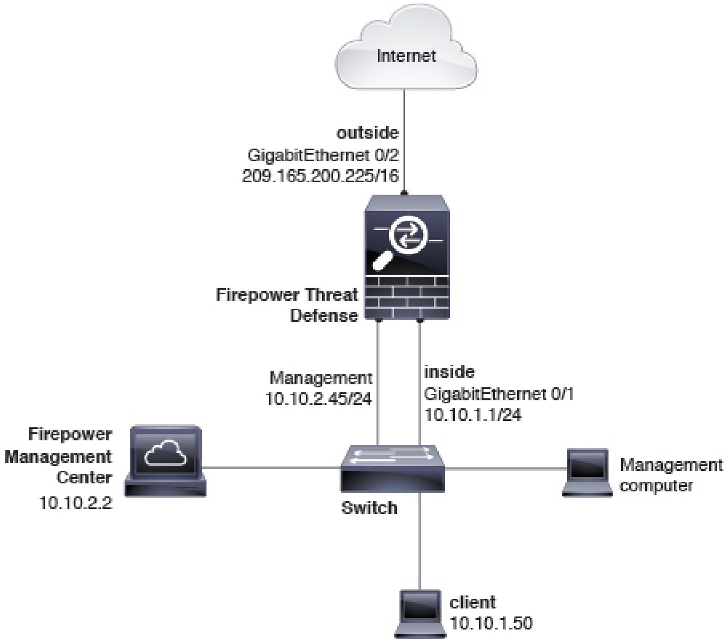
About the Network Setup, on page 2

Network Setup Task Overview, on page 4

About the Network Setup

This guide walks you through setting up the following network:

Figure 1: Sample network used in this guide



Firepower Threat Defense Interfaces

In this example network, the Firepower Threat Defense device has three interfaces: management, inside, and outside. The outside interface connects directly to the internet. Using an allow access control rule, clients attached to the inside network can connect to the internet through the Firepower Threat Defense device. This type of configuration is sometimes referred to as a *bootstrap* because this is the minimum amount of configuration you need to connect to the internet.

Management (1 / 1)
IP address 10.10.2.45. Used only to communicate with the Firepower Management Center. The management IP address must be on the same subnet as the Firepower Management Center.

Inside (GigabitEthernet 1 / 2)
IP address 10.10.2.1. Computers attached to the inside interface can have access control and intrusion prevention policies applied to them. The default gateway for the inside network is 10.10.2.254.

Outside (GigabitEthernet 1 / 1)
IP address 209.165.200.255. Used to connect to the internet. The default gateway for the outside network is 209.165.200.254.

Note This guide has sample IP addresses that you can use in your system, provided they do not conflict with addresses in your network. You can either use the same IP addresses described in this guide or you can use IP addresses that are compatible with your network. If you change IP addresses to conform with your network, make sure that the Firepower Threat Defense management interface and the Firepower Management Center interface are on the same subnet.

Note Depending on what type of device you're managing, the interfaces might be identified differently than the preceding. For example, a virtual managed device has interfaces numbered GigabitEthernet0/0, GigabitEthernet0/1, and so on. A Firepower Threat Defense 4100 or 9300 series device has interfaces numbered Ethernet1/1, Ethernet2/1, Ethernet3/1, and so on.

Firepower Management Center

The Firepower Management Center has one interface with an IP address of 10.10.2.2. This interface is used to manage Firepower Threat Defense devices, each of which must all have a management IP address on the same subnet.

Network Setup Task Overview

This topic provides a high-level overview of setting up the network discussed in About the Network Setup, on page 2.

Procedure

	Command or Action	Purpose
Step 1	Prerequisites.	What's In This Guide, on page 1
Step 2	Connect the Firepower Management Center to a switch that connects it to the Firepower Threat Defense and to a network that is accessible by the computer you'll use to access the Firepower Management Center.	
Step 3	Set up the Firepower Management Center on the network.	Access the device using SSH or a terminal server and run the **configure-network** command to set the device's management IP address, subnet, DNS servers, and so on. See Connect the Firepower Management Center to the Network, on page 7.
Step 4	Set up the Firepower Threat Defense on the network.	Firepower Threat Defense has a setup script that performs the same tasks as Firepower Management Center and also enables you to choose routed mode and to allow the device to be managed by Firepower Management Center. See Connect the Managed Device to the Network, on page 8.
Step 5	Initially configure the Firepower Management Center.	Access the Firepower Management Center with a web browser and set additional options, including time zone, time servers, automatic backup, and so on. See Configure the Firepower Management Center for the First Time, on page 11.
Step 6	License the Firepower Management Center.	Apply either a Smart License or a 90-day evaluation license. The evaluation license is fully functional but for production use, you need a Smart License. See Configure

	Command or Action	Purpose
		the Firepower Management Center for the First Time, on page 11.
Step 7	Add Firepower Threat Defense as a managed device to the Firepower Management Center.	After adding the managed device, you perform all further configuration in the Firepower Management Center. See Add a Managed Device to the Firepower Management Center, on page 15.
Step 8	Configure Firepower Threat Defense interfaces, static route, and NAT rule.	Configure the inside and outside interfaces and a NAT rule to send traffic from any network to the outside interface. Configure a static route to the outside interface. See Configure the Managed Device, on page 15.
Step 9	Edit an access control policy to allow internet access.	This temporary access control rule allows traffic to the outside interface. See Edit the Access Control Policy, on page 25.
Step 10	Connect a client to the inside network and make sure it can access the internet.	Make sure the client can access the internet and make sure the managed device is filtering the traffic. See Troubleshoot the System, on page 30.
Step 11	Troubleshoot issues you might encounter.	Typically, issues are related either to physical networking problems or improperly configured static route or NAT policy. See Test the System, on page 27.

CHAPTER 2

Set Up Devices and Connect them to the Network

The first thing you must do is connect your Firepower Management Center and Firepower Threat Defense devices to the network. Depending on how your organization manages network devices, you might need assistance to install the devices in a rack.

- Set Up Devices, on page 7
- Connect the Firepower Management Center to the Network, on page 7
- Connect the Managed Device to the Network, on page 8

Set Up Devices

Because the various models of physical and virtual devices are set up differently, consult the documentation for your Firepower Management Center and Firepower Threat Defense device to:

- (Physical appliances): Unpack, rack, and connect the device to the network using the hardware installation guide.
- (Virtual devices): Install the virtual machine image and power it up using the virtual device quick start guides.

After performing those tasks, continue with the next section to configure IP addresses and to perform the other tasks necessary to get the Firepower System running.

Connect the Firepower Management Center to the Network

This task enables you to initially configure the Firepower Management Center for access to the internet. You'll provide an IP address, subnet mask, and other parameters. Refer to the sample network diagram About the Network Setup, on page 2.

Before you begin

See Set Up Devices and Connect them to the Network, on page 7.

Step 1 Connect to the virtual machine's console in vSphere or the physical appliance's Console port or using Secure Shell (SSH).

Step 2 Log in to the Firepower Management Center as the `admin` user. (By default, the password is `Admin123`.)

Step 3 At the prompt, enter the following command:

```
sudo configure-network
```

Step 4 When prompted, enter the password **Admin123**.

Step 5 Enter the following information at the prompts:

```
Do you want to configure IPv4 (y or n)? y
Management IP address [192.168.45.45]? 10.10.2.2
Management netmask [255.255.255.0]? 255.255.255.0
Management default gateway? 10.10.2.254
Are these settings correct (y or n)? y
Do you wish to configure IPv6? n
```

Step 6 The following messages are displayed to indicate configuration was successful:

```
Updated network configuration
Updated comms. channel communication
```

What to do next

See Connect the Managed Device to the Network, on page 8.

Connect the Managed Device to the Network

Connecting a Firepower Threat Defense to the network is very similar to connecting a Firepower Management Center to the network. You'll provide an IP address and subnet mask for its management interface, DNS, and, in addition, specify the device should operate in routed mode and be managed by a Firepower Management Center. Refer to the sample network diagram About the Network Setup, on page 2.

For more information about routed mode, see About Routed Firewall Mode.

Before you begin

See Set Up Devices and Connect them to the Network, on page 7.

Step 1 Connect to the virtual machine's console in vSphere or the physical appliance's Console port or using Secure Shell (SSH).

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

Step 3 If required by your device, enter **connect ftd**.

Step 4 Press Enter to display the EULA and press Space to page through it.

Step 5 When prompted, enter **yes** to accept the EULA.

Step 6 At the **Enter new password** prompt, enter a password for your managed device and confirm the password when prompted.

Step 7 Enter the following information at the next prompts:

```
Do you want to configure IPv4 (y/n)? [y] y
Do you want to configure IPv6 (y/n)? [n] n
Configure IPv4 via DHCP or manually? (dhcp/manually) [manual] manual
Enter an IPv4 address for the management interface [192.168.45.1] 10.10.2.45
Enter an IPv4 netmask for the management interface [255.255.255.0] 255.255.255.0
Enter an IPv4 default gateway for the management interface 10.10.2.254
Enter a fully qualified hostname for this device [firepower] firepower
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.202.202] 8.8.8.8
Enter a comma-separated list of search domains or 'none' [] none
Are these settings correct (y or n)? y
```

Step 8 The following prompts are displayed:

```
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

Step 9 Enter the following information:

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

Step 10 The following prompt is displayed:

```
Configuring firewall mode ...
```

Step 11 At the next prompt, enter the following command:

```
configure manager add 10.10.2.2 cisco123
```

Step 12 The following prompt confirms the action was successful:

```
Manager successfully configured.
```

What to do next

See Configure the Firepower Management Center, on page 11.

CHAPTER 3

Configure the Firepower Management Center

Before you can manage devices and control access to the network, you must configure the Firepower Management Center with additional internet settings and a license.

- Configure the Firepower Management Center for the First Time, on page 11
- License the Firepower Management Center, on page 14

Configure the Firepower Management Center for the First Time

Before you begin

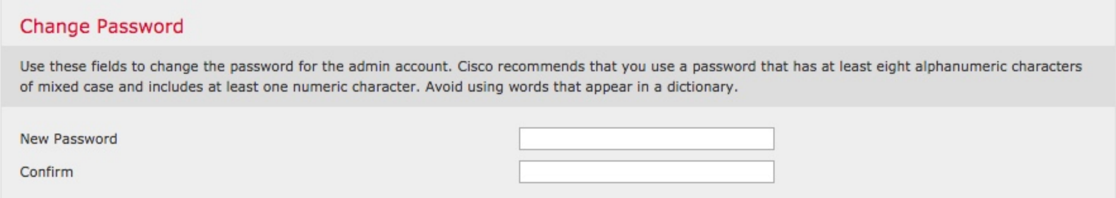
See Connect the Firepower Management Center to the Network, on page 7.

Step 1 In your browser's address or location field, enter **`https://10.10.2.2`**.

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

An initial configuration page is displayed. The following steps walk you through the configuration one section at a time.

Step 3 Enter a new Firepower Management Center password in the following fields.



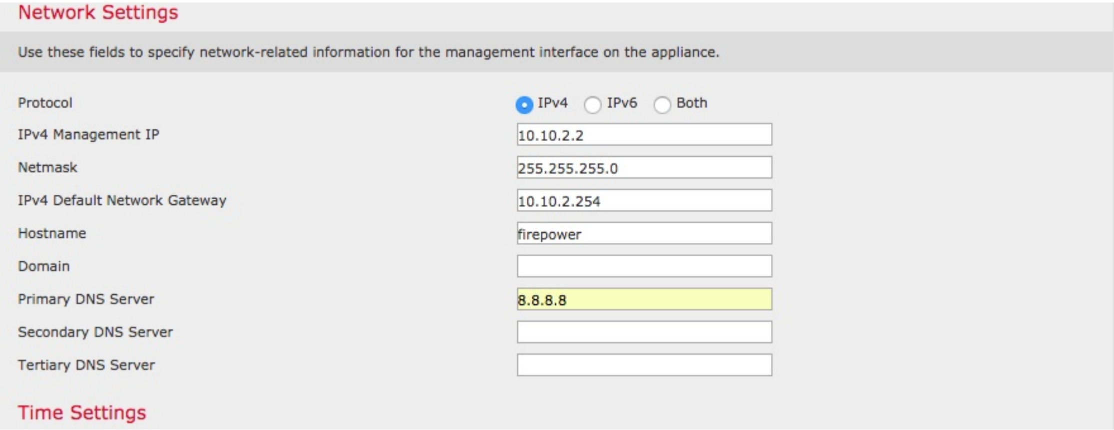
Change Password

Use these fields to change the password for the admin account. Cisco recommends that you use a password that has at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

New Password

Confirm

Step 4 Enter the network settings shown in the following figure. Enter DNS server specific to your organization, if applicable.



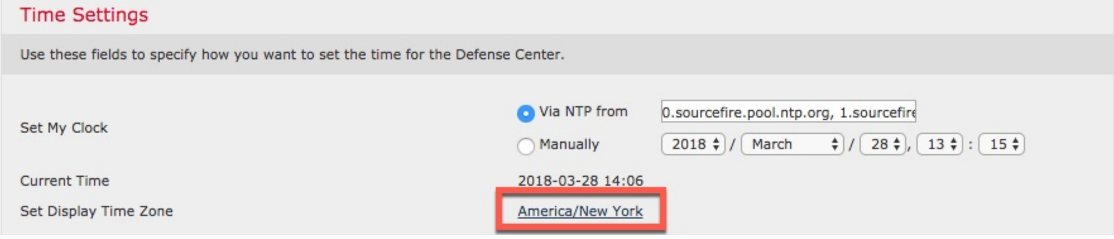
Network Settings

Use these fields to specify network-related information for the management interface on the appliance.

Protocol	● IPv4 ○ IPv6 ○ Both
IPv4 Management IP	10.10.2.2
Netmask	255.255.255.0
IPv4 Default Network Gateway	10.10.2.254
Hostname	firepower
Domain	
Primary DNS Server	8.8.8.8
Secondary DNS Server	
Tertiary DNS Server	

Time Settings

Step 5 Enter the time server and time zone settings shown in the following figure. If necessary, click **America/New York** and follow the prompts on your screen to select a time zone.



Time Settings

Use these fields to specify how you want to set the time for the Defense Center.

Set My Clock	● Via NTP from 0.sourcefire.pool.ntp.org, 1.sourcefire ○ Manually 2018 / March / 28 , 13 : 15
Current Time	2018-03-28 14:06
Set Display Time Zone	America/New York

Step 6 Select options for recurring updates and automatic backup:

- **Recurring Rule Update Imports:** As new vulnerabilities become known, the Vulnerability Research Team (VRT) releases intrusion rule updates. Rule updates provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. Rule updates might also delete rules and provide new rule categories and system variables.

  You can specify the **Import Frequency**, as well as configure the system to perform an intrusion **Policy Reapply** after each rule update. To perform a rule update as part of the initial configuration process, check **Install Now**.

  Rule updates might contain new binaries. Make sure your process for downloading and installing rule updates complies with your security policies. In addition, rule updates may be large, so make sure to import rules during periods of low network use.

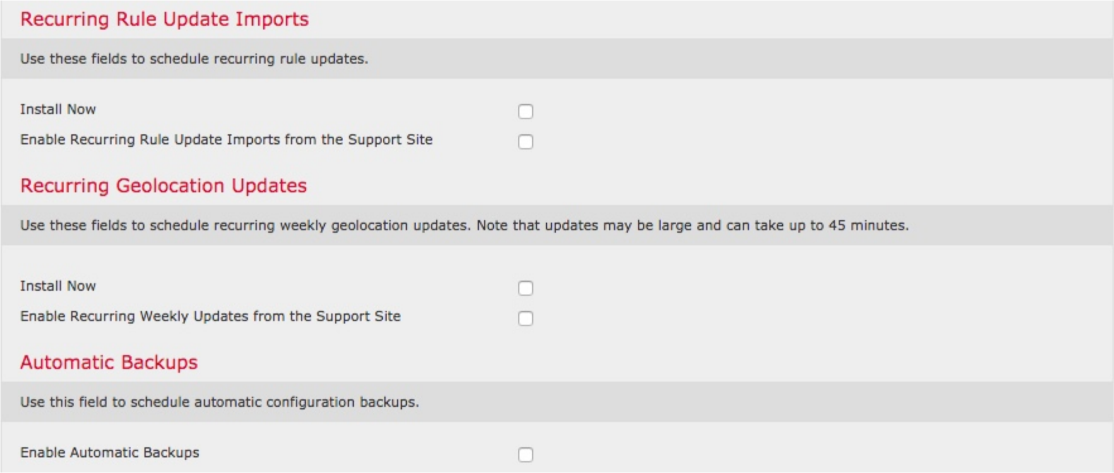
- **Recurring Geolocation Updates**: Firepower Management Centers can display geographical information about the routed IP addresses associated with events generated by the system, as well as monitor geolocation statistics in the dashboard and Context Explorer.

  The Firepower Management Center's geolocation database (GeoDB) contains information such as an IP address's associated Internet service provider (ISP), connection type, proxy information, and exact location. Enabling regular GeoDB updates ensures that the system uses up-to-date geolocation information.

  You can specify the weekly update frequency for the GeoDB. To download the database as part of the initial configuration process, check **Install Now**.

  GeoDB updates might take up to 45 minutes to install after download. You should update the GeoDB during periods of low network use.

- **Enable Automatic Backups**: Creates a scheduled task that creates a weekly backup of the configurations on the Firepower Management Center.



Recurring Rule Update Imports

Use these fields to schedule recurring rule updates.

Install Now □

Enable Recurring Rule Update Imports from the Support Site □

Recurring Geolocation Updates

Use these fields to schedule recurring weekly geolocation updates. Note that updates may be large and can take up to 45 minutes.

Install Now □

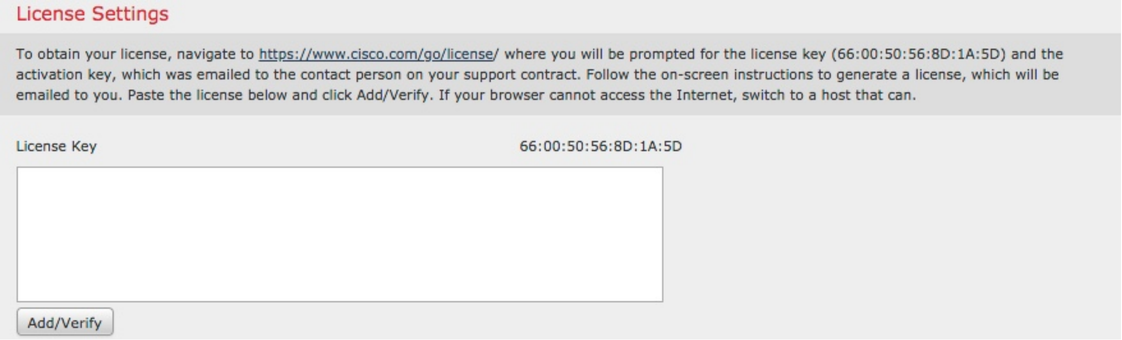
Enable Recurring Weekly Updates from the Support Site □

Automatic Backups

Use this field to schedule automatic configuration backups.

Enable Automatic Backups □

Step 7 Leave the License Settings section blank because it applies to Classic licenses only; you'll apply a Smart License later.

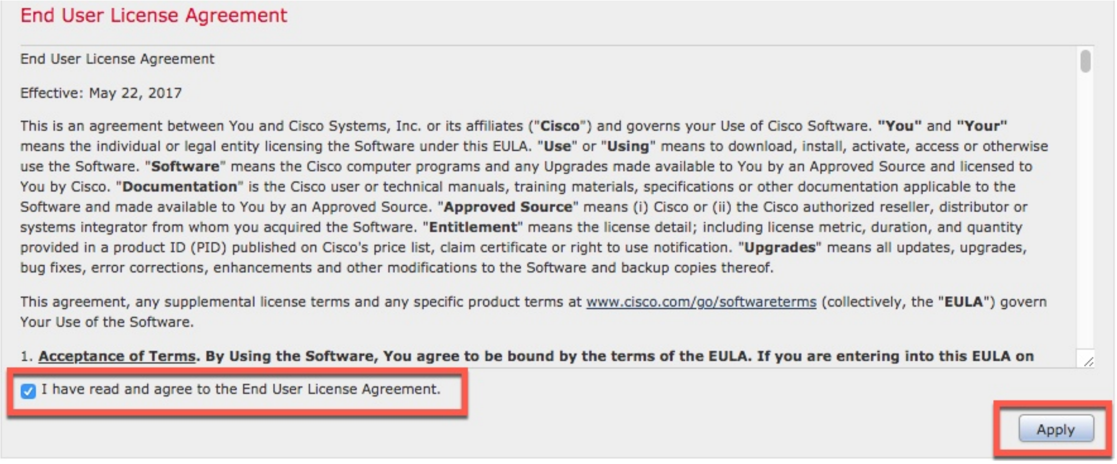


License Settings

To obtain your license, navigate to https://www.cisco.com/go/license/ where you will be prompted for the license key (66:00:50:56:8D:1A:5D) and the activation key, which was emailed to the contact person on your support contract. Follow the on-screen instructions to generate a license, which will be emailed to you. Paste the license below and click Add/Verify. If your browser cannot access the Internet, switch to a host that can.

License Key 66:00:50:56:8D:1A:5D

Step 8 Scroll through the license agreement and, if you agree, check **I have read and agree to the End User License Agreement** and click **Apply**.



End User License Agreement

End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("**Cisco**") and governs your Use of Cisco Software. **"You"** and **"Your"** means the individual or legal entity licensing the Software under this EULA. "**Use**" or "**Using**" means to download, install, activate, access or otherwise use the Software. "**Software**" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "**Documentation**" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "**Approved Source**" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "**Entitlement**" means the license detail; including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "**Upgrades**" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof.

This agreement, any supplemental license terms and any specific product terms at www.cisco.com/go/softwareterms (collectively, the "**EULA**") govern Your Use of the Software.

1. **Acceptance of Terms. By Using the Software, You agree to be bound by the terms of the EULA. If you are entering into this EULA on**

☑ I have read and agree to the End User License Agreement.

Step 9 Wait until the Firepower Management Center processes the information you entered. At that point, the Dashboard is displayed.

What to do next

See License the Firepower Management Center, on page 14.

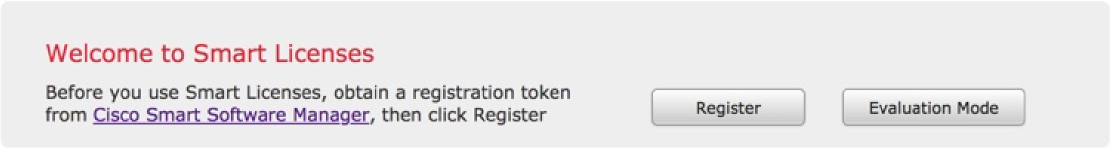
License the Firepower Management Center

This task discusses how to use a 90-day evaluation license with the Firepower Management Center and managed devices. If you have a Smart License, you can use it instead.

Step 1 If necessary, log in to the Firepower Managemet Center.

Step 2 Click **System** > **Licenses** > **Smart Licenses**.

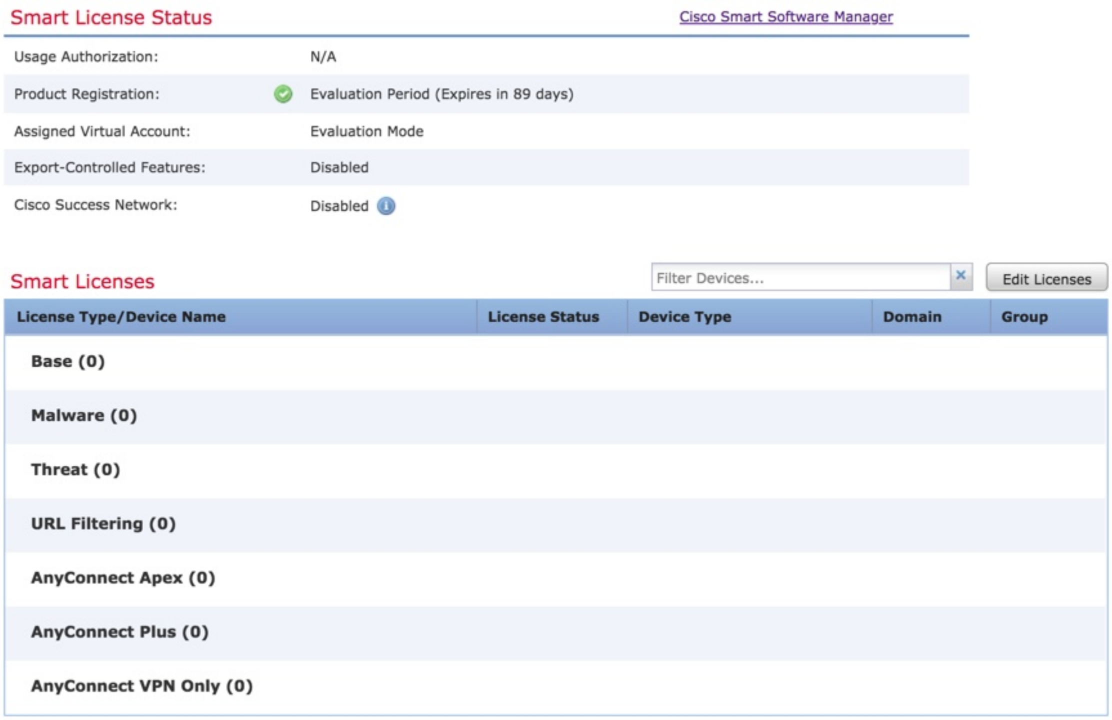
Step 3 Click **Evaluation Mode** for a 90-day evaluation license or click **Register** to register with a Smart License.



Welcome to Smart Licenses

Before you use Smart Licenses, obtain a registration token from Cisco Smart Software Manager, then click Register

Step 4 If you are using an evaluation license, click **Yes** to start the 90-day evaluation period.
If you selected an evaluation license, the following page is displayed.



Smart License Status

Cisco Smart Software Manager

Usage Authorization:	N/A
Product Registration:	✓ Evaluation Period (Expires in 89 days)
Assigned Virtual Account:	Evaluation Mode
Export-Controlled Features:	Disabled
Cisco Success Network:	Disabled

Smart Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
Base (0)				
Malware (0)				
Threat (0)				
URL Filtering (0)				
AnyConnect Apex (0)				
AnyConnect Plus (0)				
AnyConnect VPN Only (0)				

What to do next

See Configure the Managed Device, on page 15.

CHAPTER 4

Configure the Managed Device

Configuring a managed device means adding it to the Firepower Management Center and setting up its interfaces.

- Add a Managed Device to the Firepower Management Center, on page 15
- Configure Managed Device Interfaces, on page 17
- Add Static Routes, on page 19
- Add a NAT Policy, on page 20

Add a Managed Device to the Firepower Management Center

After you add a Firepower Threat Defense as a managed device, you configure it further using the Firepower Management Center.

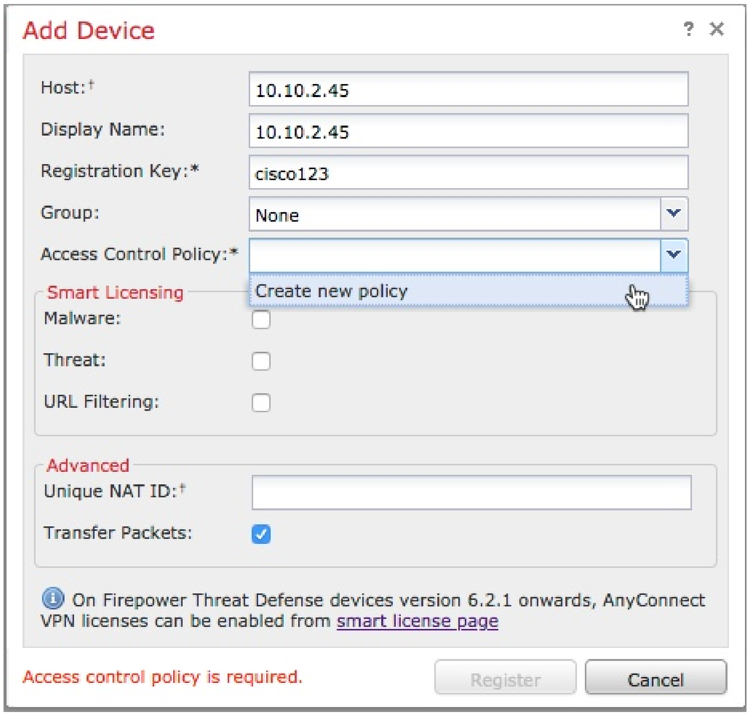
Before you begin

You must complete all of the following tasks first:

- Connect the Firepower Management Center to the Network, on page 7
- Connect the Managed Device to the Network, on page 8
- Configure the Firepower Management Center, on page 11

Step 1 In the Firepower Management Center, click **Devices** > **Device Management**.

Step 2 Click **Add** > **Device**.
Enter the information shown in the following figure.



Add Device

Host:†	10.10.2.45
Display Name:	10.10.2.45
Registration Key:*	cisco123
Group:	None
Access Control Policy:*	Create new policy

Smart Licensing

Malware:	□
Threat:	□
URL Filtering:	□

Advanced

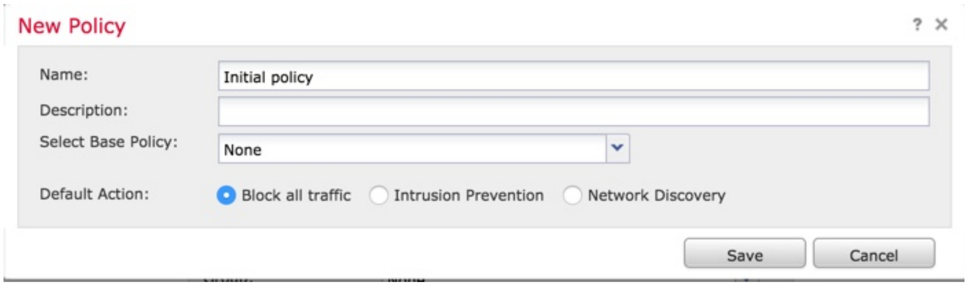
Unique NAT ID:†	
Transfer Packets:	☑

On Firepower Threat Defense devices version 6.2.1 onwards, AnyConnect VPN licenses can be enabled from smart license page

Access control policy is required.

Step 3 From the **Access Control Policy** list, click **Create New Policy**.

Step 4 In the New Policy dialog box, enter a name and, optionally, a description for the policy and click **Block All Traffic** as the following figure shows. (You'll change the default policy action later.)



New Policy

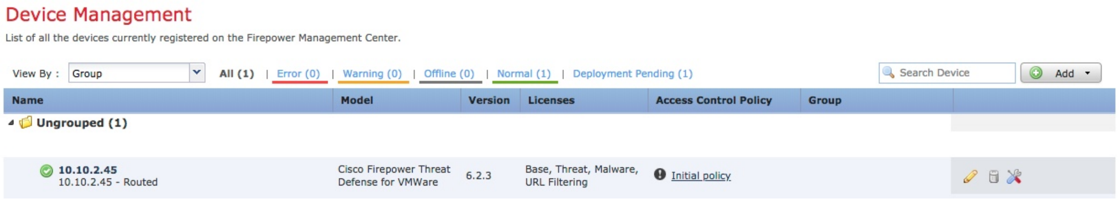
Name:	Initial policy
Description:	
Select Base Policy:	None
Default Action:	● Block all traffic ○ Intrusion Prevention ○ Network Discovery

Step 5 Click **Save**.

Step 6 In the Add Device dialog box, check all the boxes in the Smart Licensing section.

Step 7 Check **Transfer Packets**.

Step 8 Click **Register** and wait for device discovery and registration to complete.
The following page is displayed after the device has been added.



Device Management

List of all the devices currently registered on the Firepower Management Center.

View By : Group | All (1) | Error (0) | Warning (0) | Offline (0) | Normal (1) | Deployment Pending (1)

Name	Model	Version	Licenses	Access Control Policy	Group
Ungrouped (1)					
10.10.2.45 10.10.2.45 - Routed	Cisco Firepower Threat Defense for VMWare	6.2.3	Base, Threat, Malware, URL Filtering	Initial policy	

What to do next

See Configure Managed Device Interfaces, on page 17.

Configure Managed Device Interfaces

This task shows how to configure the managed device's inside and outside interfaces with IP addresses and subnet masks. Refer to the sample network diagram About the Network Setup, on page 2.

Before you begin

See Configure Managed Device Interfaces, on page 17.

Step 1 In the Firepower Management Center, click **Devices** > **Device Management**.

Step 2 Click ✎ (edit) next to your managed device.
The Interfaces tab page is displayed.

Step 3 Click ✎ (edit) next to **GigabitEthernet0/0** to configure the inside interface.

Step 4 From the **Mode** list, click **None**.

Step 5 Check **Enabled**.

Step 6 In the **Name** field, enter `inside`.

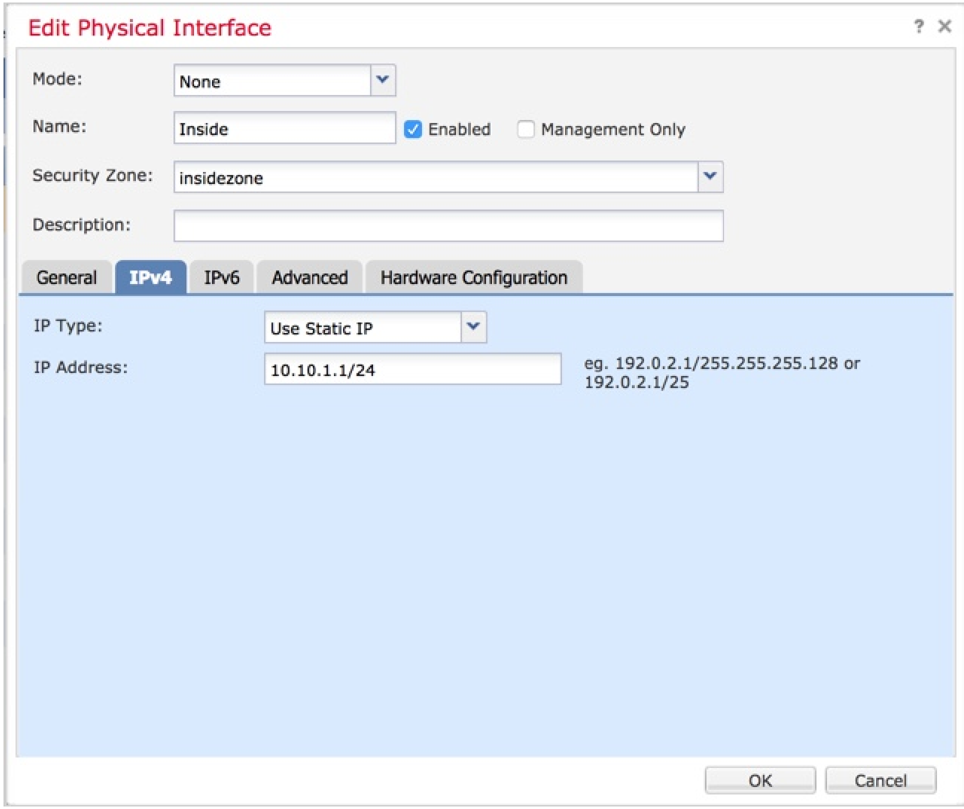
Step 7 From the **Security Zone** list, click **New**.

Step 8 In the New Security Zone dialog box, enter `insidezone` and click **OK**.

Step 9 Click the **IPv4** tab.

Step 10 From the **IP Type** list, click **Use Static IP**.

Step 11 In the **IP Address** field, enter `10.10.1.1/24`.
The following figure shows an example.



Mode: None

Name: Inside ☑ Enabled □ Management Only

Security Zone: insidezone

Description:

IP Type: Use Static IP

IP Address: 10.10.1.1/24 eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Step 12 Click **OK**.

Step 13 Repeat these tasks to configure the remaining interface as follows:

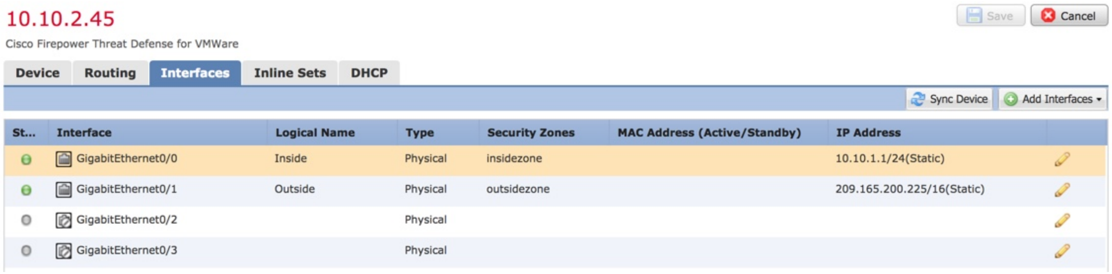
a) **Name**: `outside`
Interface: **GigabitEthernet0/1**

Security Zone: `outsidezone`

IPv4 Address: `209.165.200.255/16`

Note Depending on what type of device you're managing, the interfaces might be identified differently than the preceding. For example, a virtual managed device has interfaces numbered GigabitEthernet0/0, GigabitEthernet0/1, and so on. A Firepower Threat Defense 4100 or 9300 series device has interfaces numbered Ethernet1/1, Ethernet2/1, Ethernet3/1, and so on.

Step 14 At the top of the page, click **Save**.
Your interfaces should be displayed as follows:



St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	
●	GigabitEthernet0/0	Inside	Physical	insidezone		10.10.1.1/24(Static)	✎
●	GigabitEthernet0/1	Outside	Physical	outsidezone		209.165.200.225/16(Static)	✎
○	GigabitEthernet0/2		Physical				✎
○	GigabitEthernet0/3		Physical				✎

What to do next

See Add Static Routes, on page 19.

Add Static Routes

A static route is a one-hop route that causes network traffic to go directly to a mapped resource; in this case, the outside gateway. We recommend setting up a static route in a simple network such as this.

For more information about static and dynamic routing, see Supported Route Types.

Step 1 In the Firepower Management Center, click **Devices** > **Device Management**.

Step 2 Click ✎ (edit) next to your managed device.

Step 3 Click the **Routing** tab.

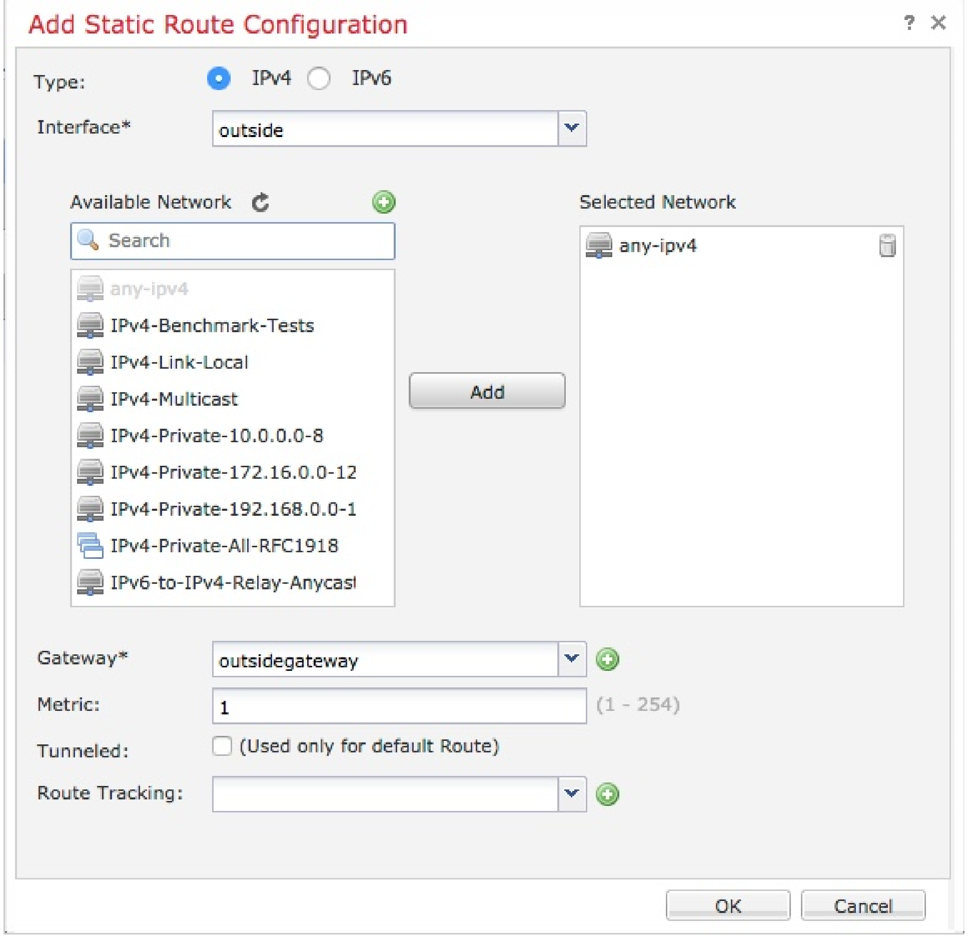
Step 4 Click **Static Route**.

Step 5 Click **Add Route**.

Step 6 Enter the following information in the Add Static Route Configuration dialog box:

Interface
Click **outside**.
Available Network
Add **any-ipv4** to **Selected Networks**
Gateway
Click ⊕ (add) and **Name** the gateway `outsidegateway` with a **Network** value of `209.165.200.254`.

The following figure shows an example.



Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*: outside

Available Network:
- any-ipv4
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12
- IPv4-Private-192.168.0.0-1
- IPv4-Private-All-RFC1918
- IPv6-to-IPv4-Relay-Anycasl

Selected Network: any-ipv4

Gateway*: outsidegateway

Metric: 1 (1 - 254)

Tunneled: □ (Used only for default Route)

Route Tracking:

Step 7 Click **OK**.

Step 8 At the top of the page, click **Save**.

What to do next

See Add a NAT Policy, on page 20.

Add a NAT Policy

The managed device uses NAT to enable communication between internal, non-routable IP addresses (like 10.10.2.1) and the internet. Routable, public IP addresses are scarce; without NAT, you would be severely restricted in the IP addresses you could use. The NAT policy you set up in this task forwards packets from the inside interface to the outside interface.

For more information about NAT, see Why Use NAT?

Step 1 In the Firepower Management Center, click **Devices** > **NAT**.

Step 2 Click **New Policy** > **Threat Defense NAT**.

Step 3 In the New Policy dialog box, enter the following information:

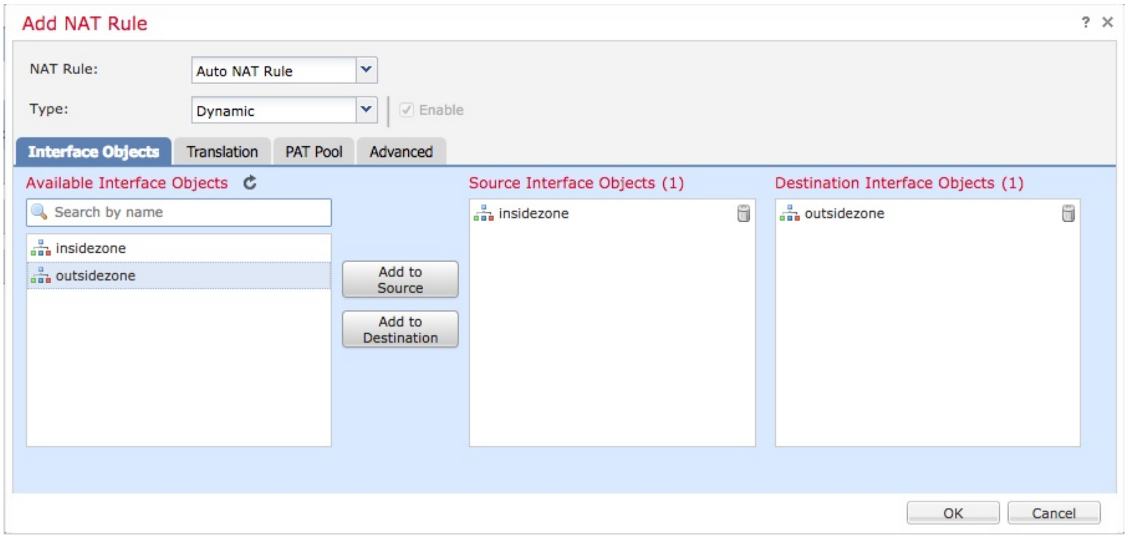
Name
Enter `Inside-Outside-NAT`
Description
Enter an optional description.
Selected Devices
Add 10.10.2.45 to **Selected Devices**.

Step 4 Click **Save**.

Step 5 After the page refreshes, click **Add Rule**.

Step 6 Click the **Interface Objects** tab.

Step 7 Add the security zones you created earlier as source and destination interface objects as follows:



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic ☑ Enable

Available Interface Objects: insidezone, outsidezone

Source Interface Objects (1): insidezone

Destination Interface Objects (1): outsidezone

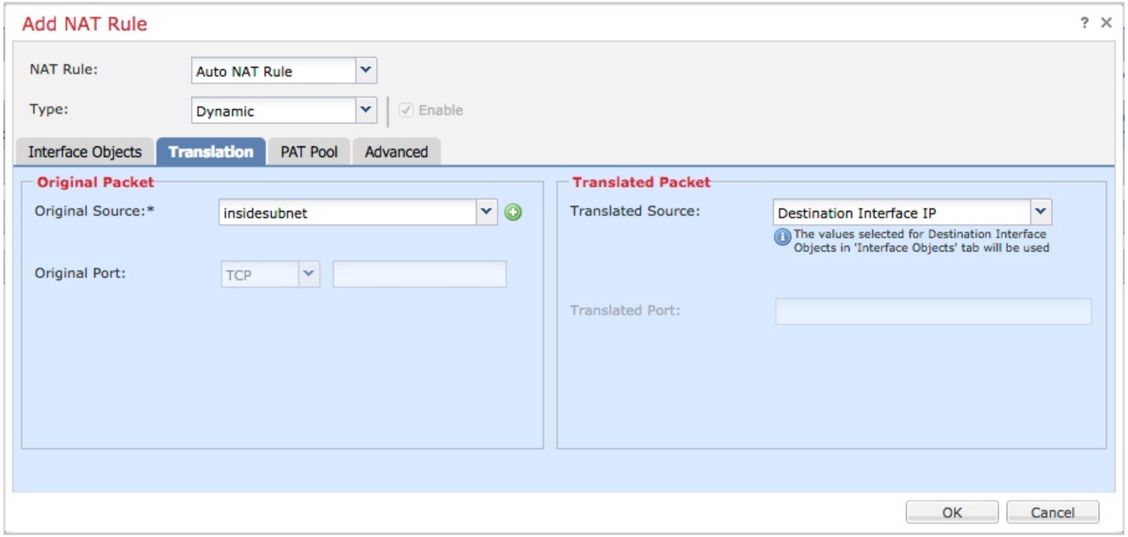
Step 8 Click the **Translation** tab.

Step 9 Click ⊕ (Add) next to **Original Source**.

Step 10 In the New Network Objects dialog box, enter the following information:

Name
Enter `insidesubnet`
Description
Enter an optional description.
Network
Enter `10.10.2.0/24`

Step 11 From the **Translated Source** list, click **Destination Interface IP**.
The following figure shows an example Add NAT Rule dialog box.



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic ☑ Enable

Original Packet

Original Source:* insidesubnet

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:

Step 12 Click **OK**.

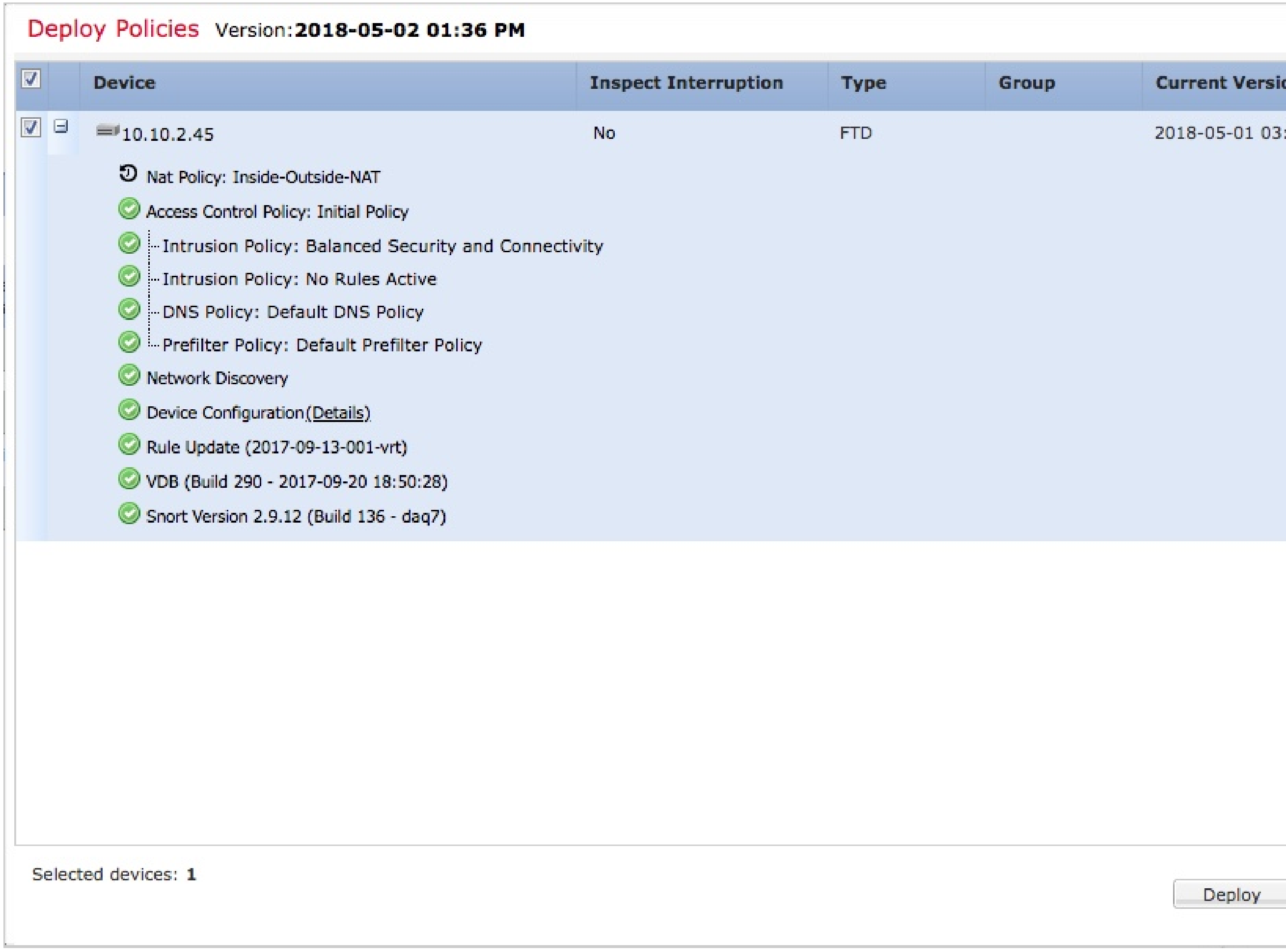
Step 13 At the top of the page, click **Save**.

Step 14 Deploy your changes.

a) At the top of the page, click **Deploy**.

b) Optional. Expand the device to display the changes you're about to make.

c) Check the box to the left of the device.
The following figure shows an example.



Deploy Policies Version:**2018-05-02 01:36 PM**

☑		Device	Inspect Interruption	Type	Group	Current Versi
☑	⊟	10.10.2.45	No	FTD		2018-05-01 03:

- Nat Policy: Inside-Outside-NAT
- ✓ Access Control Policy: Initial Policy
  - ✓ Intrusion Policy: Balanced Security and Connectivity
  - ✓ Intrusion Policy: No Rules Active
  - ✓ DNS Policy: Default DNS Policy
  - ✓ Prefilter Policy: Default Prefilter Policy
- ✓ Network Discovery
- ✓ Device Configuration(Details)
- ✓ Rule Update (2017-09-13-001-vrt)
- ✓ VDB (Build 290 - 2017-09-20 18:50:28)
- ✓ Snort Version 2.9.12 (Build 136 - daq7)

Selected devices: **1**

d) Click **Deploy**.

e) Wait while the changes are deployed; deployment can take several minutes. Messages are displayed to indicate the progress of the deployment.

What to do next

See Test the System, on page 25.

CHAPTER 5

Test the System

To make sure everything is set up properly, you'll create an access control policy to allow all traffic, connect a client to the inside network, and make sure the client can connect to the internet. Finally, you'll monitor traffic on the managed device directly as well as on the Firepower Management Center.

- Edit the Access Control Policy, on page 25
- Test the System, on page 27
- Troubleshoot the System, on page 30

Edit the Access Control Policy

You'll create a temporary access control policy to allow all traffic, with no inspection, from the inside network to the outside network to test the following:

- A client connected to the inside network can connect to the internet.
- Traffic is being filtered through the Firepower Threat Defense device. (The managed device should "see" all the traffic even if it's not being filtered.)

Before you begin

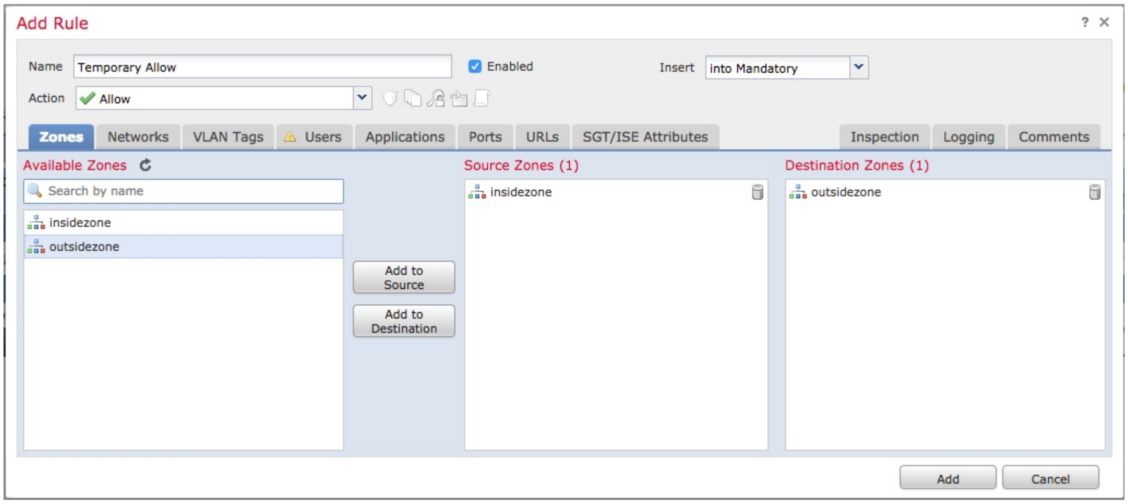
Make sure you have completed all other tasks discussed in this guide before continuing.

Step 1 In the Firepower Management Center, click **Policies** > **Access Control** > **Access Control**.

Step 2 Click ✎ (edit) next to **Initial Policy**.

Step 3 Click **Add Rule**.

Step 4 Enter the following information in the Add Rule dialog box:



Add Rule

Name: Temporary Allow ☑ Enabled Insert: into Mandatory

Action: Allow

Available Zones: insidezone, outsidezone

Source Zones (1): insidezone

Destination Zones (1): outsidezone

Step 5 Click the **Logging** tab.

Step 6 Check **Log at end of connection**.

Step 7 Click **Add**.
The policy page is displayed.

Step 8 On the Initial Policy page, from the **Default Action** list, click **Intrusion Prevention: Balanced Security and Connectivity**.

Step 9 Next to the list, click 📄 (logging).

Step 10 Check **Log at end of connection**.

Step 11 Click **OK**.

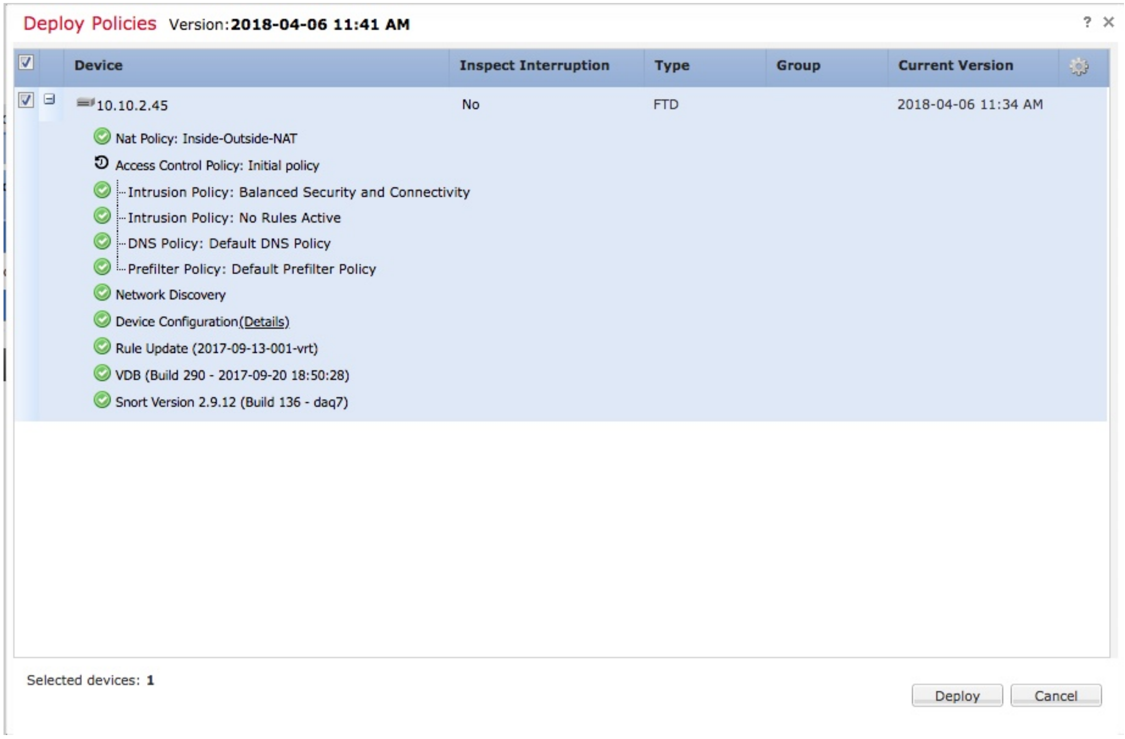
Step 12 At the top of the page, click **Save**.

Step 13 Deploy the changes:

a) At the top of the page, click **Deploy**.

b) Optional. Expand the device to display the changes you're about to make.

c) Check the box to the left of the device.
The following figure shows an example.



Deploy Policies Version:**2018-04-06 11:41 AM**

☑	Device	Inspect Interruption	Type	Group	Current Version
☑ ⊟	10.10.2.45	No	FTD		2018-04-06 11:34 AM

- ✓ Nat Policy: Inside-Outside-NAT
- Access Control Policy: Initial policy
  - ✓ Intrusion Policy: Balanced Security and Connectivity
  - ✓ Intrusion Policy: No Rules Active
  - ✓ DNS Policy: Default DNS Policy
  - ✓ Prefilter Policy: Default Prefilter Policy
- ✓ Network Discovery
- ✓ Device Configuration(Details)
- ✓ Rule Update (2017-09-13-001-vrt)
- ✓ VDB (Build 290 - 2017-09-20 18:50:28)
- ✓ Snort Version 2.9.12 (Build 136 - daq7)

Selected devices: **1**

d) Click **Deploy**.

e) Wait while the changes are deployed; deployment can take several minutes. Messages are displayed to indicate the progress of the deployment.

What to do next

See Test the System, on page 27.

Test the System

To make sure the system is operating normally, connect a client to the inside network and make sure it can reach the internet. While the client is connecting to the internet, use diagnostics in the Firepower Management Center to make sure traffic is passing through it. You can also view connection events.

Before you begin

See Edit the Access Control Policy, on page 25.

Step 1 Connect a client to the managed device's inside network.
The client can run any operating system: Windows, Mac, UNIX, and so on. The details of how to connect the client depend on how your network is set up and are beyond the scope of this guide. If you have access to the network rack in which the managed device is installed, you can directly connect a client to the device's GigabitEthernet 0/1 port.

Step 2 Set up the client with a static IP address of 10.10.1.50 , a default gateway of 10.10.1.1, and any accessible DNS server.

The default gateway should be the IP address of the inside interface. The client contacts this gateway first before sending any traffic to inside or outside addresses.

Step 3 Log in to the Firepower Management Center.

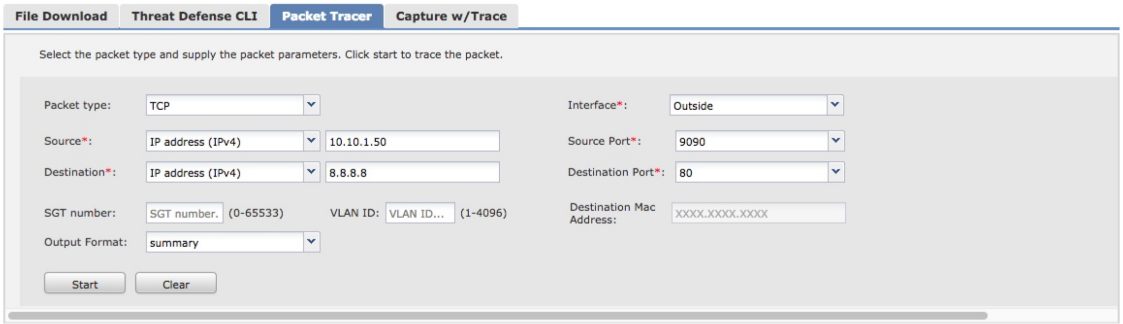
Step 4 Click **Devices** > **Device Management**.

Step 5 Next to your managed device, click 🔧 (Troubleshoot).

Step 6 Click **Advanced Troubleshooting**.

Step 7 Click the **Packet Tracer** tab.

Step 8 Enter the following information in the Packet Tracer tab page.



Select the packet type and supply the packet parameters. Click start to trace the packet.

Packet type: TCP

Source*: IP address (IPv4) 10.10.1.50

Destination*: IP address (IPv4) 8.8.8.8

SGT number: SGT number. (0-65533)

VLAN ID: VLAN ID... (1-4096)

Output Format: summary

Interface*: Outside

Source Port*: 9090

Destination Port*: 80

Destination Mac Address: XXXX.XXXX.XXXX

The values for **Source** IP address and **Source Port** can be anything. What's being tested is whether or not traffic is forwarded from the inside interface to the outside interface. Only the **Destination** IP address and **Destination Port** values are used in this example.

Step 9 On your client, ping or browse to an internet site.

Step 10 On the Packet Tracer tab page, click **Start**.

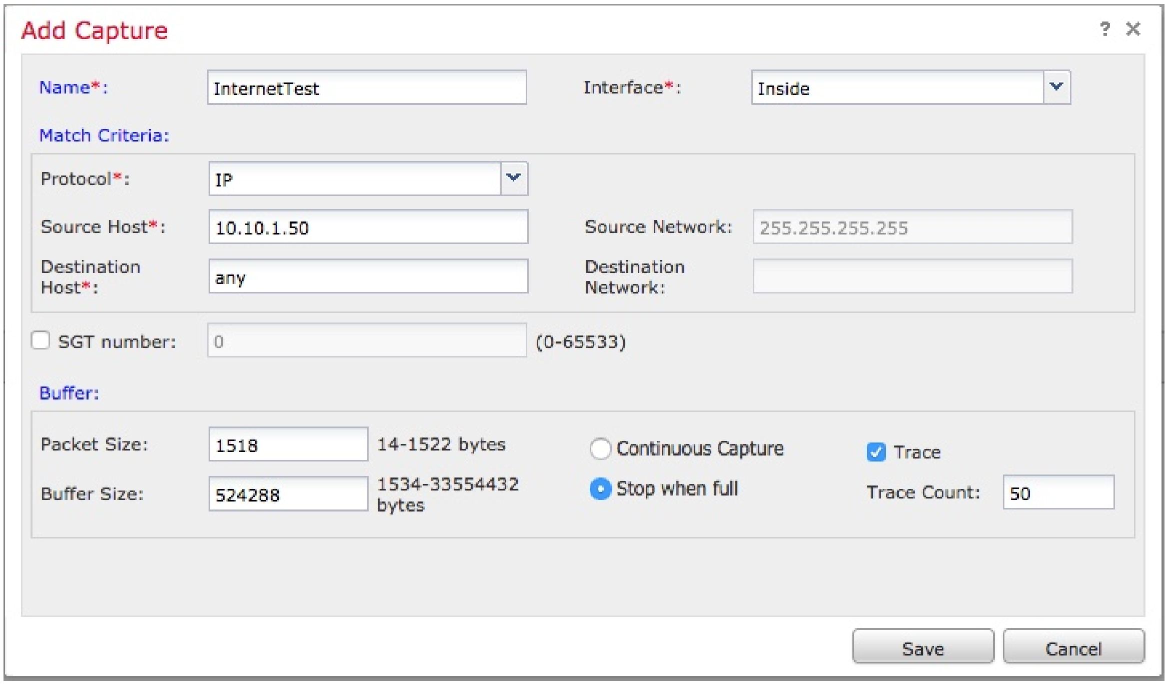
For information about interpreting the results, see Interpret the Results, on page 31.

Step 11 Click the **Capture w/ Trace** tab.

Step 12 Check **Enable Auto-Refresh** and change the refresh interval if desired.

Step 13 Click **Add Capture**.

Step 14 Enter the following information in the Add Capture dialog box.



Add Capture

Name*:	InternetTest	Interface*:	Inside

Match Criteria:

Protocol*:	IP		
Source Host*:	10.10.1.50	Source Network:	255.255.255.255
Destination Host*:	any	Destination Network:	

□ SGT number: 0 (0-65533)

Buffer:

Packet Size:	1518	14-1522 bytes	○ Continuous Capture	☑ Trace	
Buffer Size:	524288	1534-33554432 bytes	● Stop when full	Trace Count:	50

Step 15 Click **Save**.

Step 16 On your client, ping or browse to an internet site.

Step 17 In the bottom pane, click ⟳ (Refresh).

The Firepower Management Center bottom pane displays results of the packet capture and trace. Look for messages like the following, which confirms traffic from the managed device's inside interface is matching your access control policy:

```
Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 2101701398, ack 3091508482
AppID: service HTTP (676), application Adobe Analytics (2846), out-of-order
Firewall: allow rule,  'Temporary Allow Policy' , allow
Snort id 1, NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
```

For additional information about interpreting the results, see Interpret the Results, on page 31.

For more information about the packet tracer, see Packet Tracer Overview.

Step 18 Click **Analysis** > **Connections** > **Events**.

Step 19 In the upper right corner, click ⏱ to adjust the frequency of page updates.

Step 20 Click the **Preferences** tab.

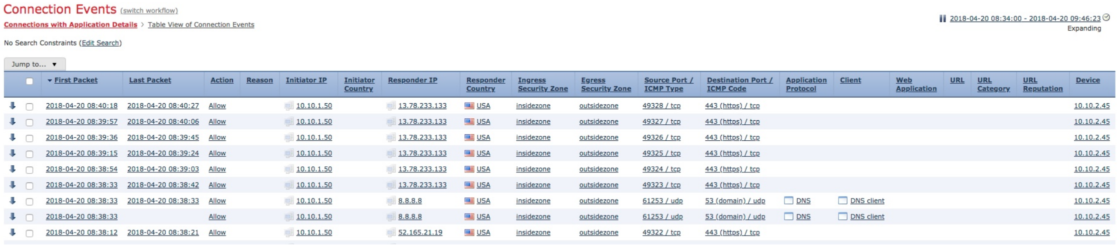
Step 21 In the **Refresh Interval (minutes)** field, enter `1`.

Step 22 Click **Apply**.

Step 23 Navigate away from the page and come back to the Connection Events page.

Step 24 Wait for the page to refresh.

Connection events similar to the following should be displayed.



Connection Events (switch workflow)

Connections with Application Details > Table View of Connection Events

No Search Constraints (Edit Search)

2018-04-20 08:34:00 - 2018-04-20 09:46:23
Expanding

Jump to... ▼

	□	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device
↓	□	2018-04-20 08:40:18	2018-04-20 08:40:27	Allow		10.10.1.50		13.78.233.133	USA	insidezone	outsidezone	49328 / tcp	443 (https) / tcp							10.10.2.45
↓	□	2018-04-20 08:39:57	2018-04-20 08:40:06	Allow		10.10.1.50		13.78.233.133	USA	insidezone	outsidezone	49327 / tcp	443 (https) / tcp							10.10.2.45
↓	□	2018-04-20 08:39:36	2018-04-20 08:39:45	Allow		10.10.1.50		13.78.233.133	USA	insidezone	outsidezone	49326 / tcp	443 (https) / tcp							10.10.2.45
↓	□	2018-04-20 08:39:15	2018-04-20 08:39:24	Allow		10.10.1.50		13.78.233.133	USA	insidezone	outsidezone	49325 / tcp	443 (https) / tcp							10.10.2.45
↓	□	2018-04-20 08:38:54	2018-04-20 08:39:03	Allow		10.10.1.50		13.78.233.133	USA	insidezone	outsidezone	49324 / tcp	443 (https) / tcp							10.10.2.45
↓	□	2018-04-20 08:38:33	2018-04-20 08:38:42	Allow		10.10.1.50		13.78.233.133	USA	insidezone	outsidezone	49323 / tcp	443 (https) / tcp							10.10.2.45
↓	□	2018-04-20 08:38:33	2018-04-20 08:38:33	Allow		10.10.1.50		8.8.8.8	USA	insidezone	outsidezone	61253 / udp	53 (domain) / udp	DNS	DNS client					10.10.2.45
↓	□	2018-04-20 08:38:33		Allow		10.10.1.50		8.8.8.8	USA	insidezone	outsidezone	61253 / udp	53 (domain) / udp	DNS	DNS client					10.10.2.45
↓	□	2018-04-20 08:38:12	2018-04-20 08:38:21	Allow		10.10.1.50		52.165.21.19	USA	insidezone	outsidezone	49322 / tcp	443 (https) / tcp							10.10.2.45

Step 25 To customize the view, click **Table View of Connection Events**.

For more information, see Connection and Security Intelligence Event Fields and Using Connection and Security Intelligence Event Tables.

Step 26 If you see packet capture messages and connection events, congratulations! You have set up your system successfully.

What to do next

If errors are displayed or if your client cannot connect to the internet, see Troubleshoot the System, on page 30.

Troubleshoot the System

This topic discusses solutions to problems you might encounter with your system; typically, no internet access for your network client.

Check the Static Route and Default Gateway

Check the static route and default gateway by pinging an internet site from your managed device as follows:

1. Using an SSH client or a virtual device's management console, log in to your managed device.
2. If required by your managed device, enter **connect ftd**
3. Enter **ping 8.8.8.8**

   Successful results are displayed as follows:

   ```
   Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echoes to 8.8.8.8, timeout is 2 seconds:
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/av/max = 60/62/70 ms
   ```

   If you *cannot* ping an internet IP address, make sure the managed device interfaces are connected properly. Make sure the link and activity LEDs on both ends of the cable are on (activity LED should flash).

Connection Events Not Displayed

The most likely reason connection events are not displayed is that you didn't enable logging in your access control rule or access control policy. See Edit the Access Control Policy, on page 25.

Interpret the Results

This topic discusses how to interpret the results of the packet capture and `traceroute` command.

Interpret Packet Tracer

The following excerpts from the packet tracer show the significant information and decisions made in forwarding traffic from the inside interface to the outside interface. Some of the configuration information discussed in this guide is highlighted. Note the following:

- Phase 3 resolves the outside gateway to 209.165.200.254
- Phase 4 shows the first time the Temporary Allow Policy is invoked
- Phase 6 shows the NAT policy forwarding from the inside client to the outside interface
- Phase 16 shows the inspection engine (Snort) allowing the traffic according to the Temporary Allow Policy

A failure at any of these phases could result in traffic being rejected or dropped, depending on whether policies were configured incorrectly or configured to block the traffic.

```
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 209.165.200.254 using egress ifc  Outside

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip ifc Inside any ifc Outside any rule-id 268434433

access-list CSM_FW_ACL_ remark rule-id 268434433: ACCESS POLICY: Initial Policy - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434433: L7 RULE: Temporary Allow Policy
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
object network insidesubnet
 nat (Inside,Outside) dynamic interface
Additional Information:
Dynamic translate 10.10.1.50/52177 to 209.165.200.225/52177
Phase: 15
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 16
```

```
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: UDP
Session: new snort session
AppID: service DNS (617), application unknown (0)
Firewall: allow rule,  'Temporary Allow Policy' , allow
Snort id 1, NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
```

Note Packet Tracker and Capture w/ Trace might display different phase numbers but the information displayed in each phase should be very similar.

Note If there is no final SNORT phase, look for errors in the ROUTE-LOOKUP phase. For example, the following could indicate there is a problem with your outside interface. Verify its IP address and the IP address of the outside gateway.

```
Phase: 15
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 209.165.200.254 using egress ifc  outside

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-adjacency) No valid adjacency
```

Symptom: No Network Translation

If your packet capture does *not* have a line similar to the following, it likely means NAT is set up incorrectly.

```
Dynamic translate 10.10.1.50/65413 to 209.165.200.225/65413
```

Solution: Set up dynamic NAT as discussed in Add a NAT Policy, on page 20.

Symptom: Access Control Policy is Blocking Traffic

If your access control policy is configured to block traffic instead of allowing it, your packet capture contains the following line:

```
Drop-reason: (acl-drop) Flow is denied by configured rule
```

You can confirm this is the case by looking at connection events: **Analysis** > **Connections** > **Events**.

Solution: Configure your access control policy to allow traffic as discussed in Edit the Access Control Policy, on page 25.