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

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.

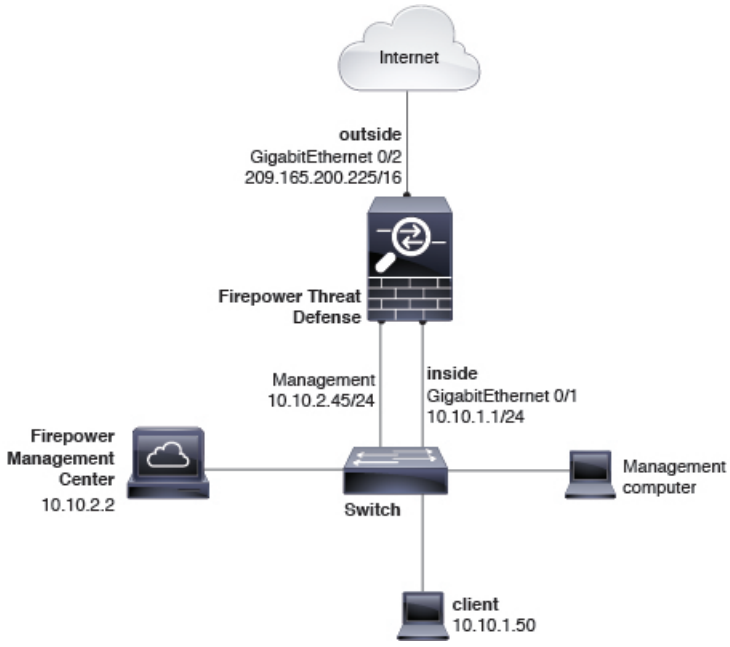
Related Topics

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.
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.
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.
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 the Firepower Management Center for the First Time.

	Command or Action	Purpose
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.
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.
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.
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.
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.