Firepower Management Center Basics

The following topics describe Firepower Management Center basics:

- The Firepower Management Center, on page 1
- Device Management, on page 1
- NAT Environments, on page 3

The Firepower Management Center

You can use the Firepower Management Center to manage the full range of devices that are a part of the Firepower System. When you manage a device, you set up a two-way, SSL-encrypted communication channel between the Firepower Management Center and the device. The Firepower Management Center uses this channel to send information to the device about how you want to analyze and manage your network traffic to the device. As the device evaluates the traffic, it generates events and sends them to the Firepower Management Center using the same channel.

Device Management

The Firepower Management Center is a key component in the Firepower System. You can use the Firepower Management Center to manage the full range of devices that comprise the Firepower System, and to aggregate, analyze, and respond to the threats they detect on your network.

By using the Firepower Management Center to manage devices, you can:

- configure policies for all your devices from a single location, making it easier to change configurations
- install various types of software updates on devices
- push health policies to your managed devices and monitor their health status from the Firepower Management Center

The Firepower Management Center aggregates and correlates intrusion events, network discovery information, and device performance data, allowing you to monitor the information that your devices are reporting in relation to one another, and to assess the overall activity occurring on your network.

You can use a Firepower Management Center to manage nearly every aspect of a device's behavior.

Note Although a Firepower Management Center can manage devices running certain previous releases as specified in the compatibility matrix available at http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html, new features are not available to these previous-release devices.

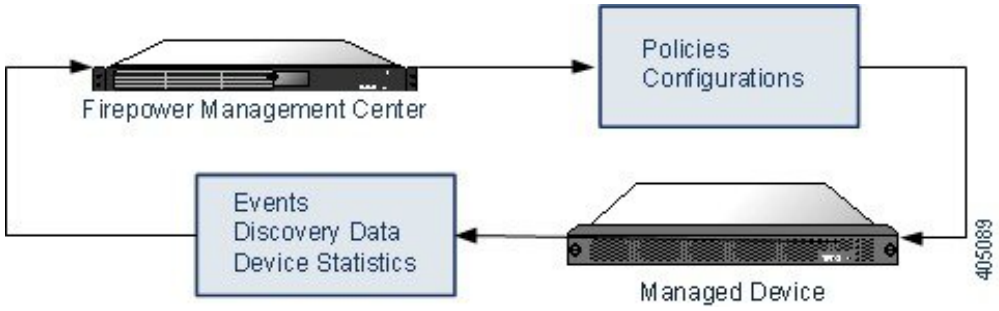
What Can Be Managed by a Firepower Management Center?

You can use the Firepower Management Center as a central management point in a Firepower System deployment to manage the following devices:

- 7000 and 8000 Series devices
- ASA FirePOWER modules
- NGIPSv devices
- Firepower Threat Defense and Firepower Threat Defense Virtual

When you manage a device, information is transmitted between the Firepower Management Center and the device over a secure, SSL-encrypted TCP tunnel.

The following illustration lists what is transmitted between a Firepower Management Center and its managed devices. Note that the types of events and policies that are sent between the appliances are based on the device type.



Beyond Policies and Events

In addition to deploying policies to devices and receiving events from them, you can also perform other device-related tasks on the Firepower Management Center.

Backing Up a Device

You **cannot** create or restore backup files for NGIPSv devices or ASA FirePOWER modules.

When you perform a backup of a physical managed device from the device itself, you back up the device configuration **only**. To back up configuration data and, optionally, unified files, perform a backup of the device using the managing Firepower Management Center.

To back up event data, perform a backup of the managing Firepower Management Center.

Updating Devices

From time to time, Cisco releases updates to the Firepower System, including:

- intrusion rule updates, which may contain new and updated intrusion rules
- vulnerability database updates
- geolocation updates
- software patches and updates

You can use the Firepower Management Center to install an update on the devices it manages.

Related Topics

Backup Files

NAT Environments

Network address translation (NAT) is a method of transmitting and receiving network traffic through a router that involves reassigning the source or destination IP address. The most common use for NAT is to allow private networks to communicate with the internet. Static NAT performs a 1:1 translation, which does not pose a problem for Firepower Management Center communication with devices, but port address translation (PAT) is more common. PAT lets you use a single public IP address and unique ports to access the public network; these ports are dynamically assigned as needed, so you cannot initiate a connection to a device behind a PAT router.

Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the Firepower Management Center specifies the device IP address, and the device specifies the Firepower Management Center IP address. However, if you only know one of the IP addresses, which is the minimum requirement for routing purposes, then you must also specify a unique NAT ID on both sides of the connection to establish trust for the initial communication and to look up the correct registration key. The Firepower Management Center and device use the registration key and NAT ID (instead of IP addresses) to authenticate and authorize for initial registration.

For example, you add a device to the Firepower Management Center, and you do not know the device IP address (for example, the device is behind a PAT router), so you specify only the NAT ID and the registration key. On the device, you specify the Firepower Management Center IP address, the same NAT ID, and the same registration key. The device registers to the Firepower Management Center's IP address. At this point, the Firepower Management Center uses the NAT ID instead of IP address to authenticate the device.

Although the use of a NAT ID is most common for NAT environments, you might choose to use the NAT ID to simplify adding many devices to the Firepower Management Center. On the Firepower Management Center, specify a unique NAT ID for each device you want to add, and then on each device, specify both the Firepower Management Center IP address and the NAT ID. Note: The NAT ID must be unique per device.