Getting Started With Firepower

Cisco Firepower is an integrated suite of network security and traffic management products, deployed either on purpose-built platforms or as a software solution. The system is designed to help you handle network traffic in a way that complies with your organization’s security policy—your guidelines for protecting your network.

In a typical deployment, multiple traffic-sensing managed devices installed on network segments monitor traffic for analysis and report to a manager:

- Firepower Management Center
- Firepower Device Manager
- Adaptive Security Device Manager (ASDM)

Managers provide a centralized management console with graphical user interface that you can use to perform administrative, management, analysis, and reporting tasks.

This guide focuses on the Firepower Management Center managing appliance. For information about the Firepower Device Manager or ASA with FirePOWER Services managed via ASDM, see the guides for those management methods.

- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager
- ASA with FirePOWER Services Local Management Configuration Guide
- Quick Start: Basic Setup, on page 1
- Firepower Devices, on page 5
- Firepower Features, on page 6
- Firepower Online Help, How To, and Documentation, on page 10
- Firepower System IP Address Conventions, on page 13
- Additional Resources, on page 13

Quick Start: Basic Setup

The Firepower feature set is powerful and flexible enough to support basic and advanced configurations. Use the following sections to quickly set up a Firepower Management Center and its managed devices to begin controlling and analyzing traffic.
Installing and Performing Initial Setup on Physical Appliances

Procedure

Install and perform initial setup on all physical appliances using the documentation for your appliance:

- **Firepower Management Center**
  - *Cisco Firepower Management Center Getting Started Guide* for your hardware model, available from
    http://www.cisco.com/go/firepower-mc-install

- **Firepower Threat Defense managed devices**
  - **Important** Ignore Firepower Device Manager documents on these pages.
  - Firepower Threat Defense for the 4100: *Cisco Firepower Threat Defense for Firepower 4100 Quick Start Guide*
    http://www.cisco.com/go/ftd-quick
  - Firepower Threat Defense for the 9300: *Cisco Firepower Threat Defense for Firepower 9300 Quick Start Guide*
    http://www.cisco.com/go/ftd-quick
  - Firepower Threat Defense for the ASA 5508-X/5516-X: *Cisco Firepower Threat Defense for the ASA 5508-X and ASA 5516-X Using Firepower Management Center Quick Start Guide*
    http://www.cisco.com/go/ftd-quick
    http://www.cisco.com/go/ftd-quick
  - Firepower Threat Defense for the ASA 5506-X: *Cisco Firepower Threat Defense for the ASA 5506-X Series Using Firepower Management Center Quick Start Guide*
    http://www.cisco.com/go/ftd-quick

- **Classic managed devices**
  - ASA FirePOWER Services managed device: *Cisco ASA FirePOWER Module Quick Start Guide*
    http://www.cisco.com/go/asafp-quick
  - 8000 Series managed device: *Cisco Firepower 8000 Series Getting Started Guide*
    http://www.cisco.com/go/8000series-install
  - 7000 Series managed device: *Cisco Firepower 7000 Series Getting Started Guide*
Deploying Virtual Appliances

Follow these steps if your deployment includes virtual appliances. Use the documentation roadmap to locate the documents listed below: http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html.

**Procedure**

**Step 1**
Determine the supported virtual platforms you will use for the Management Center and devices (these may not be the same). See the Cisco Firepower Compatibility Guide.

**Step 2**
Deploy virtual Firepower Management Centers using the documentation for your environment:

- Firepower Management Center Virtual running on VMware: *Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide*
- Firepower Management Center Virtual running on AWS: *Cisco Firepower Management Center Virtual for AWS Deployment Quick Start Guide*
- Firepower Management Center Virtual running on KVM: *Cisco Firepower Management Center Virtual for KVM Deployment Quick Start Guide*

**Step 3**
Deploy virtual devices using the documentation for your appliance:

- NGIPSv running on VMware: *Cisco Firepower NGIPSv Quick Start Guide for VMware*
- Firepower Threat Defense Virtual running on VMware: *Cisco Firepower Threat Defense for the ASA 5508-X and ASA 5516-X Using Firepower Management Center Quick Start Guide*
- Firepower Threat Defense Virtual running on AWS: *Cisco Firepower Threat Defense Virtual for AWS Deployment Quick Start Guide*
- Firepower Threat Defense Virtual running on KVM: *Cisco Firepower Threat Defense Virtual for KVM Deployment Quick Start Guide*
- Firepower Threat Defense Virtual running on Azure: *Cisco Firepower Threat Defense Virtual for Azure Deployment Quick Start Guide*

**Logging In for the First Time**

**Before you begin**

- Prepare your appliances as described in Installing and Performing Initial Setup on Physical Appliances, on page 2 or Deploying Virtual Appliances, on page 3.
Procedure

Step 1 Log in to the Firepower Management Center web interface with admin as the username and Admin123 as the password. Change the password for this account as described in the Quick Start Guide for your appliance.

Step 2 Set a time zone for this account as described in Setting Your Default Time Zone.

Step 3 Add licenses as described in Licensing the Firepower System.

Step 4 Register managed devices as described in Add Devices to the Firepower Management Center.

Step 5 Configure your managed devices as described in:

- Introduction to IPS Device Deployment and Configuration, to configure passive or inline interfaces on 7000 Series or 8000 Series devices
- About FTD Interfaces, to configure transparent or routed mode on Firepower Threat Defense devices
- About FTD Interfaces, to configure interfaces on Firepower Threat Defense devices

What to do next

- Begin controlling and analyzing traffic by configuring basic policies as described in Setting Up Basic Policies and Configurations, on page 4.

Setting Up Basic Policies and Configurations

You must configure and deploy basic policies in order to see data in the dashboard, Context Explorer, and event tables.

Note

This is not a full discussion of policy or feature capabilities. For guidance on other features and more advanced configurations, see the rest of this guide.

Before you begin

- Log into the web interface, set your time zone, add licenses, register devices, and configure devices as described in Logging In for the First Time, on page 3.

Procedure

Step 1 Configure an access control policy as described in Creating a Basic Access Control Policy.

- In most cases, Cisco suggests setting the Balanced Security and Connectivity intrusion policy as your default action. For more information, see Access Control Policy Default Action and System-Provided Network Analysis and Intrusion Policies.

- In most cases, Cisco suggests enabling connection logging to meet the security and compliance needs of your organization. Consider the traffic on your network when deciding which connections to log so
that you do not clutter your displays or overwhelm your system. For more information, see About Connection Logging.

**Step 2**
Apply the system-provided default health policy as described in Applying Health Policies.

**Step 3**
Customize a few of your system configuration settings:

- If you want to allow inbound connections for a service (for example, SNMP or the syslog), modify the ports in the access list as described in Configuring the Access List for Your System.
- Understand and consider editing your database event limits as described in Configuring Database Event Limits.
- If you want to change the display language, edit the language setting as described in Specifying a Different Language.
- If your organization restricts network access using a proxy server and you did not configure proxy settings during initial configuration, edit your proxy settings as described in Configure Firepower Management Center Management Interfaces.

**Step 4**
Customize your network discovery policy as described in Configuring the Network Discovery Policy. By default, the network discovery policy analyzes all traffic on your network. In most cases, Cisco suggests restricting discovery to the addresses in RFC 1918.

**Step 5**
Consider customizing these other common settings:

- If you do not want to display message center pop-ups, disable notifications as described in Configuring Notification Behavior.
- If you want to customize the default values for system variables, understand their use as described in Variable Sets.
- If you want to update the Geolocation Database, update manually or on a scheduled basis as described in Update the Geolocation Database (GeoDB).
- If you want to create additional locally authenticated user accounts to access the appliance, see Creating a User Account.
- If you want to use LDAP or RADIUS external authentication to allow access to the appliance, see External Authentication.

**Step 6**
Deploy configuration changes; see Deploy Configuration Changes.

---

**What to do next**

- Review and consider configuring other features described in Firepower Features, on page 6 and the rest of this guide.

---

**Firepower Devices**

In a typical deployment, multiple traffic-handling devices installed on network segments monitor traffic for analysis and report to either a physical or virtual Firepower Management Center. The Firepower Management
Center provides a centralized management console with graphical user interface that you can use to perform administrative, management, analysis, and reporting tasks.

This section describes the Firepower implementations you can install on traffic-handling devices and manage with the Firepower Management Center.


Firepower Threat Defense (NGFW)

Lightweight software that provides a unified next-generation firewall (NGFW) and next-generation IPS (NGIPS) device, on either a physical or virtual platform. In addition to the NGIPS features available on Firepower software models, NGFW and platform features include Site-to-Site VPN, robust routing, NAT, clustering, and other optimizations in application inspection and access control.

Firepower Software (NGIPS)

NGIPS software running on 7000 and 8000 Series Firepower devices, or hosted on VMware.

ASA with FirePOWER Services (NGIPS)

NGIPS software running on an ASA device. The ASA device provides the first-line system policy, then passes traffic to an ASA FirePOWER module for discovery and access control.

ASA FirePOWER has a software and a command line interface (CLI) unique to the ASA platform. You use these ASA-specific tools to install the system and to perform other platform-specific administrative tasks.

ASA FirePOWER does not support the following Firepower features:

- Features for Firepower hardware—Use the ASA CLI and ASDM to configure device high availability, stacking, switching, routing, VPN, NAT, and so on. See the ASA documentation for more information.
- Interface configuration—You cannot use the Firepower Management Center web interface to configure ASA FirePOWER interfaces. The Firepower Management Center does not display ASA interfaces when the ASA FirePOWER is deployed in SPAN port mode.
- Process management—You cannot use the Firepower Management Center to shut down, restart, or otherwise manage ASA FirePOWER processes.

Firepower Features

These tables list some commonly used Firepower features.

Appliance and System Management Features

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Configure...</th>
<th>As described in...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage user accounts for logging in to your Firepower appliances</td>
<td>Firepower authentication</td>
<td>Firepower System User Authentication</td>
</tr>
<tr>
<td>Monitor the health of system hardware and software</td>
<td>Health monitoring policy</td>
<td>About Health Monitoring</td>
</tr>
<tr>
<td>Back up data on your appliance</td>
<td>Backup and restore</td>
<td>Backup and Restore Support</td>
</tr>
<tr>
<td>Upgrade to a new Firepower version</td>
<td>System updates</td>
<td>Firepower Management Center Upgrade Guide</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Firepower Release Notes</td>
</tr>
<tr>
<td>Baseline your physical appliance</td>
<td>Restore to factory defaults (reimage)</td>
<td>The Firepower Management Center Upgrade Guide, for a list of links to instructions on performing fresh installations.</td>
</tr>
<tr>
<td>Update the VDB, intrusion rule updates, or GeoDB on your appliance</td>
<td>Vulnerability Database (VDB) updates, intrusion rule updates, or Geolocation Database (GeoDB) updates</td>
<td>System Software Updates</td>
</tr>
<tr>
<td>Apply licenses in order to take advantage of license-controlled functionality</td>
<td>Classic licensing or Smart licensing</td>
<td>About Firepower Feature Licenses</td>
</tr>
<tr>
<td>Ensure continuity of appliance operations</td>
<td>Managed device high availability and/or Firepower Management Center high availability</td>
<td>About 7000 and 8000 Series Device High Availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>About Firepower Threat Defense High Availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>About Firepower Management Center High Availability</td>
</tr>
<tr>
<td>Combine processing resources of multiple 8000 Series devices</td>
<td>Device stacking</td>
<td>About Device Stacks</td>
</tr>
<tr>
<td>Configure a device to route traffic between two or more interfaces</td>
<td>Routing</td>
<td>Virtual Routers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Routing Overview for Firepower Threat Defense</td>
</tr>
<tr>
<td>Configure packet switching between two or more networks</td>
<td>Device switching</td>
<td>Virtual Switches</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configure Bridge Group Interfaces</td>
</tr>
<tr>
<td>Translate private addresses into public addresses for internet connections</td>
<td>Network Address Translation (NAT)</td>
<td>NAT Policy Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network Address Translation (NAT) for Firepower Threat Defense</td>
</tr>
</tbody>
</table>
High Availability, Clustering, and Stacking Features by Appliance

You can deploy Firepower appliances in high availability, clustered, and stacked configurations, as described below.

High availability configurations (sometimes called failover) ensure continuity of operations. Clustered and stacked configurations group multiple devices together as a single logical device, achieving increased throughput and redundancy.

<table>
<thead>
<tr>
<th>Appliance</th>
<th>High Availability</th>
<th>Clustering</th>
<th>Stacking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower Management Center</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Firepower Management Center Virtual</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Firepower NGIPS running on:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firepower 7010, 7020, 7030, 7050</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Firepower 7110, 7115, 7120, 7125, AMP7150</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firepower 8120, 8130, AMP8050, AMP8150</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firepower NGIPS running on:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firepower 8140</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>Firepower 8250, 8260, 8270, 8290</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firepower 8350, 8360, 8370, 8390, AMP8350</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firepower Threat Defense running on:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual: VMware</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Virtual: KVM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firepower Threat Defense running on:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Cloud: AWS</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Public Cloud: Azure</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Appliance

<table>
<thead>
<tr>
<th>Appliance</th>
<th>High Availability</th>
<th>Clustering</th>
<th>Stacking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower Threat Defense running on: Firepower 9300</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Firepower Threat Defense running on: Firepower 4110, 4120, 4140, 4150</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>

### Related Topics
- About 7000 and 8000 Series Device High Availability
- About Firepower Threat Defense High Availability
- About Firepower Management Center High Availability

### Features for Detecting, Preventing, and Processing Potential Threats


<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Configure...</th>
<th>As described in...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inspect, log, and take action on network traffic</td>
<td>Access control policy, the parent of several other policies</td>
<td>Introduction to Access Control</td>
</tr>
<tr>
<td>Blacklist connections to or from IP addresses, URLs, and/or domain names</td>
<td>Security Intelligence within your access control policy</td>
<td>About Security Intelligence</td>
</tr>
<tr>
<td>Control the websites that users on your network can access</td>
<td>URL filtering within your policy rules</td>
<td>URL Conditions (URL Filtering)</td>
</tr>
<tr>
<td>Monitor malicious traffic and intrusions on your network</td>
<td>Intrusion policy</td>
<td>Intrusion Policy Basics</td>
</tr>
<tr>
<td>Block encrypted traffic without inspection</td>
<td>SSL policy</td>
<td>SSL Policies Overview</td>
</tr>
<tr>
<td>Inspect encrypted or decrypted traffic</td>
<td>Prefilter policy</td>
<td>Introduction to Prefiltering</td>
</tr>
<tr>
<td>Tailor deep inspection to encapsulated traffic and improve performance with fastpathing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rate limit network traffic that is allowed or trusted by access control</td>
<td>Quality of Service (QoS) policy</td>
<td>About QoS Policies</td>
</tr>
<tr>
<td>Allow or block files (including malware) on your network</td>
<td>File/malware policy</td>
<td>File Policies</td>
</tr>
</tbody>
</table>
If you want to... | Configure... | As described in...
---|---|---
Query a public or private cloud for continuous file analysis | AMP cloud connection | AMP Cloud Connections
Configure passive or active user authentication to perform user awareness and user control | User awareness, user identity, identity policies | About Realms and Identity Policies
Collect host, application, and user data from traffic on your network to perform user awareness | Network Discovery policies | Overview: Network Discovery Policies
Perform application detection and control | Application detectors | Overview: Application Detection
Troubleshoot issues | N/A | Troubleshooting the System

Integration with External Tools


If you want to... | Configure... | As described in...
---|---|---
Automatically launch remediations when conditions on your network violate an associated policy | Remediations | Introduction to Remediations
Stream event data from a Firepower Management Center to a custom-developed client application | eStreamer integration | eStreamer Server Streaming
Query database tables on a Firepower Management Center using a third-party client | External database access | External Database Access Settings
Augment discovery data by importing data from third-party sources | Host input | Host Input Data
Troubleshoot issues | N/A | Troubleshooting the System

Firepower Online Help, How To, and Documentation

You can reach the online help from the web interface:

- By clicking the context-sensitive help link on each page
• By choosing Help > Online

You can find additional documentation related to the Firepower system using the documentation roadmap:

Top-Level Documentation Listing Pages for Firepower Management Center Deployments

The following documents may be helpful when configuring Firepower Management Center deployments, Version 6.0+

Note
Some of the linked documents are not applicable to Firepower Management Center deployments. For example, some links on Firepower Threat Defense pages are specific to deployments managed by Firepower Device Manager, and some links on hardware pages are unrelated to Firepower. To avoid confusion, pay careful attention to document titles. Also, some documents cover multiple products and therefore may appear on multiple product pages.

Firepower Management Center

• Firepower Management Center hardware appliances:

• Firepower Management Center Virtual appliances:

Firepower Threat Defense, also called NGFW (Next Generation Firewall) devices

• Firepower Threat Defense software:

• Firepower Threat Defense Virtual:

• Firepower 4100 series:

• Firepower 9300:

• ASA 5500-X series:
License Statements in the Documentation

The License statement at the beginning of a section indicates which Classic or Smart license you must assign to a managed device in the Firepower System to enable the feature described in the section. Because licensed capabilities are often additive, the license statement provides only the highest required license for each feature.

An “or” statement in a License statement indicates that you must assign a particular license to the managed device to enable the feature described in the section, but an additional license can add functionality. For example, within a file policy, some file rule actions require that you assign a Protection license to the device while others require that you assign a Malware license.

For more information about licenses, see About Firepower Feature Licenses.

Related Topics

About Firepower Feature Licenses
**Supported Devices Statements in the Documentation**

The Supported Devices statement at the beginning of a chapter or topic indicates that a feature is supported only on the specified device series, family, or model. For example, stacking is supported only on 8000 Series devices.

For more information on platforms supported by this release, see the release notes.

**Access Statements in the Documentation**

The Access statement at the beginning of each procedure in this documentation indicates the predefined user roles required to perform the procedure. Any of the listed roles can perform the procedure.

Users with custom roles may have permission sets that differ from those of the predefined roles. When a predefined role is used to indicate access requirements for a procedure, a custom role with similar permissions also has access. Some users with custom roles may use slightly different menu paths to reach configuration pages. For example, users who have a custom role with only intrusion policy privileges access the network analysis policy via the intrusion policy instead of the standard path through the access control policy.

For more information about user roles, see Predefined User Roles and Custom User Roles.

**Firepower System IP Address Conventions**

You can use IPv4 Classless Inter-Domain Routing (CIDR) notation and the similar IPv6 prefix length notation to define address blocks in many places in the Firepower System.

When you use CIDR or prefix length notation to specify a block of IP addresses, the Firepower System uses only the portion of the network IP address specified by the mask or prefix length. For example, if you type 10.1.2.3/8, the Firepower System uses 10.0.0.0/8.

In other words, although Cisco recommends the standard method of using a network IP address on the bit boundary when using CIDR or prefix length notation, the Firepower System does not require it.

**Additional Resources**

The Firewalls Community is an exhaustive repository of reference material that complements our extensive documentation. This includes links to 3D models of our hardware, hardware configuration selector, product collateral, configuration examples, troubleshooting tech notes, training videos, lab and Cisco Live sessions, social media channels, Cisco Blogs and all the documentation published by the Technical Publications team.

Some of the individuals posting to community sites or video sharing sites, including the moderators, work for Cisco Systems. Opinions expressed on those sites and in any corresponding comments are the personal opinions of the original authors, not of Cisco. The content is provided for informational purposes only and is not meant to be an endorsement or representation by Cisco or any other party.

---

**Note**

Some of the videos, technical notes, and reference material in the Firewalls Community points to older versions of the Firepower Management Center. Your version of the Firepower Management Center and the version referenced in the videos or technical notes might have differences in the user interface that cause the procedures not to be identical.