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

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.

  - Cisco Firepower 4100 Getting Started Guide
  - Cisco Firepower 9300 Getting Started Guide
  - Cisco Firepower Threat Defense for the ASA 5508-X and ASA 5516-X Using Firepower Management Center Quick Start Guide
  - Cisco Firepower Threat Defense for the ASA 5506-X Series Using Firepower Management Center Quick Start Guide
  - Cisco Firepower Threat Defense for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X Using Firepower Management Center Quick Start Guide

- **Classic managed devices**
  - Cisco ASA FirePOWER Module Quick Start Guide
  - Cisco Firepower 8000 Series Getting Started Guide
  - 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 2.

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 a Device to the FMC.

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
- Interface Overview for Firepower Threat Defense, to configure transparent or routed mode on Firepower Threat Defense devices

- Interface Overview for Firepower Threat Defense, 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 Configure an Access List.
- 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 Set the Language for the Web Interface.

- If your organization restricts network access using a proxy serverand you did not configure proxy settings during initial configuration, edit your proxy settings as described in Modify FMC 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 FMC, see Creating a User Account.
- If you want to use LDAP or RADIUS external authentication to allow access to the FMC, 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 report to one Firepower Management Center, which you use to perform administrative, management, analysis, and reporting tasks.

Classic Devices

Classic devices run next-generation IPS (NGIPS) software. They include:

- Firepower 7000 series and Firepower 8000 series physical devices.
- NGIPSv, hosted on VMware.
- ASA with FirePOWER Services, available on select ASA 5500-X series devices. The ASA provides the first-line system policy, and then passes traffic to an ASA FirePOWER module for discovery and access control.

  Note that you must use the ASA CLI or ASDM to configure the ASA-based features on an ASA FirePOWER device. This includes device high availability, switching, routing, VPN, NAT, and so on. You cannot use the FMC to configure ASA FirePOWER interfaces, and the FMC GUI does not display

ASA interfaces when the ASA FirePOWER is deployed in SPAN port mode. Also, you cannot use the FMC to shut down, restart, or otherwise manage ASA FirePOWER processes.

Firepower Threat Defense Devices

A Firepower Threat Defense (FTD) device is a next-generation firewall (NGFW) that also has NGIPS capabilities. NGFW and platform features include site-to-site VPN, robust routing, NAT, clustering, and other optimizations in application inspection and access control.

FTD is available on a wide range of physical and virtual platforms.

Compatibility

For details on manager-device compatibility, including the software compatible with specific device models, virtual hosting environments, operating systems, and so on, see the Cisco Firepower Release Notes and Cisco Firepower Compatibility Guide.

Firepower Features

These tables list some commonly used Firepower features.

Appliance and System Management Features

To locate unfamiliar documents, see: http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html.

If you want to...	Configure...	As described in...
Manage user accounts for logging in to your Firepower appliances	Firepower authentication	Firepower System User Authentication
Monitor the health of system hardware and software	Health monitoring policy	About Health Monitoring
Back up data on your appliance	Backup and restore	Backup and Restore
Upgrade to a new Firepower version	System updates	Cisco Firepower Management Center Upgrade Guide, Versions 6.0–7.0 Firepower Release Notes
Baseline your physical appliance	Restore to factory defaults (reimage)	The Cisco Firepower Management Center Upgrade Guide, Versions 6.0–7.0, for a list of links to instructions on performing fresh installations.
Update the VDB, intrusion rule updates, or GeoDB on your appliance	Vulnerability Database (VDB) updates, intrusion rule updates, or Geolocation Database (GeoDB) updates	System Updates

If you want to...	Configure...	As described in...
Apply licenses in order to take advantage of license-controlled functionality	Classic or Smart licensing	About Firepower Licenses
Ensure continuity of appliance operations	Managed device high availability and/or Firepower Management Center high availability	About 7000 and 8000 Series Device High Availability About Firepower Threat Defense High Availability About Firepower Management Center High Availability
Combine processing resources of multiple 8000 Series devices	Device stacking	About Device Stacks
Configure a device to route traffic between two or more interfaces	Routing	Virtual Routers Routing Overview for Firepower Threat Defense
Configure packet switching between two or more networks	Device switching	Virtual Switches Configure Bridge Group Interfaces
Translate private addresses into public addresses for internet connections	Network Address Translation (NAT)	NAT Policy Configuration Network Address Translation (NAT) for Firepower Threat Defense
Establish a secure tunnel between managed Firepower Threat Defense or 7000/8000 Series devices	Site-to-Site virtual private network (VPN)	VPN Overview for Firepower Threat Defense
Segment user access to managed devices, configurations, and events	Multitenancy using domains	Introduction to Multitenancy Using Domains
View and manage appliance configuration using a REST API client	REST API and REST API Explorer	REST API Preferences *Firepower REST API Quick Start Guide*
Troubleshoot issues	N/A	Troubleshooting the System

High Availability and Scalability Features by Platform

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.

Platform	High Availability	Clustering	Stacking
Firepower Management Center	Yes Except MC750	—	—
Firepower Management Center Virtual	—	—	—
Firepower Threat Defense Virtual: • VMware • KVM	Yes	—	—
Firepower Threat Defense Virtual (public cloud): • AWS • Public Cloud: Azure	—	—	—
Firepower Threat Defense: • ASA 5500-X series	Yes	—	—
Firepower Threat Defense: • Firepower 4100/9300 chassis	Yes	Yes	—
Firepower NGIPS: • Firepower 7010, 7020, 7030, 7050 • Firepower 7110, 7115, 7120, 7125 • Firepower 8120, 8130 • AMP 7150, 8050, 8150	Yes	—	—
Firepower NGIPS: • Firepower 8140 • Firepower 8250, 8260, 8270, 8290 • Firepower 8350, 8360, 8370, 8390 • AMP 8350	Yes	—	Yes
Firepower NGIPS: • ASA FirePOWER • NGIPSv	—	—	—

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

To locate unfamiliar documents, see: http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html.

If you want to...	Configure...	As described in...
Inspect, log, and take action on network traffic	Access control policy, the parent of several other policies	Introduction to Access Control
Block or monitor connections to or from IP addresses, URLs, and/or domain names	Security Intelligence within your access control policy	About Security Intelligence
Control the websites that users on your network can access	URL filtering within your policy rules	URL Filtering
Monitor malicious traffic and intrusions on your network	Intrusion policy	Intrusion Policy Basics
Block encrypted traffic without inspection Inspect encrypted or decrypted traffic	SSL policy	SSL Policies Overview
Tailor deep inspection to encapsulated traffic and improve performance with fastpathing	Prefilter policy	About Prefiltering
Rate limit network traffic that is allowed or trusted by access control	Quality of Service (QoS) policy	About QoS Policies
Allow or block files (including malware) on your network	File/malware policy	File Policies and Malware Protection
Configure passive or active user authentication to perform user awareness and user control	User awareness, user identity, identity policies	About Realms and Identity Policies About 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

To locate unfamiliar documents, see: http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html.

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

Switching Domains on the Firepower Management Center

In a multidomain deployment, user role privileges determine which domains a user can access and which privileges the user has within each of those domains. You can associate a single user account with multiple domains and assign different privileges for that user in each domain. For example, you can assign a user read-only privileges in the Global domain, but Administrator privileges in a descendant domain.

Users associated with multiple domains can switch between domains within the same web interface session.

Under your user name in the toolbar, the system displays a tree of available domains. The tree:

- Displays ancestor domains, but may disable access to them based on the privileges assigned to your user account.
- Hides any other domain your user account cannot access, including sibling and descendant domains.

When you switch to a domain, the system displays:

- Data that is relevant to that domain only.
- Menu options determined by the user role assigned to you for that domain.

Procedure

From the drop-down list under your user name, choose the domain you want to access.

The Context Menu

Certain pages in the Firepower System web interface support a right-click (most common) or left-click context menu that you can use as a shortcut for accessing other features in the Firepower System. The contents of the context menu depend where you access it—not only the page but also the specific data.

For example:

- IP address hotspots provide information about the host associated with that address, including any available whois and host profile information.
- SHA-256 hash value hotspots allow you to add a file's SHA-256 hash value to the clean list or custom detection list, or view the entire hash value for copying.

On pages or locations that do not support the Firepower System context menu, the normal context menu for your browser appears.

Policy Editors

Many policy editors contain hotspots over each rule. You can insert new rules and categories; cut, copy, and paste rules; set the rule state; and edit the rule.

Intrusion Rules Editor

The intrusion rules editor contains hotspots over each intrusion rule. You can edit the rule, set the rule state, configure thresholding and suppression options, and view rule documentation.

Event Viewer

Event pages (the drill-down pages and table views available under the Analysis menu) contain hotspots over each event, IP address, URL, DNS query, and certain files' SHA-256 hash values. While viewing most event types, you can:

- View related information in the Context Explorer.
- Drill down into event information in a new window.
- View the full text in places where an event field contains text too long to fully display in the event view, such as a file's SHA-256 hash value, a vulnerability description, or a URL.

While viewing connection events, you can add items to the default Security Intelligence Block and Do Not Block lists:

- An IP address, from an IP address hotspot.
- A URL or domain name, from a URL hotspot.
- A DNS query, from a DNS query hotspot.

While viewing captured files, file events, and malware events, you can:

- Add a file to or remove a file from the clean list or custom detection list.
- Download a copy of the file.
- View nested files inside an archive file.
- Download the parent archive file for a nested file.
- View the file composition.
- Submit the file for local malware and dynamic analysis.

While viewing intrusion events, you can perform similar tasks to those in the intrusion rules editor or an intrusion policy:

- Edit the triggering rule.
- Set the rule state, including disabling the rule.
- Configure thresholding and suppression options.
- View rule documentation.

Intrusion Event Packet View

Intrusion event packet views contain IP address hotspots. The packet view uses a left-click context menu.

Dashboard

Many dashboard widgets contain hotspots to view related information in the Context Explorer. Dashboard widgets can also contain IP address and SHA-256 hash value hotspots.

Context Explorer

The Context Explorer contains hotspots over its charts, tables, and graphs. If you want to examine data from graphs or lists in more detail than the Context Explorer allows, you can drill down to the table views of the relevant data. You can also view related host, user, application, file, and intrusion rule information.

The Context Explorer uses a left-click context menu, which also contains filtering and other options unique to the Context Explorer.

Related Topics

Security Intelligence Lists and Feeds

Firepower Online Help 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: http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html.

Top-Level Documentation Listing Pages for FMC 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:

  http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

- Firepower Management Center Virtual appliances:
  - http://www.cisco.com/c/en/us/support/security/defense-center-virtual-appliance/tsd-products-support-series-home.html
  - http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

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

- Firepower Threat Defense software:

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw/tsd-products-support-series-home.html

- Firepower Threat Defense Virtual:

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/tsd-products-support-series-home.html

- Firepower 4100 series:

  https://www.cisco.com/c/en/us/support/security/firepower-4100-series/tsd-products-support-series-home.html

- Firepower 9300:

  https://www.cisco.com/c/en/us/support/security/firepower-9000-series/tsd-products-support-series-home.html

Classic devices, also called NGIPS (Next Generation Intrusion Prevention System) devices

- ASA with FirePOWER Services:
  - ASA 5500-X with FirePOWER Services:
    - https://www.cisco.com/c/en/us/support/security/asa-firepower-services/tsd-products-support-series-home.html

- https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html

- Firepower 8000 series:

  https://www.cisco.com/c/en/us/support/security/firepower-8000-series-appliances/tsd-products-support-series-home.html

- Firepower 7000 series:

  https://www.cisco.com/c/en/us/support/security/firepower-7000-series-appliances/tsd-products-support-series-home.html

- AMP for Networks:

  https://www.cisco.com/c/en/us/support/security/amp-appliances/tsd-products-support-series-home.html

- NGIPSv (virtual device):

  https://www.cisco.com/c/en/us/support/security/ngips-virtual-appliance/tsd-products-support-series-home.html

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 Licenses.

Related Topics

About Firepower 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, many features are supported only on Firepower Threat Defense 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.