Cisco Firepower Management Center

Contents

Product overview 3

Features and benefits 4

Exceptional visibility and insight 5

Management before, during, and after an attack 6

Automated Security for Dynamic Defense 6

Open APIs for Easy Integration 7

Threat Intelligence Director 7

Deployment options 8

Platform specifications 8

Hypervisor compatibility 11

Ordering information 12

Warranty information 13

Cisco services 13

Cisco Capital 13

For more information 13

The Cisco Firepower™ Management Center increases the effectiveness of your Cisco® network security solutions by providing centralized, integrated, and streamlined management.

Product overview

The Cisco Firepower Management Center (formerly FireSIGHT Management Center) is the administrative nerve center for select Cisco security products running on a number of different platforms. It provides complete and unified management of firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection. The Management Center is the centralized point for event and policy management for the following solutions:

- Cisco Firepower Next-Generation Firewall (NGFW)
- Cisco ASA with FirePOWER Services
- Cisco Firepower Next-Generation IPS (NGIPS)
- Cisco FirePOWER Threat Defense for ISR
- Cisco Advanced Malware Protection (AMP)

The Cisco Firepower Management Center provides extensive intelligence about the users, applications, devices, threats, and vulnerabilities that exist in your network. It also uses this information to analyze your network's vulnerabilities. It then provides tailored recommendations on what security policies to put in place and what security events you should investigate.

The Management Center provides easy-to-use policy screens to control access and guard against known attacks. It integrates with advanced malware protection and sandboxing technology, and it provides tools to track malware infections throughout your network. It unifies all these capabilities in a single management interface. You can go from managing a firewall to controlling applications to investigating and remediating malware outbreaks with ease.

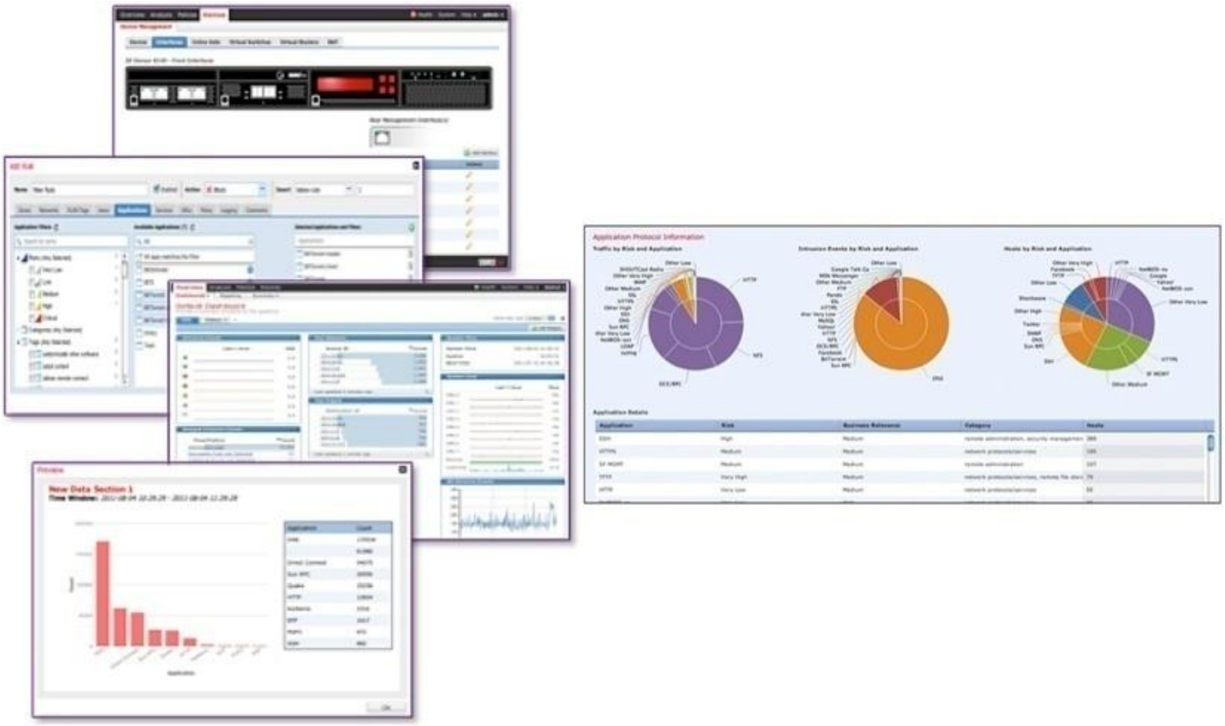

Application Protocol Information
Traffic by Risk and Application
Intrusion Events by Risk and Application
Hosts by Risk and Application
Application Details
New Data Section 1

Figure 1.
Centralized Policy, Event, and Device Management

Enterprise-Class Management

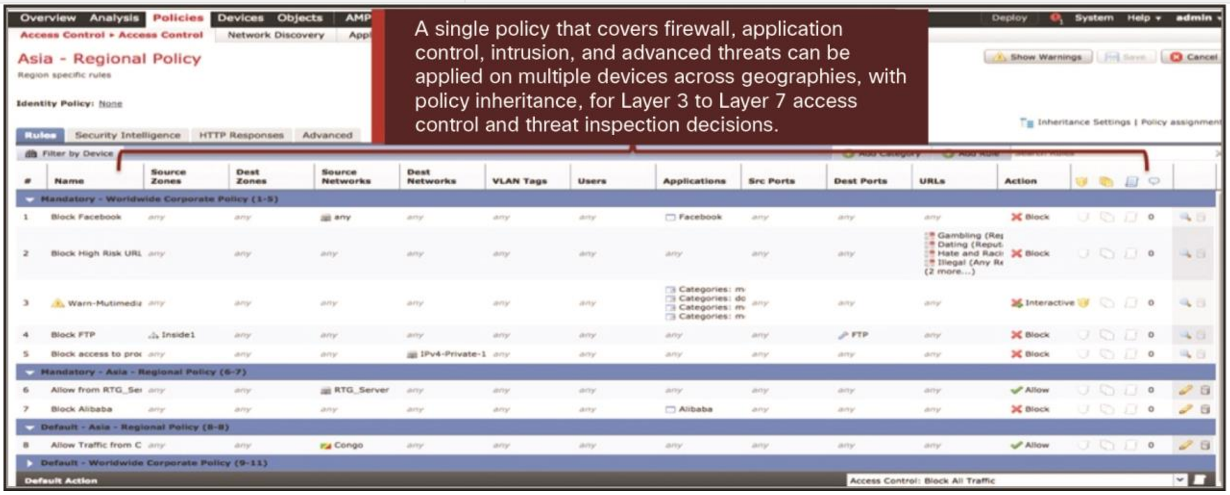
The Cisco Firepower Management Center discovers real-time information about changing network resources and operations. You get a full contextual basis for making informed decisions (see Figure 1). In addition to providing a wide breadth of intelligence, the Management Center delivers a fine level of detail, including:

- **Trends and high-level statistics.** This information helps you understand your security posture at a given moment in time as well as how it's changing, for better or worse
- **Event detail, compliance, and forensics.** These provide an understanding of what happened during a security event. They help improve defenses, support breach containment efforts, and aid in legal enforcement actions
- **Workflow data.** You can easily export this data to other solutions to improve incident response management

Features and benefits

Feature	Benefit
Unified management of multiple security functions across multiple solutions	Facilitates the centralized management of the Cisco security environment, including: ● Cisco Firepower Next-Generation Firewall (NGFW) ● Cisco ASA with FirePOWER Services ● Cisco Firepower NGIPS ● Cisco FirePOWER Threat Defense for ISR ● Cisco AMP
Integrated policy management over multiple security functions	Configures firewall access, application control, threat prevention, URL filtering, and advanced malware protection settings in a single policy Eases policy administration, reduces errors, and promotes consistency Enables a single policy to be deployed to multiple security solutions
Integrated access policy control with Cisco Identify Services Engine	Controls access based on ISE security group tag, device type and location IP, and rapid threat containment Helps enforce compliance, enhance infrastructure security, and streamline service operation
Superior threat intelligence	Integrates Cisco Talos Group's security, threat, and vulnerability intelligence for up-to-minute threat protection Addresses new attack methods with both IP-based and URL-based security intelligence Includes Cisco Umbrella for threat visibility outside the network perimeter Enables ingestion and correlation of threat intelligence from third-party threat feeds and threat intelligence platforms in STIX/TAXII or flat file formats
Application visibility and control	Further reduces threats to your network with precise control of more than 4000 commercial applications Uses the open-source standard Open App ID for detailed identification and control over custom applications
Multitenancy management and policy inheritance	Creates up to 50 management domains with separate event data, reporting, and network mapping, enforced through role-based access control Implements consistent and efficient management through its policy hierarchy structure, with each level inheriting policies above it
Reporting and dashboards	Provides the visibility you need through customizable dashboards with custom and template-based reports Delivers comprehensive alerts and reports for both general and focused information Displays event and contextual information in hyperlinked tables, graphs, and charts for

Feature	Benefit
	easy-to-use analysis Monitors network behavior and performance to identify anomalies and maintain system health
Secure boot	Secure boot is a mechanism to validate the integrity of Cisco software running on the FMC hardware as your system boots. If a signature is missing or software is invalid, it will not load and boot will fail. (FMC 1000, FMC 2500. FMC 4500 only)



A single policy that covers firewall, application control, intrusion, and advanced threats can be applied on multiple devices across geographies, with policy inheritance, for Layer 3 to Layer 7 access control and threat inspection decisions.

Asia - Regional Policy
Region specific rules

Identity Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action				
Mandatory - Worldwide Corporate Policy (1-5)																
1	Block Facebook	any	any	any	any	any	any	Facebook	any	any	any	Block				0
2	Block High Risk URL	any	any	any	any	any	any	any	any	any	Gambling (Re Dating (Reput Hate and Raci Illegal (Any R (2 more...)	Block				0
3	Warn-Mutimedi	any	any	any	any	any	any	Categories: m Categories: do Categories: m Categories: m	any	any	any	Interactive				0
4	Block FTP	Inside1	any	any	any	any	any	any	any	FTP	any	Block				0
5	Block access to pro	any	any	any	IPv4-Private-1	any	any	any	any	any	any	Block				0
Mandatory - Asia - Regional Policy (6-7)																
6	Allow from RTG_Se	any	any	RTG_Server	any	any	any	any	any	any	any	Allow				0
7	Block Alibaba	any	any	any	any	any	any	Alibaba	any	any	any	Block				0
Default - Asia - Regional Policy (8-8)																
8	Allow Traffic from C	any	any	Congo	any	any	any	any	any	any	any	Allow				0
Default - Worldwide Corporate Policy (9-11)																

Default Action: Access Control: Block All Traffic

Figure 2.
Single Policy for multiple security functions

Exceptional visibility and insight

You can't protect what you can't see. The Cisco Firepower Management Center automatically collects, collates, and displays contextual information about everything running in your environment. Table 1 illustrates the breadth of contextual awareness provided into threat vectors that more traditional security technologies do not detect. This critical insight into your network is available for use in your protection policies and gives you a level of protection that other solutions cannot.

Table 1. Full stack visibility

Category	Cisco Firepower Management Center	Typical IPS	Typical Next-Generation Firewall
Threats	Yes	Yes	Yes
Users	Yes	Yes	Yes
Web applications	Yes	No	Yes
Application protocols	Yes	No	Yes
File transfers	Yes	No	Yes
Malware	Yes	No	No
Command-and-control servers	Yes	No	No
Client applications	Yes	No	No

Category	Cisco Firepower Management Center	Typical IPS	Typical Next-Generation Firewall
Network servers	Yes	No	No
Operating systems	Yes	No	No
Routers and switches	Yes	No	No
Mobile devices	Yes	No	No
Printers	Yes	No	No
VoIP phones	Yes	No	No
Virtual machines	Yes	No	No
Vulnerability information	Yes	No	No

Management before, during, and after an attack

The Cisco Firepower Management Center provides unified management across the entire "attack continuum"—before, during, and after an attack.

Before

- Provides exceptional visibility into what is running in your network so you can see what needs to be protected
- Creates firewall rules, and controls how more than 4000 commercial and custom applications are used in your environment

During

- Defines the intrusion prevention levels, URL reputation rules, and advanced malware protection pieces to be put in place
- Applies policies such as: "When network traffic is coming from this country using this particular application with a file attached, I will apply this level of intrusion inspection and analyze the file for malware, and even send it to the integrated sandbox, if necessary"

After

- Generates a graphical representation of all the devices the attack has infected
- Provides the ability to easily create a custom rule to stop the attack from advancing
- Gives a detailed analysis of the malware to safely remediate it

Automated Security for Dynamic Defense

The Cisco Firepower Management Center continually monitors how your network is changing. It streamlines operations and improves your security by:

- Automatically correlating new attack events with your network's vulnerabilities to alert you to attacks that may have been successful. Your security team can focus on those events that matter the most

- Analyzing your network’s vulnerabilities and automatically recommending the appropriate security policies to put in place. You can adapt your defenses to changing conditions and implement security measures tailored specifically to your network
- Correlating specific events from network, endpoint, intrusion, and security intelligence sources. You’re alerted if individual hosts show signs of compromise from unknown attacks
- Applying file policy criteria. If those are met, it automatically analyzes the file to identify known malware and/or sends the file to an integrated sandbox to identify unknown malware

Open APIs for Easy Integration

The Cisco Firepower Management Center makes integration with third-party technologies possible through four powerful, feature-rich application programming interfaces. The APIs provide connection points for:

- Moving event data from the Management Center to another platform, such as a Security Information and Event Management (SIEM) solution
- Enhancing the information contained in the Cisco Firepower database with third-party data. Such data might include vulnerability management data or operating system information from active scanners
- Kicking off workflows and remediation steps that are activated by user-defined correlation rules. You could, for example, integrate your workflow with a Network Access Control (NAC) solution to quarantine an infected endpoint or initiate a digital forensic process
- Supporting third-party reporting and analytics by enabling those solutions to query the Management Center database

These APIs are also used to integrate with a number of Cisco security products and workflows. These include Cisco AMP Threat Grid for sandboxing; the Cisco Identity Services Engine for identity data and network segmentation; and Cisco Umbrella for Internet-wide domain visibility.

Threat Intelligence Director

The Threat Intelligence Director will soon be available in an upcoming release of the Cisco Firepower Management Center. Using open APIs, the director facilitates the ingestion of third-party threat intelligence from sources such as threat feeds and Threat Intelligence Platforms (TIPs). The director supports the ingestion of Structured Threat Information Expression (STIX) and the Trusted Automated Exchange of Indicator Information (TAXII) or select, flat (unformatted) file formats. The Threat Intelligence Director deconstructs the ingested intelligence into observables (IoCs), including IP (IPv4, IPv6), domain, URL, and SHA-256. These are published to Cisco security appliances, which can automatically block malicious activity inline or monitor the network for rapid response.

The Threat Intelligence Director operationalizes available threat intelligence with the following Cisco security appliances:

- Cisco Firepower NGFW
- Cisco Firepower NGIPS

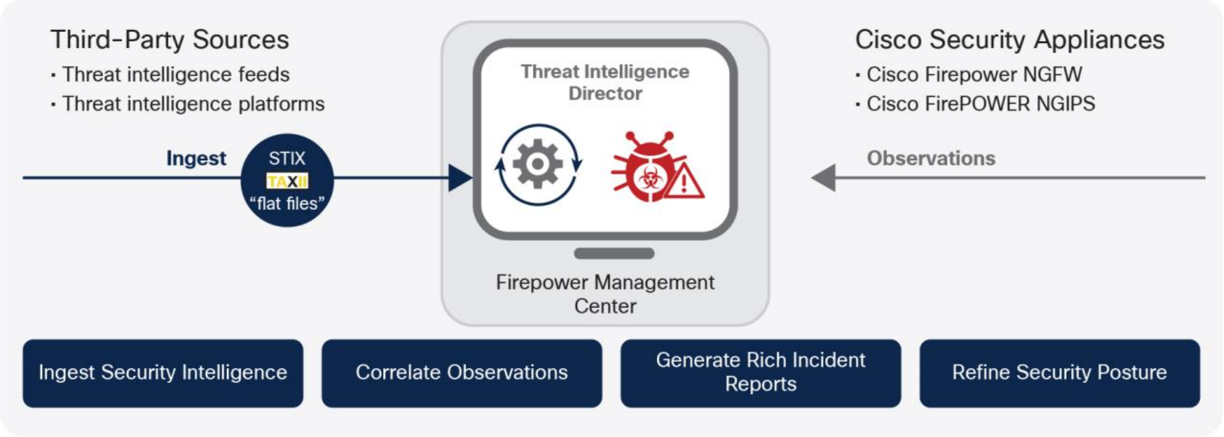

Third-Party Sources
· Threat intelligence feeds
· Threat intelligence platforms
Ingest
STIX
TAXII
"flat files"
Threat Intelligence Director
Firepower Management Center
Cisco Security Appliances
· Cisco Firepower NGFW
· Cisco FirePOWER NGIPS
Observations
Ingest Security Intelligence
Correlate Observations
Generate Rich Incident Reports
Refine Security Posture

Figure 3.
Threat Intelligence Director Integrates Third-Party Security Intelligence

To see the latest list of third-party cyber threat intelligence and TIP partners, visit the Cisco Technical Alliance Partners Listing.

Deployment options

The Cisco Firepower Management Center can be deployed as a physical or virtual appliance, or from the cloud (Table 2). You can choose which options work best for your environment. The physical appliances generally manage a higher number of sensors and provide greater event storage capabilities than their virtual counterparts. The virtual appliances provide the convenience of being able to use your existing VM infrastructure. You can also use cloud computing services to host the Management Center. These services can help you manage security without your having to invest in computing power and database storage. And they will give you the flexibility to scale quickly as needs change.

When using Threat Intelligence Director on NGFWv, for optimal performance, we recommend installing 15 GB memory on the host hardware. For FMC versions supported please visit the current release notes at https://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html.

Table 2. Deployment options

Deployment Platform
VMware ESX and ESXi hypervisors
KVM hypervisor
Amazon Web Services cloud platform

Platform specifications

There are a number of Cisco Firepower Management Center models. Choose the one that's right for your organization based on the number of sensor appliances to be monitored (both physical and virtual), the number of hosts in your environment, and the anticipated security events rate (see Table 3). All models provide the same management capabilities, including:

- Centralized device, license, event, and policy management
- Role-based management (segmented and isolated views and duties based on administrator role or group)
- Customizable dashboard with custom and template-based reports
- Comprehensive reporting and alerts for both general and focused information
- Event and contextual information displayed in hyperlinked tables, graphs, and charts
- Network behavior and performance monitoring
- Robust high-availability options to help ensure there's no single point of failure
- Correlation and remediation features for real-time threat response
- Open APIs for integration with third-party solutions and customer work streams, such as firewalls, network infrastructure, log management, SIEM, trouble ticketing, and patch management

Table 3 compares the capacities and throughputs of available Cisco Firepower Management Center appliances, both physical and virtual.

Table 3. Cisco Firepower Management Center Models

Performance and Functionality	FMC 1600	FMC 2600	FMC 4600	FMCv
Maximum number of sensors managed	50	300	750	25* 10 2
Maximum IPS events	30 million	60 million	300 million	10 million
Management interface	Two built-in RJ-45 SFP+ ports; Support for 1000 Mbps, 1 Gbps, and 10 Gbps; The primary management port is eth0. You can use eth1, eth2, and eth3 as secondary management or event ports.			-
USB Ports	Tow USB 3.0 Type A			-
VGA Ports	One 3-row 15-pin DB-15 connector; Enabled by default			-
SFP ports	Two fixed SFP+ ports			-
Supported SFP+	SFP-10G-SR (10 GB)	SFP-10G-SR (10 GB) SFP-10G-LR (10 GB)	SFP-10G-SR (10 GB) SFP-10G-LR (10 GB)	-
Memory	32 GB	64 GB	128 GB	–
RDIMMs (Internal component only; not field replaceable)	Two 16-GB DDR4-2400-MHz DIMMs	Four 16-GB DDR4-2400-MHz DIMMs	Eight 16-GB DDR4-2400-MHz DIMMs	–
CPU	One Intel Xeon 4110 processor	Two Intel Xeon 4110 processors	Two Intel Xeon 4116 processors	–
Event storage space	900 GB	1.8 TB	3.2 TB	250 GB
Maximum network map size (hosts/users)	50,000/50,000	150,000/150,000	600,000/600,000	50,000/50,000

Performance and Functionality	FMC 1600	FMC 2600	FMC 4600	FMCv
Maximum flow rate (flows per second)	5,000 fps	12,000 fps	20,000 fps	Varies*
Network interfaces	2 x 1 Gbps	2 x 1 Gbps RJ45 onboard 2 x 10 Gbps SFP+ (order SFPs via Cisco Commerce Workplace)	2 x 1 Gbps RJ45 onboard 2 x 10 Gbps SFP+ (order SFPs via Cisco Commerce Workplace)	-
Secure boot	Yes	Yes	Yes	-
Redundancy Features				
Supports high availability	Yes	Yes	Yes	No
System power	Two 770-W AC power supplies; Hot swappable and redundant as 1+1			-
Power consumption	2626 BTU/hr			
Storage	Ten 1.2 TB 10-K SAS HDDs RAID-1, hot swappable	Four 600-GB 10-K SAS SSDs RAID 5, hot-swappable	Ten 1.2 TB 10-K SAS HDDs RAID-6, hot swappable	-
RAID controller	One; The chassis has a dedicated internal riser for a PCIe-style Cisco modular RAID controller card. Internal component only; not field replaceable			-
Physical and Environmental				
Form factor	1RU	1RU	1RU	-
Dimensions (D x W x H)	29.8 x 16.9 x 1.7 (75.7 x 43 x 4.3 cm)			-
Shipping weight	32.2 lb. (16.6 kg)	34.1 lb. (16.8 kg)	36 lb. (17.0 kg)	-
Watts (max)	770W	770W	770W	-

Performance and Functionality	FMC 1600	FMC 2600	FMC 4600	FMCv
Power supply	100-240 VAC (nominal) 90-264 VAC (min/max) 9.5 amp max at 100 VAC 4.5 amp max at 208 VAC	100-240 VAC (nominal) 90-264 VAC (min/max) 9.5 amp max at 100 VAC 4.5 amp max at 208 VAC	100-240 VAC (nominal) 90-264 VAC (min/max) 9.5 amp max at 100 VAC 4.5 amps max at 208 VAC	-
Airflow	Front to back	Front to back	Front to back	-
Operating temperature	50 to 95°F (10 to 35°C)			-

* Note: 3 cost effective virtual FMC licensing options are available to manage 2, 5, or 25 sensors.

Virtual Cisco Firepower Management Center performance is highly dependent on the virtual environment chosen: CPUs, memory, storage, etc.

Shared features

- Integrated Lights-Out Management (LOM)
- Central management of Cisco next-generation security solutions: NGIPS, NGIPS plus application control, NGFW

Note: When dealing with Cisco ASA with FirePOWER Services products, the Cisco Firepower Management Center manages only the FirePOWER portion of the deployment.

Table 4 lists the supported versions of Cisco Firepower products that the Management Center is able to manage, along with associated hardware platforms.

Table 4. Supported firepower versions and their associated platforms

Management Platform	Software Revision Level	Hardware Platform
Cisco Firepower Management Center	**Cisco Firepower Threat Defense 6.x (NGFW)**	**ASA 5500-X (except ASA 5585-X)** Cisco 2100 Series (min FMC 6.2.1) Cisco Firepower 4100 Series Cisco Firepower 9300
	FirePOWER Services 6.x	**ASA 5500-X**
	Cisco Firepower NGIPS 6.x	**Cisco Firepower 7000** Cisco Firepower 8000
	FirePOWER Threat Defense for ISR 6.x (Cisco Firepower Services)	**4000 Series ISR** ISR G2
	FirePOWER Services 5.4.x	**ASA 5500-X**
	Cisco Firepower NGIPS 5.4.x	**Cisco Firepower 7000** **Cisco Firepower 8000**

Hypervisor compatibility

The Cisco Firepower Management Center virtual appliance supports the following hypervisor types. For current versions supported and compatibility with FMC versions, visit the current release notes at https://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html.

Table 5. Virtual appliance hypervisor support

Hypervisor	Version and Details
VMware vSphere	5.1, 5.5:, 6.0 ● ESXi Server ● vCenter Server (optional) ● vSphere Web Client, vSphere Client, or OVF Tool for Windows or Linux
KVM	Ubuntu 14.04 LTS Red Hat Enterprise Linux (RHEL) Version 7.1
Amazon Web Services	AWS Instance Types: c3.xlarge and c3.2xlarge

Ordering information

Licensing

Starting with version 6.0, license keys are no longer required to use the Cisco Firepower Management Center. Versions 5.4 and earlier will still require a Product Authorization Key (PAK) or smart key. Upgrading to version 6.0 will alleviate that need.

Cisco Smart Net Total Care support

The award-winning Cisco Smart Net Total Care™ technical support service gives your IT staff direct, anytime access to Cisco Technical Assistance Center (TAC) engineers and Cisco.com resources. You receive the fast, expert response and the dedicated accountability you need to resolve critical network issues.

Smart Net Total Care provides the following device-level support:

- Global access 24 hours a day, 365 days a year to specialized engineers in the Cisco TAC
- Anytime access to the extensive Cisco.com online knowledge base, resources, and tools
- Hardware replacement options that include 2-hour, 4-hour, and Next-Business-Day (NDB) advance replacement, as well as Return For Repair (RFR)
- Ongoing operating system software updates, including both minor and major releases within your licensed feature set
- Proactive diagnostics and real-time alerts on select devices with Cisco Smart Call Home

In addition, the Cisco Smart Net Total Care Onsite Service is an option that provides a field engineer who will install replacement parts at your location and help ensure that your network operates at the highest levels. For more information on Smart Net Total Care please visit: https://www.cisco.com/c/en/us/services/portfolio/product-technical-support/smart-net-total-care.html.

How to order

Table 6 provides ordering information for virtual and physical Cisco Firepower Management Center appliances and spare hardware. Please consult the Cisco Network Security Ordering Guide for additional configuration options and accessories.

Table 6. Ordering information

Cisco Firepower Management Center (Hardware) Appliances	
Part Number	**Product Description**

Cisco Firepower Management Center (Hardware) Appliances	
FMC1600-K9	Cisco Firepower Management Center 1600 Chassis, 1RU
FMC2600-K9	Cisco Firepower Management Center 2600 Chassis, 1RU
FMC4600-K9	Cisco Firepower Management Center 4600 Chassis, 1RU
Cisco Firepower Management Center (Hardware) Spare	
FMC-M5-PS-AC-770W=	Cisco AC Power Supply 770W for FMC1600, FMC2600, FMC4600
Cisco Firepower Management Center (Software) Virtual Appliance	
FS-VMW-SW-K9	Cisco Firepower Management Center, Virtual (VMware) Firepower License
FS-VMW-10-SW-K9	Cisco Firepower Management Center, Virtual (VMware) Firepower License, for 10 devices
FS-VMW-2-SW-K9	Cisco Firepower Management Center, Virtual (VMware) Firepower License, for 2 devices

To place an order, visit the Cisco ordering homepage.

Warranty information

Find warranty information on Cisco.com at the Product Warranties page.

Cisco services

Cisco offers a wide range of service programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services for security, visit https://www.cisco.com/go/services/security.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

For more information

For more information, please visit the following links:

- Cisco Firepower Management Center
- Cisco Firepower Next-Generation Firewalls
- Cisco Firepower Next-Generation IPS (NGIPS)
- Cisco Advanced Malware Protection (AMP)

- Cisco FirePOWER Threat Defense for ISR
- Cisco Security Services

For information about Cisco Firepower in service provider environments, please visit: https://www.cisco.com/c/en/us/solutions/enterprise-networks/service-provider-security-solutions/.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-736775-08 08/19