Data sheet

Cisco confidential

Cisco Secure Firewall Management Center (formerly Firepower Management Center)

The bridge to possible

Contents

Security that works together

The Cisco Secure Firewall Management Center (FMC) is your administrative nerve center for managing critical Cisco network security solutions. It provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware protection. Quickly and easily go from managing a firewall to controlling applications to investigating threats and remediating malware outbreaks. It is a key part of the broad and integrated Cisco Secure portfolio, delivering in-depth analysis, streamlined security management across the network and cloud, and accelerated incident investigation and response, working across your Cisco and third-party technologies.

Comprehensive visibility and policy control

- Provides exceptional visibility into what is running in your network and cloud so you can see what needs to be protected.
- Rapidly detects suspicious/malicious traffic and quickly creates custom rules to prevent the attack from advancing.
- Built in forensics give a detailed analysis of malware to safely remediate with a graphical representation of all the devices the attack has infected.
- Creates firewall rules and controls thousands of commercial and custom applications used in your environment.
- Shares context with Cisco Secure Workload, allowing firewalls in the network to be “workload aware” for better protection of dynamic applications everywhere in your environment.
- Defines the intrusion prevention levels, URL reputation rules, and malware threat defense policies. It solves problems such as: “When network traffic is coming from a specific country using this particular application with a file attached, I can apply this level of intrusion inspection, analyze the file for malware, and send it to the integrated sandbox, if necessary.”

Automated security for dynamic defense

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

- Automatically correlating and prioritizing 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 are 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.

Centralized Event and Policy Manager

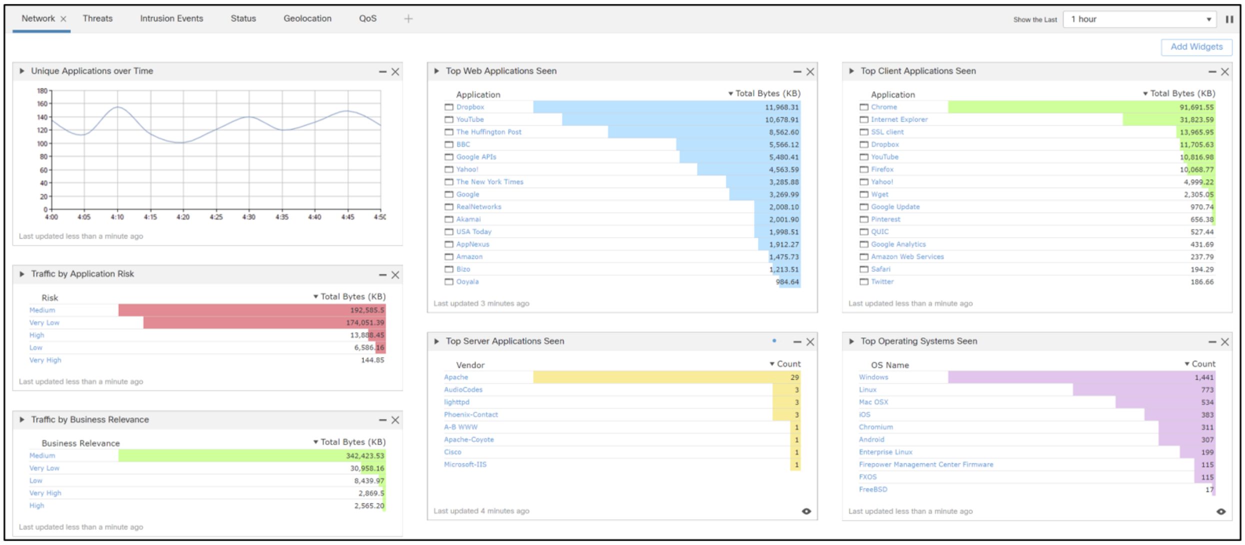
The Firewall Management Center is the centralized event and policy manager for:

- Cisco Secure Firewall Threat Defense (FTD), both on-premises and virtual
- Cisco Secure IPS (formerly Firepower NGIPS)
- Cisco Firepower Threat Defense for ISR
- Cisco Malware Defense (formerly Advanced Malware Protection, or AMP)

Enterprise-Class Management

The Firewall Management Center (FMC) discovers real-time information about changing network resources and operations. You get a full contextual basis for making informed decisions (Figure 1). In addition to providing a wide breadth of intelligence, FMC 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.
- **Real-time device health monitoring.** Quickly see the status of your devices either from a consolidated, high-level view or via detailed, customizable status pages (Figure 2).



Last updated less than a minute ago

Traffic by Application Risk

Risk	▾ Total Bytes (KB)
Medium	192,585.5
Very Low	174,051.39
High	13,888.45
Low	6,586.16
Very High	144.85

Last updated less than a minute ago

Traffic by Business Relevance

Business Relevance	▾ Total Bytes (KB)
Medium	342,423.53
Very Low	30,958.16
Low	8,439.97
Very High	2,869.5
High	2,565.20

Last updated less than a minute ago

Top Web Applications Seen

Application	▾ Total Bytes (KB)
Dropbox	11,968.31
YouTube	10,678.91
The Huffington Post	8,562.60
BBC	5,566.12
Google APIs	5,480.41
Yahoo!	4,563.59
The New York Times	3,285.88
Google	3,269.99
RealNetworks	2,008.10
Akamai	2,001.90
USA Today	1,998.51
AppNexus	1,912.27
Amazon	1,475.73
Bizo	1,213.51
Ooyala	984.64

Last updated 3 minutes ago

Top Server Applications Seen

Vendor	▾ Count
Apache	29
AudioCodes	3
lighttpd	3
Phoenix-Contact	3
A-B WWW	1
Apache-Coyote	1
Cisco	1
Microsoft-IIS	1

Last updated 4 minutes ago

Top Client Applications Seen

Application	▾ Total Bytes (KB)
Chrome	91,691.55
Internet Explorer	31,823.59
SSL client	13,965.95
Dropbox	11,705.63
YouTube	10,816.98
Firefox	10,068.77
Yahoo!	4,999.22
Wget	2,305.05
Google Update	970.74
Pinterest	656.38
QUIC	527.44
Google Analytics	431.69
Amazon Web Services	237.79
Safari	194.29
Twitter	186.66

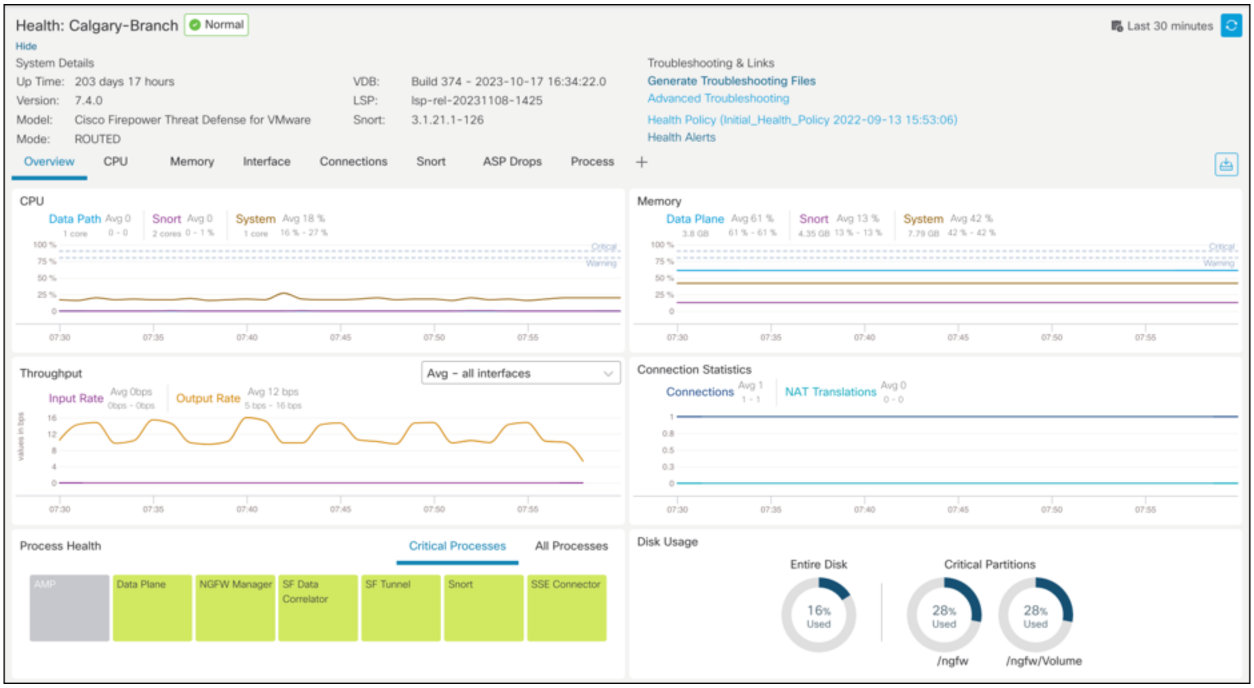
Last updated less than a minute ago

Top Operating Systems Seen

OS Name	▾ Count
Windows	1,441
Linux	773
Mac OSX	534
iOS	383
Chromium	311
Android	307
Enterprise Linux	199
Firepower Management Center Firmware	115
FXOS	115
FreeBSD	17

Last updated less than a minute ago

Figure 1.
Contextual network and security information



Health: Calgary-Branch Normal

Hide

System Details

Up Time: 203 days 17 hours

Version: 7.4.0

Model: Cisco Firepower Threat Defense for VMware

Mode: ROUTED

VDB: Build 374 - 2023-10-17 16:34:22.0

LSP: lsp-rel-20231108-1425

Snort: 3.1.21.1-126

Troubleshooting & Links

Generate Troubleshooting Files

Advanced Troubleshooting

Health Policy (Initial_Health_Policy 2022-09-13 15:53:06)

Health Alerts

Figure 2.
Real-time Device Health Monitor

Centralized Policy and Operations

- **Maintain consistent policies:** Write a policy once and scale enforcement consistently across multiple security controls throughout your network.
- **Reduce complexity:** Get unified management and automated threat correlation across tightly integrated security functions, including application firewalling, next-generation Intrusion Prevention, and file and malware protection.
- **Accelerate key security operations functions:** Increase efficiency by removing manual processes. Access security patches and new features faster by completing software upgrades in just a few clicks.

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 Secure Firewall Threat Defense • Cisco Secure IPS • Cisco Firepower Threat Defense for ISR • Cisco Malware Defense
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
Network Discovery	• Discovers users, applications, and a multitude of devices through passive analysis of network traffic • Provides context and helps to determine the impact of attacks against your specific environment • Allows you to tune Intrusion Prevention signature sets to the systems discovered on your network • Supports third-party vulnerability management integration
Separation of duties and role-based access control	• Create administrative user personas such as NetOps or SecOps to clearly define responsibilities • Granular role-based access control allows users to be given specific access rights to perform only the actions they are responsible for
Integrated Azure AD Identity based access policy control with Cisco Identify Services Engine (ISE)	• Newly supported Azure AD based User/Group based access control. • Integrates with ISE for Azure AD based User Identity integration. • Controls access based on Cisco ISE security group tag, device type and location IP, and rapid threat containment • Helps enforce compliance, enhance infrastructure security, and streamline service operation
Automatic Security Response	• Correlate security events to identify stealthy attacks • Trigger automated responses via: ◦ Email ◦ Syslog ◦ SNMP ◦ Remediation modules
Cisco Secure Dynamic Attribute Connector	• CSDAC Natively running inside from FMC 7.4 onwards • Provides an automated and programmatic way to manage policies when IP addresses and workloads are constantly changing without having to redeploy changes • Dramatically reduces the admin overhead required to keep security policies up to date • Integrates with AWS, Azure, GCP, VMware to source workload tags and to create Dynamic Objects for Policy • Integrated with SaaS services like Office365, GitHub, Azure Service Tags, Zoom, WebEx for Dynamic Objects based Access enforcement • Supports Generic text file driven IP Prefixes for open integration. They can contain for example "known IP List", or "Vulnerable IP list" etc
Threat intelligence	• Integrates with 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

Feature	Benefit
	• 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 thousands of 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 100 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
Cisco Security Analytics and Logging (SAL) integration	• Highly scalable, intuitive single view of firewall log management • Behavioral analysis provides real-time threat detection and faster response times • Continuous analysis further refines your security posture to better defend against future attempts
SecureX integration	• Leverage the SecureX™ platform to accelerate threat detection, orchestration, and remediation • Every Secure Firewall includes entitlement for Cisco SecureX • The new SecureX ribbon in Firewall Management Center enables SecOps to instantly pivot to SecureX's open platform, speeding incident response
Cisco Secure Workload integration	• Integration with Cisco Secure Workload (formerly Tetration) enables comprehensive visibility and policy enforcement for modern distributed and dynamic applications across the network and workload for consistent enforcement in a scalable manner
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 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 (Hardware FMC appliances only)

Open APIs for easy integration

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

- Moving event data from FMC to another platform, such as a Security Information and Event Management (SIEM) solution.
- Enhancing the information contained in the Cisco IPS database with third-party data. Such data might include vulnerability management.
- 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 FMC database.

These APIs are also used to integrate with several Cisco security products and workflows. These include Cisco Secure Malware Analytics (formerly Cisco AMP Threat Grid) for sandboxing; the Cisco Identity Services Engine (ISE) for identity data and network segmentation; and Cisco Umbrella® for internet-wide domain visibility.

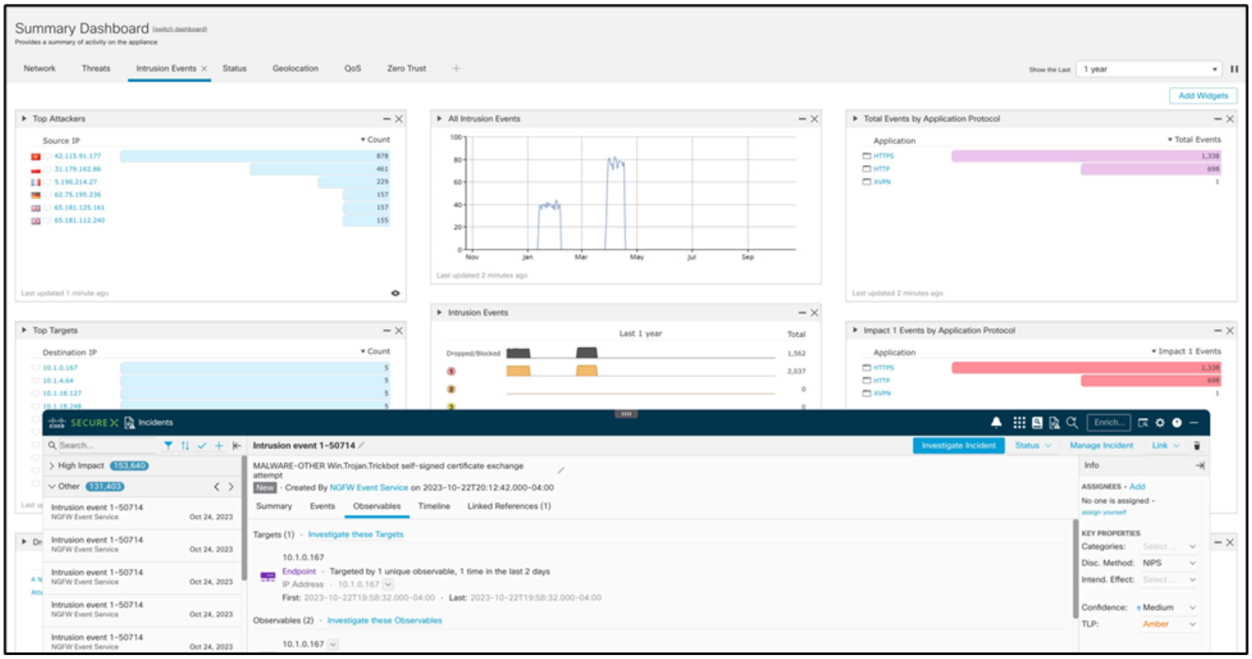
The Cisco Secure Technology Alliance is a security ecosystem that facilitates open, multivendor product integrations to improve security effectiveness through automation and operational simplicity. Cisco is actively partnering with 100s of key security vendors and integration with over ten Cisco security products. To see the latest list, visit Cisco Secure Technical Alliance Partners.

Cisco SecureX

Cisco SecureX connects the breadth of Cisco’s integrated security portfolio and your entire security infrastructure for a consistent experience that unifies visibility, enables automation, and strengthens your security across the network, endpoint, cloud, and applications. The result is simplified security, built into the solutions that you already have.

SecureX’s threat response feature (formerly CTR) integrates threat intelligence from Cisco Talos and third-party sources to automatically research Indicators of Compromise (IOCs), also known as observables, and confirm threats quickly.

For Secure Firewall customers, the SecureX ribbon in the Firewall Management Center (FMC) allows an administrator to instantly pivot back and forth for deeper threat investigation, sharing and maintaining context around incidents.



Intrusion event 1-50714

MALWARE-OTHER Win.Trojan.Trickbot self-signed certificate exchange attempt

New · Created By NGFW Event Service on 2023-10-22T20:12:42.000-04:00

High Impact 153,640

Other 131,403

Intrusion event 1-50714 NGFW Event Service	Oct 24, 2023
Intrusion event 1-50714 NGFW Event Service	Oct 24, 2023
Intrusion event 1-50714 NGFW Event Service	Oct 24, 2023
Intrusion event 1-50714 NGFW Event Service	Oct 24, 2023
Intrusion event 1-50714 NGFW Event Service	Oct 24, 2023

Targets (1) · Investigate these Targets

10.1.0.167
Endpoint · Targeted by 1 unique observable, 1 time in the last 2 days
IP Address · 10.1.0.167
First: 2023-10-22T19:58:32.000-04:00 · Last: 2023-10-22T19:58:32.000-04:00

Observables (2) · Investigate these Observables

10.1.0.167

ASSIGNEES · Add
No one is assigned · assign yourself

KEY PROPERTIES
Categories: Select ...
Disc. Method: NIPS
Intend. Effect: Select ...
Confidence: Medium
TLP: Amber

Figure 3.
SecureX in the FMC

Find here the prebuilt workflow playbooks that address common use cases for observable actions, remediations, and incident endpoint enrichment.

How does it work?

Cisco firewalls send data to SecureX with a secure intermediary cloud service. SecureX threat response queries for sightings related to the IP address being investigated and provides an analyst with the additional context. Intrusion events are promoted to investigation-worthy incidents in the Incident Manager, based on Cisco Talos reputation or user-defined filters. This allows your team to quickly investigate and triage to see analytics on intrusion events.

SecureX Orchestrator can invoke FMC API calls, which allows administrators to automate routine FMC tasks, improving efficiency. SecureX is available as a standard for customers with Cisco Secure Firewall and/or any Cisco Secure product.

Deployment options

FMC can be deployed as a physical or virtual appliance, or from the cloud. It can also be consumed as a service. The cloud-delivered FMC, through CDO, has all the benefits of FMC without the need to manage FMC software update itself. You can choose which option works best for your environment. Please visit the current Release Notes for more detailed information.

Hypervisor compatibility and cloud support

Firewall Management Center Virtual supports the following hypervisor types shown below. All models of the FMC Virtual platform will operate with the same RAM requirements: 32 GB recommended**; 28 GB** required. For current versions supported and compatibility with FMC versions, visit current Release Notes.

** Recommended to provision vFMC with additional 2 vCPU and 2GB RAM to run CSDAC

Table 1. Virtual appliance hypervisor and cloud support

Hypervisor	Version and details
VMware vSphere	• ESXi Server 5.1, 5.5, 6.0, 6.5, 6.7, 7.0 • vCenter Server (optional) • vSphere Web Client, vSphere Client, or OVF Tool for Windows or LinuxC
KVM	• Ubuntu 18.04 LTS • Red Hat Enterprise Linux (RHEL) Version 7.1
Amazon Web Services	• c3.4xlarge: 16 vCPUs, 30 GB • c4.4xlarge: 16 vCPUs, 30 GB • c5.4xlarge: 16 vCPUs, 32 GB
Microsoft Azure	Standard_D4_v2: 8 vCPUs, 28 GB
GCP	c2-standard-8: 8 vCPUs, 32 GB c2-standard-16: 16 vCPU, 64 GB
OCI	VM.Standard 2.4, 60 GB
Nutanix	Nutanix AHV (20201105.12 and later)
Hyperflex	Release 4.5(1a) 4-8 vCPUs, 28-32 GB for FMCv-2,10,25 32 vCPU, 64 GB for FMCv-300

Note: Refer to the Cisco Secure Firewall Management Center Virtual Getting Started Guide for more information.

Platform specifications

There are several Firewall Management Center models. Choose 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.

Table 2 compares the capacities of available Cisco Firewall Management Center physical appliances.

Table 2. Cisco Secure Firewall Management Center hardware models

Performance and functionality	FMC 1600	FMC 2600	FMC 4600	FMC 1700	FMC 2700	FMC 4700
Maximum number of sensors managed	50	300	750	50	300	1,000
Maximum IPS events	30 million	60 million	300 million	30 million	60 million	400 million
Management interface	Two built-in RJ-45 SFP+ ports; support for 100 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.			Two built-in 10GbE RJ45 OCP3.0 NIC; support for 100 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	Two USB 3.0 Type A			Two USB 3.0 Type A		
VGA ports	One 3-row 15-pin DB-15 connector; enabled by default			One 3-row 15-pin DB-15 connector; enabled by default		
SFP ports	Two fixed 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)	SFP-10G-SR (10 GB) SFP-10G-LR (10 GB)	SFP-10G-SR (10 GB) SFP-10G-LR (10 GB)	SFP-10G-SR (10 GB) SFP-10G-LR (10 GB) SFP-25G-SR-S (25 GB) SFP-10/25G-LR-S (25GB) SFP-10/25G-CSR-S (25 GB)
Memory	32 GB	64 GB	128 GB	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	Two 16-GB DDR4-3200-MHz DIMMs	Four16-GB DDR4-3200-MHz DIMMs	Eight 16-GB DDR4-3200-MHz DIMMs
CPU	One Intel Xeon 4215 processor	Two Intel Xeon 4215 processors	Two Intel Xeon 4214 processors	AMD 1P Rome 7232P	AMD 1P Rome 7282	AMD 1P Rome 7352

Performance and functionality	FMC 1600	FMC 2600	FMC 4600	FMC 1700	FMC 2700	FMC 4700
Event storage space	900 GB	1.8 TB	3.2 TB	900 GB	1.8 TB	3.2 TB
Maximum network map size (hosts/users)	550,000/ 50,000	150,000/ 150,000	600,000/ 600,000	550,000/ 50,000	150,000/ 150,000	600,000/ 600,000
Maximum event rate (events per second)	5000 eps	12,000 eps	20,000 eps	5000 eps	12,000 eps	30,000 eps
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)	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)	2 x 1 Gbps RJ45 onboard 2 x 10/25 Gbps SFP+ (order SFPs via Cisco Commerce Workplace)
Secure boot	Yes	Yes	Yes	Yes	Yes	Yes
Redundancy features						
Supports high availability	Yes	Yes	Yes	Yes	Yes	Yes
System power	Two 770-W AC power supplies; hot swappable and redundant as 1+1			Two 1050-W AC power supplies; hot swappable and redundant as 1+1		
Power consumption	2626 BTU/hr			2626 BTU/hr		
Storage	Two 1.2-TB 10-K SAS HDDs RAID-1, hot swappable	Four 600-GB 10-K SAS HDDs RAID 5, hot-swappable	Ten 1.2-TB 10-K SAS HDDs RAID-6, hot swappable	Two 1.2-TB 10-K SAS HDDs RAID-1, hot swappable	Four 600-GB 10-K SAS HDDs 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.			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	1RU	1RU	1RU
Dimensions (D x W x H)	29.8 x 16.9 x 1.7 in (75.7 x 43 x 4.3 cm)			30 x 16.9 x 1.7 in (76.2 x 42.9 x 4.3 cm)		
Shipping weight	32.2 lb. (16.6 kg)	34.1 lb. (16.8 kg)	36 lb. (17.0 kg)	32.2 lb. (16.6 kg)	34.1 lb. (16.8 kg)	36 lb. (17.0 kg)
Watts (max)	770W	770W	770W	1,050W	1,050W	1,050W

Performance and functionality	FMC 1600	FMC 2600	FMC 4600	FMC 1700	FMC 2700	FMC 4700
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-amp max at 208 VAC	100-240 VAC (nominal) 90-264 VAC (min/max 9.2-amp max at 100 VAC 5.2-amp max at 230 VAC	100-240 VAC (nominal) 90-264 VAC (min/max 9.2-amp max at 100 VAC 5.2-amp max at 230 VAC	100-240 VAC (nominal) 90-264 VAC (min/max 9.2-amp max at 100 VAC 5.2-amp max at 230 VAC
Airflow	Front to back	Front to back	Front to back	Front to back	Front to back	Front to back
Operating temperature	50° F to 95° F (10° C to 35° C)			50° F to 95° F (10° C to 35° C)		

Table 3 compares the capacities of available Cisco Secure Firewall Management Center virtual appliances.

Table 3. Cisco Firewall Management Center Virtual (FMCv) models

Performance and functionality	FMCv(2/10/25)	FMCv300
Maximum number of sensors managed	2 10 25	300
Maximum IPS events	10 million	60 million
Memory	32 GB	64 GB
CPU	8/4 vCPUs	32 vCPUs
Event storage space	250 GB	2.2 TB
Maximum network map size (hosts/users)	50,000/50,000	150,000/150,000
Maximum event rate (events per second)	Varies	12,000 eps
Hypervisor and cloud support	VMware, KVM, AWS, Azure, GCP, OCI, Nutanix, Hyperflex, OpenStack	VMware, AWS, OCI
Supports high availability	VMware, AWS, OCI (Not supported on FMCv2)	VMware, AWS, OCI

Cloud-delivered FMC can be scaled for your needs. Please refer to our Release Notes for more detailed information on compatibility, supported versions, deployments, and browser requirements.

Ordering information

For ordering and licensing information on virtual and physical appliances as well as cloud-delivered service, please consult the Cisco Network Security Ordering Guide. To place an order, visit the Cisco Ordering Home Page, contact your Cisco sales representative, or call us at 1 800 553 6387.

Warranty information

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

For more information

- Cisco Security Management Portfolio
- Cisco Secure Firewall
- Cisco Secure Firewall Management Center Release Notes
- Secure IPS (NGIPS)
- Malware Defense
- Cisco Security Analytics and Logging
- Network Security and Trust for Service Providers
- Services for Security
- Cisco Firepower Management Center (Previous Models) Data Sheet

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 C78-736775-16 12/23