Cisco M-Series Content Security Management Appliance for Email and Web Security Appliances

Product Overview

Cisco M-Series Content Security Management Appliances centralize and consolidate policy and runtime data in a single management interface, providing a central platform for all reporting and auditing for Cisco Email Security Appliances and Web Security Appliances. Unified reporting provides visibility and insight into email activity and trends, and web usage and trends, ensuring IT administrators can react and respond quickly to policy infractions and other known and emerging security risks.

Built on Cisco's high-performance AsyncOS operating system, Cisco M-Series Content Security Management Appliances provide industry-leading scalability and supportability to easily meet the demands of large enterprises and ISPs. Features include:

- **Built-In Data Loss Prevention (DLP) Capabilities**—Cisco M-Series Content Security Management Appliances provide detailed information on policy violations, filter matches, and user activity—even for events that may have occurred months or years ago. This long-term visibility allows administrators to quickly and easily respond to trend analyses and audits that are critical to the remediation workflow for DLP and compliance.
- **Reduced Administration**—Cisco M-Series Content Security Management Appliances are built on Cisco's fully managed, robust AsyncOS operating system, which features an easy-to-use intuitive interface. Upgrades and new features are delivered directly from Cisco for approval and then automatically installed and managed.
- **Modular Design**—The Cisco M-Series Content Security Management Appliance's modular design enables organizations to run all security features on a single appliance, or to dedicate specific appliances to individual applications for high-volume deployments.

Email Security: Features and Benefits

Cisco M-Series Content Security Management Appliances feature two types of email reporting:

- **Advanced Message Tracking**—This feature enables administrators to know where and when an email communication took place. Message telemetry for multiple email security appliances can be searched based on sender, recipient, message subject, and many other advanced parameters. Administrators can then report the full scanning results, such as spam/virus verdicts or policy violations, as well as delivery details, such as email authentication.
- **Cisco Spam Quarantine**—This self-service solution features an easy-to-use, web- or email-based interface and simple integration into existing directory and mail systems. Operations are automatic and self-managing, so there is no risk of capacity overload. The solution requires no maintenance by administrators or end users. Users can be authenticated against a corporate LDAP directory or by using their regular email password for any standards-based IMAP or POP server. Message distribution lists can be managed through one-click authentication from quarantine message digests.

Additional email security features include:

- **Redundant Data Aggregation**—Organizations can aggregate email reporting and messaging tracking information on two separate Cisco M-Series Content Security Management Appliances.

Cisco M-Series Content Security Management Appliances also provide the ability to:

- Manage email security systems through a single interface that centralizes and consolidates policy and runtime data
- Determine which users are in violation of acceptable use policies and track infractions across any department or site
- Generate detailed, accurate information that can be integrated into interactive reports suitable for all levels of the organization
- Protect corporate network integrity by increasing deployment flexibility
- Ensure top performance from Cisco Email Security Appliances

Web Security: Features and Benefits

Cisco M-Series Content Security Management Appliances provide the following features:

- **Comprehensive web reporting:** Quickly identify and troubleshoot malware threats, potential infections, and botnet activity.
- **Centralized web reporting:** View the biggest network threats; which users are encountering the most blocks or warnings; and which websites and URL categories are posing the biggest risk. Network operations personnel also can use the system capacity report to track growth over time and plan for system capacity.
- **Actionable reports:** Generate detailed and accurate information that can be integrated into interactive reports suitable for all levels of an organization.
- **Granular visibility:** Determine which users are in violation of acceptable use policies; track policy infractions across any department or site; and monitor usage of resource-intensive applications such as Facebook, YouTube, or instant messaging.

Cisco M-Series Content Security Management Appliances also provide the ability to:

- Ease burden on resource-strapped IT organizations and reduce management overhead
- Refine policies, plan infrastructure, and measure productivity using unprecedented insight into current operational data provided by a unique threat correlation engine
- Manage web security systems through a single interface that centralizes and consolidates reporting data from multiple Cisco Web Security Appliances, aggregated in near-real time
- Generate detailed, accurate information that can be integrated into interactive reports suitable for all levels of the organization
- Ensure top performance from Cisco Web Security Appliances by monitoring when devices are exceeding recommended CPU capacity, the number of transactions per second and latency, as well as response time and proxy buffer memory

- Protect corporate network integrity with increased deployment flexibility

Product Specifications

Cisco M-Series Content Security Management Appliances are built to meet the requirements of organizations of different sizes and complement all Cisco Email Security Appliances and Cisco Web Security Appliances.

Table 1 provides product specifications for the three models in the M-Series.

Table 1. Product Specifications

	Cisco M1070	Cisco M670	Cisco M170
Image			
Usage Scenario			
Description	The M1070 provides flexible management and complete security control at the network gateway	This cost-effective model for midsized organizations has the same features and functionality as the M1070	This cost-effective model is designed for organizations and branches with fewer than 1000 users
Number of users*	10,000+	Up to 10,000	Up to 1,000
Chasis			
Form factor	2U	2U	1U
Dimensions (H x W x D)	3.5 in. x 17.5 in. x 26.8 in. (8.9 x 44.5 x 68.1 cm)	3.5 in. x 17.5 in. x 26.8 in. (8.9 x 44.5 x 68.1 cm)	1.67 in. x 16.9 in. x 15.5 in. (4.24 x 42.9 x 39.4 cm)
Total weight (lbs.)	57.5	52.2	26.96
Power supply	870W, 100/240V	870W, 100/240V	400W, 100/240V
Redundant power supply	Yes	Yes	No
Processor, Memory, and Disks			
CPUs	2x4 (2 quad cores)	2x4 (2 quad cores)	1x2 (1 dual cores)
Memory	4 GB	4 GB	4 GB
Disk space and count	3.6 TB (600 * 6)	1.8 TB (300 * 6)	500 GB (250 * 2)
Hot-swappable hard disk	Yes	Yes	Yes
RAID level and controller	RAID 10, hardware	RAID 10, hardware	RAID 1, software
Interfaces			
Ethernet	4 Gigabit NICs, RJ-45	4 Gigabit NICs, RJ-45	2 Gigabit NICs, RJ-45
Speed (mbps)	10/100/1000, auto-negotiate	10/100/1000, auto-negotiate	10/100/1000, auto-negotiate
Duplex	Half or full, auto-negotiate	Half or full, auto-negotiate	Half or full, auto-negotiate
Serial	1xRS-232 (DB-9), Serial	1xRS-232 (DB-9), Serial	1xRS-232 (RJ-45)
Fiber	Yes	No	No
USB	0	0	2
Configuration, Logging, and Monitoring			
Web interface	GUI-based (HTTP)	GUI-based (HTTP)	GUI-based (HTTP)
Command-line interface	SSH or Telnet (command-based)	SSH or Telnet (command-based)	SSH or Telnet (command-based)
Logging	Squid, Apache, Syslog, W3C	Squid, Apache, Syslog, W3C	Squid, Apache, Syslog, W3C
Centralized reporting	Supported	Supported	Supported
File transfer	SCP, FTP	SCP, FTP	SCP, FTP

	Cisco M1070	Cisco M670	Cisco M170
Configuration files	XML-based	XML-based	XML-based
Centralized configuration	Supported	Supported	Supported
Monitoring	SNMPv1-3, email alerts	SNMPv1-3, email alerts	SNMPv1-3, email alerts
Environmental Operating Ranges			
Total current (A)	3.7	2.8	4.85 (max)
Input voltage (V)	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC
Operating power (W)	399.3	306.8	400W (max)
Total heat dissipation (BTU/Hr)	1904	1801.6	432.6
Leakage current (mA)	3.5	3.5	3.5
Fan exhaust volume (CFM)	43.1	37.4	Idle at 24℃: 12.3 Full fan speed: 34.4
Full fan speed: 34.4	6.3	6.1	Idle: 41.3 dBa Stress: 64.2 dBa max.
Ambience noise (bels)	94,400	94,400	107,356
Operating			
Temperature (℃)	10℃ to 35℃	10℃ to 35℃	-5℃ to 45℃
Relative humidity (%)	20% to 80% (noncondensing)	20% to 80% (noncondensing)	20% to 80% (noncondensing)
Altitude (m)	3,048	3,048	3,000
Vibration	0.26 Grms at 5 to 350Hz	0.26 Grms at 5 to 350Hz	0.41 Grms at 3 to 500Hz
Non-Operating			
Temperature (℃)	-40℃ to 65℃	-40℃ to 65℃	-25℃ to 70℃
Relative humidity	5% to 95% (noncondensing)	5% to 95% (noncondensing)	5% to 95% (noncondensing)
Altitude (m)	10,600	10,600	4,570
Vibration	1.54 Grms at 10 to 250Hz	1.54 Grms at 10 to 250Hz	1.12 Grms at 3 to 500Hz
Industry Certifications			
RoHS	Yes	Yes	Yes
Other certifications			Safety: cULus, CB, CCC, BSMI EMC: CE, FCC, VCCI, C-TICK, KC

Table 2. Ordering Information

Product Name	Part Number
Cisco M170 – for organizations with up to 1,000 users	SMA-M170-K9
Cisco M670 – for organizations with up to 10,000 users	SMA-M670-K9
Cisco M1070 – for organizations with more than 10,000 users	SMA-M1070-K9

Why Cisco?

Security is more critical to your network than ever before. As threats and risks persist, along with concerns about confidentiality and control, security is necessary for providing business continuity, protecting valuable information, maintaining brand reputation, and adopting new technology. A secure network enables your employees to embrace mobility and securely connect to the right information. It also allows your customers and partners to conduct business with you more easily.

No organization understands network security like Cisco. Our market leadership, unmatched threat protection and prevention, innovative products, and longevity make us the right vendor to serve your security needs.

For More Information

For more information about the Cisco M-Series Content Security Management Appliances, visit http://www.cisco.com/go/sma or contact your local account representative.

The best way to understand the benefits of the Cisco M-Series Content Security Management Appliances is to participate in the Try Before You Buy program. To receive a fully functional evaluation appliance to test in your network, free for 30 days, visit http://www.cisco.com/go/sma.

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 **www.cisco.com/go/offices.**

Printed in USA C78-721194-00 01/13