Cisco Content Security Management Appliance

Centralize management and reporting functions across multiple Cisco® Email Security Appliances (ESAs) and Cisco Web Security Appliances (WSAs) with the Cisco Content Security Management Appliance (SMA). The integration of Cisco SMA with Cisco ESAs and WSAs simplifies the planning and administration of email and web security, improves compliance monitoring, makes possible a consistent enforcement of acceptable-use policies, and enhances threat protection.

Organizations must often coordinate the management and administration of multiple appliances across geographically dispersed teams with a limited staff and budget. Built on a robust platform optimized for reporting and tracking, the Cisco SMA delivers high performance and scalability plus industry-leading protection and control for long-term investment value.

Features and Benefits

Features and benefits of the Cisco SMA are discussed in the following sections and described in more detail in Table 1.

Simplified Administration and Planning

Using the Cisco SMA's easy-to-use intuitive interface, network managers can publish policy settings and configuration changes from a single console to multiple Cisco ESAs and WSAs. Alternatively, organizations can dedicate specific appliances to individual applications for high-volume deployments.

In addition, network managers can be notified when security appliances exceed their recommended capacity. The Cisco SMA reports the number of transactions per second and the system's latency, response time, and proxy buffer memory. This information enables network managers to determine when they need to reconfigure the system or install additional appliances.

Improved Compliance Monitoring and Enforcement

Centralized reporting and tracking help determine which users are in violation of acceptable use policies, identify policy infractions across any department or site, and monitor the use of Web 2.0 applications such as Facebook and YouTube as well as visits to URLs in specific categories such as “gambling” or “sports.”

By centralizing the management of multiple appliances, administrators can enforce consistent acceptable use policies across the organization.

Enhanced Threat Protection

The Cisco SMA delivers a comprehensive view of an organization’s security operations, providing better threat intelligence, defense, and remediation. Important features include the centralized management of email spam quarantine, comprehensive threat monitoring across multiple web security gateways, web reputation scoring, and botnet detection. The Cisco SMA’s reporting capabilities can also be used to help administrators identify and address activities involving data loss prevention (DLP).

High Performance and Scalability

The Cisco SMA has two proprietary databases optimized for reporting and tracking, rather than a single generic database. Appropriate computations are applied to each query for the rapid generation of real-time reports.

Built on the high-performance Cisco AsyncOS® operating system, the Cisco SMA provides industry-leading scalability to meet the demands of small, medium-sized, and large enterprises as well as service providers.

Flexible Deployment with the Cisco Content Security Management Virtual Appliance

The Cisco Content Security Management Virtual Appliance (SMAV) significantly lowers the cost of managing email and web security, especially in highly distributed networks. Your network manager can create instances where and when they are needed, using your existing network infrastructure. The Cisco SMAV is a software version of the Cisco SMA and runs on top of a VMware ESXi hypervisor and Cisco Unified Computing System™ (Cisco UCS®) servers. You will receive an unlimited number of Cisco SMAV instances with the purchase of a SMA software license for any of the Cisco Email or Web Security software bundles.

With the Cisco SMAV, you can respond instantly to increasing traffic growth with simplified capacity planning. You don’t need to buy and ship appliances, so you can support new business opportunities without adding complexity to a data center or having to hire additional staff.

Table 1. Features and Benefits of the Cisco SMA and SMAV

Feature	Benefits
Centralized management and reporting	The Cisco SMA simplifies administration by publishing configurations from a single management console to multiple Cisco ESAs and WSAs. Updates and settings are managed centrally on that console rather than on the individual appliances. Organizations can dedicate specific appliances to individual applications for high-volume deployments. Fully integrated reporting allows traffic data from multiple Cisco ESAs and WSAs to be consolidated.
Message tracking	Data is aggregated from multiple Cisco ESAs, including data categorized by sender, recipient, message subject, and other parameters. Scanning results, such as spam and virus verdicts, are also displayed, as are policy violations.
Web tracking	A record of individual web transactions is maintained, with information such as IP address, username, domain name, time accessed, and other details. Visibility is provided into employee use of Web 2.0 applications such as Facebook, YouTube, and instant messaging.
Web reporting	Web tracking information is aggregated in real time and displayed in a high-level, easy-to-use graphical format. Reporting features help administrators determine the websites, URL categories, and applications that employees can access on company devices.

Feature	Benefits
Spam quarantining	Spam and marketing messages are stored centrally with the easy-to-use self-service Cisco Spam Quarantine solution. Large enterprises with multiple Cisco ESAs can offload their spam traffic to one location for easier tracking and provide a single point for employee access.
Threat monitoring	Data about web-based threats is provided in real time, including, for example, which users are encountering the most blocks or warnings, and which websites and URL categories pose the biggest risks. Malware and other threats that Cisco WSAs have detected and blocked are also reported.
Reputation scoring	This feature provides detailed information about the reputation scores of the websites that users access. These scores are based on data provided by Cisco WSAs, which analyze web server behavior and assign a score to each URL that reflects the likelihood that it contains malware.
Botnet detection	Ports and systems with potential malware connections are displayed. Data from the Layer 4 traffic monitoring feature on Cisco WSAs can help organizations detect and remediate botnet-infected hosts.

Product Specifications

Cisco SMAs are built to meet the requirements of organizations of different sizes and to complement all Cisco ESAs and Cisco WSAs. Table 2 presents the performance specifications, Table 3 presents the hardware specifications, and Table 4 presents the ordering information for the Cisco SMA.

Table 2. Cisco SMA Performance Specifications

	Number of Users*	Model	Disk Space	RAID Mirroring	Memory	CPUs
Large enterprise	10,000 or more	Cisco SMA M680	4.8 TB (8 x 600-GB SAS)	Yes (RAID 10)	32 GB	12 (2 hexa cores) 2.00 GHz
Midsize office	2000 to 10,000	Cisco SMA M380	2.4 TB (4 x 600-GB SAS)	Yes (RAID 10)	32 GB	12 (2 hexa cores) 2.00 GHz
Small business or branch office	Up to 2000	Cisco SMA M170	500 GB (2 x 250-GB SATA)	Yes (RAID 1)	4 GB	2 (1 dual core) 2.00 GHz

* Please confirm sizing guidance with a Cisco content security specialist to help ensure that your solution will meet your current and projected needs.

Table 3. Cisco SMA Hardware Specifications

	Cisco SMA M680	Cisco SMA M380	Cisco SMA M170
Hardware platform			
Form factor	2 rack units (2RU)	2RU	1RU
Dimensions (H x W x D)	3.5 x 19 x 29 in. (8.9 x 48.3 x 73.7 cm.)	3.5 x 19 x 29 in. (8.9 x 48.3 x 73.7 cm.)	1.67 x 16.9 x 15.5 in. (4.24 x 42.9 x 39.4 cm)
Redundant power supply	Yes	Yes	No
Remote power cycle	Yes	Yes	No
DC power option	Yes	Yes	No
Hot-swappable hard drive	Yes	Yes	Yes
Fiber option	Yes (accessory)	No	No
Ethernet	4 Gigabit Ethernet NICs, RJ-45	4 Gigabit Ethernet NICs, RJ-45	2 Gigabit Ethernet NICs, RJ-45
Speed (Mbps)	10/100/1000, autonegotiate	10/100/1000, autonegotiate	10/100/1000, autonegotiate

Table 4. Cisco SMAV

SMA Users				
SMA Users	**Model**	**Disk**	**Memory**	**Cores**
Evaluations only	Cisco SMAV M000v	250 GB (10K RPM SAS)	4 GB	1 (2.7 GHz)
Small Enterprise (up to 1K)	Cisco SMAV M100v	250 GB (10K RPM SAS)	6 GB	2 (2.7 GHz)
Medium Enterprise (up to 5K)	Cisco SMAV M300v	1024 GB (10K RPM SAS)	8 GB	4 (2.7 GHz)
Large enterprise or service provider	Cisco SMAV M600v	2032 GB (10K RPM SAS)	8 GB	8 (2.7 GHz)
Servers				
Cisco UCS			**VMware ESXi 5.0, 5.1 and 5.5 Hypervisor**	vmware

Table 5. Ordering Information for the Cisco SMA

Part Number	Description
SMA-M680-K9	Cisco M680 (for organizations of more than 10,000 users)
SMA-M380-K9	Cisco M380 (for organizations of up to 10,000 users)
SMA-M170-K9	Cisco M170 (for organizations of up to 1000 users)

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, and maintaining brand reputation. Cisco security solutions embedded into the fabric of your network enable you to connect to the right information with a high degree of security without disrupting your business. No organization understands network security like Cisco. Our market leadership, industry-leading 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 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 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 45 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 C78-721194-05 05/15