Cisco Content Security Management Appliances for Email and Web Security

What Is the Value of Cisco Content Security Management Appliances?

Organizations must often coordinate the management and administration of multiple security appliances across geographically dispersed teams and must do so with limited staff and budget. To address these challenges, the Cisco® Content Security Management Appliance (SMA) centralizes management and reporting functions across multiple Cisco Email Security Appliances and Cisco Web Security Appliances. This integration simplifies administration and planning, improves compliance monitoring, enables a consistent enforcement of policy, and enhances threat protection.

Built on a robust platform optimized for reporting and tracking, the Cisco SMA also delivers high performance and scalability for lasting investment value.

Centralized Management

The Cisco SMA simplifies administration by publishing configurations from a single management console to multiple Cisco Web and Email Security Appliances. Updates and settings are managed centrally on the SMA console rather than on the individual appliances. Alternatively, organizations can dedicate specific appliances to handle individual applications in high-volume deployments.

Centralized Reporting

Fully integrated reporting allows real-time traffic data from multiple Cisco Email and Web Security Appliances to be consolidated. Reporting features of the Cisco SMA include:

- **Message tracking:** Data is aggregated from multiple Cisco Email Security Appliances, including data categorized by sender, recipient, message subject, and other parameters. Scanning results, such as spam and virus verdicts, are also displayed, along with policy violations.
- **Web tracking:** A record of individual Web transactions is maintained, with information such as IP address, user name, domain name, time accessed, and other details. Visibility is provided into employee usage of Web 2.0 applications such as Facebook, YouTube, and instant messaging.
- **Web reporting:** Web tracking information is aggregated in realtime and displayed in a high-level, easy-to-use graphical format. Reporting functionality helps administrators determine the Web sites, URL categories, and applications that employees can access on company devices.

Enhanced Threat Protection

The Cisco SMA delivers a comprehensive view of an organization's security operations, providing greater threat intelligence, defense, and remediation. Threat protection features include:

- **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 Email Security Appliances 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 realtime, including which users are encountering the most blocks or warnings, and which Web sites and URL categories pose the biggest risks, for example. Malware and other threats that Cisco Web Security Appliances have detected and blocked are also reported.
- **Reputation scoring:** This feature provides detailed information about the reputation scores of the Web sites that users access. These scores are based on data provided by Cisco Web Security Appliances, which analyze Web server behavior and assign a score to each URL that reflects the likelihood that it contains malware.
- **Data loss prevention:** Detailed information is available on policy violations, filter matches, and user activity, even for events that may have occurred months or years ago. Long-term visibility allows administrators to identify and address main activities and trends for remediation and prevention.
- **Botnet detection:** Ports and systems with potential malware connections are displayed. Data from the Layer 4 traffic monitoring feature on Cisco Web Security Appliances can help organizations detect and remediate botnet-infected hosts.

Compliance Monitoring and Enforcement

Centralized reporting and tracking helps to determine which users are in violation of acceptable use policies. The features also help to 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 categories such as "gambling" or "sports."

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

Simplified Administration and Planning

The Cisco SMA provides an easy-to-use intuitive interface. Upgrades and new features are delivered directly from Cisco for the customer's approval and then automatically installed and managed.

In addition, administrators 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 allows administrators to determine when they need to reconfigure the system or install additional appliances.

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 large enterprises and service providers.

Cisco Content Security Management Appliance Models

The Cisco SMA platform is built to meet the requirements of organizations of different sizes and to support all Cisco Email and Web Security Appliances:

Deployment	Users*	Model	Description
Large enterprise	10,000+	Cisco SMA 1070	For large enterprises with multiple Cisco Email and Web Security Appliances
		Cisco SMA M680	For the most demanding deployments; the highest-performing model in the Cisco SMA product line
Medium sized enterprise	1000 to 10,000	Cisco SMA M670	For organizations with multiple Cisco Email and Web Security Appliances and up to 10,000 users
		Cisco SMA M380	For midsize deployments; built on the latest generation of appliance hardware
Small business or branch office	Up to 1000	Cisco SMA M170	For organizations and branch offices with fewer than 1000 users

For More Information

For more information about the Cisco SMA platform, visit http://www.cisco.com/go/sma or contact your Cisco local account representative.

The best way to understand the benefits of the Cisco SMA platform 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.

C45-720312-01 10/13