Cisco IronPort M-Series Security Management Appliance

Introduction

IT organizations are being asked to take on additional responsibilities, often with the same or even less headcount. Administrators are expected to be experts in numerous different areas, from security to communications systems, and must also be familiar with - and able to use - multiple different products and systems in each area. And as organizations expand and grow, the level of management overhead can increase exponentially.

The Cisco IronPort™ M-Series Security Management Appliance centralizes and consolidates important management and reporting insight in a single interface, providing a central platform for all reporting and auditing information for Cisco IronPort web and email security systems.

Centralized Management and Reporting

For distributed networks with multiple locations, the Cisco IronPort M-Series Security Management Appliance enables centralized, consistent policy across different C-Series or S-Series appliances, and across geographic boundaries. Built on the Cisco IronPort AsyncOS® operating system, the Cisco IronPort M-Series provides industry-leading robustness, scalability, and supportability, easily supporting large enterprise and ISP customers.

Email Reporting

Advanced message tracking enables administrators to know where and when an email communication took place. They can search message telemetry for multiple email security appliances based on sender, recipient, message subject, or a host of advanced parameters. They can then report the full scanning results, such as spam/virus verdicts or policy violations, as well as delivery details such as TLS statistics, email authentication, or Cisco IronPort Email Encryption technology.

Cisco IronPort Spam Quarantine is a self-service solution with an easy-to-use web- or email-based interface and simple integration into existing directory and mail systems. All operations are automatic and self-managing, so there is no risk of a capacity overload. Most importantly, Cisco IronPort Spam Quarantine requires no maintenance by the administrator or the end user. End 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 the quarantine message digests. Cisco IronPort Spam Quarantine fully integrates the capability for end users to create their personal safelists and blocklists.

Web Reporting

Cisco IronPort reporting data from multiple web security appliances can be consolidated and centralized to provide fully integrated security reporting. A unique threat correlation engine provides unprecedented insight into even the highest-volume networks in the world. Detailed and accurate information is integrated into interactive and actionable reports, suitable for all levels of an organization. Cross-application reporting provides insight into the threats being blocked from inside and outside the network, as well as internal user behavior and critical content security policy. Administrators can see which users are visiting websites or web applications in violation of acceptable use policies, and can track policy infractions across any department or site.

Comprehensive web reports allow network security administrators to identify and troubleshoot malware threats, potential infections, and botnet activity. With centralized web reporting, system administrators can view the biggest threats to their network, which users are encountering the most blocks or warnings, and which websites and URL categories are posing the biggest risk.

Product Line

- **Cisco IronPort Security Management Appliance M1070:** Consolidated management appliance designed to meet the needs of the most demanding networks in the world.
- **Cisco IronPort Security Management Appliance M670:** Designed for organizations with multiple gateway security appliances and thousands of users.
- **Cisco IronPort Security Management Appliance M170:** Designed for organizations with multiple gateway security appliances and less than 1000 users.

	Cisco IronPort M1070	Cisco IronPort M670	Cisco IronPort M170
Chassis			
Form Factor	2U	2U	1U
Dimensions	3.5" (h)x 17.5" x 26.8"(d)	3.5" (h) x 17.5” x 26.8” (d)	1.67" (h) x 16.9” x 15.5” (d)
Total Weight (lb)	57.5	52.2	26.96
Power Supply	870W, 100/240V	870 watts, 100/240V	400 watts, 100/240V
Redundant Power Supply	Yes	Yes	No
Processor, Memory and Disks			
CPUs	2x4 (2 Quad Cores)	2x4 (2 Quad Cores)	1x2 (1 Dual Core)
Memory	4 GB	4 GB	4 GB
Disk Space & Count	3.6 TB (600 * 6)	1.8 TB (300 * 6)	500GB (250 * 2)
Hot Swappable Hard Disk	Yes	Yes	Yes
RAID Level & 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

	Cisco IronPort M1070	Cisco IronPort M670	Cisco IronPort M170
Configuration Logging and Monitoring			
Web Interface	GUI-based (HTTPS)	GUI-based (HTTPS)	GUI-based (HTTPS)
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
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
Ambience Noise (bels)	6.3	6.1	Idle: 41.3 dBa Stress: 64.2 dBa max.
Effective MTBF (Hours)	94400	94400	107356
Operating			
Temperature (°C)	10℃ to 35℃	10℃ to 35℃	-5°C to 45°C
Relative Humidity (%)	20% to 80% (noncondensing)	20% to 80% (noncondensing)	20% to 80% (noncondensing)
Altitude (m)	3048	3048	3000
Vibration	0.26 Grms at 5-350Hz	0.26 Grms at 5-350Hz	0.41Grms, at 3Hz-500Hz
Non - Operating			
Temperature (°C)	-40℃ to 65℃	-40℃ to 65℃	-25°C to 70°C
Relative Humidity (%)	5% to 95% (noncondensing)	5% to 95% (noncondensing)	5% to 95% (noncondensing)
Altitude (m)	10,600	10,600	4570
Vibration	1.54 Grms at 10-250Hz	1.54 Grms at 10-250Hz	1.12Grms at 3Hz-500Hz
Industry Certifications			
RoHS	Yes	Yes	Yes
Other Certifications			Safety: cULus, CB, CCC, BSMI EMC:CE, FCC, VCCI, C-TICK, KC

Conclusion

The Cisco IronPort M-Series Security Management Appliance complements Cisco's best-of-breed security appliance product line. By ensuring top performance from web security appliances and email security gateways, the Cisco IronPort M-Series provides a single location for monitoring all corporate policy settings and audit information.

Designed and built as a flexible management tool to centralize and consolidate policy and runtime data, the Cisco IronPort M-Series delivers a robust and scalable security management solution that allows administrators to easily and effectively manage their day-to-day operations. Centralized reporting provides administrators with visibility and insight into web usage and email activity and trends, ensuring that they can react and respond quickly to emerging threats.

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 C78-622041-05 05/12