

Cisco IronPort M-Series Security Management Appliance

FLEXIBLE MANAGEMENT AND COMPLETE
SECURITY CONTROL AT THE NETWORK GATEWAY



The Cisco® IronPort M-Series security management appliance is the perfect complement to Cisco's best-of-breed protection. The Cisco IronPort® M-Series centralizes and consolidates important policy and runtime data, providing administrators and end-users with a single interface for managing their email security systems. It ensures top performance from Cisco IronPort C-Series appliances, and protects corporate network integrity by increasing deployment flexibility.

This security management appliance provides the central platform for managing all reporting and auditing information for Cisco IronPort email security appliances. Optional management features allow you to coordinate all your security operations from a single security management appliance, or to spread the load across multiple appliances.

THE CISCO IRONPORT DIFFERENCE

Cisco IronPort email and web security products are high-performance, easy-to-use and technically-innovative solutions, designed to secure organizations of all sizes. Purpose built for security and deployed at the gateway to protect the world's most important networks, these products enable a powerful perimeter defense.

Leveraging the Cisco Security Intelligence Operations center and global threat correlation makes the Cisco IronPort line of appliances smarter and faster. This advanced technology enables organizations to improve their security and transparently protect users from the latest Internet threats.

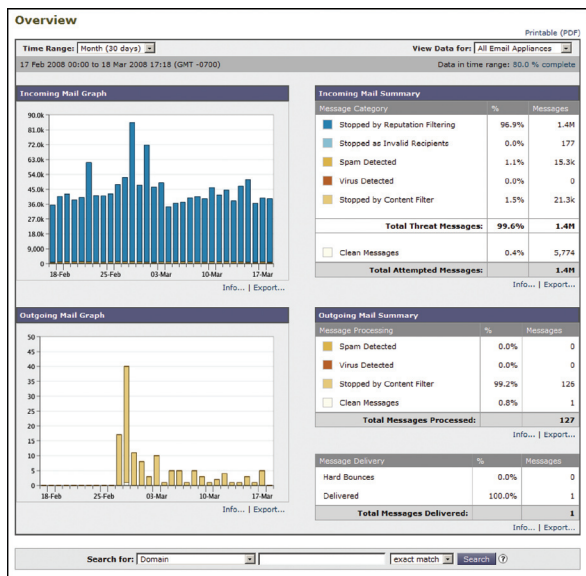


FEATURES

Security Management Functionality

Each Cisco IronPort M-Series appliance can host one or more of the unique security management features available from Cisco to ease administrator workload.

Centralized reporting allows for consolidation of Cisco IronPort Email Security Monitor reporting data from multiple email security appliances to provide fully integrated security reporting. The unique threat correlation engine provides unprecedented insight into even the highest volume networks in the world. Detailed and accurate information is coalesced 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 your network, internal user behavior and critical content security policy. See which users are sending the most mail, and track policy infractions across any department or site. The powerful reporting engine enables you to capture the current view of any report in an Adobe Portable Document Format (PDF) file, create regularly-scheduled reports that are automatically delivered via email, or even download the reporting data in CSV format for easy integration with existing monitoring solutions.



Aggregate reports provide a centralized view into email threats, while allowing you to obtain additional information on a specific email security appliance.

Advanced message tracking enables administrators to know where, and when, an email communication took place. Search message telemetry for multiple email security appliances based on the sender, recipient, message subject, or a host of advanced parameters. 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.

Message Tracking

Search

Available Time Range: 01 Nov 2007 17:36 to 18 Mar 2008 17:25 (GMT -0700) | Data in time range: 75.81% complete

Envelope Sender: [Begins With] [v]

Envelope Recipient: [Begins With] [v]

Subject: [Begins With] [v]

Date and Time Range: Start Date: [mm/dd/yyyy] [v] Time: [HH:MM:SS] [v] and End Date: [mm/dd/yyyy] [v] Time: [HH:MM:SS] [v] (GMT -0700)

Sender IP Address: [v]

Message Event: [v] Search rejected connections only [v] Search messages

Selecting multiple events will expand your search to include messages that match each event type.

Virus Positive Hard bounced

Spam Positive Soft bounced

Suspect Spam Currently in Outbreak Quarantine

Delivered

Message ID Header: [v]

IronPort MID: [v]

IronPort Host: [All Hosts] [v]

Query Settings: [v] Query timeout: [3 minute] [v] Max. results returned: [250] [v]

Clear [v] Search [v]

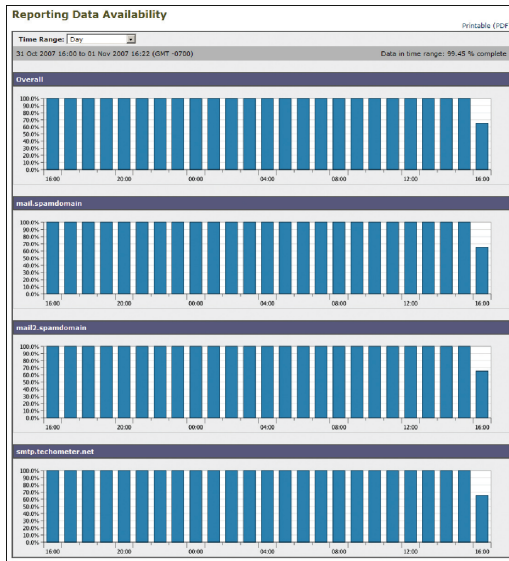
An intuitive and powerful search interface provides administrators with an easy way to quickly track emails for troubleshooting or auditing purposes.

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, the 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. The Cisco IronPort Spam Quarantine fully integrates the capability for end-users to create their personal safelists and blocklists.



FEATURES (CONTINUED)



The Data Availability report helps easily answer the question, "Is my reporting data complete, or is there information missing?"

BENEFITS

Maximize Your Security Budget The Cisco IronPort M-Series stretches your dollar, by providing a centralized location for storing and processing email security data. Reporting data, message tracking information and quarantines can all be managed by the Cisco IronPort M-Series — letting you dedicate your other appliances to keeping security threats at bay.

Reduce Your Administration with AsyncOS Unlike other management and quarantine solutions that require one or more separate servers, the Cisco IronPort M-Series is built on Cisco IronPort AsyncOS — a fully-managed, high-performance operating system. All upgrades and new features are delivered directly from Cisco for your approval, then automatically installed and managed. Intuitive user interfaces make this powerful platform incredibly easy to use.

Security Management Platform

Built on the Cisco IronPort AsyncOS® operating system, the Cisco IronPort M-Series provides industry-leading robustness, scalability and supportability.

The next generation architecture of the Cisco IronPort M-Series enables it to easily support large enterprises and ISP customers, which handle tens of millions of messages every day.

Redundant data aggregation provides customers the ability to aggregate the same email reporting and message tracking information on two separate Cisco IronPort M-Series appliances.

A modular design allows customers to run all Cisco IronPort M-Series security features on a single appliance, or dedicate specific appliances to individual applications for high-volume deployments.

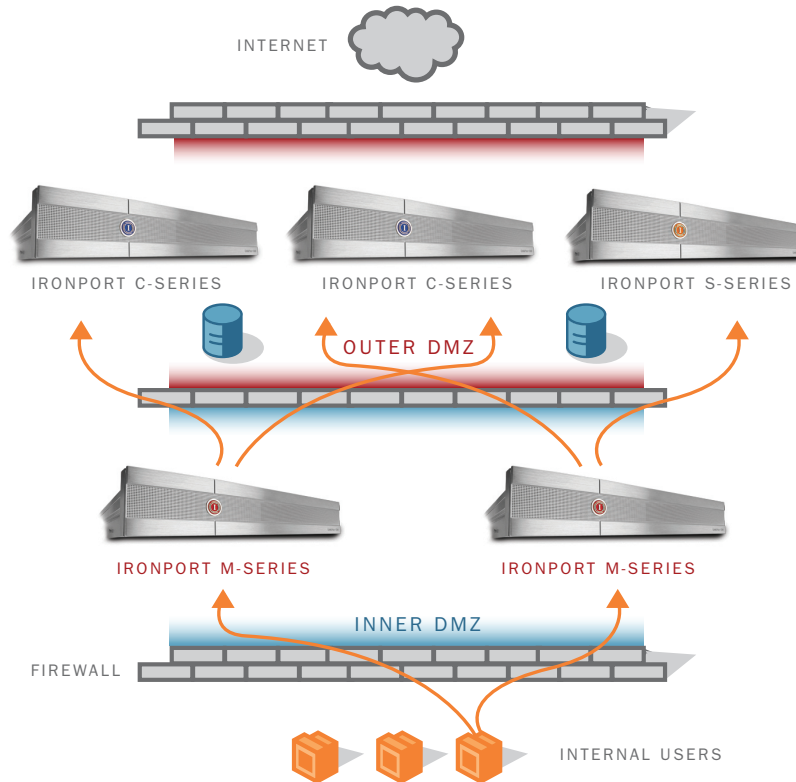
Built-in DLP capabilities The Cisco IronPort M-Series provides detailed information on policy violations, filter matches, and user activity — even for events that may have occurred months or years ago. This long-term visibility allows messaging administrators to quickly and easily respond to requests for trend analyses and audits that are critical to the remediation workflow for data loss prevention and compliance.



FIGURE 1

Cisco IronPort M-Series Deployment

The Cisco IronPort M-Series centralizes and consolidates important policy and runtime data, providing administrators and end-users with a single interface for managing their email security systems.



SPECS (MODEL DEPENDENT)

	Cisco IronPort M1070	Cisco IronPort M670	Cisco IronPort M160
Chassis			
Form Factor	19" rack-mountable, 2U rack height	19" rack-mountable, 2U rack height	19" rack-mountable, 1U rack height
Dimensions	3.4" (h) x 17.44" (w) x 26.8" (d)	3.4" (h) x 17.44" (w) x 26.8" (d)	1.75" (h) x 17.5" (w) x 21.5" (d)
Power Supplies	570 watts (Energy Smart), 90-264 VAC	570 watts (Energy Smart), 90-264 VAC	345 watts, 100/240 volts
Processor, Memory, and Disks			
CPU	2x4 (Quad) Core Intel	2x4 (Quad) Core Intel	1x2 (Dual) Core Intel
Memory	4 GB	4 GB	4 GB
Disk Space	3.6 TB	1.8 TB	500 GB
RAID	RAID 10, battery-backed 256MB cache	RAID 10, battery-backed 256MB cache	RAID 1
Interfaces			
Ethernet	4xGigabit NICs, RJ-45	4xGigabit NICs, RJ-45	2xGigabit NICs, RJ-45
Fiber	Yes	No	No
Web Interface	GUI-based (HTTP or HTTPS)	GUI-based (HTTP or HTTPS)	GUI-based (HTTP or HTTPS)

Compatibility: Interfaces with all Cisco IronPort gateway security appliances.



PRODUCT LINE

Sizing Up Your Security Management Solution

The Cisco IronPort email and web security product line address issues faced by organizations ranging from small businesses to the Global 2000.

Cisco IronPort M1070	Consolidated management appliance designed to meet the needs of the most demanding networks in the world.
Cisco IronPort M670	Suggested for organizations with multiple gateway security appliances and thousands of users.
Cisco IronPort M160	Designed for organizations with multiple gateway security appliances and less than 2000 users.

SUMMARY

Centralized Security Management

The Cisco IronPort M-Series security management appliance complements Cisco's best-of-breed security appliance product line. By ensuring top performance from your email security gateways, the Cisco IronPort M-Series provides one location for you to monitor 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 messaging operations — ensuring that they can react and respond quickly to emerging threats.

CONTACT US

Cisco sales representatives, channel partners and system engineers are ready to help you evaluate how Cisco IronPort products can make your corporate network infrastructure secure, reliable and easier to manage. If you believe that your organization could benefit from these industry-leading products, please call 650-989-6530 or visit us on the web at www.ironport.com/leader.



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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco.Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

P/N 435-0130-7 04/10