Ⓘ IRONPORT®

FLEXIBLE MANAGEMENT AND COMPLETE SECURITY CONTROL AT THE NETWORK GATEWAY

IronPort M-Series Security Management Appliance

OVERVIEW

IRONPORT M-SERIES—CONSOLIDATED MANAGEMENT FOR EMAIL AND WEB SECURITY

One location to manage, store, and monitor all corporate policy settings and audit information.

The *IronPort M-Series*™ security management appliance is the perfect compliment to IronPort's best-of-breed email and Web security protection. The *IronPort M-Series* centralizes and consolidates important policy and runtime data, providing administrators and end-users with a single interface for managing their application layer security systems. The *IronPort M-Series* ensures top performance from your *IronPort C-Series*™

and *IronPort S-Series*™ appliances, and protects corporate network integrity by increasing your deployment flexibility.

This security management appliance provides the central platform for managing all policy, reporting, and auditing information for IronPort's email and Web 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.

FEATURES

SECURITY MANAGEMENT PLATFORM

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

The end-user 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 *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.

IRONPORT M-SERIES OPTIONS

Centralized reporting allows for consolidation of traffic data from multiple email and Web security appliances to provide fully integrated security reporting across all protocols. IronPort's third-generation reporting technology provides unprecedented insight into even the highest volume networks in the world. Detailed and accurate information is coalesced into clear and informative 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 machines are infected with different threats, see which users are sending the most mail, and track policy infractions across any department, site, or communication medium.

End-to-end communications auditing enables administrators to know where, and when, a communication took place. Search message telemetry for multiple email security appliances or request-response data from the Web and report the full scanning and delivery details.

Consolidated policy management provides security policies across logical business groups, then deploys them across physical security appliances.
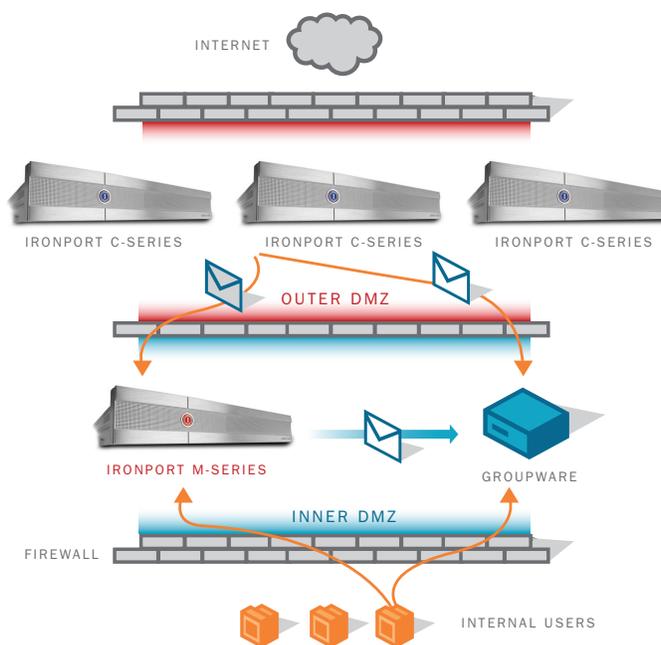
Bring the flexibility and ease-of-use of *IronPort Email Security Manager™* to all of your protected applications.

Until now, security for communication applications has been handled by various disparate point solutions, all with their own complex policy settings. Ensuring accurate and complete security coverage against all threats required intensive manual administration, using several different interfaces. IronPort provides a common policy language across various application security gateways, reducing administrative overhead and ensuring complete enforcement of security policies across all application security boundaries.

FIGURE 1.

IRONPORT M-SERIES DEPLOYMENT

Maintain Corporate Firewall Integrity

By centralizing all end-user data to a dedicated *IronPort M-Series,* end-user access can be limited to internally protected networks. There is no longer any need to punch holes through to a secure border DMZ.

INTERNET

IRONPORT C-SERIES   IRONPORT C-SERIES   IRONPORT C-SERIES

OUTER DMZ

IRONPORT M-SERIES   GROUPWARE

INNER DMZ

FIREWALL

INTERNAL USERS

BENEFITS

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

Centralize Your Security By defining administrative policies across multiple protocols and consolidating policy configuration for discrete business units, the *IronPort M-Series* can manage and report on all security telemetry from a centralized location—significantly reducing network vulnerabilities.

Reduce Your Administration with AsyncOS™ Unlike other management and quarantine solutions that require a separate Windows server, the *IronPort M-Series* is built on IronPort's *AsyncOS*—a fully managed, high-performance operating system. All upgrades and new features are delivered directly from IronPort for your approval, then automatically installed and managed.

TECHNICAL DETAILS

SPECIFICATIONS

	M600	M1000
Chassis/Processor		
Form Factor	19" Rack-Mountable, 2U rack height	19" Rack-Mountable, 2U rack height
Dimensions	3.5" (h) x 19" (w) x 29" (d)	3.5" (h) x 19" (w) x 29" (d)
CPU	2 x 2.8GHz Intel Xeon	2 x 3.6GHz Intel Xeon
Power Supplies	Hot-plug redundant, 700 watts, 100/240 volts	Hot-plug redundant, 700 watts, 100/240 volts
Storage		
RAID	RAID 10 configuration; Dual channel; Battery-backed cache	RAID 10 configuration; Dual channel; Battery-backed cache
Drives	4 x 146GB UltraSCSI	4 x 300GB UltraSCSI
Connectivity		
Ethernet	One Intel 10/100 BaseT and two Broadcom Gigabit BaseT Ethernet ports	One Intel 10/100 BaseT and two Broadcom Gigabit BaseT Ethernet ports
Interfaces/Configuration		
Web Interface	Accessible by HTTP or HTTPS	Accessible by HTTP or HTTPS

Compatibility: Interfaces with all IronPort email and Web security appliances.

PRODUCT LINE

CONSOLIDATING SECURITY MANAGEMENT

IronPort Systems provides industry-leading email and Web security products for organizations ranging from small businesses to the Global 2000.

IronPort M1000	Consolidated management appliance designed to meet the needs of the most demanding networks in the world.
IronPort M600	Suggested for organizations with multiple gateway security appliances and thousands of users.

SUMMARY

CONSOLIDATED MANAGEMENT FOR EMAIL AND WEB SECURITY

The *IronPort M-Series* security management appliance compliments IronPort's best-of-breed email and Web security appliances. By ensuring top performance for all of your application security gateways, the *IronPort M-Series* provides one location for you to manage, store and monitor all corporate policy settings and audit information. Designed and built as a flexible management tool to centralize and consolidate policy and runtime data, administrators have a single interface to manage all of their application layer security systems.

CONTACT US

HOW TO GET STARTED WITH IRONPORT

Through a global salesforce and reseller network, IronPort offers a free "Try Before You Buy" program for the *IronPort M-Series* security management appliance. To learn if you qualify call 650-989-6530 or visit us on the Web at www.ironport.com/try

I IRONPORT®

IronPort Systems, Inc.
950 Elm Avenue, San Bruno, CA 94066
TEL 650.989.6500 FAX 650.989.6543
EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems is the leading email and Web security products provider for organizations ranging from small businesses to the Global 2000. IronPort provides high-performance, easy-to-use, and technically innovative products for those faced with the monumental task of managing and protecting their mission-critical networks from Internet threats.

IRONPORT S-SERIES
04/06
DOC RELEASE