Cisco IronPort X1070 Email Security System

As the battle to protect the email perimeter continues, two predominant trends emerge: higher mail volumes and more resource-intensive scanning. The Cisco® IronPort X1070 is purpose-built, on the foundation of the Cisco IronPort® AsyncOS operating system, to provide power for today's volumes and high-performance scanning for tomorrow's threats. This unparalleled performance delivers dial-tone availability—saving hours of productivity and thousands of dollars during peak traffic times, such as damaging virus outbreaks or spam attacks.

The world's largest organizations and ISPs need a secure and easy-to-manage email security solution that protects all facets of their complex email infrastructures. The Cisco IronPort X1070 provides Cisco's exclusive preventive filters and signature-based reactive filters, combined with data loss prevention (DLP) and best-of-breed encryption technology, to provide the highest level of email security available today—while delivering unprecedented visibility and management tools.

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

The Cisco IronPort X1070 provides the world's most powerful multi-layered approach to email security.

Spam Protection

Cisco provides defense in depth against spam by providing two layers of protection—a preventive layer of reputation filters, followed by reactive filters.

Cisco IronPort Reputation Filters provide an outer layer of defense using Cisco SenderBase® data to perform a real-time email traffic threat assessment and identify suspicious email senders.

Cisco IronPort Anti-Spam utilizes the industry's most innovative approach to threat detection, based on a unique Context Adaptive Scanning Engine (CASE). Cisco IronPort CASE examines the complete context of a message, including: "What" content the message contains, "How" the message is constructed, "Who" is sending the

message, and “Where” the call to action of the message takes you. By combining these elements, Cisco IronPort Anti-Spam stops the broadest range of threats with industry-leading accuracy.

Cisco IronPort Spam Quarantine is a self-service end-user solution, with an easy to use web- or email-based interface. This feature provides end-users with their own safe holding area for spam messages and integrates seamlessly with existing directory and mail systems.

Virus Protection

Cisco IronPort Outbreak Filters identify and stop viruses hours before traditional virus signatures are available.

Sophos Anti-Virus technology provides a fully integrated second layer of virus protection with the highest-performance virus scanning technology in the industry.

McAfee Anti-Virus technology is incorporated to provide an additional layer of protection (either in conjunction with, or as an alternative to, Sophos) for maximum virus security.

Data Loss Prevention

Integrated data loss prevention (DLP) is provided with RSA Email DLP. Cisco has partnered with RSA, the leader in DLP technology, to enable RSA Email DLP on Cisco IronPort email security appliances.

Cisco IronPort Email Encryption gives administrators the ability to secure confidential data and comply with partner, customer or regulatory requirements. This encryption technology enables simple, secure communication from the gateway to any recipient inbox— while TLS, PGP and S/MIME technology provide security between partner email gateways.

Compliance Quarantine provides delegated access to emails that have been flagged by the content scanning engine.

Email Authentication

DomainKeys Identified Mail (DKIM), and DomainKey verification and signing digitally process messages to establish and protect identities with email senders and receivers on the Internet.

Cisco IronPort Bounce Verification tags messages with a digital watermark to provide filtering of bounce attacks at the network edge.

Directory Harvest Attack Prevention tracks spammers who send to invalid recipients and blocks attempts to steal email directory information.

Enterprise Management Tools

Email Security Manager is a powerful, graphical management tool that yields fingertip control to manage all security— including preventive and reactive anti-spam and anti-virus filters, email encryption and content filtering.

Intuitive GUI enables unprecedented visibility and control. The integrated web-based user interface enables real-time and historical reporting along with the ability to configure policies, search, and selectively release quarantined messages.

Centralized Management eliminates a single point of failure with superior “peer to peer” architecture, and makes managing multi-box installations of Cisco IronPort email security appliances simple. The ability to manage configuration at multiple levels allows organizations to manage globally while complying with local policies.

Email Security Monitor delivers real-time threat monitoring and reporting. This technology tracks every system connecting to the Cisco IronPort appliance to identify Internet threats (such as spam, viruses and denial-of-service attacks), monitor internal user trends and highlight compliance violations.

SNMP Enterprise MIB facilitates hands-off monitoring and alerting for all system parameters including hardware, security, performance, and availability.

Cisco IronPort MTA Platform

AsyncOS®, Cisco's proprietary operating system, was built from the ground up to address the requirements of modern email gateways and to position customers for the future of SMTP. The Cisco IronPort C670 supports thousands of simultaneous incoming and outgoing connections—ensuring that the email infrastructure is never overwhelmed, even during the largest outbreaks or attacks.

Benefits

Reporting Insight Proves ROI

The Cisco IronPort X1070 offers very sophisticated management, monitoring and reporting tools designed to satisfy the large global enterprises and ISPs that make up Cisco's customer base. Each appliance has a unique reporting system, providing both a real-time and historical look at mail flowing through an organization's email infrastructure. Cisco provides system administrators with the necessary information to make critical security decisions and demonstrate Return On Investment (ROI).

Reduced TCO

The Cisco IronPort MTA platform enables massive reduction in Total Cost of Ownership (TCO) by consolidating email operations and security into a single platform. Self-managing security services provide the lowest maintenance solution in the industry with minimal configuration requirements.

Increased End-User Productivity

Improved Administrative Efficiency

The Cisco IronPort Reputation Filtering system was the first in the industry and remains the most sophisticated. In its default settings, the system will block over 80 percent of incoming mail at the connection level. By eliminating these unwanted messages, companies save bandwidth (the message is never accepted) and system resources. CPU-intensive spam and virus filters are only used when needed, and rate limiting is a very effective defense against "hit and run" spam or denial-of-service attacks.

Minimized Downtime

The comprehensive Cisco IronPort X1070 solution ensures the availability and security of the email infrastructure. Cisco offers a variety of security applications for spam and virus filtering, content scanning, and policy enforcement. Together these features reduce the risk and potential downtime posed by security threats.

Figure 1. The Cisco IronPort X1070 enables DomainKeys; a cryptographic-based means to establish the true identity of email senders.

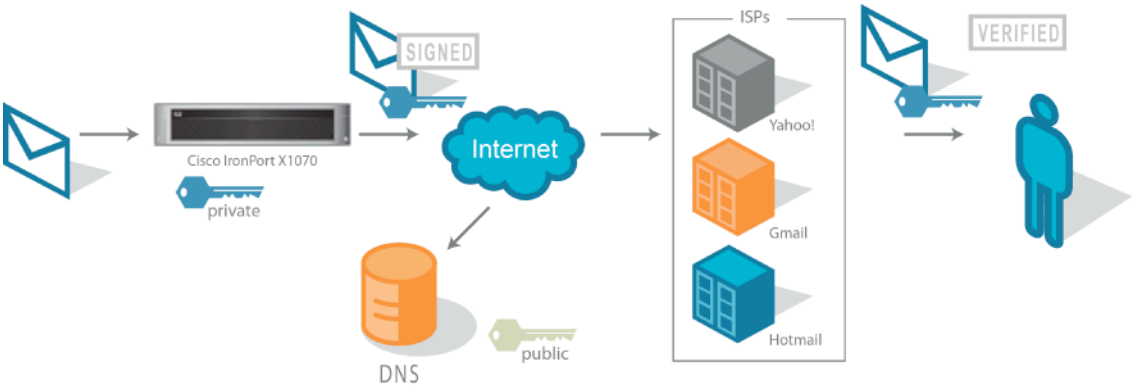
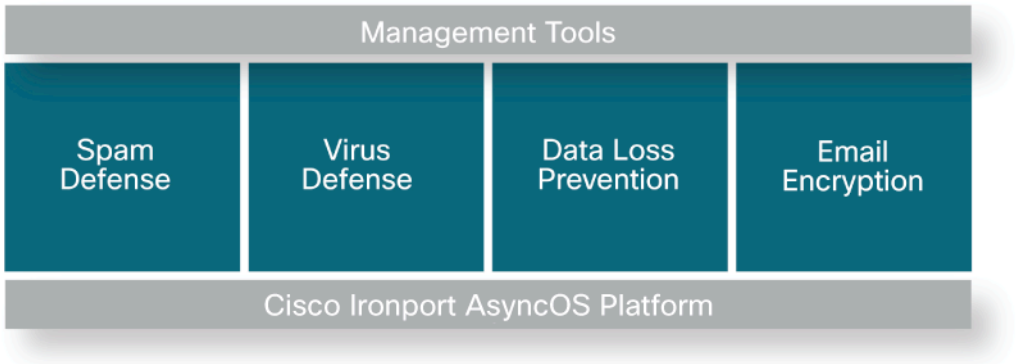


Figure 2. Power at the Perimeter: The Cisco IronPort X1070 provides multi-layered security on a single appliance by combining revolutionary Cisco IronPort technology with additional market-leading solutions.



Specifications

Chassis/Processor

Form Factor	19” Rack-Mountable, 2U rack height
Dimensions	3.4” (h) x 17.4” (w) x 26.8” (d)
CPU	Two Intel Multi-Core Processors
Power Supplies	Hot-plug redundant, 750 watts, 100/240 volts

Storage

RAID	RAID 1+ 0 configuration; dual-channel hardware with battery-backed cache
Drives	Six hot-swappable, 300 GB Serial Attached SCSI
Capacity	70 GB effective queue capacity

Connectivity

Ethernet	Four Gigabit Ethernet Ports
Serial	One RS-232 (DB-9) serial port

Mail Operations	
Mail Injection Protocols	SMTP, ESMTP, Secure SMTP over TLS
DNS	Internal resolver/cache; Can resolve using local DNS or Internet root servers
LDAP	Integrates with Active Directory, Notes, Domino and OpenLDAP servers.
Interfaces/Configuration	
Web Interface	Accessible by HTTP or HTTPS
Command Line Interface	Accessible via SSH or Telnet; Configuration Wizard or command-based
File Transfer	SCP or FTP
Programmatic Monitoring	XML over HTTP(S)
Configuration Files	XML-based configuration files archived or transferred to cluster
Cryptographic Algorithms	
TLS (Encrypted SMTP)	56-bit DES, 168-bit 3DES, 128-bit RC4, 128-bit AES and 256-bit-AES
DomainKeys Signing	512, 768, 1024, 1536 and 2048-bit RSA
SSH for System Management	768 and 1024-bit RSA
HTTPS for System Management	RC4-SHA and RC4-MD5

Product Line

Sizing Up Your Email Security Solution

Cisco provides industry leading email security products for organizations ranging from small businesses to the Global 2000.

Cisco IronPort X1070	Built to meet the needs of the most demanding networks in the world.
Cisco IronPort C670	Designed for large enterprises and service providers.
Cisco IronPort C370	Suggested for medium to large enterprises.
Cisco IronPort C370D	Recommended for any company with unique outbound email communication needs.
Cisco IronPort C170	An affordable, and easy to use, all-in-one appliance for small to medium enterprises.

Summary

Industrial Strength Email Security

The Cisco IronPort X1070 is the most sophisticated email security appliance available today. Cisco IronPort appliances are in production at eight of the ten largest ISPs and more than 40 percent of the world's largest enterprises. This system has a demonstrated record of unparalleled security and reliability.

By reducing the downtime associated with spam, viruses and a wide variety of other threats, the Cisco IronPort X1070 enables the administration of complex corporate mail systems, reduces the burden on technical staff, and quickly pays for itself. It is the advanced technology within these appliances that leads to the simplicity of management, and also the highest levels of security in the world. Cisco IronPort email security appliances are carrier class offerings that can support and protect email systems—not only from today's threats, but from those certain to evolve in the future.

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 C78-703237-00 03/12