Cisco IronPort C370 for Medium-Sized Enterprises and Satellite Offices

Medium-sized enterprises face the same daunting challenges as the Fortune 500 and Global 2000 - higher mail volumes and new, evolving threats. The Cisco IronPort® C370 Email Security Appliance is built on the foundation of the Cisco IronPort AsyncOS® operating system to provide power for today's mail volumes and high-performance scanning for tomorrow's threats. The Cisco IronPort C370 delivers industry-leading protection from inbound spam and virus attacks and outbound data loss possibilities, in an easy-to-use appliance.

Today's email-borne threats consist of virus attacks, spam, false positives, distributed denial-of-service (DDoS) attacks, spyware, phishing (fraud), regulatory compliance violations, and data loss. The Cisco IronPort C370 incorporates preventive and reactive security measures that are easy to deploy and manage.

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. Built for security and deployed at the gateway to protect the world's most important networks, these products enable a powerful perimeter defense.

Using the Cisco® Security Intelligence Operations (SIO) 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 C370 contains a powerful multilayered approach to email security - providing advanced threat prevention, blocking spam and viruses, and enabling corporate data loss prevention and remediation.

Spam Protection

Cisco defends against spam with 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 uses 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-performing virus scanning technology in the industry.

McAfee Anti-Virus technology provides an additional layer of protection (either in conjunction with, or as an alternative to, Sophos) for maximum 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. RSA Email DLP offers easy management, comprehensive protection, and unparalleled accuracy to help organizations ensure compliance with industry and government regulations worldwide and prevent confidential data from leaving customer networks.

Cisco IronPort Email Encryption gives administrators the ability to secure confidential data and comply with partner, customer, or regulatory requirements. This 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.

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

Email Authentication

DomainKeys Identified Mail (DKIM) and DomainKeys 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 enable filtering of bounce attacks at the network edge.

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

Enterprise Management Tools

Cisco IronPort Email Security Manager is a powerful graphical management tool that yields fingertip control to manage all security - including preventive and reactive antispam and antivirus filters, email encryption, and content filtering.

An 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 and makes managing multibox 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.

Cisco IronPort 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 DoS 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.

Benefits

Unprecedented Insight

Cisco IronPort technology demonstrates return on investment through sophisticated management, monitoring, and reporting tools. Each appliance has a unique reporting system, providing both a real-time and historical look at mail flowing through an organization's email infrastructure. These tools provide system administrators with the necessary information to make critical security decisions.

Figure 1. The Cisco IronPort C370 Integrates Easily Into Existing Messaging Infrastructures - Delivering In-Depth Security with Carrier-Proven Technology and the Management Capabilities Required by Large Enterprises and ISPs

Reduced Administrative Burden

The Cisco IronPort C370 uses the industry's most advanced technology to deal with threats and anomalies in a fully automated manner. This allows highly skilled IT staff to focus on other problems and leave the email issues to Cisco.

Lower TCO

The Cisco IronPort MTA platform enables a massive reduction in cost 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.

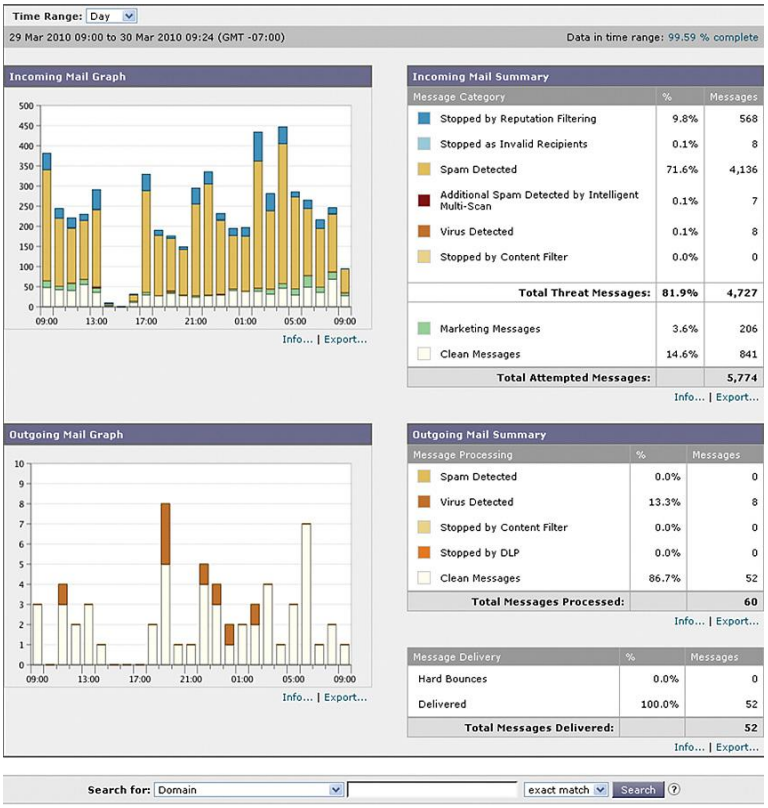
Increased End-User Productivity

By securing the network at the gateway level, the Cisco IronPort C370 acts as a "shock absorber" in front of the groupware server(s). This helps ensure that end users are not bogged down by spam, viruses, and other threats. Unlike other solutions, Cisco security services do not rely on end users to "train" the system. Instead, high accuracy is maintained through continuous and automatic rule updates.

Improved Network Efficiency

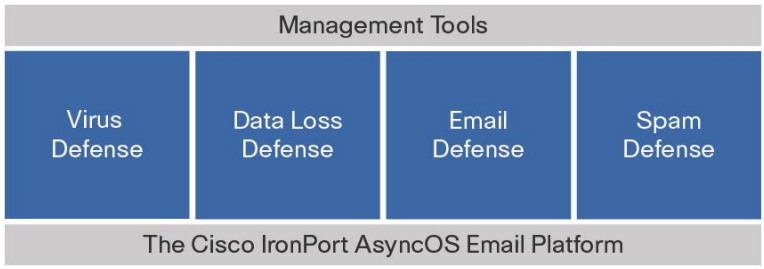
The Cisco IronPort Reputation Filtering system was the first in the industry and remains the most sophisticated. In its default settings. The system will block more than 80 percent of incoming mail at the connection level. By eliminating these unwanted messages, companies save bandwidth (the message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

Figure 2. The Email Security Monitor's Intuitive Graphical User Interface Enables Real-Time and Historical Visibility Into Email Traffic



Today's email-borne threats consist of virus attacks, spam, false positives, DDoS attacks, directory harvest attacks, phishing (fraud), data loss, and more. The Cisco IronPort C370 addresses the issues faced by medium-sized enterprises and satellite offices by uniquely combining powerful performance with preventive and reactive security measures that are easy to deploy and manage.

Figure 3. Power at the Perimeter: The Cisco IronPort C370 Provides Multilayered Security on a Single Appliance by Combining Revolutionary Cisco IronPort Technology with Additional Market-Leading Solutions



Specifications

Chassis/Processor	
Form Factor	19-in. rack-mountable, 2 RU height
Dimensions (H x W x D)	3.4 x 17.4 x 26.8 in.
CPU	One Intel multicore processor
Power Supplies	Hot-plug redundant, 750W, 100/240V
Storage	
RAID	RAID 1+ 0 configuration; dual-channel hardware with battery-backed cache
Drives	Two hot-swappable, 300 GB serial attached SCSI
Capacity	35 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 Open LDAP 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	For the most demanding networks in the world
Cisco IronPort C670	For large enterprises and service providers
Cisco IronPort C370	For medium-sized and large enterprises
Cisco IronPort C370D	For any company with unique outbound email communication needs
Cisco IronPort C160	An affordable and easy to use all-in-one appliance for small to medium-sized enterprises

Summary

Industrial-Strength Email Security

Cisco IronPort offers the most sophisticated email security system available today. In production at 8 of the 10 largest ISPs and at more than 40 percent of the world's largest enterprises, Cisco IronPort email security appliances have a demonstrated record of unparalleled security and reliability.

This same code base that powers Cisco's most sophisticated customers is also available in the Cisco IronPort C370 Email Security Appliance, helping to protect the email systems of medium-sized enterprises and satellite offices. By reducing the downtime associated with spam, viruses, and a wide variety of other threats, the Cisco IronPort C370 enables the administration of corporate mail systems, reduces the burden on technical staff, and quickly pays for itself. The advanced technology within the appliance leads to the simplicity of management - and the highest levels of security in the world. Cisco IronPort email security appliances support and protect email systems not only from today's threats, but also from those certain to evolve in the future.

Contact Us

How to Get Started with Cisco IronPort

Cisco IronPort sales representatives, channel partners, and support engineers are ready to help you evaluate how Cisco products can make your infrastructure secure, reliable, and easier to manage. If you believe that your organization could benefit from Cisco's industry-leading products, please call 650-989-6530 or visit us online at http://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.

Printed in USA C78-701392-00 02/12