IronPort C-Series Overview

High performance email security appliances. Carrier-proven technology, enterprise-class management.

The IronPort C-Series email security appliances provide advanced threat prevention, block spam and viruses, and enable corporate email policy enforcement.

All companies face the same email risks

Today's email-borne threats consist of virus attacks, spam, false-positives, DoS Attacks, misdirected bounces, and phishing (fraud). The IronPort C-Series™ email security appliance addresses the issues faced by corporations large and small by incorporating preventive and reactive security measures that are easy to deploy and manage.

THE IRONPORT C-SERIES FEATURES:

High Performance MTA Platform

IronPort Systems™ built the IronPort C-Series email security appliance from the ground up to address the requirements of modern email gateways and to position our customers for the future of SMTP. The IronPort C-Series high performance platform ensures your email infrastructure is never overwhelmed, even during the largest virus outbreaks or spam attacks—while you save money on hardware, rack space, power, and IT administration time.

IronPort's Exclusive Preventive Filters

Threat Prevention with IronPort Reputation Filters™
IronPort's reputation filtering technology identifies suspicious email senders. Suspect senders are rate limited or blocked, preventing malicious traffic from even entering the network.

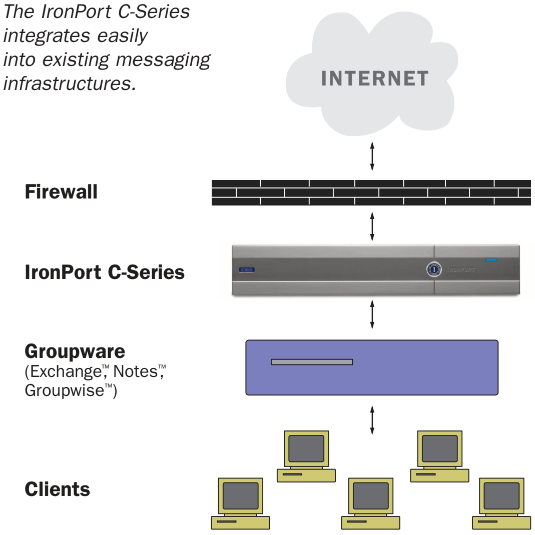
Virus Prevention with IronPort Virus Outbreak Filters™
The IronPort C-Series email security appliance detects new virus outbreaks in real-time and dynamically responds to prevent suspicious traffic from entering the network. IronPort Virus Outbreak Filters quarantine suspect messages, offering protection until new signature updates are deployed – often 6 to 8 hours before an update is released by the reactive anti-virus filters.

Signature Based Reactive Filters

Spam Detection with Symantec Brightmail Anti-Spam
The IronPort C-Series fully integrates industry-leading Symantec Brightmail anti-spam. Known as the most accurate spam detection technology available, Symantec Brightmail eliminates the headache of spam without the risk of false positives.

Virus Protection with Sophos Anti-Virus
Sophos anti-virus powers the IronPort C-Series virus protection. This is the highest performance virus scanning technology in the industry with unique Denial of Service (DoS) prevention.

The IronPort C-Series integrates easily into existing messaging infrastructures.



IronPort C-Series **Overview**

IronPort C-Series

High Performance Email Security Appliances

IronPort C10 For companies with up to 500 employees.

IronPort C60 For large enterprises and ISPs.

IronPort C30 For small and medium enterprises.

Content Filtering for Policy Enforcement

The IronPort C-Series includes the world's fastest content scanning engine. This IronPort technology allows for fine-grained enforcement of corporate email policies, based on keyword searches of messages and attachments. With content filtering, administrators have the capability to quarantine messages based on message content.

IronPort's content scanning engine can perform in-depth analysis of messages—matching it to a large library of language encoding and enforcing email policy across the entire organization.

Easy Administration in a Complex Network

Email Security Manager™

IronPort's Email Security Manager provides administrators with fingertip control to manage all email security, including preventive and reactive anti-spam and anti-virus filters, email encryption, and content filtering.

Centralized Management

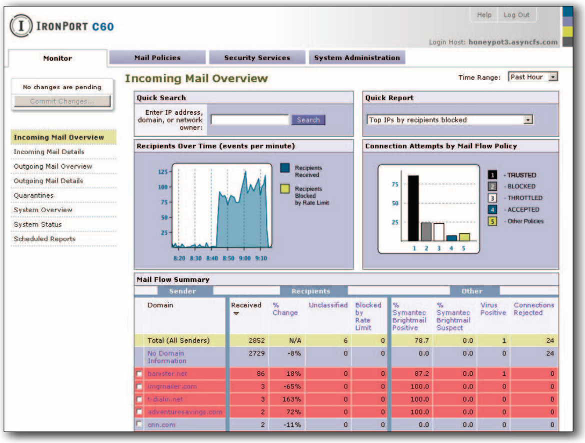
The superior "peer-to-peer" architecture eliminates a single point of failure and enables administrators to manage multiple appliances without purchasing any additional hardware. The ability to manage configuration at three different levels allows organizations to manage globally while complying with local policies.

Unprecedented Visibility and Reporting

IronPort provides system administrators with the necessary information to make critical security decisions.

Mail Flow Monitor™

With IronPort's monitoring and reporting tools, you can easily view all mail flowing through your email infrastructure. IronPort's unique Mail Flow Monitor delivers complete real-time visibility into who's sending you email. Intelligent alerts notify administrators of suspicious traffic, allowing them to take immediate action.



Login Host: honeypot3.asyncfs.com

No changes are pending

Incoming Mail Overview

Time Range: Past Hour

Quick Search

Enter IP address, domain, or network owner:

Quick Report

Top IPs by recipients blocked

Recipients Over Time (events per minute)

Connection Attempts by Mail Flow Policy

Mail Flow Summary

Sender	Recipients				Other			
Domain	Received	% Change	Unclassified	Blocked by Rate Limit	% Symantec Brightmail Positive	% Symantec Brightmail Suspect	Virus Positive	Connections Rejected
Total (All Senders)	2852	N/A	6	0	78.7	0.0	1	24
No Domain Information	2729	-8%	0	0	0.0	0.0	0	24
□ banister.net	86	18%	0	0	87.2	0.0	1	0
□ imgmailer.com	3	-65%	0	0	100.0	0.0	0	0
□ t-dialin.net	3	163%	0	0	100.0	0.0	0	0
□ adventuresavings.com	2	72%	0	0	100.0	0.0	0	0
□ cnn.com	2	-11%	0	0	0.0	0.0	0	0

***Mail Flow Monitor** Gain important insight with IronPort's unique Mail Flow Monitor, yielding a complete real-time view of all mail flowing into or out of the corporation.*

Periodic Reports

User configurable reports provide the detail and flexibility necessary for communicating to IT staff as well as senior management in support of important decisions to protect critical email infrastructure.

Mail Flow Central™

Easily find the status of any message that has traversed your infrastructure with IronPort Mail Flow Central. With this centralized reporting tool, administrators and support staff can quickly answer and end user inquiries such as, "what happened to my email?"

IRONPORT™

IronPort Systems, Inc.
1100 Grundy Lane, Suite 100
San Bruno, California 94066
tel 650.989.6500 **fax** 650.989.6543
email info@ironport.com
www.ironport.com

ABOUT IRONPORT SYSTEMS

IronPort Systems is the leading email security products provider for organizations ranging from small businesses to the Global 2000. The company has developed a family of email security appliances, the IronPort C-Series™, that offer breakthrough performance, unprecedented ease of use and reduced total cost of ownership. IronPort is driving new standards and providing innovative products for those faced with the monumental task of managing, protecting, and growing mission-critical email systems. For more information on IronPort products and services, visit: www.ironport.com

IronPort C-Series

Powering and Protecting Business Email

The IronPort C-Series™ email security appliance is built on IronPort's revolutionary MTA platform. It incorporates email threat prevention with IronPort Reputation Filters™ and IronPort Virus Outbreak Filters.™ Additional capabilities include: the IronPort content scanning engine, anti-spam and anti-virus technology.

Spam Detection with Symantec Brightmail Anti-Spam

The industry's most accurate anti-spam solution and the lowest cost of administration. Period.

Symantec Brightmail is the industry leader in anti-spam technology. Their technology protects over 300 million mailboxes and 2,000 businesses from the productivity loss and IT costs of unsolicited commercial email (spam).

Symantec Brightmail on AsyncOS

The IronPort C-Series includes integrated Symantec Brightmail 6.0 spam-fighting technology. Optimized for IronPort's AsyncOS™ operating system, Brightmail technology is extremely high performance and highly accurate. Automatic rule updates are integrated into the platform requiring zero administrator intervention.

BRIGHTMAIL WINS EDITOR'S CHOICE FOR ANTI-SPAM

PC MAGAZINE EDITORS' CHOICE

"Brightmail Anti-Spam's false-positive score speaks for itself. If you want to make sure that important messages get through to your employees, BAS is the best answer we know of."

LARRY J. SELTZER
PC Magazine

Catches Over 95% of Spam

Brightmail Anti-Spam integrates six unique technologies for a robust, multi-layered defense eliminating spam at the gateway. Rules are downloaded directly from the Brightmail servers and are typically updated every ten minutes for real-time defense.

Lowest False Positive Rate

False positives cost companies money in lost productivity and lost opportunities. Brightmail has the lowest false positive rate in the industry with less than one in one million messages being a false positive. This accuracy is only achievable by Brightmail because of the real-time methods they use to identify spam through their Probe Network.™

Lowest Total Cost of Administration

Brightmail runs the world's most advanced anti-spam operations center which delivers the most complete and up to date set of filters. The operations center runs 24x7x365 analyzing spam, generating rules, and ensuring a low false positive rate. Brightmail writes 30,000 new rules per day, so you don't have to.

"IronPort combines Brightmail's solution with its own reputation-based filter, resulting in even better detection while maintaining the extremely low false-positive rate."

FORRESTER RESEARCH

Spam Handling Flexibility

Administrators have several choices on how to handle messages that are flagged as spam by Symantec Brightmail. Choices include sending the message to a end-user web quarantine, marking up the subject header, adding an additional "X-header", sending the message to an alternate folder in the user's mailbox, deleting or bouncing the message, or a combination of these actions. The Brightmail system shares information with the IronPort C-Series Mail Flow Monitor™ and Mail Flow Central™ making real-time and historical reports instantly available at any time.

IRONPORT™

IronPort C-Series

Powering and Protecting Business Email

The IronPort C-Series™ email security appliance is built on IronPort's revolutionary MTA platform. It incorporates email threat prevention with IronPort Reputation Filters™ and IronPort Virus Outbreak Filters.™ Additional capabilities include: the IronPort content scanning engine, anti-spam and anti-virus technology.

IronPort C-Series **Sophos Anti-Virus**

IronPort C-Series **Sophos Anti-Virus**

Virus Protection with Sophos Anti-Virus

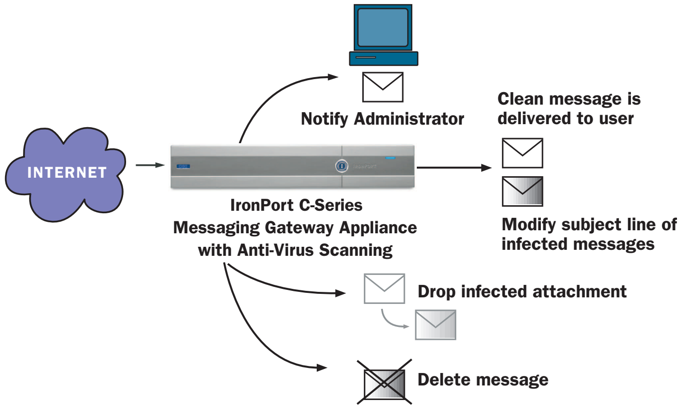
Protect your network perimeter from even the most pervasive virus outbreaks.

SOPHOS **The IronPort C-Series has the industry's highest performance virus protection with unique denial of service prevention.**

The speed and variety of recent virus attacks has highlighted the importance of a robust, secure messaging platform to protect your network perimeter. Being able to simply identify and block known viruses is no longer enough, as today's attacks can easily overwhelm most email gateways with a sudden spike in message volume, creating a Denial of Service (DoS) situation.

Robust Platform: No Denial of Service during Large-Scale Outbreaks

The IronPort C-Series appliance with the proprietary AsyncOS™ operating system can process up to 140 messages per second and sustain up to 10,000 concurrent SMTP sessions. Traditional MTAs can only handle 10 to 20 messages per second and hundreds of concurrent sessions. The unparalleled performance of the IronPort C-Series appliance protects your email infrastructure from being overwhelmed by large-scale virus outbreaks and ensures that your mission critical email will continue to be accepted.



The IronPort C-Series with Sophos anti-virus provides two layers of defense against against potential viruses.

Market Leading Sophos Anti-Virus Engine

Sophos®' market leading anti-virus scanning engine is integrated into the IronPort C-Series appliance to provide the most effective virus protection at the gateway today. Sophos is focused on providing the most advanced anti-virus solution for enterprise customers and its engine employs multiple techniques to detect and clean all major forms of viruses. It also includes advanced emulation technology to detect polymorphic viruses and an online decompressor for scanning multi-layer attachments. The robust engine supports multiple scanning modes to optimize performance.

Multiple Options for Virus Handling

Administrators have multiple options to handle infected messages. As viruses evolve, new strains of attacks try to bypass anti-virus protection by concealing viruses within password protected files or mal-formed messages. The IronPort solution will detect these messages, giving the administrator full control over how these messages are handled by the system.

High Performance Content Scanning Technology

During any virus outbreak, there is invariably a period of time between virus detection and when the actual anti-virus identity file is deployed. During this period, administrators can utilize IronPort's high performance content scanning technology to identify viruses based on known patterns and delete or archive the messages until new identity files can be updated.

IRONPORT™

IronPort C-Series

Powering and Protecting Business Email

The IronPort C-Series™ email security appliance is built on IronPort's revolutionary MTA platform. It incorporates email threat prevention with IronPort Reputation Filters™ and IronPort Virus Outbreak Filters.™ Additional capabilities include: the IronPort content scanning engine, anti-spam and anti-virus technology.

IronPort C-Series **Virus Outbreak Filters**

IronPort C-Series **Virus Outbreak Filters**

IronPort Virus Outbreak Filters

A high-performance preventive security system protects your network from infections.

IronPort email security appliances intelligently quarantine suspicious mail during the earliest stage of a virus outbreak.

IronPort Virus Outbreak Filters act to provide a critical first layer of defense against new outbreaks. The IronPort email security appliances perform a threat assessment of inbound and outbound messages. The assessment returns a virus score that triggers an automated response. Suspicious messages are quarantined temporarily and re-scanned through the traditional reactive anti-virus solutions once signature updates are in place.

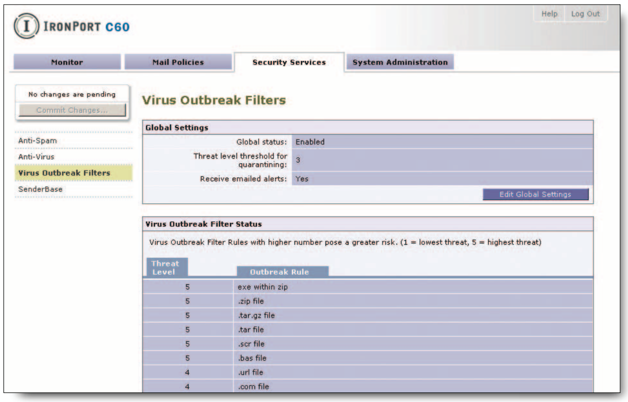
Detect New Virus Outbreaks in Real-time

New virus outbreaks are detected in real-time, hours before signatures used by reactive anti-virus solutions are updated. Detection is based on SenderBase,™ the world's largest email traffic monitoring network. Today, SenderBase captures data from over 50,000 contributing organizations and has a view into a remarkable 25% of the world's email traffic. IronPort's detection technology uses historical SenderBase data to create a statistical view of normal global traffic patterns. Realtime data from the global SenderBase network is compared and correlated with the baseline, to identify anomalies that are proven predictors of an outbreak. The IronPort Threat Operations Center (TOC) publishes rules which are used by the appliance to determine the threat level and quarantine suspicious email.

Ensure and Automate, Tailored Response

The IronPort email security appliances dynamically apply policies based on the threat level. When the threat level is elevated mail is automatically filtered and suspicious messages are quarantined. Immediate and automated response to new outbreaks provides protection until up-dated signatures are in place. At that point, mail is released and re-scanned through the traditional anti-virus filters.

Administrators can set policies based on their specific needs. The Web-based administration tool in the IronPort appliance lets administrators easily configure policy parameters, as well as view, search, test, and selectively release quarantined messages.



Virus Outbreak Filters

Global Settings

Global status:	Enabled
Threat level threshold for quarantining:	3
Receive emailed alerts:	Yes

Virus Outbreak Filter Status

Virus Outbreak Filter Rules with higher number pose a greater risk. (1 = lowest threat, 5 = highest threat)

Threat Level	Outbreak Rule
5	exe within zip
5	.zip file
5	.tar.gz file
5	.tar file
5	.scr file
5	.bas file
4	.url file
4	.com file

Unprecedented visibility and control. *The integrated Web-based user interface enables realtime and historical visibility plus the ability to configure policies, search, and selectively release quarantined messages.*

Build a Defense in Depth

IronPort Virus Outbreak Filters complement traditional anti-virus solutions. Virus Outbreak Filters detect and react to new threats in real-time to provide a critical first line of defense, preventing infections during the initial stages of a new outbreak. Reactive anti-virus solutions continue to play a critical role, accurately scanning for known viruses and cleaning, stripping or deleting email once updated signatures are in place.

IRONPORT™

IronPort Systems, Inc. 1100 Grundy Lane, Suite 100 San Bruno, California 94066 **tel** 650.989.6500 **fax** 650.989.6543 **email** info@ironport.com **web** www.ironport.com

IronPort C-Series

Powering and Protecting Business Email

The IronPort C-Series™ email security appliance is built on IronPort's revolutionary MTA platform. It incorporates email threat prevention with IronPort Reputation Filters™ and IronPort Virus Outbreak Filters.™ Additional capabilities include: the IronPort content scanning engine, anti-spam and anti-virus technology.

Threat Prevention with Advanced Reputation Filters

A flexible response to suspicious senders keeps hostile traffic off your network.

IronPort C-Series email security appliance intelligently throttles suspicious senders—the more hostile they appear, the slower they go.

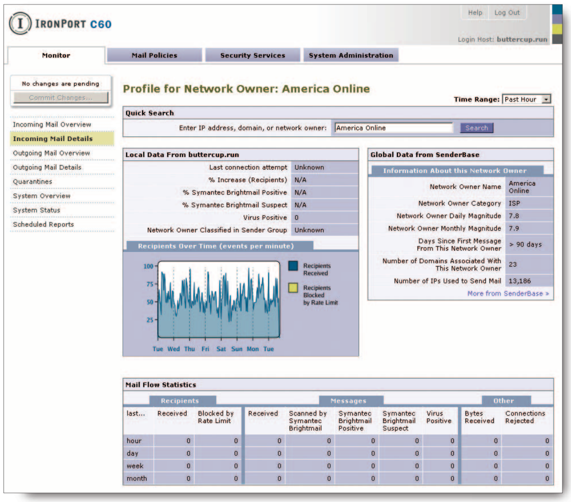
Reputation filters provide the outer layer of defense for your email infrastructure. The IronPort C-Series email security appliance receives inbound mail and performs a threat assessment of the sender. This assessment returns a reputation score that allows the IronPort C-Series to apply mail flow policies as specified by the administrator. More suspicious senders are throttled or eventually blocked. Recognized senders, such as customers or corporate partners are allowed access and can bypass filters per the administrator's needs.

Assessing the Threat with SenderBase

IronPort Systems™ created SenderBase™—the leading sender reputation service. SenderBase is an open database, rapidly adopted by more than 50,000 ISPs, corporations and universities. SenderBase processes queries for more than 3 billion messages per day, providing a real-time view into the global volume of mail being sent by any given IP address. SenderBase also measures other parameters such as whether an IP address is an open proxy, if mail receivers are sending spam complaints about the IP address, if its DNS resolves properly and accepts return mail, its country of origin, and its presence on a variety of blacklists. These parameters are rolled up in a statistical algorithm that scores the reputation of the sender on a -10 to +10 scale.

Flexible Response to Threats

The IronPort C-Series applies mail flow policies to senders based on their reputation score. Suspicious senders are throttled, preventing large traffic bursts from entering the network. Recognized senders are granted more generous policies such as bypassing spam filters, larger message sizes and TLS encryption. True threats are blocked at the network level, guarding precious system resources.



Login Host: buttercup.run

No changes are pending

Profile for Network Owner: America Online

Time Range: Past Hour

Quick Search

Enter IP address, domain, or network owner: America Online

Local Data From buttercup.run

Last connection attempt	Unknown
% Increase (Recipients)	N/A
% Symantec Brightmail Positive	N/A
% Symantec Brightmail Suspect	N/A
Virus Positive	0
Network Owner Classified in Sender Group	Unknown

Global Data from SenderBase

Information About this Network Owner

Network Owner Name	America Online
Network Owner Category	ISP
Network Owner Daily Magnitude	7.8
Network Owner Monthly Magnitude	7.9
Days Since First Message From This Network Owner	> 90 days
Number of Domains Associated With This Network Owner	23
Number of IPs Used to Send Mail	13,186

Mail Flow Statistics

	Recipients		Messages					Other	
last...	Received	Blocked by Rate Limit	Received	Scanned by Symantec Brightmail	Symantec Brightmail Positive	Symantec Brightmail Suspect	Virus Positive	Bytes Received	Connections Rejected
hour	0	0	0	0	0	0	0	0	0
day	0	0	0	0	0	0	0	0	0
week	0	0	0	0	0	0	0	0	0
month	0	0	0	0	0	0	0	0	0

The IronPort C60 email security appliance intelligently applies mail flow policy to your incoming email senders.

Stop Email Threats, Not Legitimate Traffic

The flexible response to suspicious traffic is a very effective defense against Denial of Service (DoS) attacks, directory harvest attacks, or fraudulent mail. Variable response is also very effective at reducing false positives.

Improve Overall Performance

Reputation filters are extremely high performance, processing messages at the IP address level. These filters can reduce the load on the subsequent virus or spam filter stages by over two-thirds, enhancing the availability of your mail, even during heavy virus or spam outbreaks.

IronPort C-Series

Powering and Protecting Business Email

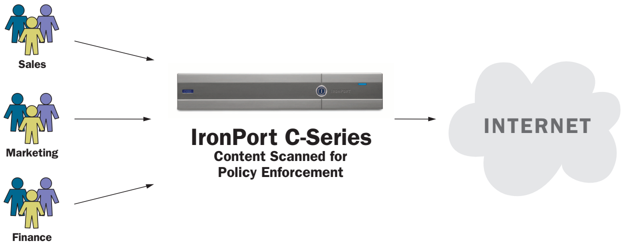
The IronPort C-Series™ email security appliance is built on IronPort's revolutionary MTA platform. It incorporates email threat prevention with IronPort Reputation Filters™ and IronPort Virus Outbreak Filters.™ Additional capabilities include: the IronPort content scanning engine, anti-spam and anti-virus technology.

Policy Enforcement with Content Scanning

Enforce corporate mail use policy and comply with regulatory requirements.

The IronPort C-Series inspects messages for inappropriate content or company intellectual property before leaving your corporation.

A powerful and easy to use content scanning system allows administrators to configure filters to search for keywords or phrases that are unique to a corporation's business. Filters can be set to search for language that has been deemed inappropriate for your organization, or to search for intellectual property to ensure that your valuable information does not get into the wrong hands. The system can search any parameter of a message— the headers, body, and even attachments based upon the administrator's settings.



Any outbound corporate email can be scanned by the IronPort C-Series appliances, ensuring that corporate policy is enforced.

World's Fastest Content Scanner

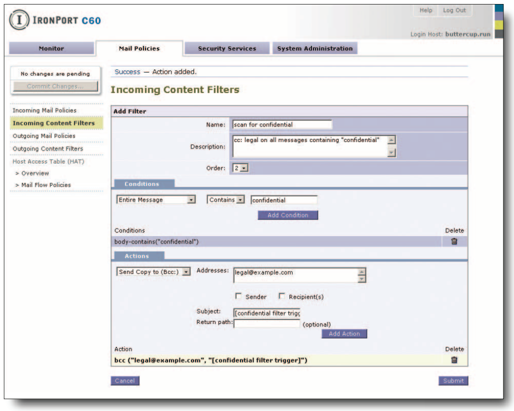
The IronPort C-Series offers the fastest message throughput in the industry. Due to the resource-intensive nature of most content scanning applications, traditional MTAs suffer severe performance degradation. With IronPort Systems' purpose-built MTA, message inspection occurs in a rapid and CPU-friendly manner, creating a new standard in message scanning performance.

Tailor Policies for Specific Groups using LDAP

Different policies can be applied to different organizations using IronPort's LDAP directory capability. (i.e. Active Directory™, Domino™/Notes™, Netscape Directory Server, Novell eDirectory™, etc.). Corporate policy screening that may be appropriate for engineering will use a separate set of filters from the finance department.

Advanced Attachment Filtering

Email attachments remain one of the main areas for exposure to email threats and corporate policy violations. Attachment file extensions can be easily re-written and MIME types can be spoofed to bypass filters. IronPort's AsyncOS™ provides advanced identification of attachments by file specific fingerprinting. Attachment fingerprinting performs an in-depth analysis of the file, matching it to a known library of signatures, providing an accurate verdict to the filtering action for appropriate handling. Once attachments are identified, operators can specify that certain types be removed from the email while the rest of the message is delivered to the intended recipient.



Login Host: buttercup.run

No changes are pending

Success — Action added.

Incoming Content Filters

Add Filter

Name: scan for confidential

Description: cc: legal on all messages containing "confidential"

Order: 2

Conditions

Entire Message | Contains | confidential

Conditions	Delete
body-contains("confidential")	

Actions

Send Copy to (Bcc:) Addresses: legal@example.com

□ Sender □ Recipient(s)

Subject: [confidential filter trig

Return path: (optional)

Action	Delete
bcc ("legal@example.com", "[confidential filter trigger]")	

Easily set and manage email policies with the intuitive GUI.

IronPort C-Series

Powering and Protecting Business Email

The IronPort C-Series™ email security appliance is built on IronPort's revolutionary MTA platform. It incorporates email threat prevention with IronPort Reputation Filters™ and IronPort Virus Outbreak Filters.™ Additional capabilities include: the IronPort content scanning engine, anti-spam and anti-virus technology.

Revolutionary MTA Platform

The IronPort C-Series email security appliance has been built from the ground-up to address the requirements of the modern email gateway.

IronPort's AsyncOS™ operating system is purpose-built for the email gateway. It ensures availability for inbound connections, reduces latency of mail processing, shields users from address harvesting, protects the reputation of your outbound IP addresses, and provides unprecedented visibility into mail flow.

Ensured Connection Availability

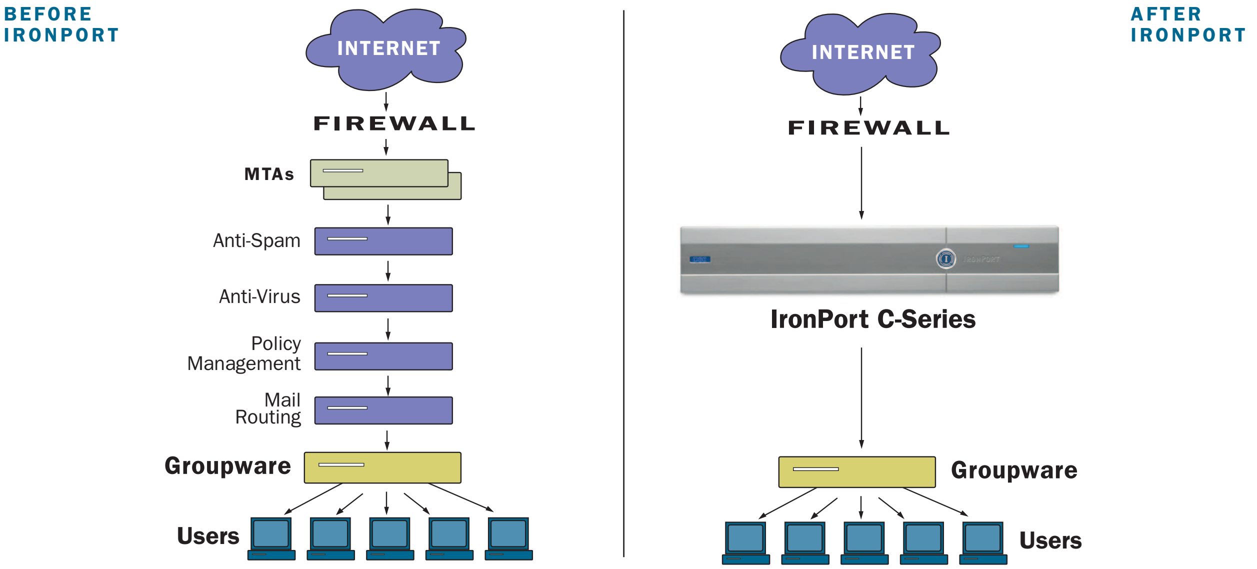
Denial of Service (DoS) due to too many open SMTP connections is a real threat to mail gateways as seen recently in virus outbreaks like "MyDoom". Resource exhaustion occurs in legacy systems that can only handle hundreds of simultaneous open connections.

IronPort's unique Stackless Threads™ technology allows a single IronPort C-Series email security appliance to handle up to 10,000 simultaneous connections. That's over twenty times the amount allowed by systems built on traditional operating systems.

Reduced Mail Processing Latency

Email is a critical business application and yet traditional platforms subject messages to minutes of latency while traveling through the email gateway. IronPort appliances are 10 to 20 times faster than competitive products and legacy platforms. IronPort's AsyncOS has a unique I/O driven scheduler, optimized for maximum I/O throughput, capable of delivering over 500,000 per hour.

> > >



The IronPort MTA platform enables massive reduction in Total Cost of Ownership (TCO) and provides a single platform/interface for email management.

Hardened Operating System

AsyncOS is founded on a rock-solid UNIX™-based kernel stripped of all non-essential components ensuring that hackers can't take advantage of your systems. IronPort's appliances have passed examination by the Internet's most rigorous security teams and are running in production at some of the world's largest email infrastructures.

Advanced Message Queuing

Traditional MTAs use a single queue for all messages. If a receiving domain goes down, it can block all outbound deliveries. IronPort's AsyncOS maintains a separate queue for each destination domain. Retry intervals and delivery parameters can be set on a per-domain basis. This allows the IronPort C-Series to gracefully handle error conditions on the Internet without manual administrator intervention, reducing administrative burden by as much as 75%.

Protected Outbound IP Reputation

The IP addresses you use to send outbound email have built up a reputation on the Internet. The businesses and organizations that you send mail to are using this reputation to determine whether to accept your email. IronPort's Virtual Gateway™ technology separates mail from different sources (e.g. marketing mail and corporate mail) and delivers it via separate IP addresses to protect your good reputation.

Private Communications with Partners

Email typically travels over the Internet in clear text — meaning that anyone can eavesdrop on your confidential business communications. The IronPort C-Series encrypts connections between gateways using Secure Socket Layer (SSL)/Transport Layer Security (TLS) — the same technology used by eCommerce companies to secure credit card information over the Web.

Directory Harvest Prevention

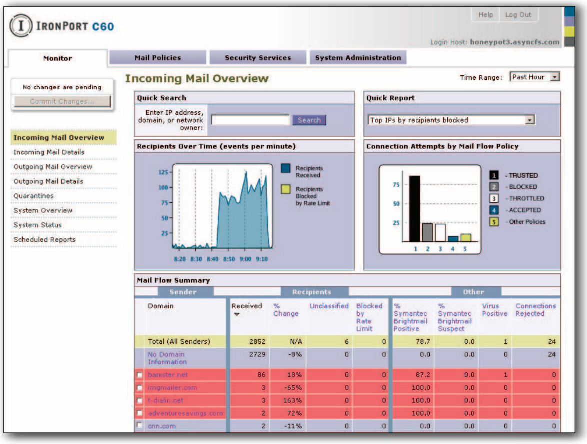
AsyncOS prevents malicious agents from harvesting your email directory by dispensing with responses to fake addresses during the SMTP conversation. This limits future spam attacks and reduces the load on your groupware servers by performing validation on the mail gateway.

Powerful LDAP Routing

The IronPort C-Series appliance has sophisticated message routing capabilities. It supports domain based routing, alias tables, and LDAP look-ups. IronPort's LDAP system is compatible with Microsoft's Active Directory™, Lotus Notes™, Novell eDirectory™, Netscape Directory Server, and other leading directory servers. The IronPort C-Series also supports domain masquerading for outbound mail to protect internal network details.

Industry-Leading Encryption with PGP Universal

When the IronPort C-Series is deployed with industry-leading encryption from PGP® Universal and PGP Universal Web Messaging, enterprises receive a comprehensive email security solution. PGP Universal Server automatically handles all encryption, decryption, and digital signatures for gateway and end-to-end email security. As a joint solution, administrators can create and manage a full range of email security solutions from a single console — reducing administrative burden, ensuring consistent policies, and streamlining change-management.



Incoming Mail Overview

Time Range: Past Hour

Quick Search

Enter IP address, domain, or network owner:

Quick Report

Top IPs by recipients blocked

Recipients Over Time (events per minute)

Connection Attempts by Mail Flow Policy

Mail Flow Summary

Sender	Recipients				Other			
Domain	Received	% Change	Unclassified	Blocked by Rate Limit	% Symantec Brightmail Positive	% Symantec Brightmail Suspect	Virus Positive	Connections Rejected
Total (All Senders)	2852	N/A	6	0	78.7	0.0	1	24
No Domain Information	2729	-8%	0	0	0.0	0.0	0	24
□ banister.net	86	18%	0	0	87.2	0.0	1	0
□ imgmailer.com	3	-65%	0	0	100.0	0.0	0	0
□ t-dialin.net	3	163%	0	0	100.0	0.0	0	0
□ adventuresavings.com	2	72%	0	0	100.0	0.0	0	0
□ cnn.com	2	-11%	0	0	0.0	0.0	0	0

Unprecedented Visibility

The Mail Flow Monitor™ feature provides real time and historical visibility into the systems connecting to your email gateway. Spam and viruses are tracked according to IP or domain. This unique visibility into mail flow increases security and reduces administration time by consolidating all this information into one view. Mail Flow Monitor is only available from IronPort.