

MESSAGING GATEWAY™ APPLIANCE

IronPort C60™

Powering and Protecting Business Email



FEATURING:

- Anti-Spam
- Email Access Control
- Mail Flow Monitor™
- Corporate Policy Enforcement
- Enterprise Class Solution
- World's Fastest Gateway
- Powered by AsyncOS™

IronPort C60

Powering and Protecting Business Email



BRIGHTMAIL.

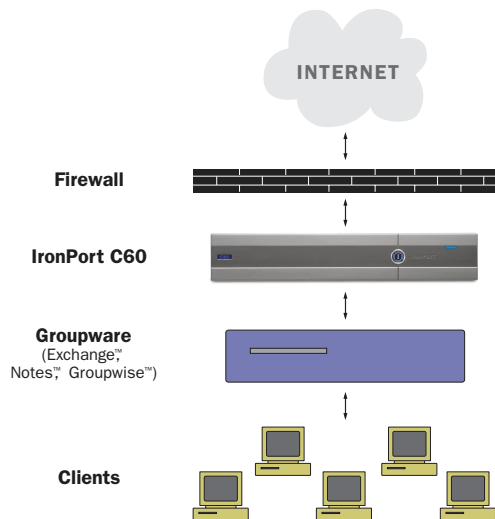
With Industry leading BRIGHTMAIL™ anti-spam technology.

Overview

The IronPort C60: Powering and Protecting Business Email

The IronPort C60™ Messaging Gateway™ appliance eliminates spam, enforces corporate policy, secures the network perimeter, and reduces the Total Cost of Ownership (TCO) of enterprise email infrastructure.

The appliance deploys between the firewall and groupware servers to power and protect email flowing in from or out to the Internet. Built on the highest performance gateway platform in the world, the IronPort C60 is a multi-function device that provides a single easy-to-use interface for the management of corporate mail flow.



The IronPort C60 integrates easily into existing messaging infrastructures.

FEATURING:

Anti-Spam

The most effective spam control in the industry with two layers of protection. The outer layer is IronPort's unique reputation filter, the inner layer is Brightmail filtering.

Email Access Control

Reputation filters automatically assign policy limits to email senders based on their trustworthiness. Untrustworthy senders have throttled delivery rates.

Mail Flow Monitor™

Automated anomaly detection and complete view of mail flow into or out of the corporate network.

High Performance

The world's fastest gateway, processing more than 500,000 messages per hour.

Corporate Policy Enforcement

Flexible message filter language allows for corporate policy enforcement. Scan message headers, bodies and attachments for keywords.

Enterprise Class Solution

Alias tables for message routing, domain masquerading hides internal network details, domain-based routing for hosting multiple domains.

AsyncOS™

IronPort's hardened operating system optimized for messaging. Highly secure with all unused services removed.



IronPort C60

Powering and Protecting Business Email

Built for the Enterprise

The IronPort C60 is built on Enterprise class hardware. Dual processors, four hot-swap SCSI drives, hardware RAID, dual hot swap power supplies and fans, and dual NICs.

The IronPort C60 also has Enterprise grade features. Multi-user login. Powerful logs and reports. XML programmatic interface. Command Line Interface via SSH/Telnet for power users.



The IronPort C60 is a rack-mounted Messaging Gateway appliance designed for the enterprise environment. One IronPort C60 can replace several layers of existing infrastructure.

SPECIFICATIONS

Chassis/Processor

Form Factor	19" Rack-Mountable, 2U rack height
Dimensions	3.5" (h) x 19" (w) x 29" (d)
CPU	Two Intel® Xeon Processors
Power Supplies	Dual Hot-plug redundant; 500 Watts, 100/240 Volts
LCD	Front mounted LCD alphanumeric display shows error messages illuminates different colors to indicate system status

Storage

RAID	RAID 10 configuration; Dual channel hardware with battery-backed cache
Drives	Four hot-swappable, 72 GB Ultra 3 (Ultra 160) SCSI
Capacity	40GB queue capacity, 80 GB discretionary capacity (mail flow database, logs, configuration, archives)

Connectivity

Ethernet	Two Broadcom® Gigabit BaseT and One Intel® 10/100 BaseT Ethernet ports
Serial	One RS-232 (DB-9) Serial Port

Mail Operations

Mail Injection Protocols	SMTP, ESMTP, Secure (Encrypted) SMTP over TLS(Supports 128-bit RC4, DES, 3DES)
Mail Delivery Protocols	SMTP, ESMTP, Secure (Encrypted) SMTP over TLS(Supports 128-bit RC4, DES, 3DES)
DNS	Internal resolver/cache; Can resolve using local DNS or Internet DNS 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

Logging

Log Subscriptions	User-defined subscriptions to logging services; Aggregated by FTP or SCP; push or poll; Rolled over by time period and/or file size
Mail Logging	Delivery logs for key parameters or Full logs. Binary, Text, or XML output

Monitoring and Management

Monitoring	Mail flow monitoring database records details based on source IP, domain, or organization
Alerts	Sent via email; Alert events include application, queue, and file transfer errors
Planned Outage Modes	Offline (delivery and injection suspended), Suspend Delivery, Shutdown, Reboot



IronPort C60

Powering and Protecting Business Email



The IronPort C60™ is a high performance appliance designed to meet the email infrastructure needs of the most demanding enterprise networks. The IronPort C60 eliminates spam, enforces corporate policy, secures the network perimeter, and reduces the Total Cost of Ownership of enterprise email infrastructure.

Anti-Spam


Eliminate spam to increase individual user productivity and reduce the management burden on email administrators.

The IronPort C60 has an integrated, layered approach to spam control. Built on IronPort's AsyncOS™ operating system, the IronPort C60 spam control system is the highest performance and most accurate solution available.

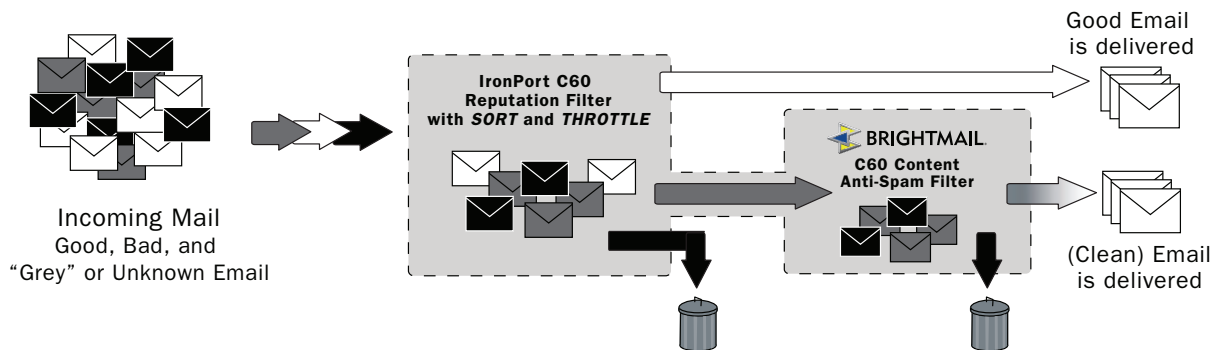
The defensive outer layer: IronPort Reputation Filtering

The IronPort C60 has unique reputation filtering technology. The reputation filter combines your corporate email data as well as data from IronPort's SenderBase™ Email Sender Reputation Service to determine the trustworthiness of the source of the email. Messages from known or highly trusted sending entities such as customers and partners are delivered directly to the end user with little or no restrictions applied. Unknown or less trustworthy senders can be throttled by the number of messages you are willing to accept – the less trustworthy a sender appears, the lower the acceptance rate. Highly untrustworthy senders are refused connections or their mail is tagged or deleted, based on your preference. The variable response of the reputation filter is a powerful defense against the growing problem of hit-and-run spam or directory harvest attacks.

The anti-spam inner layer: Brightmail on AsyncOS

The IronPort C60 includes integrated Brightmail spam-fighting technology. Optimized to leverage IronPort's AsyncOS operating system, Brightmail technology is extremely high performance and highly accurate. Brightmail is the  **BRIGHTMAIL**, proven leader in spam control, powering the largest corporations and ISPs. Brightmail's patented Probe Network™ ensures industry leading accuracy and effectiveness. The Brightmail engine employs multiple techniques to fight spam, including BrightSig™, which offers protection from polymorphic spam attacks. Rules are updated every few minutes providing real time protection against the latest spam attacks.

Administrators have several choices on how to handle messages that are flagged as spam by Brightmail. Choices include 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 C60's Mail Flow Monitor making real-time and historical reports instantly available at any time.



The IronPort C60 combines Reputation Filtering with Brightmail content filtering to eliminate spam.



IronPort C60 Anti-Spam

IronPort C60 Anti-Spam

IronPort C60

Powering and Protecting Business Email



The IronPort C60™ is a high performance appliance designed to meet the email infrastructure needs of the most demanding enterprise networks. The IronPort C60 eliminates spam, enforces corporate policy, secures the network perimeter, and reduces the Total Cost of Ownership of enterprise email infrastructure.

Email Access Control

Secure the network by dynamically applying unique mail flow policies to senders or groups of senders. Take control of your corporate mail flow.

The IronPort C60 intelligently applies mail flow policy to unfamiliar senders based on their trustworthiness as reported by SenderBase.™

Mail flow policies are quickly and easily assigned to familiar senders using the IronPort C60. For example, your business partners can be assigned a different policy than your customers. Senders are identified and grouped based on their IP address, domain name or organization data as collected in SenderBase.

For each email policy, administrators can specify any of the following parameters:

- Message acceptance rate (recipients per hour)
- Maximum message size

- Number of connections allowed
- Brightmail content filtering bypass
- Maximum number of messages per connection
- Maximum number of recipients per message
- Addition of custom headers

IronPort Reputation Filtering

Reputation filters provide an automatic and powerful defense against hit-and-run spammers, denial of service attackers, or email virus outbreaks without constant monitoring by the administrator.

SenderBase: Internet's preeminent email sender reputation service

Over 9,000 ISPs, universities, and corporations use data from SenderBase to combat spam and prevent false positives. As a result of this very large scale

adoption, SenderBase has unique access to a number of criteria about an email sender including global volume, complaint data, network data such as IP addresses and domains for that sender and date of registration, and, geographic location of the sender.



Real-time scores

These data are rolled into a score that is provided in real-time to the IronPort C60 to determine the trustworthiness of any sender. The IronPort C60 uses this data to assign the sender to the appropriate sender group and enforce the appropriate mail flow policy.

The screenshot shows the IronPort C60 web interface. At the top, there are tabs for 'Incoming Mail', 'Outgoing Mail', and 'System'. Below that, there are navigation links for 'Overview', 'Reporting', and 'Configuration'. The main content area is titled 'Mail Flow Summary' and includes a 'FILTER SUMMARY' dropdown set to 'Top Unclassified'. A table displays recipient data with columns for Domain, Received, % Increase, From Unknown Sender, Blocked by Policy, % Brightmail Positive, Delivered to Sender, and Connections Rejected. The 'greatbigoptin.com' row is highlighted in orange, showing a 798% increase and 89% Brightmail Positive score.

Domain	Received	% Increase	From Unknown Sender	Blocked by Policy	% Brightmail Positive	Delivered to Sender	Connections Rejected
✓ fidelity.com	12,642	23%	0	0	0%	9,951	0
✓ dtigroup.com	10,962	-5%	0	0	0%	11,182	0
✓ jpmchase.com	9,763	15%	0	0	0%	10,235	0
✓ yahoo.com	7,200	31%	7,200	0	3%	9,860	0
✓ hotmail.com	6,105	5%	6,105	0	1%	8,665	0
✓ morganstanley.com	5,987	-25%	0	0	0%	3,854	0
✓ greatbigoptin.com	5,884	798%	5,884	3,680	89%	0	0
✓ rr.com	3,210	-14%	3,210	562	6%	1,108	0
✓ aol.com	2,058	5%	2,058	0	0%	3,684	0
✓ newpartner.com	1,732	8500%	1,732	0	0%	1,485	0
✓ gs.com	1,521	2%	0	0	0%	3,698	0

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



IronPort C60

Powering and Protecting Business Email



The IronPort C60™ is a high performance appliance designed to meet the email infrastructure needs of the most demanding enterprise networks. The IronPort C60 eliminates spam, enforces corporate policy, secures the network perimeter, and reduces the Total Cost of Ownership of enterprise email infrastructure.

Mail Flow Monitor

*Monitor corporate mail traffic and correct anomalies in real-time.
Track a return on your investment with historical reporting.*

The IronPort C60's Mail Flow Monitor™ is a powerful web-based console that provides complete visibility into all Enterprise mail traffic.

The IronPort C60's mail flow monitoring database tightly integrates into the system, collecting data from every step in the process including anti-spam, policy enforcement, and message delivery. The database identifies and records each email sender by IP address, while interfacing with SenderBase for real-time identity information. Administrators can instantly report on any email sender's local mail flow history and pull up a profile including the sender's global record on the Internet. Mail Flow Monitor allows your security team to close the loop on who is sending mail to your users.

For any given email sender, the Mail Flow Monitor database captures critical parameters such as:

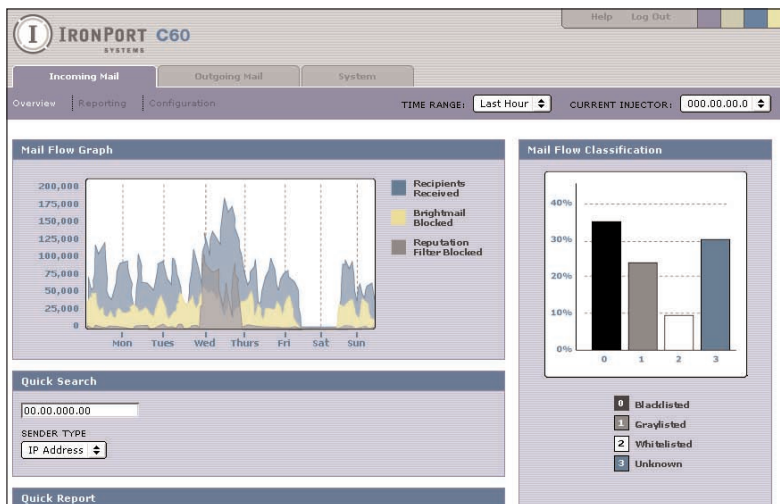
- Message volume
- Connection history
- Accepted vs. rejected connections
- Acceptance rates and throttle limits
- Reputation filter matches
- Brightmail spam filter matches

Realtime detection, Realtime reporting

Alerts are generated for anomalies such as a sudden change in the volume from any sender, reaching the acceptable message limit for a specified time, or a high rate of Brightmail spam filter matches. When a sender falls outside of the normal traffic profile, it is identified by the IronPort C60 and the administrator can take corrective action by assigning that sender to a sender group or refining the access profile of the sender.

Monitor traffic, take corrective action

Mail Flow Monitor provides an unprecedented view into your traffic. Trusted partners stand out in reports and allowing administrators to easily apply favorable mail flow policies. Senders that have experienced a recent change are highlighted in the interface, allowing easy classification with a few mouse clicks. Outbound mail has a similar monitoring capability, with a view into the top domains in the mail queue and the status of that receiving host.



Mail Flow Monitor is the mail administrator's cockpit



IronPort C60

Powering and Protecting Business Email



The IronPort C60™ is a high performance appliance designed to meet the email infrastructure needs of the most demanding enterprise networks. The IronPort C60 eliminates spam, enforces corporate policy, secures the network perimeter, and reduces the Total Cost of Ownership of enterprise email infrastructure.

High Performance: Power, Speed, and Deliverability

*Reduce costs by replacing up to 10 servers with a single 2U appliance.
At the same time, ensure your business critical email always gets delivered.*

The IronPort C60 is the fastest gateway in the world.
Built on IronPort's proprietary operating system AsyncOS, the IronPort C60 processes more than **500,000 messages per hour peak.**

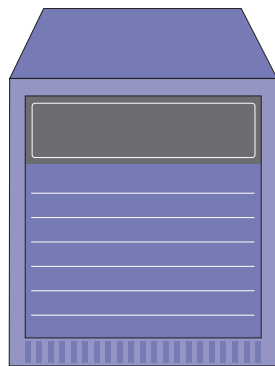
With the Brightmail™ and reputation filters enabled, the sustained throughput is approximately 250,000 messages per hour. A single 2U IronPort appliance will outperform a high end UNIX™ server with 8 CPUs and a Fibre Channel disk array.

Prevent your outbound email from getting blocked

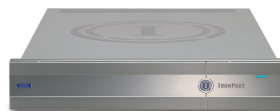
As the spam problem has gotten worse, ISPs and corporations have been forced to deploy more aggressive spam blocking filters. These filters can sometimes inadvertently block legitimate business email. The IronPort C60 has a number of features designed to ensure that legitimate email gets through to the recipient.

Segment your outbound email traffic

IronPort's unique Virtual Gateway™ technology detects distinct classes of email and assigns them to unique outbound IP addresses. This allows administrators to segment commercial traffic such as newsletters and transaction confirmations to a separate set of IP addresses from those used for normal employee email traffic. This way if the commercial email causes any delivery problems, employee email will proceed unaffected.



Before



After

An 8 CPU high-end server can be replaced with the 2U IronPort C60.



IronPort C60

Powering and Protecting Business Email



The IronPort C60™ is a high performance appliance designed to meet the email infrastructure needs of the most demanding enterprise networks. The IronPort C60 eliminates spam, enforces corporate policy, secures the network perimeter, and reduces the Total Cost of Ownership of enterprise email infrastructure.

Corporate Policy Enforcement

Enforce corporate mail use policy and comply with regulatory requirements.

The IronPort C60 inspects messages for inappropriate content or company intellectual property before leaving your corporation.

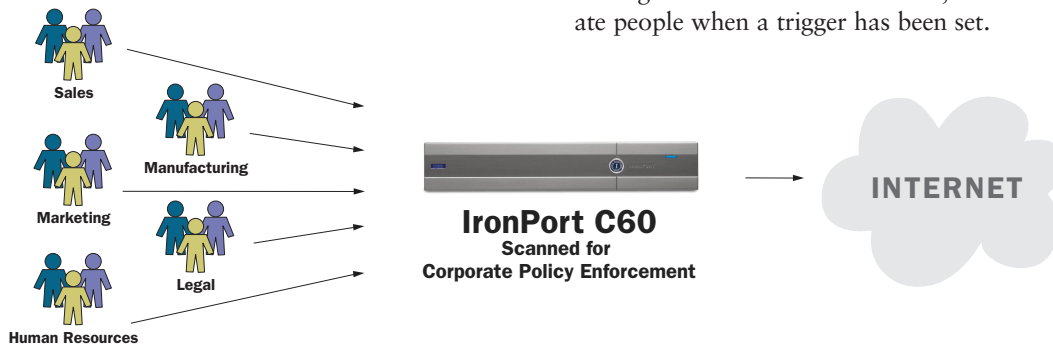
A powerful and easy to use message filtering system allows administrators to configure filters to search for keywords or phrases that are unique to a corporation's business. Filters can be set to search for language that has been deemed inappropriate for your organization, or can alternately search for 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. The IronPort C60 offers several alternatives for what to do when a filter finds the content that it is looking for including block, drop, or archive the message, send a copy to another user (e.g. the legal department), or simply notify someone of the message's existence. This highly versatile capability allows the IronPort C60 to adapt to the needs of any corporation.

Identifying encrypted messages

As companies have increased the use of policy enforcement technologies in the corporate mail flow this has led to an increase in unscrupulous employees encrypting messages at the client to get past the content filters. The IronPort C60 can also identify client encrypted messages and block them from leaving your corporation. On the other hand, some businesses require that certain employees send client encrypted messages. The IronPort C60 can also enforce this corporate policy.

Regulatory Compliance

Email has made communications with customers and between businesses economical and reliable, but this free exchange of information has led to the rise of regulatory requirements that can be a big headache for the unprepared. The IronPort C60 allows companies to easily monitor the email communications leaving the organization in order to enforce compliance with rules like the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act (GLB). Using message filtering technology the IronPort C60 can identify and block messages that violate regulations, archive messages that set off certain filters, or alert the appropriate people when a trigger has been set.



Any outbound corporate email can be scanned by the IronPort C60 ensuring that corporate policy is enforced.



IronPort C60

Powering and Protecting Business Email



The IronPort C60™ is a high performance appliance designed to meet the email infrastructure needs of the most demanding enterprise networks. The IronPort C60 eliminates spam, enforces corporate policy, secures the network perimeter, and reduces the Total Cost of Ownership of enterprise email infrastructure.

Enterprise Class Solution

Security features, routing capabilities and high availability hardware meet the needs of the largest corporations.

The IronPort C60 has routing and security features that allow for an easy migration from legacy systems. Favorite powerful features of familiar open source MTAs are available, although they are redesigned for the future.

The IronPort C60 is expressly designed for corporations that have complex infrastructures requiring the advanced routing and flexibility. The IronPort C60 “fits in” by supporting critical functions such as alias tables, domain masquerading, domain-based routing, and in some cases accepting data in legacy system formats. The IronPort C60 “stands out” by providing highly differentiated features built to Enterprise standards.

Professional features

The IronPort C60 provides out of the box support for complicated routing schemes involving alias tables and domain-based routing. Popular sendmail features such as domain masquerading, generic header rewriting are supported. The IronPort C60 leverages XML for saving/loading configuration files and logs. It also includes an XML over HTTP monitoring interface for programmatic

tool integration. Highly configurable logs can log every step in the mail flow pipeline or specific things like debugging the SMTP conversation with a specific domain. In addition, alerts can be generated when critical system parameters are exceeded.

Multi-user login and administration

The IronPort C60 is designed to be administered by corporations with technical staff in different roles. Users have their own accounts with defined levels of access or privilege. Any changes made to the system are logged along with the user that made the changes. System configuration is saved in an XML file, and can be pushed to multiple machines.

High availability hardware

The system is built on an enterprise class hardware chassis. The IronPort C60 includes dual Xeon™ processors, four 72GB hot-swap SCSI drives with hardware RAID controller, dual hot swap power supplies and fans, dual NICs, and plenty of RAM for the highest performance. IronPort also offers a hot spares program where a fully featured (but reduced price) system can be installed and running alongside a production unit ready to receive fail-over traffic.



The IronPort C60 is built to meet the needs of the most demanding enterprise networks.



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 C60

Powering and Protecting Business Email



The IronPort C60™ is a high performance appliance designed to meet the email infrastructure needs of the most demanding enterprise networks. The IronPort C60 eliminates spam, enforces corporate policy, secures the network perimeter, and reduces the Total Cost of Ownership of enterprise email infrastructure.

AsyncOS: Built for Security

Neutralize the threat of devious persons monitoring your communications or entering your network through the mail gateway.

The IronPort C60 is designed to meet the security needs of the largest corporations. IronPort's AsyncOS™ operating system is optimized for messaging and hardened making it next to impossible to exploit. Connections are encrypted between trusted partners ensuring privacy of your communications.

Email typically travels over the Internet in clear text – meaning that anyone can eavesdrop on your confidential business communications. Businesses are demanding increased security in their email delivery as a result. The IronPort C60 has the ability to encrypt communications 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. A security certificate issued by a trusted third party known as a Certificate Authority is used to encrypt the communications, ensuring that the gateway on the other end of the line is who they say they are.

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. Services like HTTPS, and FTP have been written from the ground up using a mature run-time language that is not susceptible to the buffer overflows and exploits of legacy systems. IronPort's appliances have passed examination by the Internet's most rigorous security teams and are running in production at the largest sites.

No Denial of Service

The largest real threat to mail gateways is malicious or unintentional Denial of Service (DOS) due to too many open SMTP connections. Resource exhaustion occurs prematurely in legacy systems because they can only handle hundreds of simultaneous open connections. IronPort's unique Stackless Threads™ technology allows the IronPort C60 to open up to 10,000 simultaneous connections over the Internet. That's over twenty times the amount allowed by systems built on traditional operating systems.

