Executive Summary

The IronPort All-In-One Appliance Combines Purpose-Built MTA with Preventive Security, Reactive Security and System Control

Email has become the dominant form of business communication – rivaling, if not exceeding, the importance of voice networks. Indeed, email has had such an extraordinary impact that, like the fax and ATM, it's hard to imagine life before its widespread adoption over the last decade. The very power of the medium has also attracted a disturbingly large and growing number of security threats – spam, fraud, viruses, regulatory violations and intellectual property theft.

The volume and sophistication of email security threats continues to grow at an unchecked pace. Most customers observe that as much as 90 percent of their incoming mail is invalid (spam, viruses, etc), and the total number of incoming messages is doubling every year, even if the number of employees stays constant. These email security threats are fueled by a powerful profit motive associated with spam, fraud and information theft. This creates resources that bring professional engineers into the business of developing new threats, further exacerbating the situation. As this cycle does not appear to have a natural equilibrium, threats are expected to continue to grow in volume and sophistication for the foreseeable future.

IronPort® email security appliances are designed to protect networks from today's and tomorrow's email threats. These appliances are built on IronPort's proprietary AsyncOS™ operating system. Optimized for messaging, AsyncOS provides the foundation that allows a single IronPort appliance to process mail more than ten times more efficiently than traditional UNIX-based systems. On top of this highly scalable platform, IronPort offers a variety of security applications for spam and virus filtering, content scanning and policy enforcement. Also contained are unique technologies developed by IronPort as well as tightly integrated filtering technology from best of breed partners. The modular design of the system allows these applications to be turned on or off, to meet the specific needs of each customer.

To follow is a technical overview of the major components of the IronPort email security appliance, broken into the following sections:

• The Foundation – IronPort AsyncOS

• Advanced Queue Design and Connection Management

• Email Authentication

• SenderBase®

• IronPort Reputation Filters™ and Flow Control

• IronPort Virus Outbreak Filters™

• Content Scanning and Policy Enforcement

• Content-based Anti-spam

• Signature-based Anti-virus

• IronPort Email Encryption™

• Management, Monitoring and Reporting

• IronPort Centralized Management™

THE FOUNDATION – ASYNCOS

Many of the limitations of a traditional UNIX-based gateway program lie not in the application itself, but in the way the applications interact with the underlying operating system. To address these limitations, IronPort has developed a unique operating system called AsyncOS, specifically optimized for the asynchronous task of relaying email messages.

Email is a connection intensive medium. Any reasonably sized network may easily have thousands of simultaneous mail connections coming in or going out. These connections are often relatively slow, as they may be connected to a busy mail server at the other end of the Internet. A traditional MTA has difficulty dealing with a large number of simultaneous connections. Most traditional MTAs running on general-purpose operating systems such as UNIX

or Windows are limited to 100 or maybe 200 simultaneous connections be-cause the operating system limits the number of threads that can be opened at the same time. This is because the traditional threading model requires a dedicated memory stack for each thread, and the system cannot provide more memory to open new threads. IronPort's AsyncOS features a stackless threading model that does not require a large memory stack for each thread. This allows the IronPort MTA to support a massive concurrency and offers performance that is far superior to traditional MTAs.

This massive concurrency ensures that, for all practical purposes, the Iron-Port MTA will never be connection bound. Solving the concurrency bottleneck means that the bottleneck shifts to I/O. Since all messages in an MTA must be safely written to disk, the MTA is an I/O intensive application.

The I/O bottleneck is addressed by AsyncOS in two ways. The first is through IronPort's I/O driven scheduler. AsyncOS takes advantage of the asynchro-nous nature of messages to process them in any order that is optimal. If a thread is actively using I/O, the system allows it to finish its I/O transaction, and will not incur the overhead of a context switch induced by a time-based scheduler. This increases the efficiency of the I/O system dramatically.

The second I/O optimization is in the AsyncOS file system. Traditional MTAs use the file system to maintain the state of the application. If a major receiv-ing domain becomes unavailable and a queue starts to grow, the overhead associated with a traditional file system begins to drag down the overall throughput of the machine. So, when the receiving mail domain comes back online, the MTA needs to resume delivery and clear the queue. But, at the moment the MTA needs maximum throughput to clear the queue, the file system overhead actually makes the throughput minimal. So the queue grows, causing more overhead. This, in turn, results in a bigger queue until the system finally grinds to a halt, requiring administrator intervention.

ADVANCED QUEUE DESIGN AND CONNECTION MANAGEMENT

On top of this heavily-optimized operating system, IronPort has developed a completely new MTA architecture. The IronPort appliance contains a unique independent queue design. The system maintains a separate queue for every destination domain. It also maintains an awareness of the state of all receiving domains. If a major domain (such as Hotmail) goes down, the system marks the domain as being down, and all new messages from the groupware servers are placed in the queue for that domain. But queuing a message for a downed domain will not initiate a separate retry cycle for each new message received. Instead the IronPort email security appliance parks all messages for the downed domain, and performs a single, global retry on that domain. When the receiving domain comes back up, all messages are delivered. This solves a very common problem for traditional MTAs. They frequently become paralyzed by large numbers of retries to a popular host that is down.

Similarly, the IronPort MTA has the ability to set the retry schedule on a per-domain basis. This solves another very common MTA problem: large numbers of bounced spam messages that slow the system queues. Spam attacks frequently have high rates of invalid email addresses. These bounce messages are often going to a domain that never accepts mail in the first place, sending a traditional MTA into a fit of retries for mail that was junk to begin with. This usually requires a system administrator to intervene, sort through the queue, and destroy or remove all messages bound for the offending domain. By adjusting the retry on a per-domain basis, administrators can set the retry to zero for suspect domains and allow the IronPort appliance to clear these messages automatically. These capabilities allow the IronPort appliance to act as a "shock absorber," in front of the groupware servers, queuing messages gracefully without manual attention.

IronPort appliances also have a unique feature called Virtual Gateway™ technology. Virtual Gateway technology allows the system to identify and assign unique classes of mail to unique outbound IP addresses. This can be used to separate the outgoing mail for different organizations onto different outbound IP addresses. Virtual Gateway technology is a very powerful feature for managing issues of deliverability. If any of the different mail streams cause problems with a receiving ISP that leads the ISP to block that mail, the blockage will only be limited to the IP that caused the problem, allowing mail from the other mail streams to flow without interruption. This capability is a must for service providers that have shared infrastructure – each customer can be given their own unique IP address, ensuring no one customer will impact the mail flow of another. The other critical use of this is to separate commercial mail such as bill payments or transactions from employee-generated mail. This approach isolates operational impact if there is a problem with one mail stream.

The IronPort queuing engine builds separate queues for each destination domain on a per virtual gateway basis, extending the robust queuing across multiple virtual gateways. Thus a popular receiving domain (like Hotmail) might have a separate queue for each virtual gateway set up, ensuring that if one virtual gateway is blocked the others continue to send mail. Virtual gateways can also be used to prioritize time-sensitive mail such as email alerts or pager messages. By putting these messages into their own virtual gateway, they will have their own queue and not have to sit behind lower priority messages already enqueued.

In addition to advanced queuing and bounce management, the IronPort MTA design has excellent connection management. The system queues and groups all messages going to a common domain. It sends multiple messages per connection, and opens multiple connections per host. Traditional MTAs will open a new connection for each message delivery, adding massive overhead to both the sending and receiving MTA.

IRONPORT®

IronPort's "Good Neighbor" algorithm calculates the aggregate data rate across all connections to a given domain. When the data rate starts flattening out, it drops the newest connection, ensuring the receiving mail server does not become overloaded. The IronPort appliance also has an on-board DNS cache that is extremely high performance and matched to the throughput of the system. The cache will store the IP addresses of all MXs for a receiving domain, and spread connections across the various MXs — according to the MX preference advertised by the receiver.

EMAIL AUTHENTICATION

Although the lack of email authentication went largely unexploited for 20 years, the last few years have seen massive abuse of this weakness. Today, almost 80 percent of all email is spam — with the vast majority spoofing the sender's identity for all sender attributes. Spoofing of the sender's domain allows phishing email to defraud consumers, damage corporate brands and create bounce-based distributed denial-of-service attacks. It also makes spam more difficult to identify. Bounce messages are becoming an increasing problem for email administrators. Often spammers will send messages with a forged return address (otherwise known as a "joe-job" or misdirected bounce attack) that contains a known spam or virus payload. IronPort Bounce Verification™ provides email administrators the tools required to protect themselves from bounce attacks with minimal overhead and no ongoing maintenance. Bounce Verification digitally signs the envelope's return address (SMTP's Mail From:) with a private key.

Normally, the envelope's return address is:

MAIL FROM: support@bigbank.com

Bounce Verification converts the address to:

MAIL FROM: pvrs=support=3201EA1CF@bigbank.com

When bounce messages are sent to an email gateway the existence of the correct signature will help determine legitimate bounces from fraudulent bounces.

IronPort's solution provides additional functionality to support deleting, quarantining or marking the subject line of fraudulent bounces.

What is unique about IronPort Bounce Verification is that, unlike other email authentication technologies, it does not require industry adoption to be effective. The uni-directional nature of IronPort Bounce Verification provides immediate benefit to those who deploy the technology.

IronPort email security appliances support DomainKeys technology. In the DomainKeys scheme, a sender makes a hash of every outgoing message and encrypts that hash using a private key in a PKI pair. The public key from the pair is then published in a DNS text record for that sender's domain. A

I IRONPORT®

receiving mail server authenticates the message by extracting the sending domain from the email, retrieving the public key from the sender's published DNS text record, and validating the signature against the message's contents. Email with a valid signature is authenticated, while email with an invalid signature fails authentication. Although the protocol is flexible, DKIM almost always validates the domain in the "From:" header. Since this header is always presented in email clients to end-users, this technology is an excellent solution to the phishing problem.

The IronPort appliance includes a high performance LDAP client. Incoming addresses can be verified using any standard directory, such as Microsoft's Active Directory. Addresses can either be verified during the SMTP conversation – with a bounce error message delivered before a message is accepted, or mail can be accepted and then verified, with bounce messages creating an NDR – non-delivery receipt back to the original sender. A conversational SMTP bounce code solves the misdirected bounce problem as the message is bounced during the SMTP conversation and does not require an NDR back to the sender. However, it has the disadvantage of exposing the corporate email directory to a "dictionary" attack – where a spammer guesses at valid addresses and gets confirmation from the SMTP conversation. This concern is the reason most large enterprises have implemented a delayed bounce policy.

To address these concerns over directory security, the IronPort appliance supports Directory Harvest Attack Prevention (DHAP) technology. DHAP technology keeps track of the number of invalid recipient addresses from a given sender. Once that sender crosses an administrator defined threshold (say ten bad addresses per hour) the sender is deemed to be untrusted and mail from that sender is blocked with no NDR or error code generated. The threshold can be configured differently, based on the reputation of the sender (a detailed discussion of IronPort's Reputation Filtering system follows). Untrusted or suspicious senders can have a low DHAP threshold, trusted or reputable senders can have a high DHAP threshold.

IronPort's DHAP system makes it safe for administrators to return to conversational bounces and reduce bounce problems. If the administrator prefers to use delayed bounces, the DHAP system will cut down on the misdirected bounces generated by spam attacks.

SENDERBASE – FIRST, LARGEST, BEST IN REPUTATION

SenderBase is the industry's first and largest email and Web traffic monitoring network. SenderBase tracks a variety of network parameters about any given IP address sending mail on the Internet. These parameters include the global volume of mail sent by any given IP address, how long that IP has been sending mail, country of origin, open proxy or open relay detection, appearance on any black- or whitelists, proper DNS configuration, ability of the sender to receive mail in return, etc.

IRONPORT®

SenderBase collects data from an astounding 100,000 different networks around the world. These networks represent more than 25 percent of the world's email and Web traffic. SenderBase is the only traffic monitoring service that collects data from a variety of sources, both within and outside of the IronPort customer base. SenderBase tracks more than 120 different parameters about any given sender. By accessing a broad set of data, across a very large sample size, SenderBase is able to make extremely accurate assessments of a sender's behavior and reputation.

SenderBase has algorithms that analyze these objective, network level parameters and distill a "reputation score" of -10 to +10. This score is then made available to the appliance in real time, as a message is received from any sender. A variety of policies can be tied to a sender's reputation, everything ranging from the DHAP threshold (discussed above) to flow control parameters or attachment size or type restrictions.

IronPort has a large staff of multi-lingual technicians and statisticians working in the 24x7 IronPort Threat Operations Center (TOC), monitoring and managing the data in SenderBase. The TOC team has developed a data quality engine that processes and weights data from different sources for accurate interpretation. This team ensures that SenderBase data is up to date and precise, so administrators can rely on SenderBase data to automatically classify their mail, eliminating the need for time consuming manual blacklist and whitelist management.

REPUTATION FILTERING AND FLOW CONTROL

The IronPort appliance performs a look-up on the reputation score of each incoming piece of mail, using a light DNS text record (similar to an RBL mechanism). The IronPort can then apply a unique email security policy to that sender, based on the reputation score (this is called reputation filtering). Attachment size, type and filename limits, spam, virus and content filtering schemes, and flow control parameters are all dynamically applied to senders, based on reputation. Thus, a suspicious sender may be given very limited privileges. For example, a suspicious sender may be allowed no more than ten recipients per hour, no executable attachments, full spam, virus and keyword scans. A trusted sender can be given very generous privileges – 1,000 recipients per hour, large attachments and varied attachment types, and TLS (Transport Layer Security) encryption. Administrators set up these various policies once (using the Web interface), then simply provide supervision as appropriate while the system automatically classifies senders. Many administrators will perform a monthly review of policy and mail flow, and will not have occasion to touch the IronPort appliance beyond this.

IronPort's flow control capabilities are very unique. While most commercial systems available today offer some type of "throttling," they do so by limiting the number of connections from a given host. Spammers easily thwart this

approach by sending multiple messages per connection and sending multiple recipients per message. The IronPort system can limit recipients per hour accepted. When linked to reputation, this is a very effective technique. In short, the more "spammy" a sender appears, the slower they go. Having the ability to rate limit senders allows the appliance to deal with the "grey area". Obvious spammers can be readily identified and blocked. Similarly, known trusted senders can be routed directly through to the anti-virus scanners without spam filtering. These two classes of senders typically make up 80 percent of incoming mail flow. The remaining 20 percent is rate limited and spam filtered.

IronPort's Reputation Filtering system was the first in the industry and remains the most sophisticated. In its default settings it will block 80 percent of incoming mail at the connection level, saving 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 attacks or denial of service attacks.

The IronPort flow control capability is also very useful in controlling outbound mail delivery. The IronPort appliance is a very high performance device, but has built in controls that ensure a receiving domain will never be overwhelmed, resulting in blacklisting. Furthermore, the rate limiting can also be used for internal routing of mail. Mail destined for the main Microsoft Exchange or IBM Lotus Notes clusters can be delivered at high rates, but mail destined for remote office servers can be throttled to ensure overall mail system stability.

IRONPORT VIRUS OUTBREAK FILTERS

Although signature-based anti-virus systems have been deployed for some time, many customers find they still have problems with virus outbreaks that spread prior to signature availability. The reason for this is that virus signatures are inherently reactive. No matter how good the signature vendor, it takes a finite amount of time to detect, isolate and characterize the virus. It then takes an additional phase to create, test and deploy a signature. This time ranges anywhere from 6 to 48 hours, depending on the outbreak. In that interval, a virus will propagate rapidly around the world.

There is no normal form of human communication that spreads as rapidly as a modern email-borne virus, so a major outbreak creates huge anomalies in global email traffic patterns. IronPort's Threat Operations Center (TOC) has developed algorithms that detect outbreak-related anomalies such as a surge in new IP addresses sending mail that have never sent mail before, and a corresponding surge in messages with a certain attachment size, type, or name. The TOC then automatically generates alerts and creates a rule which is approved by the TOC technicians. This rule is then automatically pushed to the IronPort appliances and mail that matches the anomaly is placed into

a system quarantine. An alert is sent to the system administrator, as well as information updates about the outbreak as it progresses. Administrators have tools to look into the quarantine and test, release or delete select messages or all messages. When signatures have been updated administrators can test the messages against the new signatures to ensure they are fully protected, and then release the messages which are scrubbed and handled according to anti-virus policy settings. Only IronPort Virus Outbreak Filters continuously re-scan and re-evaluate quarantined messages (based on the latest, increasingly fine-grained rules), resulting in a minimal cost of coarse filtering or misclassifications. IronPort's Dynamic Quarantine then releases any messages that do not match the new rules. This Dynamic Quarantine combines the most immediate protection with the highest accuracy possible.

IronPort Virus Outbreak Filters have been in production for over a year and have achieved outstanding results, averaging protection 16 hours ahead of signature availability, and stopping hundreds of millions of infected messages that would otherwise have gone straight to the desktop. The response time for a few recent outbreaks is shown in Figure 1. Considering that "Average cleanup cost per virus disaster in 2004 was $130,000." (Source: ICSA Labs 10th Annual Virus Prevalence Survey), the value of Virus Outbreak Filters is easy to imagine.

Figure 1: IronPort Virus Outbreak Filters stop viruses before any other technology.

Virus	Date	Virus Threat Level Raised	First Anti-virus Signature Available	Outbreak Filter Lead Time
Zotob.C	8/16/05	1:56 AM	4:47 AM	2:51 HOURS
MyTob.G	8/16/05	11:30 PM	12:58 PM (the next day)	13:28 HOURS
Sober.L	3/24/2005	4:10 PM	6:23 PM	2:13 HOURS
Mydoom.BB	2/15/2005	6:08 PM	10:54 PM (the next day)	28:46 HOURS

CONTENT SCANNING AND COMPLIANCE CAPABILITY

The IronPort appliance has fast, flexible and fine-grained message filtering capabilities. Custom filters can be written using "if-then-else" logic, very similar to C programming, that allows administrators to deal with any conceivable request. The parameters that can filtered on in the "if" field include source or destination IP, domain or address, headers, keywords in message body or attachments, attachment size or type, reputation of a sender or data available in an LDAP query. The actions taken include quarantine, redirect, notify, tag, archive, bounce, encrypt, etc.

One example of these filters in action is creating a rule that says if a message is bound for a certain sender (defined as an email address or an LDAP query) or from a certain sender then limit the attachment size and make an

IRONPORT®

archive copy. This capability is very useful in dealing with the many varied needs of a large enterprise and that these "special requests" are easily accommodated with simple message filters.

The most common use of message filters is for regulatory compliance. IronPort has created pre-loaded dictionaries that identify common medical terms required for HIPAA compliance. Similar pre-built dictionaries for Sarbanes Oxley (SOX) and SEC regulatory compliance are also available. IronPort supports onboard TLS encryption that can be selectively applied only to mail that requires encryption. For more advanced encryption needs, IronPort Email Encryption secures message content – rather than just the transport layer – using IronPort PXE™ technology, as well as legacy PKI-based technologies such as PGP and S/MIME.

Filters can be created either from the GUI or from a scriptable command line interface. Once policies have been created they are managed by IronPort Email Security Manager™. This powerful Web interface provides a comprehensive view of the entire email policy, spam, virus, attachment and compliance. Rules can be set up with clear hierarchy – a default rule and then specific rules in order of priority execution. For multi-recipient messages, the IronPort appliance supports message splitting – recipients that hit one rule set are grouped together, recipients on another are grouped and treated differently. This is a critical feature for managing enterprise policies that can become fairly complex in short order. Email Security Manager makes it simple.

CONTENT-BASED ANTI-SPAM AND ANTI-VIRUS

IronPort provides defense in depth against spam by offering two layers of protection. A preventive outer layer of reputation filters and an inner layer reactive filters.

IronPort's Reputation Filtering system is a critical first line of defense, blocking up to 80 percent of incoming spam at the connection level. IronPort Reputation Filters™ also (in default mode) route mail from known trusted senders directly to the inbox, avoiding unnecessary CPU utilization and risk of false positives introduced by scanning known good mail. But for the 20 percent of mail that is in the "grey zone," it is critical to rate limit and content scan each message. IronPort Anti-Spam™ addresses this "grey zone" by utilizing the industry's most innovative approach to threat detection. In addition to reviewing sender reputation, IronPort's unique Context Adaptive Scanning Engine™ (CASE) examines the complete context of a message, including:

- content
- methods of message construction
- reputation of the sender

When the CASE score is combined with sender reputation, the end result is more accurate than traditional spam filtering techniques. IronPort's Web

IRONPORT®

Reputation™ technology measures the behavior and traffic patterns of a web-site to assess its trustworthiness. IronPort's CASE determines the reputation of any URL within a message body, so that a more accurate analysis of the messages can be performed. This enables IronPort Anti-Spam to immediately protect users from spam, phishing and spyware threats distributed over email.

For organizations who prefer to offer management of spam to their end users, IronPort appliances provide the IronPort Spam Quarantine™. The 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.

IronPort also has anti-virus signatures from Sophos, fully integrated into the IronPort appliance — with elegantly unified management and reporting. The Sophos anti-virus engine is tightly coupled with IronPort Virus Outbreak Filters, allowing messages to be scanned in a test mode prior to release from the quarantine, IronPort and Sophos collaborate on identifying and stopping virus outbreaks, with a goal of optimum protection for our customers. The Sophos engine uses in-memory message passing for maximum performance. A message is queued to disk once and then repeatedly scanned in memory. Dispositions are fully integrated into IronPort's message filters. So one LDAP group (say engineering) can have spam deleted, but another group (say sales) can have spam tagged.

EMAIL ENCRYPTION

IronPort offers a variety of encryption capabilities, providing customers with the flexibility to securely communicate with all email users while complying with both business and regulatory requirements.

Built-in support for TLS encrypts the link between SMTP gateways to provide link-level protection. While TLS is appropriate for established business-to-business relationships, its capabilities are limited in securing communications with customers or new partners. TLS cannot guarantee that the link will remain encrypted to the final recipient's inbox if the message is routed through multiple SMTP hops.

IronPort Email Encryption improves security relative to TLS, guaranteeing that the message is never in the clear on the Internet by encrypting the message content. Even if the link is unprotected, the message content remains secure. Multiple encryption options are supported:

- IronPort PXE™ Technology: encrypts the message in a secure encryption envelope that may be decrypted and read only by the intended recipient through any email client, without the need to install client software. Additionally, IronPort PXE (formerly the PostX Envelope) provides business-class email features such as guaranteed read receipts and true message recall and expiration capabilities.

- IronPort PKI Encryption: supports legacy public key encryption schemes such as OpenPGP and S/MIME for communication between partner gateways. PKI requires pre-exchange of keys or certificates before encrypted messages can be sent.

IronPort PXE technology provides an easy-to-use, easy-to-manage approach to encryption. Messages can be received and opened by any email client without client software installation or PKI certificates, making it an ideal platform for broad deployment in business-to-consumer and ad hoc business-to-business communication. IronPort PXE messages are encrypted using proven industry-standard algorithms and the per-message encryption key. Keys can be distributed through either the managed IronPort Hosted Key Service or stored locally on the IronPort Encryption Appliance. Message recipients are asked to authenticate with the key service using a password, at which point the key is released and the decrypted message displayed. The end-user experience is much simpler than traditional public-key based systems, and the advanced email control features of IronPort PXE make it ideal for both ad hoc and regular communications with customers and business partners.

IronPort PKI Encryption provides a best-of-breed solution for OpenPGP and S/MIME encryption between partner gateways. While the cost and complexity of PKI are prohibitive to broad deployment, PGP and S/MIME remain popular and sometimes regulatory-required options for secure email exchange between close business partners.

IronPort Email Encryption is triggered based on centrally defined content filtering policies on IronPort's email security appliances. Policies may specify not just an encryption action, but the type of encryption to use, providing maximum flexibility to meet all requirements.

Encryption is a key feature of a complete email security solution. Until now, the difficulty of managing public key infrastructures and the limitations of link-level encryption such as TLS have limited the wide deployment of email encryption systems. IronPort's easy-to-deploy and easy-to-use technology solves the complexity in providing email encryption for all business communications, whether driven by regulatory compliance needs or smart business policies.

MANAGEMENT, MONITORING AND REPORTING

IronPort provides very sophisticated management, monitoring and reporting capabilities designed to satisfy the large global enterprises and ISPs that make up IronPort's customer base. Each appliance has a unique real-time reporting system called Mail Flow Monitor™. Email Security Monitor is a real-time threat monitoring and reporting system that is integrated into every IronPort email security appliance. This technology tracks every system connecting to your IronPort appliances to identify where Internet threats (such as spam, viruses, and denial-of-service attacks) are coming from, who is

sending you legitimate email and what they have done in the past. Extensive reports on content filters and internal users allow you to effectively enforce and manage corporate compliance policies.

Combating constantly evolving Internet-based threats requires a robust enterprise email security system, capable of providing accurate information and constant feedback. To provide administrators with the critical information needed to make complex security decisions, IronPort offers unprecedented real-time monitoring and reporting capabilities. IronPort Email Security Monitor is tightly integrated with IronPort's industry-leading SenderBase Network, and provides you with full details on traffic to your local site as well as visibility into a sender's global behavior.

Administrators can use Email Security Monitor to see if the system is rate limiting, and if so how many messages have been throttled – a unique capability, because most approaches to throttling simply slow a connection so there is no way to know how much mail has actually been throttled. If the administrator wants to change the policy being automatically applied to a given sender, they can do so with a few simple clicks from the Email Security Monitor interface.

In addition to the real-time reporting and management provided by Mail Flow Monitor, IronPort offers centralized historical reporting capability called Mail Flow Central™. This feature pulls log data off multiple systems and loads it into a SQL database. It then has powerful Web-based tools that generate historical trend analyses on spam virus and content filter performance. Mail Flow Central also has a very powerful message tracking capability that can search for mail to or from a given sender, with a given subject, attachment type, etc. The message tracker system creates huge gains in efficiency for system administrators that previously would have had to "grep" through logs from three or four separate systems to troubleshoot a given message. Mail Flow Central software that can be scaled up and down as appropriate for the customer. The intended use case is to have Mail Flow Central running on a desktop or server that is not in the DMZ, so historical reporting and tracking will never impact a production DMZ machine. IronPort also publishes the schema for the Mail Flow Central to allow for custom queries.

IronPort provides both email and SNMP monitoring for critical system functions. System health and security application level events are communicated via SNMP traps and configurable email alerts. All real-time system data is also accessible via an XML "status" on the system. The IronPort Systems engineering team has developed a variety of scripts that can be used to pull select real-time system status information into a larger network monitoring system.

IRONPORT®

CENTRALIZED MANAGEMENT

With Centralized Management, if a change is made on any one system, the administrator can push that change to any other specific machine, group of machines, or the entire cluster. This multi-master system is very powerful and sophisticated, and was developed to meet the needs of globally distributed carriers and enterprises. The system is implemented using a peer-to-peer mesh network, where the configuration of any one machine is stored on that machine's peers. This allows ultimate flexibility, as changes can be made from any machine and rolled out across the cluster. If any one machine fails, a new machine is given an IP address and it will automatically contact its peers and reconfigure itself. All system configuration information is also available as an XML file for permanent back up. All changes are logged by administrator, and there are three levels of access – read only, administrator and super user.

CONCLUSION

The IronPort email security appliance is the most sophisticated system available today. In production at eight of the ten largest ISPs and more than 20 percent of the world's largest enterprises, this system has a demonstrated record of unparalleled security and reliability.

This same code base that powers IronPort's most sophisticated customers is also available in easy to use 1U appliances such as the IronPort C150™. The goal of IronPort's development team is to create highly intelligent and capable machines that can automatically deal with error conditions, such as virus outbreaks or a major receiving domain going down. These events are handled intelligently and automatically, reducing administrative burden by as much as 75 percent. Many administrators report that they only touch their appliances once per month to "check up" on them. It is the advanced technology within IronPort's appliances that leads to the simplicity of management, and also the highest levels of security in the world.

Ⓘ **IRONPORT**®

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

IronPort Systems, a Cisco business unit, is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase, the world's largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use—providing breakthrough performance and playing a mission-critical role in a company's network infrastructure.

IronPort is now
part of Cisco.

ı|ıı|ıı
CISCO™