IronPort Streamlines Email at One of the World's Largest Computer Vendors.

THE SITUATION

As one of the world's top suppliers of computer systems, Dell Inc. receives millions of email messages every day. Outbound email volumes are also in the millions, especially during intensive email marketing campaigns. Not surprisingly, this flood of messages puts a tremendous burden on Dell's email servers.

In 2003, Dell's email engineers realized that the company was quickly outgrowing its existing email gateway infrastructure in a number of different ways. MTA, spam, content filtering, recipient validation, and non-delivery receipt (NDR) handling processes were spread across multiple systems, making system administration inefficient.

DELL AT A GLANCE

Founded: 1984

Employees: 69,700

Revenues (FY2006): $55.9 billion

Worldwide locations: 50+

Mailboxes (employees, contractors, and process mailboxes worldwide): approx. 100,000

SMTP addresses (individuals, aliases, mailing lists, and processes): 305,000+

Average number of attempted inbound messages per day: 29 million

Percentage of those messages that are spam or contain viruses: 95 percent

THE IRONPORT ADVANTAGE

- Replaced an email system, consisting of 103 disparate servers, with a streamlined infrastructure using 12 IronPort systems:
    —10 IronPort X1000 appliances (8 for inbound mail; 2 for outbound corporate mail)
    —2 IronPort C300D appliances (for outbound marketing mail)
- Dramatically reduced the amount of spam getting into the system
- Reduced spam traffic to internal mail servers
- Virtually eliminated false positives
- Created more efficient mail handling and eliminated capacity problems
- Allowed Dell to eliminate 12 of its Microsoft Exchange servers, due to decreased traffic load of undeliverable messages
- Decreased the employee time required to manage the email gateway systems by 75 percent

THE SITUATION
(CONTINUED)

In fact, Dell was using 103 different servers to handle incoming and outgoing email. The inbound machines included 40 inbound MTA gateways for the primary MX records, 2 more for secondary records, 18 servers for content filtering, and 12 for recipient validation and non-delivery receipts. The remaining 15 systems were dedicated to storing quarantined spam for several days in case a user should report a missing legitimate message. For outgoing mail, Dell used 6 MTA servers for corporate mail and 4 for marketing campaigns. Ahead of the corporate MTAs were 6 content-filtering servers, to ensure that no inappropriate messages originated from the company.

Managing Dell's email had become particularly difficult not only because there were so many layers to the infrastructure of the legacy system, but also because it had been scaled out and excessively load-balanced. The capacity problem was already to the point where downtime and email delays were significant issues—and email volumes were increasing at a staggering pace. Finally, the anti-spam solutions that had served Dell well over the previous few years were quickly showing weakness against new spam attack variants.

> **"IronPort has performed beyond any of our initial expectations."**
>
> — Erich Stokes, Systems Engineer, 2006

All of these mail system problems were taking their toll—not only on employee productivity, but also on IT budgets. Two full-time employees were needed to keep the systems running properly. Incoming mail had to be checked daily for false positives, and anti-spam rule sets needed to be adjusted at least once a week. Frequently, additional technical personnel had to be called in to deal with capacity spike issues. From both performance and cost standpoints, it was clearly time for Dell to overhaul its email infrastructure.

TECHNICAL CHALLENGES

According to Erich Stokes, a systems engineer in Dell's Global Technology Engineering Services group, the company had two major criteria for a new email solution: high capacity and robust spam filtering. To be exact, because of the huge amount of mail that travels in and out of Dell every day, Stokes says that their goals were, "Capacity, capacity, capacity—and spam filtering."

As mentioned earlier, Dell's email system sends and receives millions of messages per day. It has to accept and route mail for more than 300,000 SMTP addresses that link to nearly 100,000 actual mailboxes. The mailboxes serve Dell employees and contractors around the world (each of whom may be on multiple distribution lists), plus process mailboxes such as *support@dell.com*.

The new system had to integrate smoothly with the Microsoft Exchange servers that Dell uses around the world. It also had to support the many different application servers that generate SMTP traffic inside the company. And it had to work with Dell's Active Directory servers, which contain the user account and email information for those 100,000 mailboxes around the world.

THE IRONPORT ADVANTAGE

The IronPort X1000 integrates easily into existing messaging infrastructures — delivering defense-in-depth security with carrier-proven technology and the management capabilities required by large enterprises and ISPs.

Initially, Dell brought in a few IronPort® systems to supplement its existing email infrastructure. Those systems helped handle the massive volumes of email generated during direct-email marketing campaigns—as many as three to four million messages per day. Dell's email engineers were so impressed with the performance of the IronPort appliances that they decided to streamline the company's email infrastructure by going to an all-IronPort solution.

INTERNET

FIREWALL

IRONPORT X1000

EXCHANGE SERVERS

CLIENTS
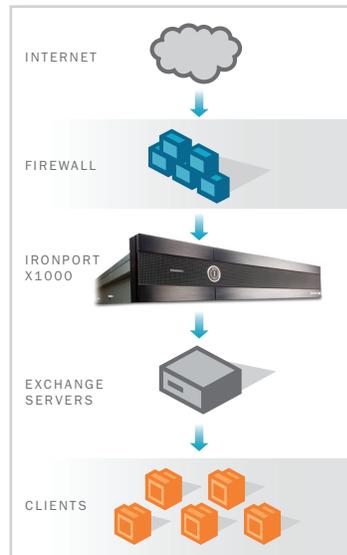
As a result of the transition, Dell was able to reduce its number of email servers by nearly 90 percent. The 103 disparate servers were replaced by ten IronPort C60™ appliances and two IronPort A60™ units. In early 2006, these original products were upgraded to IronPort X1000™ and C300D™ systems, respectively, to take advantage of newer technologies.

Eight of the IronPort X1000 appliances handle Dell's inbound mail; the other two are for outbound corporate mail. The two IronPort C300D units handle outbound marketing messages. Dell chose to keep separate inbound and outbound mail systems for easier migration from their previous servers, and because the company has traditionally separated the two services. The systems are equally divided and load-balanced between Dell's data centers.

IronPort appliances are the most sophisticated email security systems available today. Currently in use at eight of the ten largest Internet service providers (ISPs) and more than 20 percent of the world's largest enterprises, these systems have a demonstrated record of unparalleled security and reliability. They support and protect email systems not only from today's threats, but also from those certain to evolve in the future.

The IronPort X1000 high-performance appliance is built to protect the most demanding networks in the world. ISPs and large enterprises continue to be the primary targets of spam and viruses. The IronPort X1000 provides industry-leading email security on a platform that can meet today's demands for innovation and tomorrow's demands for scalability. IronPort's exclusive preventive filters and signature-based reactive filters, combined with content filtering and best-of-breed partner technology, provide the highest levels of email security available today—while delivering unprecedented visibility and management tools.

> **"The IronPort appliances were able to not only match but exceed our requirements and configuration needs. They did not require Dell-specific customizations."**
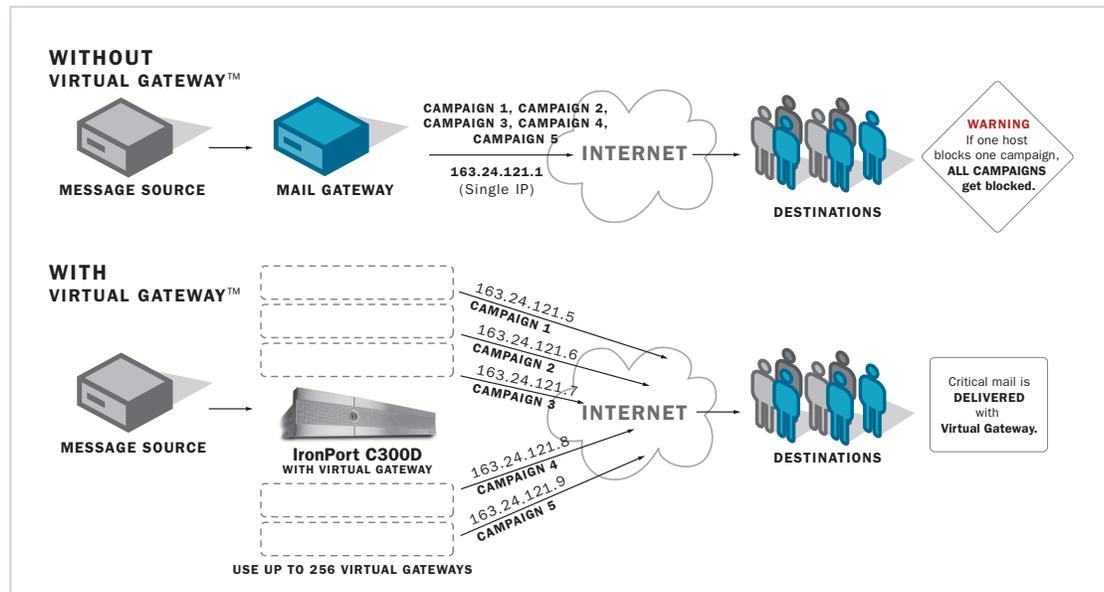>
> — Erich Stokes, Systems Engineer, 2006

The IronPort C300D email security appliance is a specialized IronPort C-Series™ product optimized to meet the unique requirements of email transaction confirmations, investor updates, and marketing newsletters. With the latest in email sender authentication technology, the IronPort C300D ensures timely and efficient communications with customers—while allowing enterprises to manage and protect their corporate identities on the Internet. Powerful enterprise monitoring integration and custom alerting make the systems truly "set and forget." This allows administrators to focus on priorities other than mail delivery.

THE IRONPORT ADVANTAGE
(CONTINUED)

IronPort's Virtual Gateway technology allows each campaign to be assigned its own IP address, segregating different classes of email running through the system. This results in a consistent reputation for each class.

WITHOUT VIRTUAL GATEWAY™

MESSAGE SOURCE → MAIL GATEWAY → CAMPAIGN 1, CAMPAIGN 2, CAMPAIGN 3, CAMPAIGN 4, CAMPAIGN 5
163.24.121.1 (Single IP) → INTERNET → DESTINATIONS

WARNING If one host blocks one campaign, ALL CAMPAIGNS get blocked.

WITH VIRTUAL GATEWAY™

MESSAGE SOURCE → IronPort C300D WITH VIRTUAL GATEWAY

163.24.121.5 CAMPAIGN 1
163.24.121.6 CAMPAIGN 2
163.24.121.7 CAMPAIGN 3
163.24.121.8 CAMPAIGN 4
163.24.121.9 CAMPAIGN 5

INTERNET → DESTINATIONS

Critical mail is DELIVERED with Virtual Gateway.

USE UP TO 256 VIRTUAL GATEWAYS

No custom integration or coding was required to integrate the IronPort products into Dell's IT infrastructure. Stokes recounts that an IronPort systems engineer helped them migrate from their previous email gateways without any problems. "The configuration and customizations of our previous email gateways were extensive. The IronPort appliances were able to not only match but exceed our requirements and configuration needs. They did not require Dell-specific customizations. On top of that, they provide a much more easily managed interface, which aided in housekeeping and cleanup of the customizations."

BENEFITS

With an IronPort solution in place at Dell, previous mail-handling problems disappeared, and resources (both personnel and systems) were able to be reallocated. Dell's email engineers were also able to consolidate outbound email globally, onto a single gateway. Additionally, the switch from 103 disparate servers to 12 seamlessly integrated servers gave the engineers more control over their company's email traffic.

HIGHER CAPACITY AND INCREASED RELIABILITY—WITH FEWER SERVERS

When Dell switched to IronPort email security appliances, the total number of servers in the company's email infrastructure was dramatically reduced—from 103 to 12. Stokes explains, "To us, the most important feature of the IronPort systems is performance, based on number of concurrent connections. No other MTA can touch them—even when we had 10 times as many servers as we now have from IronPort."

Despite the greatly reduced number of servers, the IronPort appliances have easily kept up with astronomical increases in mail volume, without requiring hardware upgrades or constant load-balancing attention by administrators. The entire system has become more stable. Because the previous systems were all running at capacity, they had stability issues at least monthly, if not weekly. When problems arose, Dell's email engineers had to call in an extra two or three people to help. Today, maintenance of the company's email system requires only half of a full-time employee's work week.

REDUCED TRAFFIC LOAD

Dell's email gateway infrastructure isn't the only thing that benefited from the switch to IronPort products. The company has also been able to reduce the number of Microsoft Exchange servers in its corporate hub (which sends and receives email from the IronPort appliances). This number dropped from 25 with capacity issues, down to 10 without any capacity problems.

According to Stokes, "This was a direct result of the IronPort systems' ability to perform conversational recipient acceptance validation to our Active Directory servers via LDAP. We can now filter out all the emails to invalid addresses in the SMTP inbound conversation, before we ever accept the email into the gateways. Our previous email gateways were not configured to do that, so our Exchange connectors were clogged with invalid recipients and taxed with generating non-delivery reports (NDRs) for all the invalid recipient emails."

Conversational LDAP accept lets the mail server do a lookup in the company's Active Directory during the SMTP session, and reject the message immediately if the recipient name isn't valid. That eliminates the problem of having to generate NDRs for spam messages that are accepted into the mail system and then cannot be delivered because they have invalid recipients. In Dell's case, the huge amount of NDRs being generated every day was clogging their mail servers. In addition, the "from" addresses on spam messages are usually forged, resulting in NDRs going to companies and individuals who had nothing to do with the original mailing.

The IronPort gateways even keep track of how many invalid recipients come from a specific IP address. If that number goes over a certain amount, messages from that address are blocked for a certain amount of time. This feature provides directory harvest attack prevention—keeping spammers from going through Dell's Active Directory, looking for valid recipient names.

LESS SPAM

Dell has also seen a significant reduction in the amount of spam getting into its network. The IronPort X1000 appliances utilize IronPort Reputation Filters™ as the outer layer of spam protection for a company's email infrastructure. IronPort Reputation Filters provide the first line of defense on IronPort email security appliances—disposing of up to 85 percent of incoming spam at the connection level. Blocking such a high percentage of unwanted mail saves

bandwidth, conserves system resources, and yields the highest levels of security for critical messaging systems. A proven preventive solution, IronPort Reputation Filters defend the largest ISP and enterprise networks, as well as small and medium-sized businesses, in production environments worldwide.

IronPort Reputation Filters leverage the information provided by IronPort's remarkable Sender-Base®, the world's largest email and Web traffic monitoring network. SenderBase collects data on more than 25 percent of global email and Web traffic, providing an unprecedented real-time view into security threats from around the world. It helps ISPs and other companies differentiate legitimate senders from spammers, and provides email administrators with visibility into who is sending them email.

> **"False positives are virtually non-existent. In two years, I can still count them on one hand."**
>
> — Erich Stokes, Systems Engineer, 2006

Over 100,000 organizations participate in the SenderBase Network, enabling the world's largest email and Web traffic monitoring system.

Completing Dell's anti-spam defenses is IronPort Anti-Spam™—the industry's leading spam-fighting technology. Integrated directly into IronPort's email security appliances, IronPort Anti-Spam protects millions of mailboxes at thousands of organizations from the productivity loss and IT costs of unsolicited commercial email. IronPort stops spam attacks in real time, without compromising accuracy. Dell considers the combination of IronPort Reputation Filters, SenderBase Network, and IronPort Anti-Spam technology the winning combination in the war against spam.

Perhaps even more important than catching so much illegitimate mail was the virtual elimination of false positives—legitimate email messages incorrectly flagged as spam. Stokes points out that, since Dell's switch to IronPort email security appliances, "false positives are virtually non-existent. In two years, I can still count them on one hand."

MORE EFFICIENT MAIL HANDLING

In Dell's overtaxed legacy email infrastructure, mail delays had become all too common. Dell's email engineers consider delays above 45 minutes critical, and they were seeing more and more of those in the latter half of 2003, before the IronPort appliances were brought in. In fact, capacity problems sometimes resulted in inbound email delays of up to three hours.

The old infrastructure had one layer consisting of the email gateway MTA and spam filtering, another that handled email content filtering, and a third layer responsible for recipient validation and non-delivery reports (NDRs). Now, all email gateway functions are on a single layer of IronPort machines. This consolidation has dramatically improved the efficiency of Dell's email traffic handling.
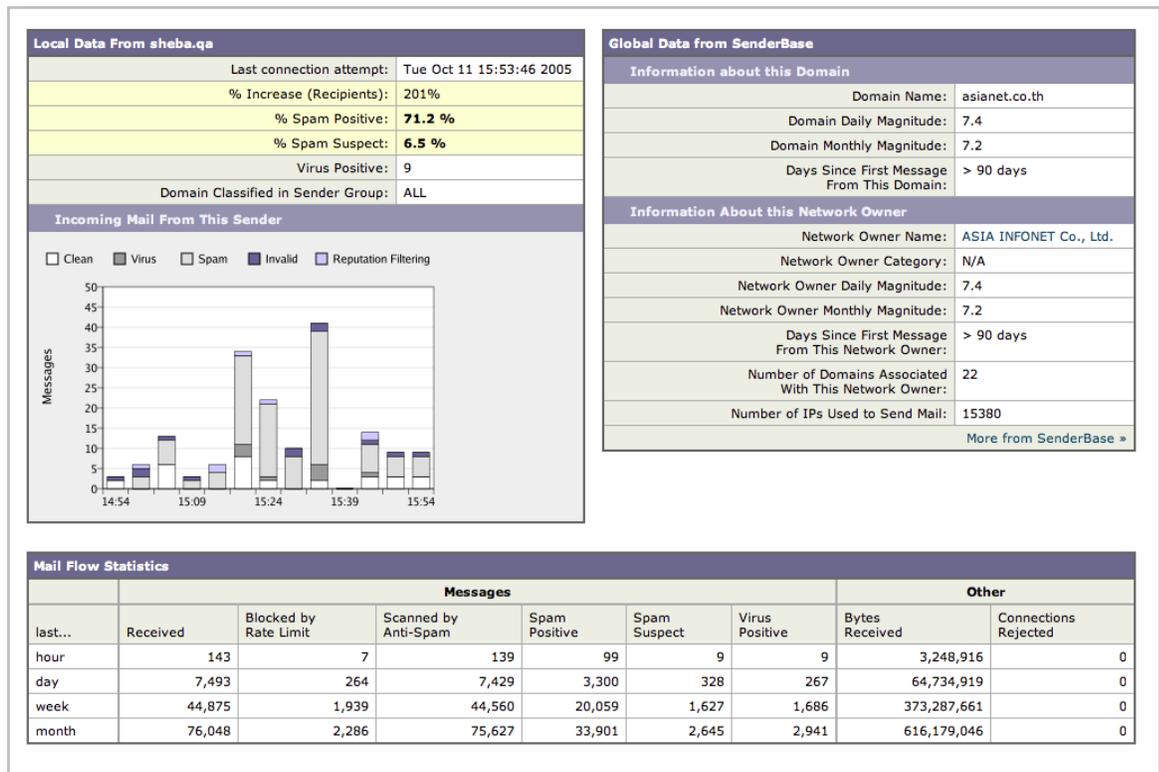
BENEFITS
(CONTINUED)

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

EASIER CONFIGURATION AND ADMINISTRATION

Now that Dell's email infrastructure has been streamlined, managing it is much easier. With the deployment of an all-IronPort solution, Dell has been able to reduce its email gateway technical staff from two full-time employees to a single half-time job. This has enabled the company to reassign valuable technical assets to other projects, such as implementing important new networking technologies.

By integrating SenderBase data, IronPort's Mail Flow Monitor provides you with an accurate assessment of the threat level of every message.

Local Data From sheba.qa

Last connection attempt:	Tue Oct 11 15:53:46 2005
% Increase (Recipients):	201%
% Spam Positive:	**71.2 %**
% Spam Suspect:	**6.5 %**
Virus Positive:	9
Domain Classified in Sender Group:	ALL

Incoming Mail From This Sender

☐ Clean   ☐ Virus   ☐ Spam   ☐ Invalid   ☐ Reputation Filtering

Global Data from SenderBase

Information about this Domain

Domain Name:	asianet.co.th
Domain Daily Magnitude:	7.4
Domain Monthly Magnitude:	7.2
Days Since First Message From This Domain:	> 90 days

Information About this Network Owner

Network Owner Name:	ASIA INFONET Co., Ltd.
Network Owner Category:	N/A
Network Owner Daily Magnitude:	7.4
Network Owner Monthly Magnitude:	7.2
Days Since First Message From This Network Owner:	> 90 days
Number of Domains Associated With This Network Owner:	22
Number of IPs Used to Send Mail:	15380

More from SenderBase »

Mail Flow Statistics

last...	Messages						Other	
	Received	Blocked by Rate Limit	Scanned by Anti-Spam	Spam Positive	Spam Suspect	Virus Positive	Bytes Received	Connections Rejected
hour	143	7	139	99	9	9	3,248,916	0
day	7,493	264	7,429	3,300	328	267	64,734,919	0
week	44,875	1,939	44,560	20,059	1,627	1,686	373,287,661	0
month	76,048	2,286	75,627	33,901	2,645	2,941	616,179,046	0

BENEFITS
(CONTINUED)

Although the actual number of people administering Dell's email has decreased, the number of people qualified to do so has gone up. Even though the IronPort systems have more capabilities, and are thus in some sense more complex, their ease of use has allowed Dell to train more people to administer them. That means Dell no longer has to pull specific people off of other important tasks to attend to email gateway issues, or worry about keeping the systems going when those employees are sick or on vacation.

SUPERIOR SUPPORT

IronPort offers world-class support programs that are tailored around an array of technical support services, designed to meet the needs of a variety of different organizations. Stokes sums up the customer support experience, saying, "IronPort is unique in that they assume that anyone contacting their support is a knowledgeable email engineer, so they've put equally knowledgeable people on their first level of support. They don't have the traditional first layer of support you have to go through to get to the people who really know what's going on. They've obviously recruited some of the brightest people around. It makes life simple for us. And we usually get a response to our emailed questions in an hour or less." IronPort customers expect outstanding support and IronPort works hard to deliver exceptional service—ensuring continued customer satisfaction and success.

IRONPORT
07/07
DOC RELEASE

Ⓘ IRONPORT®

IronPort Systems, Inc.
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.

ıllıılı CISCO™