

the Web Security report

A MESSAGING MEDIA PUBLICATION • JULY 2007 EDITION • WWW.WEBSECURITYREPORT.COM

ABOUT THIS PUBLICATION

The Web Security Report acts as a publishing partner for Internet security solutions providers, testing labs, research entities and trade organizations. Published monthly by Messaging Media, LLC, the Web Security Report has an online and print audience of over 120,000 readers
publish@websecurityreport.com

707

Cisco and IronPort:

A Promising Horizon on a Threatening Landscape

TABLE OF CONTENTS

Cisco and IronPort: A Promising Horizon on a Threatening Landscape	1
Web Security News	8
Sponsor Profile	10
In This Edition	12

By Paul Gargaro

When Cisco Systems opened the year with the announcement of its planned acquisition of IronPort Systems for \$830 million in cash and stock, it strengthened the promise of wide traffic inspection for delivery of comprehensive email and Web security—from the network through the application layer.

This new opportunity marks a milestone for enterprises and other organizations as they seek a universal means to impede the flow of spam, viruses and fraud that populate their computing infrastructures.

"We feel that there is enormous potential for enhanced email and message protection solutions to be integrated into the existing Cisco Self-Defending Network framework," says Richard Palmer, Senior Vice President for Cisco's Security Technology Group. "Using the network as a flexible platform to integrate IronPort's technologies,

> *continued on page 2*

Better Together

On June 25, 2007, Cisco Systems announced the

IronPort is now part of Cisco.



completion of the acquisition of IronPort Systems.

Moving forward, IronPort will operate as a business unit in Cisco's Security Technology Group.

The acquisition marks a significant step in Cisco's evolution as a leader in security and defines the future of information technology security. IronPort's products and technology will enable Cisco to extend its Self-Defending Network strategy to provide customers with integrated end-to-end IT security never before offered by a single company.

in the next issue

SPONSORED BY
IRONPORT SYSTEMS



Web Security and Vulnerability Scanners With discussion of tools, products and services, the Web Security Report explains how and when remediation should be applied, underlying methodology and policy requirements, and why scanning alone is not enough to demonstrate a solid security posture.

Regular features include: Web Security News, Company Spotlight and Sponsor Profile.

Cisco will be able to build new security applications as customer demands evolve.”

Indeed, this acquisition paves the way for the fusion of IronPort’s array of proven security solutions into Cisco’s vast network infrastructure—and comes as the battle intensifies against email and Web-based threats that now are largely profit-driven. Asked why he robbed banks, notorious thief Willie Sutton offered this now-famous reply, “Because that’s where the money is.” That rationale may also be attributed to the creators of modern spam, phishing and associated malware.

Anatomy of the Threat

After a brief slowdown in the rate of spam and malware attacks through the first half of the decade, threats were once again on the rise by late 2006. Today, friends unwittingly send links via email to corrupted Web servers, while trusted websites

are routinely compromised to silently serve up spyware. Fueled by the money to be made from pushing bogus information to inflate a stock’s sale price, connect illicit offshore pharmaceuti-

cal suppliers with consumers, or capture sensitive corporate or personal financial data, these new threats are often designed by professional engineers, who are blending email and Web technology, social engineering as well as intelligent command and control systems to deliver highly sophisticated and potent attacks for commercial gain.

Tom Gillis, IronPort’s Vice President of Marketing, offers the following example of how email and Web technology was recently deployed to devise a well-coordinated attack.

On March 30, a Microsoft exploit that took advantage of an ANI (Animated Cursor Handling)

vulnerability was seen in the wild. ANI functionality enables users to choose a cute bug or smiley face or other character instead of the standard windows cursor. In the exploit, an ‘anih’ chunk in an animated cursor file was read into a stack buffer of a fixed size (36 bytes) but the actual operation provided the attacker an easy way to overflow the stack and gain control of the process on the remote client. It revealed that harmful code could be delivered onto an end-user’s PC without the user’s knowledge or consent.

Although this vulnerability has existed since December 2006, its first exploit served as a proof of concept—to simply deliver harmless pop-up advertising software. However, within 24 hours of this relatively innocuous attack, malicious Trojans emerged and began to utilize the exploit. After 48 hours, more than 90 URLs were on the attack. Many of the sites were hosted in China with other servers detected in the US and Korea. Some used common misspellings of legitimate URLs (such as www.mircosoft.com) to advance their strategy. Others were stealthy domains that had legitimate sounding names but received no actual traffic. To drive traffic to these new sites, phishing and spam emails were sent out within 24 hours of the exploit’s initial announcement. By accurately mimicking Yahoo! Greeting cards, these phishing emails were extremely hard to detect.

The ANI exploit illustrates the effectiveness of email and Web technologies to engage and deceive end-users. This blend highlights the fact that 80 percent of today’s spam contains a URL. The ability to analyze both traffic streams is more critical than ever. In other words, Web filters will be most effective when they draw on data from email traffic, while email filters will work best by incorporating Web traffic data.

The exploit also underscores the rapid evolution of modern attack strategy. Two years ago, the average life of a zombie used in a spam attack was more than 90 days. 80 percent of today’s zombies

“We feel that there is enormous potential for enhanced email and message protection solutions to be integrated into the existing Cisco Self-Defending Network framework.”

Richard Palmer, Cisco Systems

are used for less than 30 days, making the threats' sources much more difficult to trace. During the ANI exploit, new domains were introduced hourly. This created a huge challenge for first-generation Web or email security solutions, which were designed for acceptable use policy enforcement—like preventing users from accessing certain classes of content (such as pornography) on the Web. The solutions for such enforcement were typically based on classified lists of good and bad sites that were manually created and maintained. Email security relied on similar lists of known spam servers. Clearly, the use of static or slowly updated lists is no longer effective. IronPort recently profiled a pharmaceutical spam attack in which spam sources would rotate their IP addresses on average every 12 minutes, and would rotate different URLs every 15 minutes. List-based systems simply cannot keep up with this rate of obfuscation—by the time the list is updated and published, the threat has moved on.

Finally, the ANI exploit reflects the changing volume and stealth behind these new attacks. Malware writers, such as those who launched the ANI attack, are turning to lower volume, but more targeted assaults that are able to bypass traditional signature based defenses for longer periods. The goal of malware writers is to penetrate networks, not to gain notoriety, thus we now see a rise in small outbreaks that are variants of a known virus. Gillis recalls the Stration virus outbreak of 2006 as an excellent example. This highly polymorphic attack, with proof of concept variants deployed in October, led to a series of sustained attacks late into the fall. With its multiple variations on a basic theme, the outbreak significantly delayed anti-virus signature vendors' response times.

A graph of the outbreak, as detected by IronPort's SenderBase Network, is shown in Figure 1. No single attack was designed to be massively distributed. Instead, the attack took a 'divide and conquer' approach—using many variants in smaller attacks that were harder to characterize with signatures.

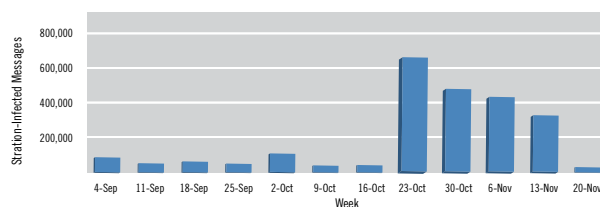


Figure 1: The many variants of the Stration virus created an ongoing attack.

Wide Traffic Inspection

Complex attacks place greater demands on enterprise IT and network administrators. According to Gillis, the answers to their challenges rest in smarter security solutions that offer a broader view of the network—so that when a message arrives, and is determined to be a phishing attack, any of the URLs it contains can be passed on to a Web security device to ensure that other end-users won't be hit with a variant of the same attack. Additionally, when that Web security device detects malicious content from a Web server, that server must be carefully examined or blocked.

“This level of cooperation must extend beyond the perimeter,” Gillis explains. “When a desktop client analyzes behavior of suspicious code and detects a new ‘zero day’ attack, the signature of that code should be captured and sent to perimeter equipment to block further spread of the attack.”

Similarly, the cooperation needs to span all networking levels—from the packet level to the content level. If packet-level analysis identifies suspicious traffic patterns, the content from that transaction should be examined more carefully with content-aware devices, such as an email or Web security appliance.

Gillis believes that the next generation of security systems must take a global view of every active email and Web server on the Internet. Systems

Two years ago, the average life of a zombie used in a spam attack was more than 90 days. 80 percent of today's zombies are used for less than 30 days, making the threats' sources much more difficult to trace.

that can share threat data across protocols, across network boundaries, and across the entire Internet are capable of performing wide traffic inspection.

“Wide traffic inspection is an ambitious endeavor, and it will take years to fully develop,” he acknowledges. “But the combination of IronPort and Cisco takes a major step forward in this effort. The

combined company is integrating IronPort’s industry leading content security appliances, IronPort’s SenderBase (the world’s first and largest email and Web traffic monitor-

ing service) and Cisco’s broad array of network infrastructure and security products.”

“Wide traffic inspection is an ambitious endeavor, and it will take years to fully develop. But the combination of IronPort and Cisco takes a major step forward in this effort.”

Tom Gillis, IronPort Systems

A Foundation for Secure Infrastructure

Launched as a business dedicated exclusively to combating email-borne spam, IronPort has achieved a hard-earned reputation as a leading Internet security provider. The company’s strength is based on an advanced operating system and reputation monitoring network, which are the cornerstones of its high-capacity gateway security appliances.

Over the years, IronPort has expanded its powerful anti-spam capabilities to provide anti-spyware, data encryption and compliance services, as well as content inspection for Web traffic. Last fall, it acquired PostX (an encryption service provider) to help seamlessly deliver secure, reliable email content protection to every mailbox on the Internet—regardless of what software is being used to access email. A month earlier, IronPort entered into a partnership with Webroot to bolster spyware detection by adding the company’s premium software into IronPort’s latest Web security appliances.

All of these factors reflect the promise of Cisco’s IronPort acquisition—to deliver a complete, fully-integrated new security infrastructure for applications including email, instant messaging and voice over IP. IronPort’s success is built upon the strength of its proprietary technologies and world-class partnerships that power a highly-advanced product portfolio. This foundation features:

IronPort AsyncOS, a revolutionary operating system that delivers the industry’s highest performance and best security features. The system is designed to handle the inbound and outbound needs of the world’s largest and most demanding infrastructures. It provides robust message queue management, bounce handling and connection management. This ensures that the infrastructure is never overwhelmed—even during the largest threat outbreaks or attacks—while saving money on hardware, rack space, power and IT administration time.

IronPort’s SenderBase, the world’s largest email and Web traffic monitoring network, provides comprehensive data that can be used to differentiate legitimate senders from spammers and other attackers—giving administrators increased visibility. With data on more than 25 percent of the world’s Internet traffic, IronPort’s SenderBase Network affords an unprecedented real-time view into global security threats. SenderBase is at the heart of IronPort Reputation Filters and the SenderBase Reputation Score (SBRS), which boils down SenderBase data into a single score indicating the threat level for each incoming message and URL. SenderBase is also utilized by IronPort Virus Outbreak Filters, which protect customers from viruses—hours before traditional anti-virus vendors publish virus signatures.

IronPort customers can ‘opt in’ to data sharing with the SenderBase Network, enabling their appliances to automatically respond to new attacks as they hit their own networks. The vast majority of IronPort

customers chose to partake in sharing data with the SenderBase Network, because participation directly enhances the efficacy of their appliances. To accommodate a wide range of corporate security policies, IronPort provides the ability to participate at different levels of granularity, as well as very clear guidelines about what data is collected and how that data is handled.

IronPort's SenderBase collects and correlates data on the behavior of virtually every active email and Web server on the Internet. It measures factors such as:

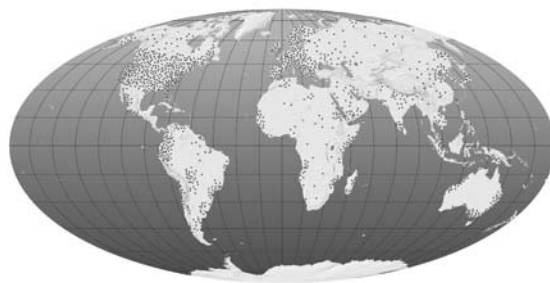
- How long has the server been delivering email or Web content?
- What is the country of origin?
- What does the volume of the server look like over time?
- Is any of the content from the server proving to be spam or malware?
- What is the appearance of the DNS configuration?
- Is the server located in a consumer broadband network?

These data points are then rolled into a numerical score similar to a consumer credit rating. The scores range from -10 to +10, and are made available to the IronPort appliances to then apply appropriate security policies. Very negative scores indicate a connection that can be dropped or blocked. Neutral scores indicate that the content should be sent to one or many different content scanning engines to perform a more detailed analysis of the payload. Positive scores indicate that the content may get a different set of content scanning—such as virus scanning, but not spam scanning.

The accuracy of the scores in IronPort's SenderBase is dramatically enhanced by the analysis of wide traffic. During the earlier profiled ANI exploit, the IronPort Web security appliances were the first to detect the exploit URLs. The reputation score of

these URLs was immediately affected. When the phishing emails associated with the attack began to arrive at IronPort email appliances, the content of the phishing emails was identical to legitimate content, and would have very easily slipped past a traditional content based spam filter. By using wide traffic inspection, IronPort email appliances were able to stop the phishing emails immediately, preventing the further spread of the ANI outbreak.

IronPort's product line-up includes the award-winning IronPort C-Series and X-Series email security appliances—first launched in 2003. Designed for small or large businesses as well as major internet service providers, these appliances slash the downtime associated with controlling spam, viruses and other related threats. The products are armed with state-of-the art software to provide: reputation filtering that eliminates 80 percent of spam at the connection level; anti-spam controls to check known and emerging threats; virus outbreak filters that assess threats contained in inbound and outbound messages and quarantine suspicious traffic until anti-virus vendors can supply the appropriate signatures; signature-based anti-virus protection that consolidates protection against viruses, Worms and Trojans by utilizing rigorous scanning and denial of service prevention technology; and compliance solutions—including filters, encryption, content scanning, archiving, monitoring and reporting tools.



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

the Web Security report

IronPort email security appliances equip IT managers with the ability to scrutinize both historic and real-time email traffic. When it comes to dealing with threats or suspicious mail, the appliances provide full automation to reduce the management burden on IT staff. By consolidating email operations and security onto a single platform, they require little maintenance and configuration, which ultimately lead to a low cost of ownership. Ultimately, the products serve as shock-absorbers—ensuring that end-users aren't slowed down by spam, viruses and other threats.

In June, IronPort introduced the newest addition to its email security product line, the IronPort X1050.

IronPort appliances provide visibility into past threats and problems as they are emerging, while supplying a clear graphical interface, automated updates and comprehensive monitoring.

Fully-enabled, the appliance can process more than 2.5 million messages per hour. This massive throughput means it can handle increased

spam volumes, while applying more CPU processing power to each message and more advanced spam filtering algorithms.

IronPort S-Series Web security appliances protect enterprises (at the network perimeter) from spyware and other malware. Its features include: Web reputation technology that uses the SenderBase Network to accurately gauge the integrity of a URL; an anti-malware system that rapidly scans Web content as it is downloaded; a dynamic vectoring and streaming engine that performs thorough scanning; and a signature-based verdict engine to protect against adware, tracking cookies, browser hijacks, phishing, pharming and more.

Like the company's email security appliances, IronPort's Web security appliances reduce the time and expenses associated with Web-based threat prevention. Full integration of the IronPort S-Series delivers set-up, management and cost efficiencies. The appliances provide visibility into past threats and problems as they are emerging, while supplying

a clear graphical interface, automated updates and comprehensive monitoring.

IronPort M-Series security management appliances deliver agile management and security control at the network gateway. This central platform serves as the ideal tool for enterprises to manage policy, reporting and auditing data for IronPort's email security and Web security appliances. The IronPort M-Series offers a consolidated view of the enterprise's application-specific security gateways.

The IronPort Web security appliances are better able to filter Web traffic because of the data coming from the email traffic captured by the IronPort email security appliances. Conversely, the IronPort email security appliances are better able to stop spam because of the data flowing from the IronPort Web security appliances. IronPort security management appliances ensure top performance from both the email and Web security appliances, and protect corporate network integrity by increasing deployment flexibility. This 'better together' effect is at the heart of wide traffic inspection technology.

Better Together

While it has been acquired by Cisco, IronPort will continue to operate as a separate business unit, building on a track record of success in the email and Web security realms. Since its founding in 2000, IronPort has cultivated a customer-base of leading organizations. Today, its technology and appliances protect thousands of customers around the world, including eight of the ten largest ISPs and more than 20 percent of the world's largest enterprises. Dell Inc. JetBlue Airways, Ryder Systems, Tellabs, Johns Hopkins University and Aéroports de Paris are representative of its diverse clientele list.

With an eye for high-performance and innovative solutions to protect its own networks, Cisco was an early adopter of IronPort technology. A customer since 2002, the company has now standardized on

IronPort infrastructure worldwide. Cisco utilizes IronPort technology at eight locations around the world to significantly reduce the organization's administrative burden, and increase network security. IronPort enables Cisco to centrally manage a global infrastructure.

Moving forward, Cisco and IronPort will focus on development resources into extending the family of tools that deliver wide traffic inspection.

"The most obvious application of wide traffic inspection is in the firewall," Gillis says. "When advanced firewall systems like Cisco's Adaptive Security Appliance (ASA) have access to the reputation data in IronPort's SenderBase, these devices can enable even more advanced security services."

If, for example, botnet software infects a client PC, Gillis notes that it will typically try to 'phone home' (connect to a central command server). To avoid detection, this connection attempt will frequently use some port other than Port 80. While the firewall may block the port, the ability to identify that a client is probing the firewall and attempting to connect to a server with a poor reputation is very useful. The connection attempts can be characterized and lead to the conclusion that the client has been compromised with malware. Often, based on the connection patterns, the type of malware can be revealed. As Network Access Control (NAC) systems begin to be incorporated into wide traffic inspection, the illicit activity detected at the firewall can be shared with the NAC systems—ensuring that the infected client can be quarantined and remediation measures can be launched.

The wide traffic inspection framework can be extended beyond individual networks. Most legitimate consumer mail systems connect to the ISPs message store or 'POP server', where the mail is then relayed onto the Internet. If the high-speed switches in a carrier's network contain appropriate instrumentation, they can identify suspicious traffic patterns (such as a consumer PC sending mail

directly to the Internet). As these switches pass information on to the shared database, a receiving email security appliance can see that a message came down a suspicious data path. Combined with an analysis of its content, the message can then be more accurately identified as spam.

"Next-generation security solutions will need to take advantage of techniques like wide traffic inspection," Gillis reiterates. "The breadth of the product line from IronPort and Cisco makes for a particularly compelling security system."

As wide traffic inspection is implemented in a growing variety of devices, threat writers will have an increasingly difficult time creating new attacks that avoid detection. Sharing of data across protocols and networks makes for an improved overall system. Gillis sums up, "Cisco and IronPort offer this capability, which is what makes us better together." ■

About the Author

Paul Gargaro is a freelance writer whose work has appeared in such publications as *The New York Times* and *Detroit Monthly*. He has held staff positions with *The Bridgeport Post*, *Crain's Detroit Business* and *Bloomberg News*.

Web Security Market to Hit \$58 Billion

Recent research suggests that the global IT security market will grow to \$58 billion by 2010. Market research firm ReportBuyer.com predicts the 16 percent annual growth (that began in 2005) will continue through 2010—largely due to steadily rising demand from the government, healthcare and financial sectors. Firewalls and content management solutions currently represent the largest share of the market, but unified threat management products

will account for more of the market as customers implement defence-in-depth security strategies. Also, the research suggests that though the largest markets today are the US and Europe, Asian economies like China and India are quickly catching up.

To learn more, or to purchase the full report, visit: <http://www.reportbuyer.com/go/BCC00046>

Survey Says: Hidden Charges Anger Consumers

A recent survey of more than 2,400 Web users, commissioned by MoreComputers.com, found consumers increasingly irritated by deceptive website tactics. 'Philfing' is the name given to the practice of "purposely hiding what I'm looking for"—holding back the real cost of extras (such as charges for tax, delivery, credit cards, baggage and insurance) until the last minute. The research reveals so-called 'free delivery' that turn out to require an extra purchase or spending over a certain amount frustrate consumers immensely. As do hidden surcharges for paying by

credit card. Another consequence of philfing is that shopping comparison websites are finding it increasingly difficult to maintain a level playing field when listing prices. 93 percent of those surveyed were annoyed by sneaky website charges, with 64 percent of those surveyed saying the charges have actually caused them to abandon a purchase entirely.

MoreComputers has set up an informative website, and is asking users to submit philfing examples, at: <http://philfing.info>

Are Laws Threatening Security Research?

What if a Web researcher found a bug on your website today, but was too afraid of the law to tell you? A new report, by a Computer Security Institute (CSI) working group, concludes that fear of prosecution may discourage Web researchers from disclosing security holes to website operators. New legislation may make it easier for site owners to prosecute those who locate and disclose vulnerabilities. This could result in less disclosure, and ultimately more unknown vulnerabilities for hackers to exploit.

The group's inaugural report offers insights and discussions from security researchers, computer crime

law experts and representatives from law enforcement agencies. It also shines a spotlight on Web 2.0 technologies that make it easier for users to pay bills, order medication and swap photos online. The current legal framework makes it difficult to highlight security flaws in these next-generation Internet applications, which are quickly becoming ubiquitous. Moving forward, the group plans to create disclosure guidelines which will help site owners write policies and help security researchers understand them.

The full report is available at: http://i.cmpnet.com/gocsi/db_area/pdfs/CSIWebSecurityResearchLaw.pdf

Hackers Target Legitimate Sites

Over 10,000 legitimate websites have been infected with malicious software that could install keyloggers and other malware whenever a user visits the sites. The compromised sites are all devoted to legitimate subjects such as taxes, jobs, tourism and cars. This new outbreak of Web hijacking is thought to be the result of a Russian-developed malware kit called MPack. The MPack kit enables hackers to quickly

develop code that exploits browser vulnerabilities, and is said to be 'browser aware'. Security experts warn that the kit contains attack code capable of infecting machines using at least three major Web browsers: Internet Explorer, Firefox and Opera.

The complete story can be viewed at: <http://news.bbc.co.uk/1/hi/technology/6221306.stm>

FBI Aims to Bust Botnets

The FBI recently announced that an ongoing cyber-crime initiative, dubbed "Operation Bot Roast", has identified more than one million PCs compromised with bot software and resulted in charges against three people for violations of the Computer Fraud and Abuse Act. The goal of the operation is to disrupt the activities of criminals (known as 'bot masters' or 'bot herders') who compromise their victims' machines to use for sending spam or attacking other computers. The Bureau is working with industry

partners, including the CERT Coordination Center at Carnegie Mellon University, to notify the victim owners of the computers. Through this process, the operation may uncover additional incidents in which botnets have been used to facilitate other criminal activity.

The FBI's full press release is available at: <http://www.fbi.gov/pressrel/pressrel07/botnet06130>

company spotlight

ActivIdentity, Inc.

ActivIdentity isn't passive when it comes to security. The company is the trusted provider of identity assurance solutions for the enterprise, government, healthcare and financial services markets worldwide. Its products are used to control and monitor access to intranets, extranets and the Internet—enabling businesses to authenticate

and manage the digital identities of employees, customers and trading partners. More than 15 million users and 4,000 customers rely on solutions from ActivIdentity. The company also offers professional services such as consulting, support and training. ActivIdentity is headquartered in Fremont, CA. www.actividentity.com

The logo for ActivIdentity, featuring the company name in a bold, italicized, sans-serif font with a trademark symbol.

IRONPORT SYSTEMS, a Cisco business unit, is a leader in Internet Gateway Security. The company has developed the IronPort S-Series Web Security Appliance. This enterprise class solution delivers the industry's most comprehensive malware protection by integrating processing at both the network layer and at the application proxy layer. Furthermore, the IronPort S-Series is now the industry's first and only Web security appliance to combine URL filtering, reputation filtering and anti-malware filtering on a single, integrated platform. By combining these innovative technologies, the IronPort S-Series allows organizations to address the growing challenges posed by securing and controlling Web traffic.

Network-Layer Protection

The IronPort S-Series™ has an integrated Layer (L4) Traffic Monitor. This wire-speed device can sit inline or on a network tap. It monitors all network activity, looking for malicious traffic that is trying to “phone home” or connect to a rogue server. The L4 traffic monitor shares data with IronPort's Web reputation system, to identify and stop malware before it does harm. The L4 traffic monitor also does an excellent job of identifying the most infected PCs on a corporate network—allowing IT administrators to proactively and efficiently launch desktop clean up efforts.

Application-Layer Processing

The IronPort S-Series also includes an extremely high-performance Web proxy, along with integrated caching and content acceleration capabilities. Built on IronPort's proprietary operating system, AsyncOS™, the IronPort S-Series proxy can support up to 100,000 simultaneous connections—as much as 10x more than traditional UNIX-based proxy servers. Being a Web proxy allows for comprehensive content inspection at the application layer — a critical requirement for ensuring accuracy against Web-based malware.

Accelerated Signature Scanning

IronPort® developed its proprietary Dynamic Vectoring and Streaming (DVS) engine™ to accelerate the signature scanning of Web content and minimize latency. The DVS engine performs intelligent scanning and reputation-based caching to minimize the amount of scanning that actually needs to take place. When an object does need to be

scanned, the DVS engine has a unique streaming capability. It can scan an object while simultaneously receiving the remainder of it and buffering it though to the end-user. This combination of intelligent scanning and streaming of data yields a decrease in latency that approaches 1/10th that of traditional ICAP-based signature scanning systems — making the IronPort S-Series imperceptible to end-users.

By combining the DVS engine with best of breed signatures, the IronPort S-Series protects organizations against the broadest range of Web-based malware. The IronPort Anti-Malware System™ quickly and accurately detects and blocks a full range of known and emerging threats, including adware, Trojans, system monitors, keyloggers, rootkits, malicious/tracking cookies, browser hijackers, browser helper objects, phishing and more.

The World's First Web Reputation System

IronPort invented the concept of reputation filtering more than three years ago. This capability is at the heart of the IronPort S-Series. For each Web request, IronPort makes an assessment of the reputation (or trustworthiness) of the URL requested. This reputation score is based on over 45 different parameters, including such factors as:

- How long has the domain been registered?
- What is the country of origin?
- What is the IP range of the hosting server?
- How does the name server infrastructure behave?
- How much traffic is the URL getting?

By analyzing these objective parameters, the IronPort Web reputation system can make a very accurate determination



The IronPort S-Series Web security appliance: an industry-leading solution for securing and controlling Web traffic.

about every active Web server on the Internet. Based on configurable thresholds, the IronPort S-Series will reject traffic that is clearly hostile—without wasting system resources on a full signature scan. Similarly, known good traffic with a sufficiently positive reputation score will bypass DVS scanning and move right through to the end-user. Web traffic with a neutral or slightly negative score will be passed to the DVS engine for further analysis.

By assigning a reputation score, and using that input to make scanning decisions, IronPort Web Reputation Filters™ maximize system throughput, reduce latency and increase overall accuracy by as much as 20 percent.

Integrated URL Filters

IronPort URL Filters™ include one of the industry's largest databases to address acceptable use policy concerns incurred due to Web traffic usage. With over 50 categories, approximately 20 million sites covered (corresponding to over 3 billion webpages) and global coverage across 70 languages and 200 countries, IronPort URL Filters offer the broadest reach and the highest accuracy rate in filtering Web content. With automatic daily updates and more than 100,000 new sites being added on a weekly basis, enterprises can rest assured that their policies are always applied against the most current rules.

Enterprise Management Tools

Global corporations need powerful management and reporting systems to optimize their investment and minimize the required administration time. The IronPort S-Series is built on IronPort's proprietary AsyncOS operating system and thus it inherits the world class management and

reporting capability that has made the IronPort C-Series™ the number one choice among enterprises for email security.

IronPort S-Series appliances include a flexible policy control platform called IronPort Web Security Manager™ which unifies policy creation for all filtering services on the appliance and provides granular options for the Enterprise based on authenticated or non-authenticated users in their network.

Along with flexible policy creation tools, every IronPort S-Series appliance comes with IronPort Web Security Monitor™ — a real-time threat monitoring and reporting system. The system tracks all network traffic to provide a single location from which to monitor acceptable use policy violations and a broad range of Web security threats. This provides security officers and administrators with comprehensive visibility and actionable insight into their Web traffic infrastructure.

The IronPort Advantage

IronPort Systems is focused on building comprehensive gateway security for enterprise customers. IronPort is a clear leader in the industry, pioneering technical breakthroughs like reputation systems and unique proxy appliance designs. IronPort's industry-leading systems have a demonstrated record of unparalleled performance, accuracy and reliability. To secure greater protection for your company's Web or email messaging system, visit www.ironport.com or call 650-989-6530.



www.ironport.com

PAGE 1 Cisco and IronPort:

A Promising Horizon on a Threatening Landscape

With Cisco's acquisition of IronPort, a unique multi-level solution represents the latest from these two organizations—delivering on a vision of integrating intelligent security into the network infrastructure. What will this new effort mean for the future of IT security?

PAGE 8 Web Security News

Your source for short takes on Web security tales, tools, tips and trends.

PAGE 10 Sponsor Profile

Web Security Report sponsor, IronPort Systems, is developing revolutionary technologies to help make the Internet safe.

THE WEB SECURITY REPORT

A Messaging Media Publication

BUSINESS OFFICES

Messaging Media, LLC
P.O. Box 643084
Los Angeles, CA 90064
Phone: 866-808-4200
Fax: 310-836-4067

ADVERTISING/SPONSORSHIP INFORMATION

Managing Partner: Tim Matteson
publish@websecurityreport.com
866-808-4200 (ext. 361)

the Web Security report

Messaging Media, LLC
10536 Putney Road
Los Angeles, CA 90064