

Case Study

IronPort Helps a Nationwide Carrier Stop Wireless Threats

THE SITUATION

Wireless communications continues to grow and evolve in a dynamic fashion. One particular area of emerging technology is wireless messaging. With large numbers of subscribers, wireless operators continue to look for ways to increase Average Revenue Per User (ARPU) with advanced features such as Short Message Service (SMS) and Multi Media Messaging (MMS).

“ According to Ferris Research, SMS is rapidly expanding and will experience dramatic growth in the next 12-24 months. ”

WIRELESS COMMUNICATIONS AT A GLANCE

- Global wireless subscriber growth will be over 2 billion by 2009
- By 2010, the market for mobile-phone content will grow to nearly \$36 billion, up from \$7.7 billion in 2005
- SMS is rapidly expanding and will continue to experience dramatic growth
- Spam can exceed well over 50 percent of all SMS traffic

THE IRONPORT ADVANTAGE

- Secures SMTP traffic at the gateway
- Robust MTA ensures that infrastructure is never overwhelmed, even during the largest outbreaks or attacks
- Eliminates over 95 percent of spam
- Increased throughput and availability
- Dramatic reduction in Total Cost of Ownership



TECHNICAL CHALLENGES

SMS provides an effective way to communicate with wireless subscribers. Several avenues exist to initiate a message to a wireless handset, from other mobile handsets, from legitimate content providers and from Internet-based SMTP traffic. This SMTP traffic is converted to a handset readable SMS message and delivered to the handset via the SMPP protocol.

Total daily volumes of SMTP originated traffic represents a small fraction of total SMS traffic, however, SMTP traffic currently represents the primary avenue for attack from spammers.

According to Ferris Research, SMS is rapidly expanding and will experience dramatic growth in the next 12-24 months.

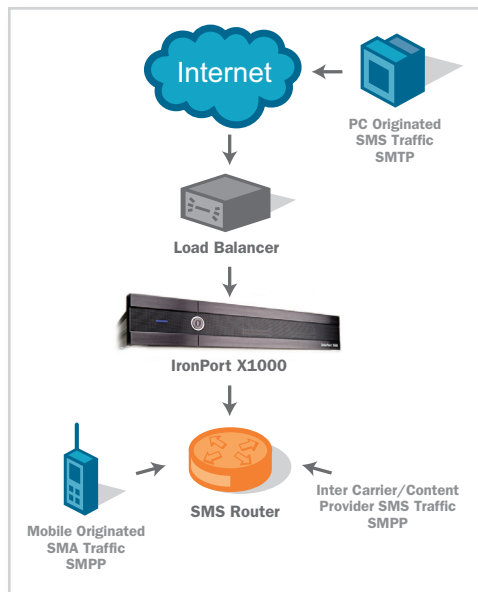
Since SMS leverages the same infrastructure as wireless voice calls, the effect of spam is substantially more severe. The risks associated with spam to wireless providers represent not only a nuisance and financial burden to subscribers, but also threaten the mobile switching infrastructure itself. A spammer could potentially overload the wireless switching systems making voice calls on cell phones impossible, thereby creating a Denial of Service (DoS) for wireless communications. The business ramifications of DoS attacks against wireless infrastructure would likely lead to dramatic churn and loss of wireless subscribers.

Before choosing IronPort® to address this problem, a major wireless provider had been fighting spam using open source anti-spam solutions – running on an open source Mail Transfer Agent (MTA). This approach had several shortcomings. It was manually intensive, consuming the time of advanced system administrators to tweak and tune the anti-spam engine. While this was able to filter some spam, it was not able to keep pace with the rapid evolution of spam techniques used by malicious senders. On some days, spam exceeded well over 50 percent of all SMS traffic. This represented costly customer care calls and decreased customer satisfaction that was extremely visible.

Legacy open source MTAs experience difficulty in scaling to meet the volume demands of SMTP originated SMS traffic. Open source MTAs also have limited management visibility, limited reporting functionality and require expensive general purpose servers

THE IRONPORT ADVANTAGE

The location of the IronPort X1000 sanitizes SMTP-based SMS traffic prior to reaching the SMS router, thereby increasing throughput and scalability of the overall architecture.



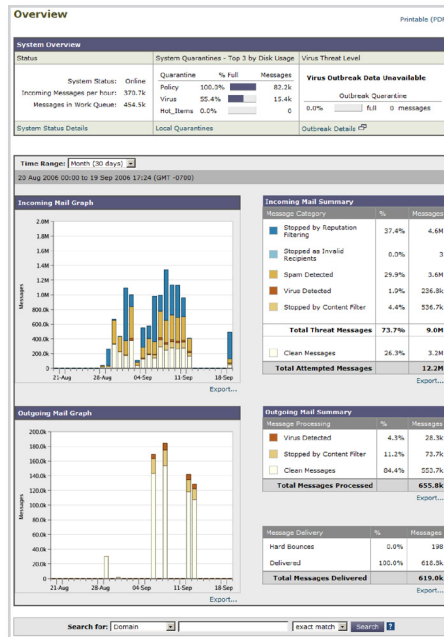
IronPort delivered a solution that eliminated in excess of 95 percent of spam and increased throughput and availability. As a testament to IronPort’s flexibility and ease-of-deployment, the provider installed IronPort X1000™ email security appliances between the load balancing equipment and email security wireless router that manages SMS routing and delivery.

Leveraging industry-leading IronPort Anti-Spam™ technology, the IronPort X1000 utilizes the patented probe network that develops spam signatures unique to SMS-based spam. The location of the IronPort X1000 sanitizes SMTP-based SMS traffic prior to reaching the SMS router, thereby increasing throughput and



THE IRONPORT ADVANTAGE
(CONTINUED)

IronPort X1000 features, such as IronPort Email Security Monitor™, enable real-time and historical visibility into email traffic and potential threats.



scalability of the overall architecture. IronPort technology at the perimeter provides the ability to intelligently classify senders into unique groups and apply policies that are commensurate with the quality of message traffic. Malicious senders can be rejected during the SMTP conversation, or even refused at the TCP level. IronPort email security appliances are unique in their ability to apply this type of policy to a network owner, IP address range or domain name. The IronPort X1000 delivers a high performance, highly accurate gateway solution – in an easy-to-use appliance.

IronPort’s unique operating system, AsyncOS™, is purpose built for high-performance MTA operations — making it ideally suited to support the volume demands of SMS traffic. The nature of IronPort AsyncOS allows graceful incorporation of protocols like SMTP to address both current and future SMS-based threats.

The GUI management console helps operators dramatically lower Total Cost of Ownership (TCO) by quickly and easily developing mail flow policies unique to the needs of their messaging subscribers.

SMS messaging volumes continue to grow. IronPort ensures that wireless providers will always be able to protect their business model by maintaining safe, reliable infrastructures.



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.

Copyright © 2000-2007 Cisco Systems, Inc. All rights reserved. IronPort, the IronPort logo and SenderBase are registered trademarks of Cisco Systems, Inc. All other trademarks are the property of Cisco Systems, Inc. or their respective owners. While every effort is made to ensure the information given is accurate, Cisco does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice. P/N 451-0107-1 10/07

