

Case Study



Leading University Turns to IronPort for an Education in Threat Protection

THE SITUATION

Unlike a private, commercial enterprise, California State University, Long Beach (a major public university) places a premium on maintaining an open email environment – so that its students, faculty and staff can enjoy as much access as possible to the knowledge and information they need to pursue their studies, research and correspondence. However, with up to 400,000 messages traversing its email network daily, Cal State Long Beach faced increasing delays and backups as it attempted to manually control suspicious email traffic and thwart aggravating spam or potentially devastating viruses. Indeed, its previous solutions were proving increasingly inadequate – at times reducing its delivery rates to a trickle. The University required a new solution to enhance its overall threat detection, improve its rate of delivery of legitimate mail and keep administrative oversight to a minimum.



Our administrative efforts have been reduced from 10 to 20 hours per week to two hours per week or less. ”

CSU LONG BEACH AT A GLANCE

Year Founded: 1949

Student Population: 35,000

Professional Population: 2,500 tenured and part-time faculty; 1,500 staff and administrators

Daily email traffic: Up to 400,000 messages

THE IRONPORT ADVANTAGE

- Extremely high throughput, speed and efficiency
- Precise reputation filtering with SenderBase
- Superior spam detection with minimal false positives
- Hassle-free administration



**TECHNICAL
CHALLENGES**

With thousands of student laptops, dormitory desktop systems and a large network of faculty and staff computers, Cal State Long Beach turned to IronPort Systems to provide the right email solution, without compromising its free flow of information. After researching its options, the University installed two IronPort C600™ email security appliances as its border gateways for inbound and outbound messaging.

Prior to its IronPort adoption, Cal State Long Beach executed its anti-spam and anti-virus initiatives directly on its email system. By moving those tasks to IronPort's front-end gateway appliance, it greatly improved the performance of its email system by freeing it up to do what it does best - namely, deliver messages to users' inboxes or route traffic to the next hop. By the University's own estimates, more than 75 percent of all spam and email-borne virus was originating from zombie PCs with a DSL or dial up connection. Cal State Long Beach's attempts to block these threats included time-intensive blacklisting, which rejected messages with "DSL" in their DNS host names, and requests that its senders with DSL connections obtain DNS names from their service providers, or redirect their outbound messages through their providers' SMTP gateways. The approach was not well received, particularly from legitimate senders whose messages were being blocked.

"We were very concerned about false positives and the perception that we were too controlling," said Matthew Black, Cal State Long Beach's Network Analyst. "We were spending a lot of time blacklisting, and making manual modifications to the spam control list. It was a real pain."

**THE IRONPORT
SOLUTION**

IronPort C-Series™ email security appliances correct these problems by drawing on the industry's best solutions for spam and virus protection. The IronPort C600 delivers exceptional security against virus outbreaks, spam attacks, phishing, false positives, DOS and misdirected bounces, as well as advanced content filtering. Additionally, the system provides hassle-free, centralized management that enables administrators to manage multiple appliances without having to integrate additional hardware. No matter the size or scope of the threat, email networks protected by IronPort will not be overwhelmed – even during the worst threat outbreaks.

Superior Virus Detection and Preventive Filtering

Powered by IronPort's SenderBase® – the world's largest email traffic monitoring network, with contributed data from over 100,000 organizations that comprise 25 percent of global email traffic – IronPort Virus Outbreak Filters™ identify virus threats in real-time at their initial outbreak and quarantine them for scanning, typically several hours before anti-virus signatures are made available. In addition to Sophos virus scanning technology, the IronPort C600 provides industry-leading spam detection from Symantec Brightmail, which delivers the most effective spam detection, without burdensome false positives.

"We no longer deliver email that is positively identified as spam," Black said.

The IronPort C600 offers further threat protection by providing LDAP recipient verification at the gateway, immediately bouncing messages not bound for valid recipients within Cal State Long Beach's active directories.



THE IRONPORT SOLUTION

Management Ease

IronPort’s efficient manageability has dramatically diminished the University’s email administrative time. “The IronPort appliance requires very little intervention,” he noted. “Our administrative efforts have been reduced from 10 to 20 hours per week to two hours per week or less. We keep a webpage open to monitor system status, but do not need to actively manage the appliance.”



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 451-0110-1 10/07

IronPort is now
 part of Cisco. 