

Case Study



IronPort Powers Web Security Solutions to Meet the Needs of a Busy Business

OVERVIEW

East China Electric Power Design Institute (ECEPDI) is a unit of China Power Engineering Consulting Group Corporation. As leader of the electric power design field in China, ECEPDI provides comprehensive engineering, consulting, project management and contracting services for fossil fuel and conventional island nuclear power plants, substations and transmission projects including long-span river crossings. This busy business requires that its employees have access the Web and internal enterprise applications at all times. With this in mind, ECEPDI recognized the need to adopt a set of Web security solutions with high performance, full integration and easy management.

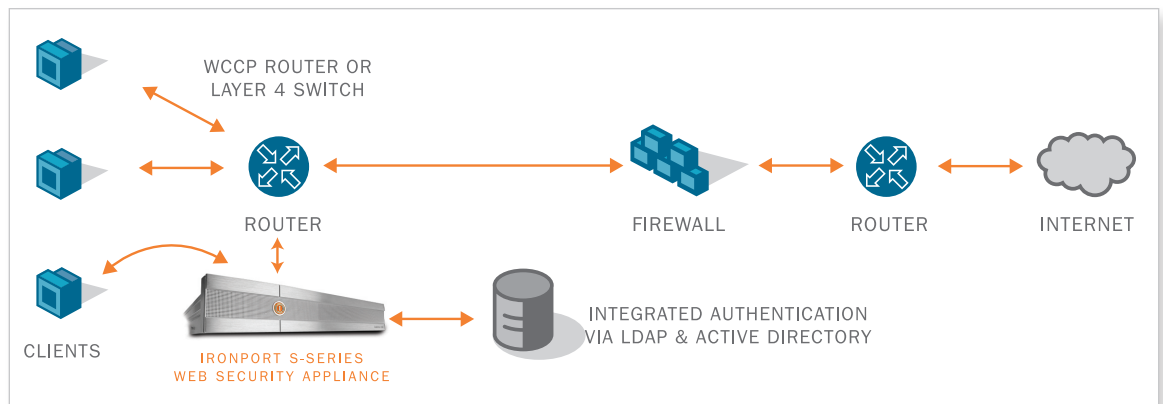
EAST CHINA ELECTRIC POWER DESIGN INSTITUTE AT A GLANCE

Headquarters: Shanghai, China
 Employees: 966
 Year Founded: 1953
 Business: Regional electric power planning, geotechnical investigation, surveying and engineering institute

THE IRONPORT ADVANTAGE

- First and only Web security gateway appliance to combine security applications such as Web reputation filtering, malware blocking and traffic monitoring on a single platform
- Highly-effective URL filtering, malware scanning and assessment engine, and powerful Layer 4 Traffic Monitor to catch threats in real time
- Powerful proxy functionality greatly saves bandwidth and improves network efficiency
- Single gateway appliance with easy deployment and management reduces Total Cost of Ownership (TCO)

The IronPort S-Series Web security appliance can be easily integrated into an existing network environment.



THE SITUATION

Like other organizations, ECEPDI has become increasingly aware of the rising threat of Web-based malware and its impact on daily business. The company tried a variety of other solutions for its Web security needs, but was unimpressed with the results. Issues including increased network latency, as well as dangerous traffic from Trojans and other malware helped the organization recognize that it needed an easy-to-use Web security system to protect its users, ensure policy compliance and unburden its network. Based on the company's satisfaction with the IronPort C-Series™ email security appliance, ECEPDI turned to IronPort® and the IronPort S-Series™ Web security appliance to provide the stability and security it sought.

TECHNICAL CHALLENGES

In order to effectively deal with malware threats and improve network efficiency, ECEPDI looked to deploy Web security at the gateway. The company wanted a solution with excellent management and real-time reporting capabilities as well as the ability to respond rapidly to malware and virus threats and effectively filter suspicious traffic. The ideal system would also demand little daily maintenance or management time and operate with virtually no performance disruption for users.

Section Chief Ji, head of the Network Administration, Information and Technology department at ECEPDI, said, "Upon installing the IronPort Web security appliance, we found that over 50 clients' IPs had been infected in our internal network. The IronPort S-Series blocks malware up to 160,000 times a week, which is far beyond our original expectations."

THE IRONPORT ADVANTAGE

Real-time scanning of Web traffic has traditionally been plagued by poor performance and high latency. Consequently, enterprises have shied away from deploying signature-based protection at the HTTP layer. At ECEPDI, the IronPort S-Series is deployed as a transparent proxy at the network edge – eliminating the need for any modifications to end-users' browsers. All HTTP requests are transmitted to the IronPort Web security appliance, where the requested websites are tested by IronPort's Web reputation filtering and malware scanning technology. Secure content is returned to end-users, while malicious content is blocked. IronPort S-Series appliances scale to meet the unique scanning needs of Web traffic, thereby ensuring that the end-user experience is maintained.



After deploying the IronPort Web security appliance, our network ran much faster and the amount of malware hitting our system dropped dramatically. We also appreciate the in-depth visibility provided by IronPort's management and reporting tools. ”

— Section Chief Ji
Network Administration Section, Information and Technology Department
East China Electric Power Design Institute



**THE IRONPORT
ADVANTAGE
(continued)**

Leveraging the IronPort SenderBase® Network (which measures roughly one-third of the world's email and Web traffic), IronPort Web Reputation Filters use over 50 different traffic- and network-related parameters to accurately evaluate a URL's trustworthiness in real time. IronPort URL Filters enforce acceptable use policy, while the IronPort Anti-Malware System™ – with simultaneous scanning by Webroot and McAfee – enables best-of-breed protection against Web-based malware.

The IronPort S-Series provides a single, easy-to-understand view of all configured access and security policies – enabling administrators to manage all Web access policies (including those for URL filtering, reputation filtering and malware filtering) from a single location. Additionally, administrators can mix and match client-based criteria (e.g. client IP address, authenticated username, etc.) and destination-based criteria (e.g. URL, URL category, proxy port, etc.) to flexibly determine when each set of policies is applied.

IronPort offers industry-leading performance through its proprietary AsyncOS™ platform, an enterprise-grade Web proxy and cache file system, as well as an intelligent engine for rapid content scanning. Consequently, the IronPort S-Series is a platform that can address the capacity requirements of even the largest of enterprises. According to ECEPDI's own statistics, since its installation, the IronPort S-Series has been responsible for approximately 80 percent of the company's bandwidth savings.

IronPort has also established technical service and monitoring centers in China to provide timely and efficient support to its numerous Chinese customers.

With the IronPort S-Series, the company has enjoyed low TCO, simplified maintenance and configuration, greater efficacy in malware protection and higher performance through engineering optimizations. Now, ECEPDI is able to focus its energy on core business, and leave Web security to the experts: 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, now part of Cisco, 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 © 2000-2008 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 451-0148-1 7/08

IronPort is now
part of Cisco.

