



Case Study

Enumclaw School District

CISCO IRONPORT SOLUTIONS PROVIDE
AN EDUCATION IN WEB SECURITY



Located in the foothills of Washington's Cascade Mountains,

the Enumclaw School District supervises the education of K-12 students living within its 444-square-mile boundary. The district, which has been serving the area for more than 120 years, features five elementary schools, two middle schools, and one high school. To ensure its students, teachers and administrators make the most of its computing technology – while receiving only appropriate Internet content – the district sought a comprehensive web filtering and security solution.

ENUMCLAW SCHOOL DISTRICT AT-A-GLANCE

Location: King County, Washington

Year founded: 1887

Focus: Providing comprehensive primary, middle and secondary educational opportunities through eight school facilities

Population served: 4,655 students from the cities of Enumclaw, Black Diamond and several unincorporated communities

Number of workstations: 1,600

THE CISCO IRONPORT ADVANTAGE

- Revolutionary gateway appliance delivering comprehensive web security on a single platform
- Seamless, integrated authentication via such standard directories as LDAP or Active Directory
- The industry's most advanced URL and web reputation filtering, combined with malware prevention
- Clear, concise management and reporting

THE SITUATION

Responsible for the education of its communities' youth, the Enumclaw School District is required by law to strictly enforce web usage policies to prevent minors who are using the Internet from accessing inappropriate content. That means scanning and filtering pornography, web proxies, social networking

sites, representations of violence or hate, blogs and forums, games, etc. To this end, the district sought an appliance-based solution that would easily integrate with its directory, while delivering seamless, comprehensive protection against web-borne threats.

TECHNICAL CHALLENGES

The Enumclaw School District's previous filtering solution provided inadequate integration with its user directories, resulting in frequent calls to its computing help desk. Technicians were often asked to respond to server/client communications breakdowns, which compromised threat identification and frequently limited users' access.

The district recognized that it needed a better solution, preferably a redundant, cost-effective, appliance-based system from a reputable manufacturer. It required efficient filtering performance and seamless directory integration. After identifying four potential providers, and conducting rigorous

evaluations, the Enumclaw School District selected a Cisco® IronPort S-Series web security appliance – specifically, the Cisco IronPort S160.

"The Cisco IronPort S160 was an effective, elegant solution, which met all of our requirements and offered additional features as well," said Chad Marlow, technology coordinator for the district. "Our environment has users who rely on our department to advise and protect regarding web security. While we still get questions as to why a site was blocked, we are basically able to leave the decision to the appliance."



“ If there’s an identified threat, it’s blocked at the gateway – rather than on the desktop after the threat is already inside the network. The ability to dynamically block webpages is very powerful. This is something we were not able to do previously. The Cisco IronPort S160 is like a firewall for web traffic. ”

— Chad Marlow, Technology Coordinator
Enumclaw School District

THE CISCO IRONPORT ADVANTAGE

With web-based malware posing a slew of rapidly-evolving and sophisticated problems for organizational security and productivity, Cisco IronPort S-Series appliances offer comprehensive protection and control at the network gateway through a single, integrated system.

For the Enumclaw School District, this translated in a variety of critical benefits including exceptional Cisco IronPort URL filtering and additional protection through Cisco IronPort Web Reputation Filters. Leveraging Cisco IronPort SenderBase® a global database of more than 20 million sites, which correspond to over 3 billion pages and Cisco Security Intelligence Operations (SIO), Cisco IronPort Web Reputation Filters deliver powerful malware defense by analyzing more than 50 separate web-traffic and network parameters to evaluate the trustworthiness of URLs and IP addresses. Cisco Security Intelligence Operations is an advanced security infrastructure that provides threat detection, correlation, and mitigation to continuously enable the highest level of security for Cisco customers. Using a combination of threat telemetry, a team of global research engineers and sophisticated security modeling, Cisco SIO enables fast and accurate protection, allowing customers to securely collaborate and embrace new technologies.

Since deploying the Cisco IronPort S160, the district reports a daily average of:

- 200 suspicious URLs blocked by Cisco IronPort Web Reputation Filters
- 45,500 URLs stopped by Cisco IronPort URL Filters
- At least 10 malware or spyware downloads blocked

In addition, the Cisco IronPort solution provides full LDAP and Active Directory integration – making it easy to define levels of access for user groups (students, teachers, administrators) and audit Internet usage. Clear reporting, monitoring and analysis on threats and acceptable use policies, as well as the possibility for enhanced security through advanced decryption technology, ensure continuous availability and access to critical network data and content.

“I like the security of knowing that if a webpage is serving malicious code, the Cisco IronPort S160 will block it,” Marlow said. “When the threat is removed, it opens the site for access again. Overall, we’ve found the Cisco IronPort solution to be both powerful and effective.”



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0809R) P/N 451-0158-1 6/09