

Why is Web Security So Important?

The number of security threats introduced by web traffic has reached epidemic proportions. Traditional gateway defenses are proving to be inadequate against a variety of web-based malware, leaving corporate networks exposed to the inherent danger posed by these threats. The speed, variety and maliciousness of web-based malware attacks highlight the importance of a robust, secure platform to protect the enterprise network perimeter from such threats.

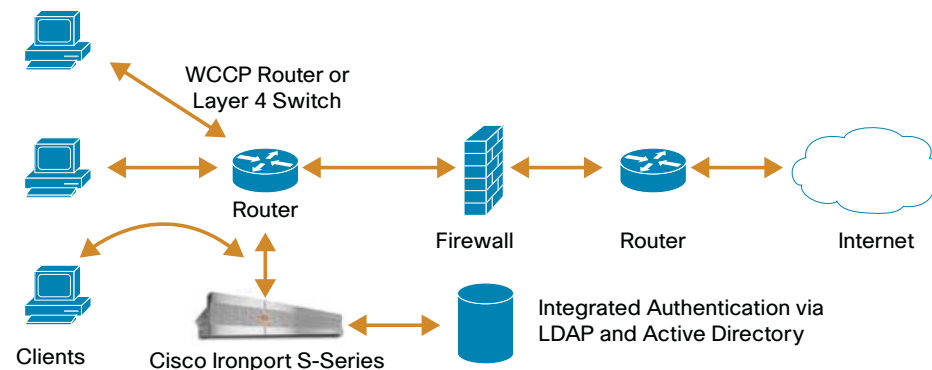
Additionally, mobile users want to easily access their corporate resources regardless of when, where and what device they use. With the lines blurring between personal and professional usage of mobile devices, seamless access and consistent security are critical to protect the end user and the company in this growing borderless network environment.

Lastly, the web has become the ubiquitous platform for application delivery in the enterprise, whether that is browser-based application platforms like Salesforce.com and Google Apps, or rich media applications like Apple iTunes or Cisco WebEx™ using web protocols as a widely available transport in and out of enterprise networks.

What Are Cisco IronPort Web Security Products?

The Cisco IronPort® S-Series is the industry's fastest web security appliance – providing a network perimeter defense for the broadest range of spyware and web-based malware. Utilizing Cisco Ironport technology, these powerful systems have a demonstrated record of unparalleled performance and reliability (Figure 1).

Figure 1: Secure and Control Web Traffic



Cisco IronPort web security appliances combine a high-performance security platform with Cisco IronPort Web Reputation technology and the breakthrough Cisco IronPort Dynamic Vectoring and Streaming (DVS) engine. This revolutionary scanning solution enables multi-vendor, signature-based spyware and malware filtering (Figure 2).

Cisco IronPort web security appliances provide:

- High-performance protection and defense against spyware and web-based threats
- Web usage controls, as well as URL, web reputation and malware filtering – all on a single appliance
- Advanced application and visibility controls
- The industry's fastest web proxy, along with integrated caching and content acceleration capabilities
- Unique outbound threat monitoring across all TCP ports
- Enforcement of acceptable use and security policies over native FTP and HTTPs-decrypted data
- Cisco AnyConnect Secure Mobility solution
- Simple data security, as well as enhanced integration with third-party DLP appliances
- Protection against malware activity and attempts to bypass Port 80
- Comprehensive management and reporting capabilities with multiple deployment modes, robust real-time and historical reports, and an easy-to-use GUI

What is Cisco Security Intelligence Operations?

Cisco Security Operations (SIO) is an advanced security infrastructure that provides threat detection, correlation and mitigation to continuously facilitate 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.

What Are Cisco IronPort's Web Security Technology Differentiators?

Cisco IronPort AsyncOS is a unique, high-performance software architecture, engineered from the ground up to address concurrency-based bottlenecks and the limitations of file-based queuing.



Cisco IronPort's Layer 4 Traffic Monitor scans all ports at wire speed, blocking spyware activity and effectively stopping malware that attempts to bypass Port 80.

Cisco IronPort's Dynamic Vectoring and Streaming (DVS) engine is designed to accelerate the signature scanning of web content and minimize latency. The DVS engine employs sophisticated object parsing and vectoring techniques, along with stream scanning and verdict caching - resulting in dramatically increased throughput.

Cisco IronPort URL Filters compare users' web traffic request against administrator-set policies for pre-defined categories. These filters easily address acceptable use policy concerns – offering the broadest reach and highest accuracy rate in controlling web content.

Cisco IronPort Web Usage Controls provide industry-leading visibility and protection from web use violations through a combination of list-based URL filtering and real-time dynamic categorization.

Cisco IronPort Web Reputation Filters provide a powerful outer layer of defense against the latest botsites and exploited legitimate sites. These filters analyze web traffic and network-related parameters to accurately evaluate a URLs trustworthiness.

The Cisco IronPort Anti-Malware System quickly and accurately detects and blocks a full range of known and emerging threats.

Cisco AnyConnect Mobile User Security solution end users connecting using Cisco AnyConnect VPN client will experience an always-on, unobtrusive remote access connection that extends web security enforcement to the mobile device.

Single Sign-On (SSO) To Software-as-a-Service (SaaS) applications use a standards-based authentication mechanism to bring this under the control of your enterprise.

Figure 2 The Cisco IronPort S-Series combines revolutionary technologies to provide multi-layered web security on a single appliance



What Sets Cisco IronPort Apart from Other Web Security Vendors?

- A Cisco IronPort Web Security Assessment can instantly provide visibility into malware traffic over Port 80.
- The Cisco IronPort web security appliance extends web security beyond the traditional proxy and URL filtering to also prevent spyware from ever entering the network.
- The Cisco IronPort Web Reputation database monitors new websites in real time and blocks access to the content these sites host.
- Cisco IronPort Web Usage Controls offer robust, dynamic categorization and reporting for end-user activity
- Cisco IronPort provides a best-of-breed solution that includes data security and DLP technologies, including integrating with external DLP solutions to enforce policies
- The Cisco IronPort S-Series is the only web security appliance to offer multiple malware signatures on an integrated platform
- Cisco SIO provides threat detection, correlation, and mitigation to help protect against adware, browser hijacks, phishing, pharming, rootkits, Trojans, worms, system monitors, and keyloggers.

What Cisco IronPort Web Security Appliance is Right for my Organization?

- **Cisco IronPort S660:** Suggested for organizations above 10,000 users
- **Cisco IronPort S360:** Recommended for organizations with 1,000 to 10,000 users
- **Cisco IronPort S160:** Designed for small businesses and branch offices with up to 1,000 users

Where Should I Go for More Information?

The best way to understand the benefits of Cisco IronPort products is to participate in the "Try Before You Buy" evaluation program. To receive a fully-functional evaluation appliance to test in your network, free for 30 days, visit: http://www.ironport.com/how_to_buy/.