

Cisco IronPort Web Security Appliances

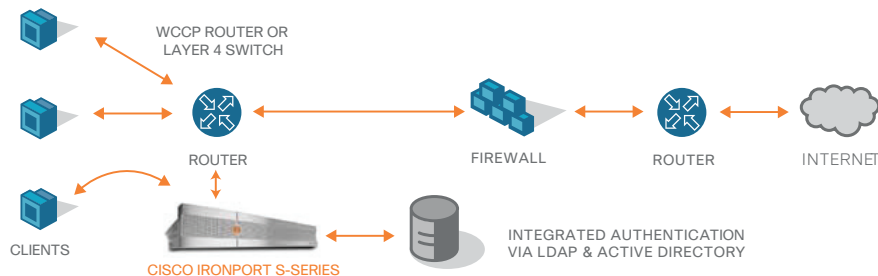
Why Is Web Security So Important?

Spyware has quickly evolved to become one of the most significant corporate security issues. According to industry estimates, approximately 75 percent of corporate PCs are infected with spyware, yet less than 10 percent of those companies have perimeter spyware defenses. Additionally, 87 percent of today's web-based threats are delivered by legitimate websites. The challenge of securing and controlling enterprise web traffic is continually growing and changing. The security risk is real, with web-based malware a rapidly growing threat that is responsible for significant corporate downtime, productivity losses and major strains on IT resources. Enterprises need control to understand when, where and how their employees are using the web. Additionally, an enterprise runs the risk of violating compliance and data privacy regulations if their networks become compromised. The legal exposure as a result of these violations comes at a significant cost. Malware infections also risk exposing an organization's business-critical data and intellectual property assets.

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 IronPort® technology, these powerful systems have a demonstrated record of unparalleled performance and reliability.

Cisco IronPort web security appliances combine a high-performance security platform with Cisco IronPort Web Reputation technology and the breakthrough Cisco IronPort



Secure and Control Web Traffic: Existing gateway defenses are proving to be inadequate against a variety of web-based malware. The Cisco IronPort S-Series provides a single platform solution to enable the industry's most powerful protection and control.

Dynamic Vectoring and Streaming (DVS) engine. This revolutionary scanning solution enables multi-vendor, signature-based spyware and malware filtering.

Cisco IronPort web security appliances provide:

- High-performance protection and defense against spyware and web-based threats
- URL, web reputation and malware filtering – all on a single appliance
- 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
- 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 the Cisco IronPort SenderBase Network?

Cisco IronPort appliances harness the power of the SenderBase® Network. This threat tracking database captures data from more than 100,000 organizations worldwide, providing a large and diverse sample of Internet traffic patterns.

- SenderBase receives over 30 billion queries daily
- Using SenderBase data increases malware catch rates by more than 20 percent over signature-based scanning alone – an unprecedented increase in efficacy
- For live threat updates and real-time access to your SenderBase Reputation Score (SBRS), visit: www.senderbase.org

What is Cisco Security Intelligence Operations?

Cisco Security Intelligence 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 communications 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 requests 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 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 URL's trustworthiness.

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

The Cisco Threat Operations Center (the TOC) provides a 24x7 view into global traffic activity – enabling Cisco to analyze anomalies, uncover new threats and track traffic trends.



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 URL Filters offer robust 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 Security Intelligence Operations (SIO) provides threat detection, correlation and mitigation to help protect against adware, browser hijackers, phishing, pharming, rootkits, Trojans, worms, system monitors and keyloggers.

Which 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: www.ironport.com/try.



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)

C45-520570-01 4/09