THE INDUSTRY'S BEST WEB SECURITY GATEWAY, PROVIDING MALWARE PROTECTION AND HIGH PERFORMANCE

IronPort S-Series Web Security Appliances

OVERVIEW

SECURE AND CONTROL WEB TRAFFIC WITH THE INDUSTRY'S LEADING WEB SECURITY APPLIANCE

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. According to industry estimates, approximately 75 percent of corporate PCs are infected with spyware, yet less than 10 percent of corporations have deployed perimeter malware defenses. 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.

Existing gateway defenses are proving to be inadequate against a variety of Web-based malware. Only the *IronPort S-Series* Web security appliance provides a single platform solution to enable the industry's most powerful protection and control.

In addition to the security risks introduced by Web-based malware and spyware, Web traffic also exposes an organization to compliance and productivity risks introduced by inappropriate usage of the Web within an organization.

The *IronPort S-Series Web Security Appliance* is the industry's first and only Web security appliance to combine traditional URL filtering, reputation filtering and malware filtering on a single platform to address these risks. By combining these innovative technologies, the *IronPort S-Series* helps organizations address the growing challenges of both securing and controlling Web traffic.

Customers enjoy low Total Cost of Ownership (TCO), as these powerful applications are integrated and managed on a single appliance. Robust management and reporting tools deliver ease of administration, flexibility and control, and complete visibility into policy-related and threat-related activities.

FEATURES

INNOVATIVE SECURITY PLATFORM DELIVERS INDUSTRY-LEADING PERFORMANCE AND ACCURACY

IronPort S-Series appliances help enterprises secure and control Web traffic by offering multiple layers of malware defense on a single, integrated appliance. These layers of defense include *IronPort Web Reputation Filters*™, multiple anti-malware scanning engines and the Layer 4 (L4) Traffic Monitor, which detects non-Port 80 malware activity. IronPort® designed and built the first solution to offer all of these features on a single appliance. With the *IronPort S-Series*, administrators enjoy low TCO, simplified maintenance and configuration, greater efficacy in malware protection and higher performance through engineering optimizations.

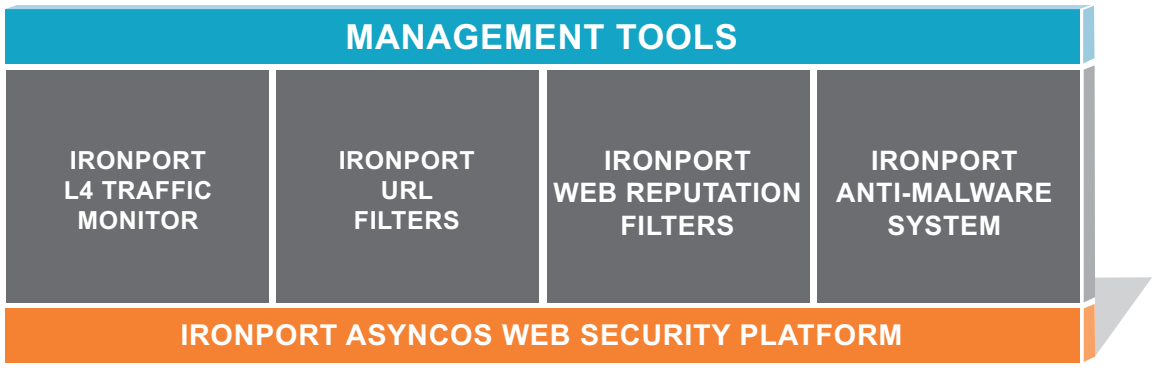
A fast Web proxy is the foundation for security and acceptable use policy (AUP) enforcement. It allows for deep content analysis, which is critical to accurately detect devious and rapidly mutating Web-based malware. Powered by *AsyncOS*™, IronPort's proprietary operating system, the Web proxy includes an enterprise-grade cache file system. This system efficiently returns cached Web content through intelligent memory, disk and kernel management – easily ensuring high performance and throughput for even the largest of networks.

An integrated Layer 4 (L4) Traffic Monitor scans all ports at wire speed, detecting and blocking spyware "phone-home" activity. By tracking all 65,535 network ports, the L4 Traffic Monitor effectively stops malware that attempts to bypass Port 80. In addition, the L4 Traffic Monitor is able to dynamically add IP addresses of known malware domains to its list of ports and IP addresses to detect and block. Using this dynamic discovery capability, the L4 Traffic Monitor can monitor the movement of malware in real time – even as the malware host tries to avoid detection by migrating from one IP address to another.

MULTI-LAYER, MULTI-VENDOR DEFENSE-IN-DEPTH

IronPort URL Filters™ offer the broadest reach and the highest accuracy rate in controlling Web content. These filters compare users' Web traffic requests against administrator-set policies for 52 pre-defined (and an unlimited number of custom) categories, easily addressing acceptable use policy concerns.

With a database that contains more than 20 million sites (corresponding to over 3 billion webpages) and global coverage across 70 languages and 200 countries, *IronPort URL Filters* offer industry-leading coverage and accuracy against Web traffic requests.



Power at the Perimeter: The *IronPort S-Series* combines revolutionary technologies to provide multi-layered Web security on a single appliance.

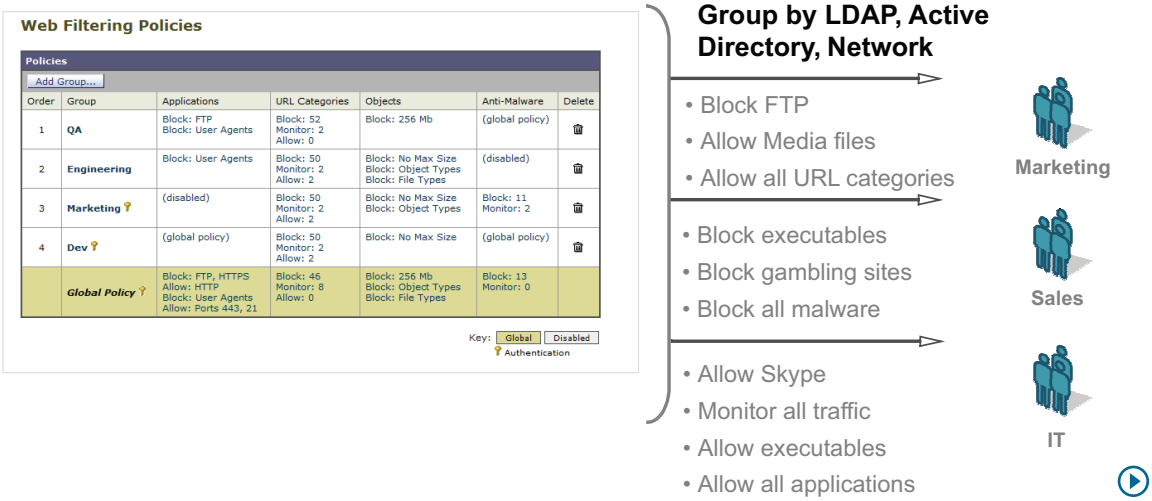
FEATURES
(CONTINUED)

The industry's first and best Web reputation filters provide a powerful outer layer of malware defense. 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. Sophisticated security modeling techniques are used to individually weigh each parameter and generate a single score (on a scale of -10 to +10) for a given URL. This score can then be used to block known bad traffic, while allowing known good traffic to proceed. In this manner, only "grey" traffic is passed on for further anti-malware scanning. *IronPort Web Reputation Filters* not only provide high levels of security and performance, but also offer effective measures against malware outbreaks.

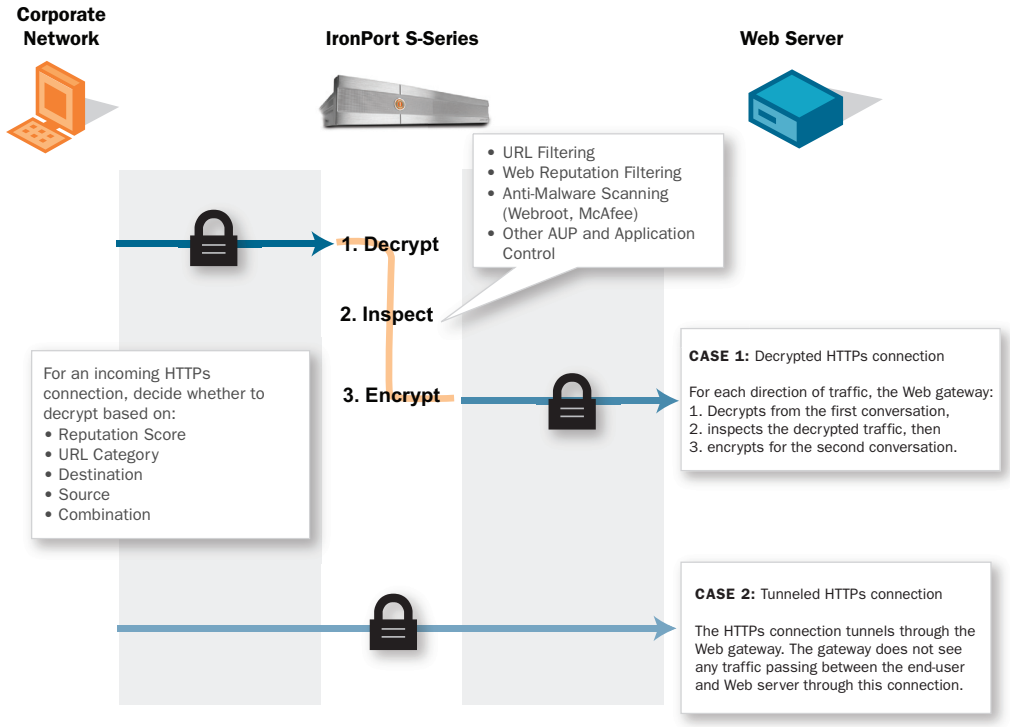
The IronPort Anti-Malware System™ enables the *IronPort S-Series* to be the first solution on the market that offers multiple anti-malware scanning engines on a single, integrated appliance. This system leverages the *IronPort Dynamic Vectoring and Streaming (DVS) engine™*, and verdict engines from Webroot and McAfee, to provide best-of-breed protection against the widest variety of Web-based threats. These threats can range from adware, browser hijackers, phishing and pharming attacks to more malicious threats such as rootkits, Trojans, worms, system monitors and key-loggers.

Scanning engines from Webroot and McAfee are fully integrated into *IronPort S-Series* appliances. The Webroot scanning engine, backed by a threat research team at Webroot, performs both request- and response-side scans. Efficacy and coverage are strengthened by Phileas (the first automated spyware detection system), which identifies existing and new threats by intelligently scanning millions of sites daily. The McAfee scanning engine is backed by Avert Labs, the world's top threat research center. The McAfee database includes both virus and malware signatures and can be configured to perform both signature-based and heuristics-based scanning.

The IronPort DVS engine was built to provide an integrated single-appliance solution with multiple anti-malware scanning engines from different vendors. It employs sophisticated object parsing and streaming techniques to provide all of IronPort's AUP and security features for Web traffic, while maximizing performance and minimizing end-user latency – even while Web content is being scanned simultaneously by Webroot and McAfee. The result is a ten-fold improvement in performance when compared to first-generation scanning solutions.



IronPort Web Security Manager makes it easy to create different sets of policies for each group of users.



Reputation-aware SSL scanning on the *IronPort S-Series* ensures privacy and security.

HTTPs Decryption enables the *IronPort S-Series* to enforce acceptable use and security policies over HTTPs-decrypted data. IronPort's Web security solution is the first to use Web reputation and URL filtering to make HTTPs decryption decisions. For example, a banking site can be bypassed for HTTPs decryption, unless its Web reputation score is low, in which case the HTTPs connection is decrypted to scan content for malware. With this ability, administrators no longer have to sacrifice security for privacy.

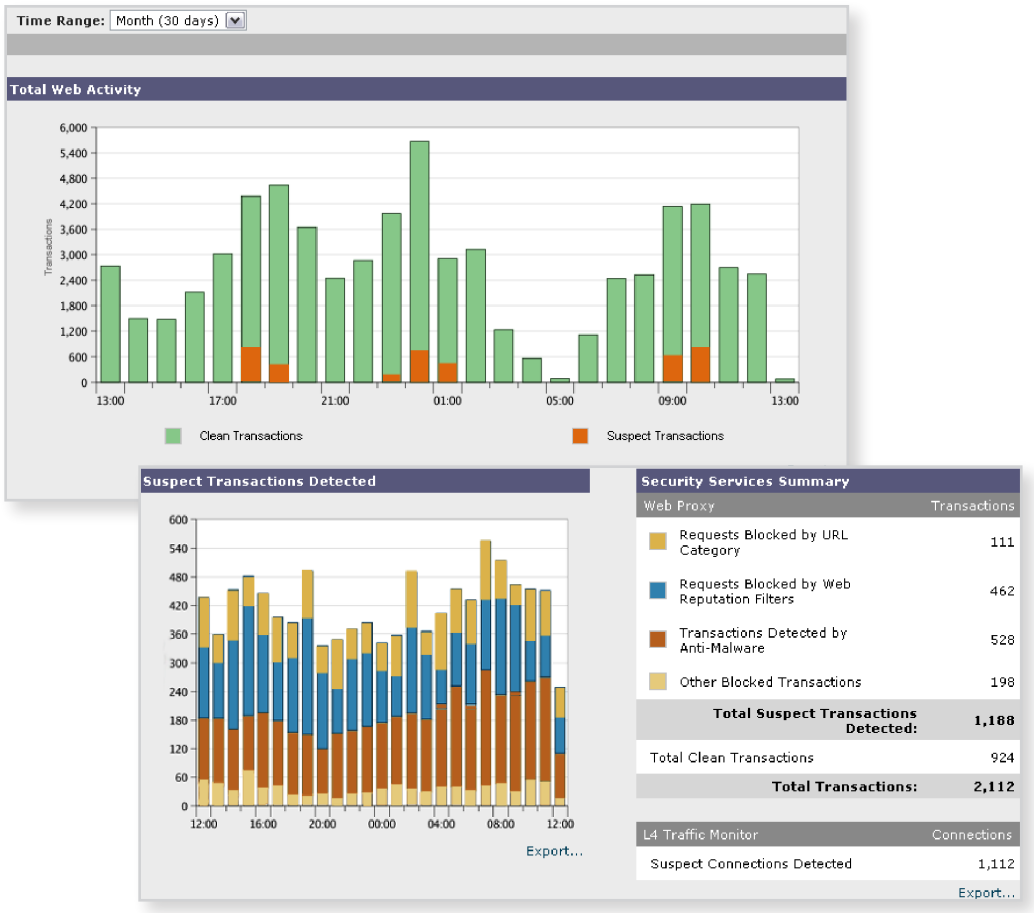
COMPREHENSIVE MANAGEMENT AND REPORTING CAPABILITIES

IronPort Web Security Manager™ provides a single, easy-to-understand view of all access and security policies configured on the appliance. Administrators 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 Web Security Monitor™ provides valuable insight into overall Web activity, as well as threat identification and prevention, within corporate networks. These on-box and off-box reports are designed to provide actionable information as well as historical trends. Enhanced reporting provides enterprises visibility into policy violations and security violations.

FEATURES
(CONTINUED)

The *IronPort S-Series'* sophisticated reporting tools yield a complete real-time and historical view of Web traffic, as well as threat activity and prevention — providing unprecedented security insight.



Multiple deployment modes enable flexibility within a corporate network. Deployment modes include deployment as an explicit forward proxy for the network or transparent deployment off an L4 switch or a WCCP router within the network. The *IronPort S-Series* appliance can be configured as a standalone proxy or to co-exist with other proxies.

An SNMP Enterprise MIB facilitates hands-off monitoring and alerting for key system metrics including hardware, performance and availability. A comprehensive enterprise class alert engine ensures oversight for all system parameters – including hardware, security, performance and availability.

Integrated authentication via standard directories (such as LDAP or Active Directory) and the ability to implement multiple authentication schemes (such as NTLM or Basic) lets enterprises deploy the *IronPort S-Series* seamlessly, while taking advantage of pre-existing authentication and access control policies within their networks. Features such as multi-realm authentication (which enables authentication against multiple authentication domains) provide flexible failover scenarios and multi-organization deployments.

Extensive logging allows enterprises to keep track of all Web traffic, benign and malware-related. Standard log formats include Apache, Squid or Squid-detailed—along with the ability to specify custom log formats, consistent with enterprise logging policies. Administrators can enable or disable log subscriptions or set log subscriptions, or set log rollover and size limits, based on log types.

BENEFITS

Single Appliance Security and Control *IronPort S-Series* offers a single appliance solution to secure and control the three greatest Web traffic risks facing enterprise networks: security risks, resource risks and compliance risks.

Mitigate Malware Risks and Costs With malware infecting up to 75 percent of corporate desktops, there is considerable overhead around managing infected desktops, ensuring minimal downtime to the end-user and minimizing the risk of information leakage.

By stopping these threats at the network perimeter with the *IronPort S-Series*, enterprises can significantly reduce the administrative costs, prevent attacker "phone-home" activity on networks, reduce support calls, enhance worker productivity and also eliminate the business exposure that accompanies these threats.

Complete, Accurate Protection IronPort designed the *IronPort S-Series* appliances from the ground up to address the broadest range of Web-based malware threats. A multi-layered defense that includes *IronPort URL Filters, IronPort Web Reputation Filters*, and multiple anti-malware scanning engines using *IronPort's DVS* technology, ensures industry-leading accuracy.

The *IronPort S-Series'* multi-layered protection is based on a deep content application-layer inspection, as well as network-layer pattern detection, checking both inbound and outbound activities. These innovations make the *IronPort S-Series* the industry's most secure Web gateway.

Enforce Acceptable Use Policies (AUP) By implementing acceptable use Web policies, enterprises can not only conserve resources for work-related Web usage, but also inform end-users to help shape Web access behavior over time. Enterprises can increase the amount of time that employees spend on business-oriented activities, reducing misuse of enterprise networks and bandwidth.

Comprehensive Visibility The *IronPort S-Series* appliances deliver real-time and historical security information, enabling administrators to quickly understand Web traffic activity. Real-time reports let administrators identify and track issues such as policy violations and security violations as they occur. Historical reports allow administrators to identify trends and report on efficacy and ROI.

Enterprise-Scale Performance Real-time scanning of Web traffic has been traditionally plagued by poor performance and high latency. Consequently, enterprises have shied away from deploying signature-based protection at the HTTP layer. *IronPort S-Series* appliances scale to meet the unique scanning needs of Web traffic, thereby ensuring that the end-user experience is maintained. 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.

BENEFITS (CONTINUED)

Low Total Cost of Ownership Legacy ICAP-based solutions typically require multiple appliances or servers to protect against security, resource and compliance risks. Unlike other solutions, the *IronPort S-Series* provides a single platform that contains a complete, in-depth defense — along with all the necessary management tools — significantly reducing initial and ongoing TCO.

Reduced Administrative Overhead Designed to minimize administrative overhead, the *IronPort S-Series* appliances offer easy setup and management with an intuitive graphical user interface, support for automated updates, and comprehensive monitoring and alerting. The solution is also easy to deploy and configure to match corporate-specific policies.

PRODUCT LINE

SIZING UP YOUR WEB SECURITY SOLUTION

IronPort Systems provides industry-leading Web security appliances for organizations of all sizes.

IronPort S650	Designed to meet the needs of the most demanding networks in the world. Suggested for organizations above 5000 users.
IronPort S350	Suggested for organizations up to 5000 users.

SPECS (MODEL DEPENDENT)

CHASSIS / PROCESSOR

Form Factor	19” Rack-Mountable, 2U rack height
Dimensions	3.5” (h) x 19” (w) x 29” (d)
CPU	2x Dual Core Intel Xeon 5140, 4 MB Cache
Memory	4 GB
Power Supplies	Hot-plug redundant, 750 watts, 100/240 volts

STORAGE

RAID	RAID 10 configuration, battery-backed 256MB cache
Drives	Six hot-swappable, 146 GB SAS Drives, 876 GB Total

CONNECTIVITY

Ethernet	6x Gigabit NICs, RJ-45
Serial	1x RS-232 (DB-9) Serial Port

INTERFACES/CONFIGURATION

Web Interface	Accessible by HTTP or HTTPS
Command Line Interface	Accessible via SSH or Telnet; Configuration Wizard or command-based
File Transfer	SCP, FTP or SYSLOG
Configuration Files	XML-based configuration files

SUMMARY

THE ULTIMATE WEB SECURITY SYSTEM

The challenges of securing and controlling enterprise Web traffic is continually growing and changing. The security risk is real, with Web-based malware posing a rapidly growing threat that is responsible for significant corporate downtime, productivity loss and resource strain on IT infrastructure. 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.

The best place to control and protect against these risks posed by Web traffic is right at the gateway. The *IronPort S-Series* provides multiple layers of defense against these risks, both horizontally (at the application layer) and vertically (up the protocol stack). *IronPort URL Filters* enforce acceptable use policy, while *IronPort Web Reputation Filters* and the *IronPort Anti-Malware System* – with simultaneous scanning by Webroot and McAfee for greater efficacy – provide protection against Web-based malware. HTTPs decryption enables the *IronPort S-Series* to apply these same access and security policies to HTTPs-encrypted traffic as well. Finally, the L4 Traffic Monitor detects and blocks "phone-home" malware activity that attempts to circumvent Port 80 security features. With threats becoming more complex and sophisticated, *IronPort S-Series* offer the industry's most comprehensive Web security solution, while also ensuring enterprise-class performance.

CONTACT US

HOW TO GET STARTED WITH IRONPORT

IronPort sales representatives, channel partners and sales engineers are ready to help evaluate how IronPort products can make your corporate network infrastructure secure, reliable and easier to manage. If you believe that your organization could benefit from IronPort's industry-leading products, please call 650-989-6530 or visit us on the Web at www.ironport.com/leader

IRONPORT S-SERIES
10/07
DOC RELEASE

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.

P/N 435-0120-5 10/07

IronPort is now part of Cisco.