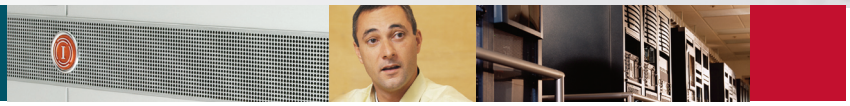
Cisco IronPort S-Series Web Security Appliances

THE INDUSTRY'S BEST SECURE WEB GATEWAY FOR ACCEPTABLE USE POLICY ENFORCEMENT, MALWARE PROTECTION AND DATA SECURITY



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. Additionally, 87 percent of today's web-based threats are delivered through legitimate websites. 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.

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 Cisco® IronPort S-Series web security appliance is the industry's first and only secure web gateway to combine traditional URL filtering, reputation filtering, malware filtering and data security on a single platform to address these risks. By combining innovative technologies, the Cisco 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, as well as complete visibility into policy- and threat-related activities.

Secure Web Gateway: *Secure, control, prevent. A comprehensive security solution to the business challenges of the web.*

THE CISCO IRONPORT DIFFERENCE

Cisco IronPort email and web security products are high-performance, easy-to-use and technically-innovative solutions, designed to secure organizations of all sizes. Purpose built for security and deployed at the gateway to protect the world's most important networks, these products enable a powerful perimeter defense.

Leveraging the Cisco Security Intelligence Operations center and global threat correlation makes the Cisco IronPort line of appliances smarter and faster. This advanced technology enables organizations to improve their security and transparently protect users from the latest Internet threats.

FEATURES

Innovative Security Platform Delivers Performance and Accuracy

Cisco IronPort web security 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 Cisco IronPort Web Reputation Filters, multiple anti-malware scanning engines and the Layer 4 (L4) Traffic Monitor, which detects non-Port 80 malware activity. The Cisco IronPort S-Series is also capable of intelligent HTTPS decryption, so that all associated security and access policies can be applied to encrypted traffic.

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 the proprietary Cisco IronPort AsyncOS 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.

Industry-Leading Acceptable Use Policy Enforcement

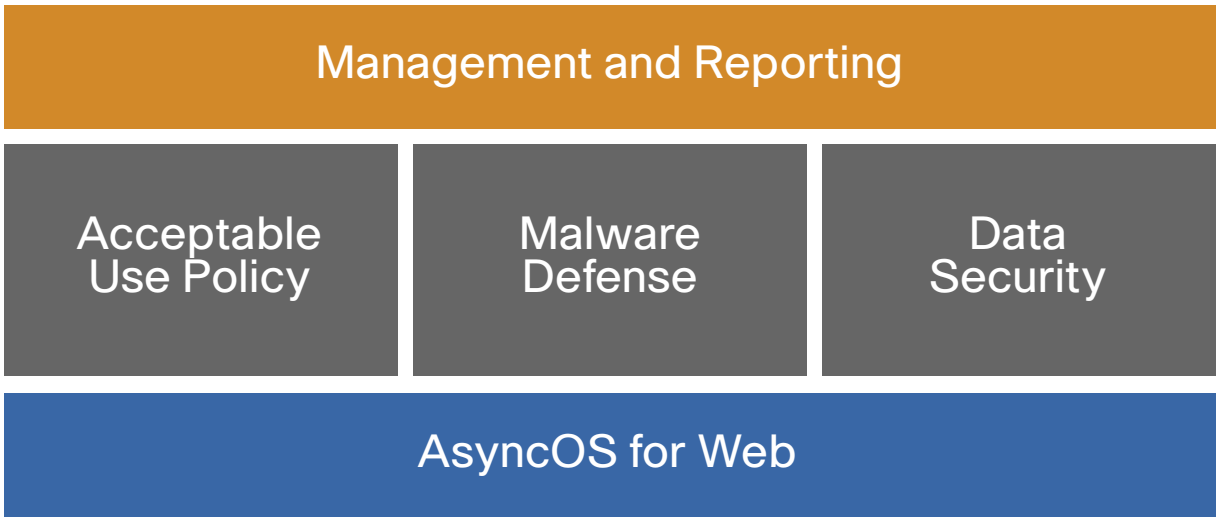
Cisco IronPort URL Filters offer the broadest reach and the highest accuracy rate in controlling web content. Cisco's database contains over 20 million sites (corresponding to over 3 billion pages), with global coverage across 70 languages and 200 countries.

Cisco IronPort URL Filters provide industry-leading coverage and accuracy against web traffic requests. An administrator can easily configure access policies based on 52 pre-defined categories and an unlimited number of custom categories. Time-based policies are also supported for truly flexible acceptable use policy management.

AUP, application and protocol control are facilitated at a granular level, regardless of the protocol or application flowing through the network perimeter. The Layer 4 Traffic Monitor looks for "phone-home" malware activity, while intelligent HTTPS decryption inspects encrypted data for security or AUP violations. The Cisco IronPort S-Series brings all of these capabilities together to provide a single touch point for administrators who want to control the data entering and leaving their networks.

Multi-Layer, Multi-Vendor Malware Defense-in-Depth

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.



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

FEATURES (CONTINUED)

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

Cisco Security Intelligence Operations is a sophisticated security ecosystem consisting of three components:

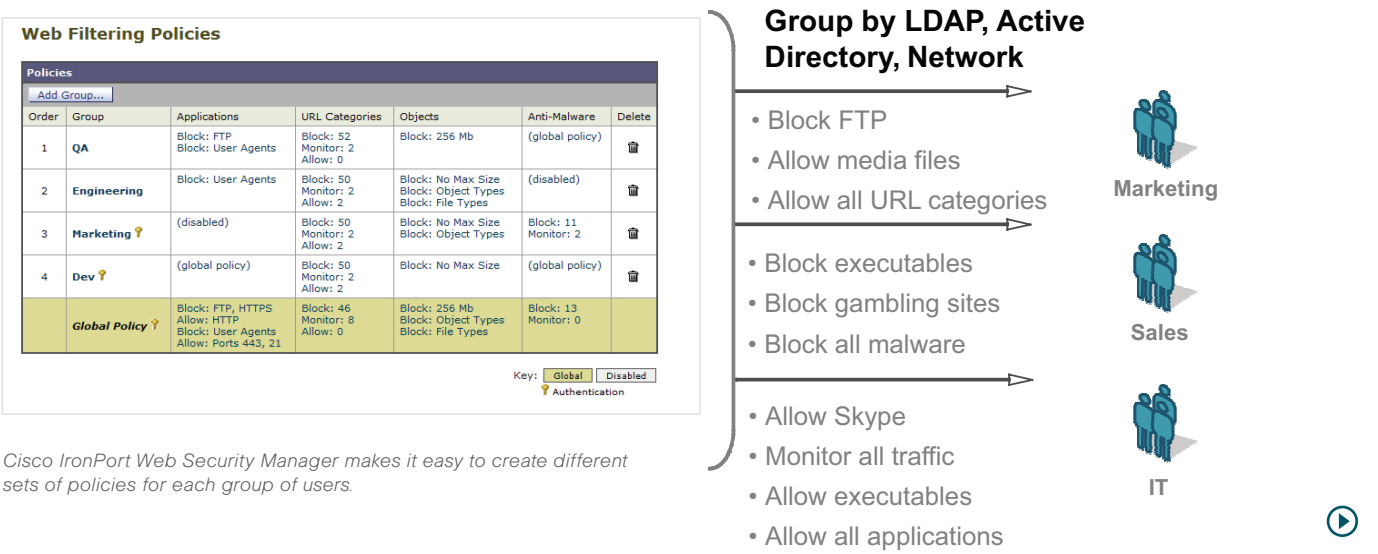
- Cisco SensorBase: The world's largest threat monitoring network that captures global threat telemetry data from a massive footprint of Cisco devices.
- Threat Operations Center: A global team of security analysts and automated systems extract actionable intelligence.
- Dynamic Updates: Real-time updates automatically delivered to security devices, along with best practice recommendations and other content, help customers track threats, analyze intelligence and ultimately improve their organization's overall security posture.

The industry's first and best web reputation filters provide a powerful outer layer of malware defense. Leveraging Cisco Security Intelligence Operations (SIO), Cisco IronPort Web Reputation Filters analyze over 50 different web traffic- and network-related parameters to accurately evaluate a URL or IP addresses' trustworthiness. Cisco IronPort Web Reputation Filters examine every request made by the browser (from the initial HTML request to all subsequent data requests) – including live data, which may be fed from different domains. This gives these filters a unique advantage over vendors that reduce web reputation to a simple URL filtering category.

Cisco IronPort Web Reputation Filters are the industry's only reputation system to include botsite protection, URL outbreak detection and exploit filtering – protecting users from exploits delivered through cross-site scripting (XSS), cross-site request forgery, SQL injections or invisible iFrames. The power behind this revolutionary reputation technology comes from the system's pattern-base assessment techniques and per-object scanning capabilities.

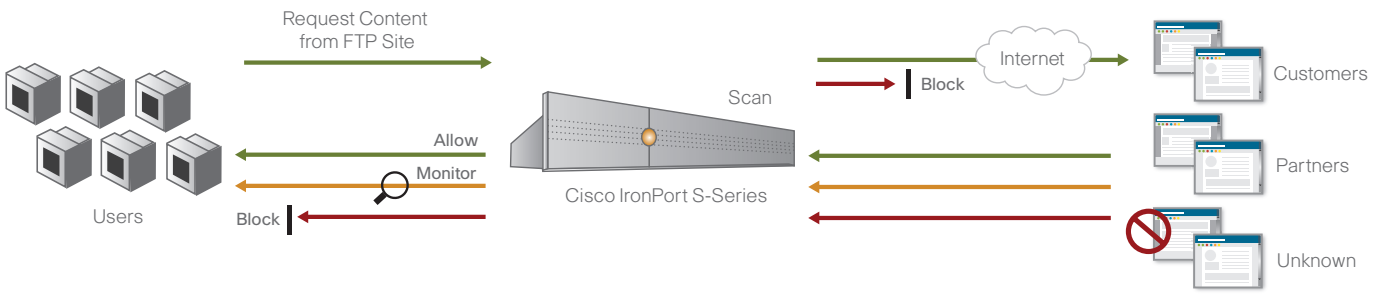
The Cisco IronPort Anti-Malware System gives the Cisco IronPort S-Series the distinction of being the first solution on the market to offer multiple anti-malware scanning engines on a single, integrated appliance. Moreover, an administrator can run these scanning engines simultaneously to enable greater protection against malware threats, with little-to-no performance degradation. This system leverages the Cisco 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 keyloggers.

Scanning engines from Webroot and McAfee are fully integrated into the Cisco IronPort web security 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.



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

FEATURES (CONTINUED)



Native FTP protection enables complete visibility into FTP usage – enforcing acceptable use and data security policies, and preventing malware infections.

The Cisco 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 enforce acceptable use policies and security features for web traffic. It simultaneously leverages hardware optimizations (such as multi-core scanning) to distribute these parallel operations and fully utilize the system's resources. The result is a ten-fold improvement in performance when compared to first-generation scanning solutions.

HTTPS decryption enables the Cisco IronPort S-Series to enforce acceptable use and security policies over HTTPS-decrypted data. This is the first solution 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, or blocked outright. With this ability, administrators no longer have to sacrifice security for privacy.

Powerful Data Security Enforcement

Data security and data loss prevention empower organizations to take quick, easy steps to enforce common sense data security policies. For example, preventing engineers from sending design files by webmail, blocking uploads by finance staff of Excel spreadsheets over 100KB, or preventing posts of content to blogs or social networking sites. These simple data security policies can be created for outbound traffic on HTTP, HTTPS and FTP.

For enterprises that have already invested in special-purpose data loss prevention (DLP) systems, the Cisco IronPort S-Series offers an option to interoperate with DLP vendors via ICAP. By directing all outbound HTTP, HTTPS and FTP traffic to the third-party DLP appliance, organizations can allow or block based on the third-party rules and policies. This also enables deep content inspection for regulatory compliance and intellectual property (IP) protection, incident severity definition, case management and performance optimization.

Native FTP protection allows Cisco IronPort web security appliances to provide complete visibility into FTP usage, enforcing acceptable use and data security policies, and preventing malware infections. Acting as an FTP proxy, the Cisco IronPort S-Series enables organizations to exercise granular control, including: allow/block FTP connections, restrict users/groups, control uploads/downloads, and restrict sent/received files to certain types or sizes.

Additionally, Cisco IronPort web security appliances can score FTP servers with Web Reputation Filters (Cisco's industry-leading reputation service) and scan downloaded content for malware and spyware payloads with the IronPort Dynamic Vectoring and Streaming (DVS) engine. Cisco's FTP protection enforces simple, common sense data security policies based on file metadata, user, URL category and reputation. Alternately, FTP traffic can be passed to an external DLP solution for additional, more granular, scanning.

The Cisco IronPort S-Series now has comprehensive coverage for the three most common protocols carrying business information across the boundary and over the Internet – HTTP, HTTPS and FTP.

FEATURES (CONTINUED)

Comprehensive Management and Reporting Capabilities

Cisco 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 URL filtering, time-based policies, 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.

Cisco IronPort Web Security Monitor offers 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 and security violations.

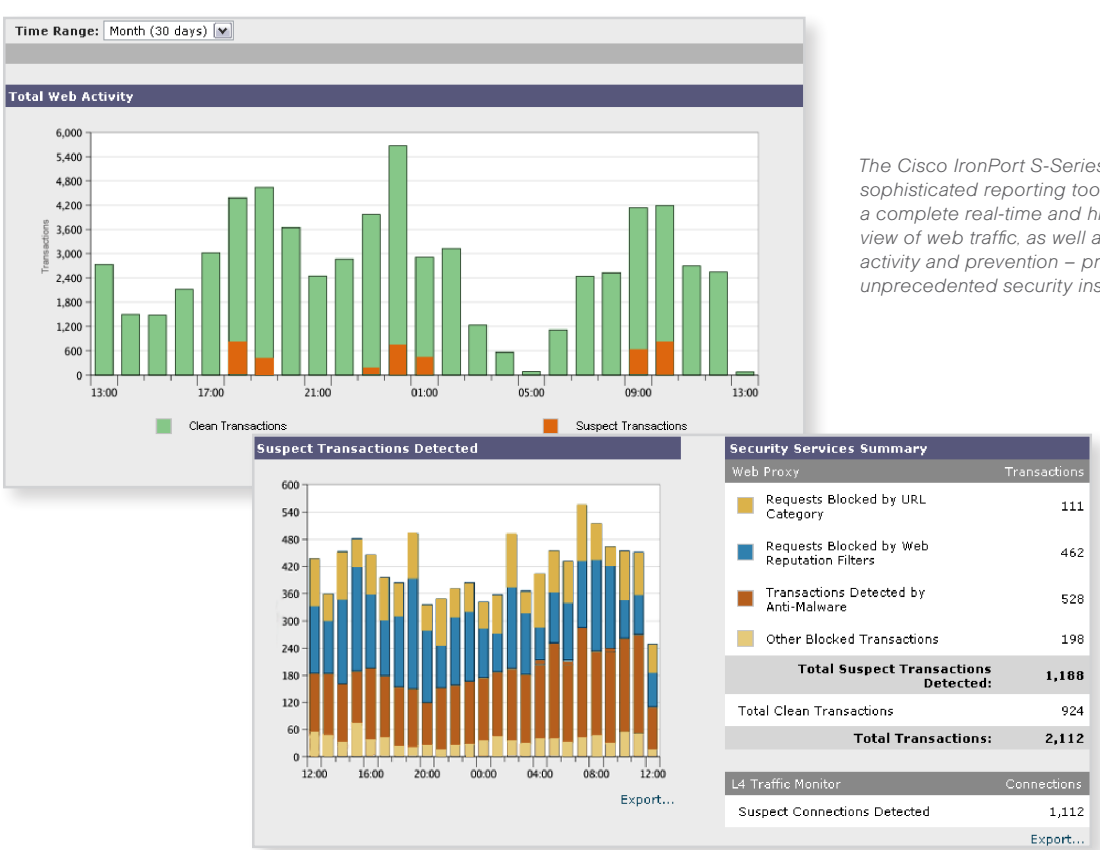
Multiple deployment modes enable flexibility within a corporate network. Modes include deployment as an explicit forward proxy for the network or transparent deployment off an L4 switch or a WCCP router within the network. Each Cisco IronPort web security appliance can be configured as a standalone proxy or to co-exist with other proxies (such as in a proxy hierarchy for conditional routing, failover and load balancing).

Enterprise-grade SNMP facilitates hands-off monitoring and alerting for key system metrics including hardware, performance and availability. Support for SNMPv1, 2, and 3, along with a comprehensive enterprise-class alert engine, ensure oversight for all system parameters – including hardware, security, performance and availability.

Integrated authentication via standard directories (such as LDAP or ActiveDirectory) and the ability to implement multiple authentication schemes (such as NTLM or Basic) lets enterprises deploy the Cisco 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.

Cisco IronPort web security appliances also enable warn/continue pages to allow the organization to educate users on corporate acceptable use and security policies, restricted guest access for visitors, and re-authentication for on-the-fly privilege override. Given the diversity of ways in which group information is stored in user directories, the Cisco IronPort S-Series supports obtaining group information from a group object, as well as from an attribute in the user's profile.

These features offer increased flexibility and richness in policy and authentication to meet the requirements of sophisticated enterprises.



The Cisco 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.

FEATURES (CONTINUED)

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

In addition to the Apache and Squid log file formats, the Cisco IronPort S-Series supports the W3C-standard Extended Log File Format (ELFF). This allows administrators to use many third-party log analyzer tools, and also enables the generation of customized logs for various audiences. For example, separate logs for IT, HR, and top management – each with a customized set of logging fields.

BENEFITS

Single Appliance Security and Control The Cisco 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 approximately 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 Cisco IronPort web security appliances, 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 Cisco IronPort S-Series appliances are designed from the ground up to address the broadest range of web-based malware threats, including those from the use of FTP and dynamic Web 2.0 sites. A multi-layered defense that includes Cisco Security Intelligence Operations, Cisco IronPort URL Filters, Cisco IronPort Web Reputation Filters and Cisco IronPort DVS technology (with multiple anti-malware scanning engines running simultaneously), ensures industry-leading accuracy.

This 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 Cisco 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.

Web Application Control

The Cisco IronPort S-Series layers additional capabilities on top of URL filtering to provide richer controls for web application usage.

BENEFITS (CONTINUED)

Simplified Data Security The data loss problem extends well beyond malware. Employees can easily use webmail to send a message including proprietary information, post confidential data on social networks and blogs, or transfer financial documents over FTP to a server outside the corporate network. Making sure that sensitive data does not leave the corporate boundary – while allowing users to leverage the full power of the Internet – is an important and challenging issue to solve.

Cisco IronPort web security appliances enable organizations to take quick, easy steps to enforce common sense data security policies for outbound traffic on HTTP, HTTPS and FTP.

Reporting Visibility The Cisco IronPort S-Series appliances deliver real-time and historical security information, allowing 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 Cisco IronPort web security appliances scale to meet the unique scanning needs of web traffic, thereby ensuring that the end-user experience is maintained. Cisco offers industry-leading performance through its proprietary IronPort AsyncOS platform, an enterprise-grade web proxy and cache file system as well as an intelligent, multi-core engine for rapid content scanning. Consequently, the Cisco IronPort S-Series is a platform that can address the capacity requirements of even the largest of enterprises.

Low Total Cost of Ownership Legacy solutions typically require multiple appliances or servers to protect against security, resource and compliance risks. Unlike other solutions, the Cisco 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, Cisco IronPort web security 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

The Cisco IronPort web security product line address issues faced by organizations ranging from small businesses to the Global 2000.

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 organizations with up to 1,000 users.

SPECS (MODEL DEPENDENT)

	Cisco IronPort S660	Cisco IronPort S360	Cisco IronPort S160
Chassis			
Form Factor	2RU	2RU	1RU
Dimensions	3.5" (h) x 17.5" (w) x 29.5" (d)	3.5" (h) x 17.5" (w) x 29.5" (d)	1.75" (h) x 17.5" (w) x 21.5" (d)
Power Supply	750 watts, 100/240 volts	750 watts, 100/240 volts	750 watts, 100/240 volts
Redundant Power Supply	Yes	Yes	No
Processor, Memory and Disks			
CPUs	2x4 (2 Quad Cores) XEONs	1x4 (1 Quad Core) XEONs	1x2 (1 Dual Core) Pentium
Memory	8 GB	4 GB	4 GB
Disk Space	1.8 TB	1.2 TB	500 GB
Hot Swappable Hard Drives	Yes	Yes	No
RAID	RAID 10, battery-backed 256MB cache	RAID 10, battery-backed 256MB cache	RAID 1, battery-backed 256MB cache
Interfaces			
Ethernet	6xGigabit NICs, RJ-45	6xGigabit NICs, RJ-45	6xGigabit NICs, RJ-45
Serial	1xRS-232 (DB-9) Serial	1xRS-232 (DB-9) Serial	1xRS-232 (DB-9) Serial
Fiber	Optional	No	No
Configuration, Logging and Monitoring			
Web Interface	GUI-based (HTTP or HTTPS)	GUI-based (HTTP or HTTPS)	GUI-based (HTTP or HTTPS)
Command Line Interface	SSH or Telnet (Configuration Wizard or command-based)	SSH or Telnet (Configuration Wizard or command-based)	SSH or Telnet (Configuration Wizard or command-based)
Logging	Squid, Apache, syslog	Squid, Apache, syslog	Squid, Apache, syslog
Centralized Reporting	Supported	Supported	Supported
File Transfer	SCP, FTP	SCP, FTP	SCP, FTP
Configuration Files	XML-based	XML-based	XML-based
Centralized Configuration	Supported	Supported	Supported
Monitoring	SNMPv1-3, email alerts	SNMPv1-3, email alerts	SNMPv1-3, email alerts

SUMMARY

The Ultimate Web Security System

The challenge 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.

SUMMARY (CONTINUED)

The best place to control and protect against these risks posed by web traffic is right at the gateway. The Cisco IronPort S-Series web security appliance provides multiple layers of defense against these risks, both horizontally (at the application layer) and vertically (up the protocol stack). Cisco IronPort URL Filters enforce acceptable use policy, while Cisco Security Intelligence Operations, Cisco IronPort Web Reputation Filters and the Cisco IronPort Anti-Malware System – with simultaneous scanning by Webroot and McAfee for greater efficacy – provide protection against web-based malware. The Cisco IronPort S-Series also has comprehensive coverage for the three most common protocols carrying business information across the boundary and over the Internet – HTTP, HTTPS and FTP. 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, Cisco IronPort S-Series appliances offer the industry's most comprehensive web security solution, while also ensuring enterprise-class performance.

CONTACT US

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

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 435-0120-7 4/09