Cisco IronPort S160
Web Security Appliance

Yesterday's defenses are no longer effective in the fight against today's sophisticated web threats. The shift from viruses and worms to exploited legitimate sites, more unique varieties of malware and the growth of social networking sites are forcing businesses to put up new defenses. These types of attacks do not discriminate, and even the smallest IT security organization needs to defend its users.

According to industry estimates, approximately 75 percent of all business PCs are infected with spyware, yet less than 10 percent of businesses have deployed perimeter malware defenses. Additionally, 87 percent of all web-based threats today are delivered by legitimate sites. The speed, variety and maliciousness of web-based malware attacks highlight the importance of a robust, secure platform to protect the network perimeter from such threats.

In addition to the security risks introduced by malware and spyware, web traffic also exposes an organization to compliance and productivity risks introduced by inappropriate Internet usage. The Cisco® IronPort S160 web security appliance combines acceptable use policy controls, reputation filtering, malware filtering and data security on a single platform to address these risks.

A single, highly-secure Cisco IronPort S160 can typically replace three comparable appliances from competing vendors. This consolidation reduces the operational costs (power, rack space, etc.) and supports green data center initiatives – all while increasing ROI and efficiency.

Extending security to the branch office should be an integral part of any web security strategy. Branch networks have become a source of many potential security vulnerabilities, yet limited protection resources have existed at the branch level. Understanding branch office risks and security requirements is critical to building an overall web security strategy. With the Cisco IronPort S160, Cisco extends the full capabilities of its powerful, secure web gateway (including all of its innovative security technologies) to remote and branch offices.

Cisco provides a manageable, and intelligent web security architecture for protecting branch offices, enabling you to do business effectively and safely.

Increasing enterprise web traffic creates new security challenges for enterprise IT. HTTP now dominates at the enterprise edge, carrying numerous applications and types of information.

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

The Cisco IronPort S160 helps businesses and remote offices 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 S160 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 networks of all sizes.

### Industry-Leading Acceptable Use Policy Enforcement

Cisco IronPort Web Usage Controls, available on all Cisco IronPort S160 web security appliances, provide industry-leading visibility and protection from web use

violations through a combination of list-based URL filtering and real-time dynamic categorization. This unique solution is powered by Cisco Security Intelligence Operations (SIO), which uses global Internet traffic visibility and analysis to target categorization efforts and provide timely updates, maximizing URL list-based efficacy.

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 S160 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.

Management and Reporting		
Acceptable Use Policy	Malware Defense	Data Security
AsyncOS for Web		
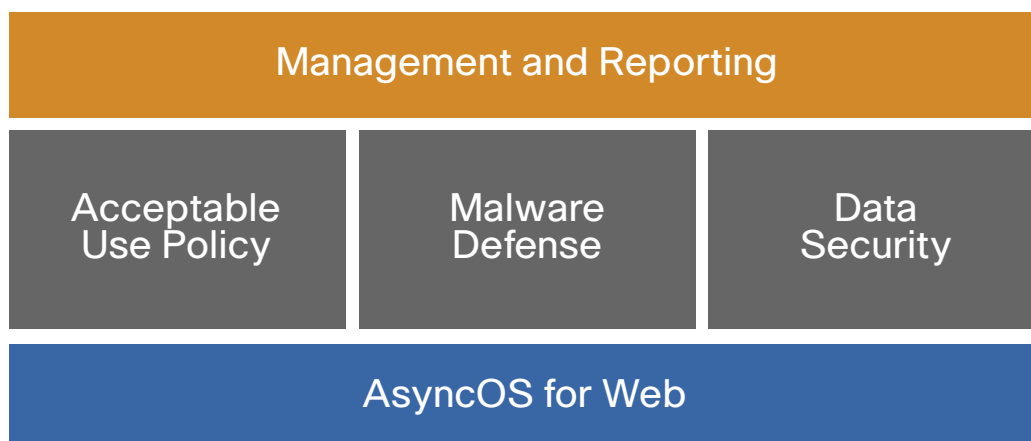
The Cisco IronPort S160 combines revolutionary technologies to provide multi-layered web security on a single appliance.

FEATURES (CONTINUED)

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.

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 assessmen techniques and per-object scanning capabilities.

The Cisco IronPort Anti-Malware System gives the Cisco IronPort S160 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 S160. The Webroot scanning engine, backed by a threat research team at Webroot, performs both request- and response-side scans. The McAfee database includes both virus and malware signatures and can be configured to perform both signature-based and heuristics-based scanning.
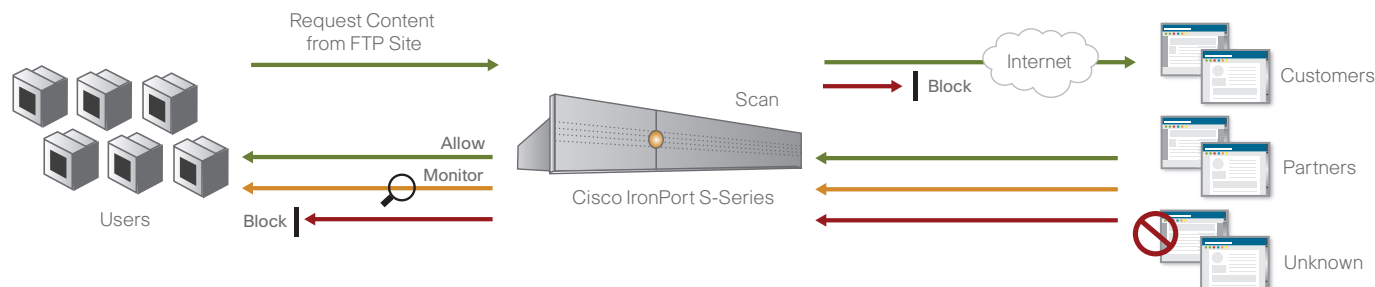
Native FTP protection enables complete visibility into FTP usage – enforcing acceptable use and data security policies, and preventing malware infections.

FEATURES (CONTINUED)
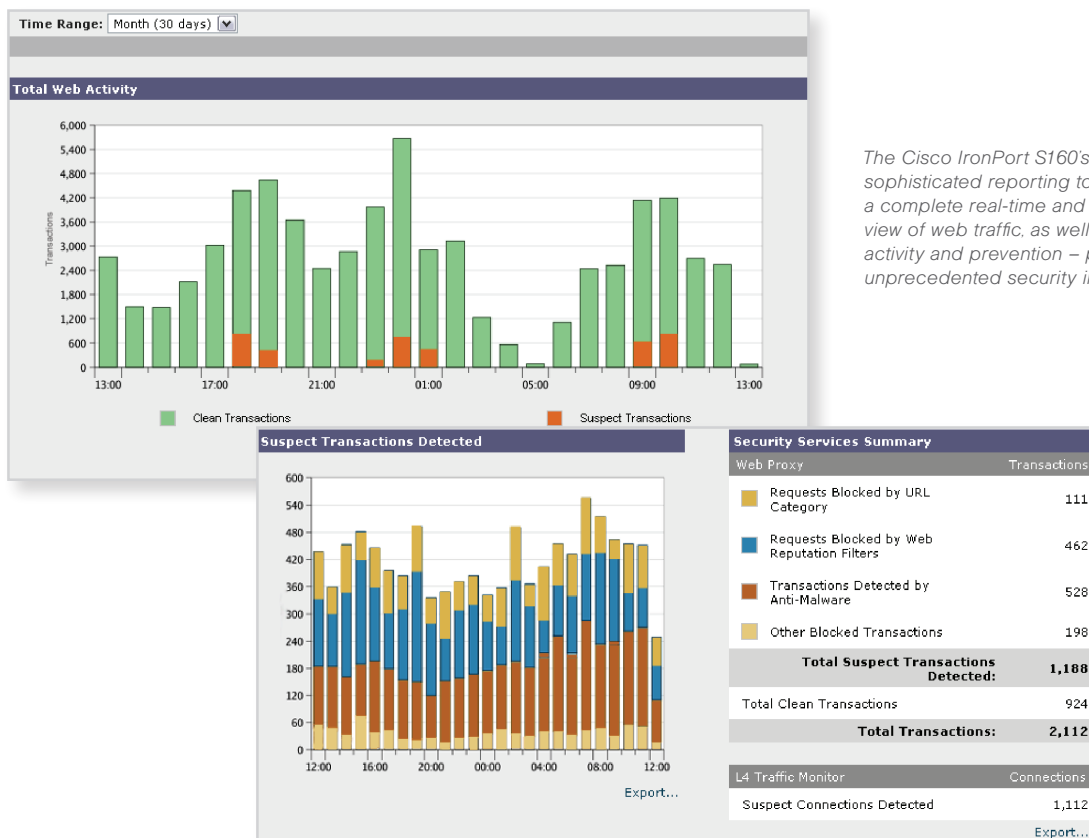
The Cisco IronPort S160's sophisticated reporting tools yield a complete real-time and historical view of web traffic, as well as threat activity and prevention – providing unprecedented security insight.

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 S160 web security appliance 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 systems, the Cisco IronPort S160 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.

FEATURES (CONTINUED)

Native FTP protection allows the Cisco IronPort S160 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 S160 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, the Cisco IronPort S160 can score FTP servers with Cisco IronPort Web Reputation Filters and scan downloaded content for malware and spyware payloads with the Cisco IronPort Dynamic Vectoring and Streaming (DVS) engine. Cisco's FTP protection utilizes Cisco IronPort Data Security to enforce simple, common sense data security policies based on file metadata, user, URL category, and reputation or can pass the FTP traffic to an external DLP solution for additional, more granular, scanning.

The Cisco IronPort S160 now has comprehensive coverage for the three most common protocols carrying business information across the boundary and over the Internet – HTTP, HTTPS and FTP.

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.
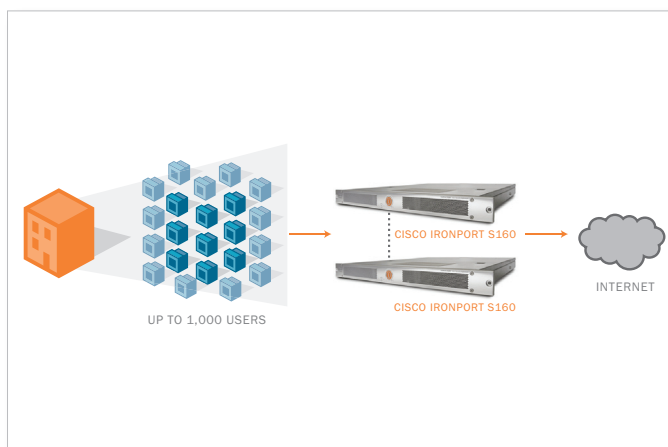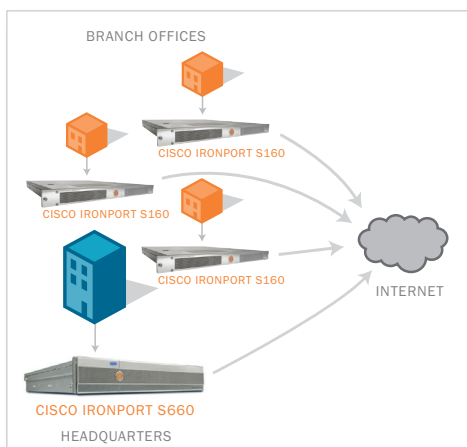
Cisco IronPort Web Security Monitor offers valuable insight into overall web activity, as well as threat identification and prevention, within corporate networks. These on-box and off-box reports are designed to provide actionable information as well as historical trends. Enhanced reporting provides enterprises visibility into policy and security violations.

Multiple deployment modes enable flexibility within a business network. Deployment modes include deployment as an explicit forward proxy for the network or transparent deployment of an L4 switch or a WCCP router within the network. The Cisco IronPort S160 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 S160 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.

The Cisco IronPort S160 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 over-ride. Given the diversity of ways in which group information is stored in user directories, the Cisco IronPort S160 supports obtaining group information from a group object, as well as from an attribute in the user's profile.

BRANCH OFFICES

CISCO IRONPORT S160

CISCO IRONPORT S160

CISCO IRONPORT S160

INTERNET

CISCO IRONPORT S660

HEADQUARTERS

UP TO 1,000 USERS

CISCO IRONPORT S160

CISCO IRONPORT S160

INTERNET

The Cisco IronPort S160 can be deployed to easily suit your enterprise and branch office architecture.

FEATURES (CONTINUED)

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

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 S160 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 S160 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. By providing comprehensive protection, even the smallest business or branch office can ensure minimal downtime to the end-user and minimize the danger of information leakage, including risks from the use of FTP and dynamic Web 2.0 sites.

Cisco's multi-layered defense includes Cisco IronPort URL Filters, Cisco IronPort Web Reputation Filters and Cisco IronPort DVS technology (with multiple anti-malware scanning engines running simultaneously) – ensuring industry-leading accuracy.

Complete, Accurate Protection Cisco IronPort S160 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 Web Usage Controls, 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 S160 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.

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.

The Cisco IronPort S160 enables 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 S160 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.

Performance in a Small Package and Low Total Cost of Ownership Cisco IronPort appliances scale to meet the unique scanning needs of web traffic, thereby ensuring that the end-user experience is maintained. The cisco IronPort S160 provides a single platform that contains a complete, in-depth defense – along with all the necessary management tools – significantly reducing the initial and ongoing TCO of small businesses and remote offices.

Reduced Administrative Overhead Perfect for small to medium businesses and remote offices, the Cisco IronPort S160 is designed to minimize administrative overhead, offering easy setup and management with an intuitive graphical user interface, support for automated updates, and comprehensive monitoring and alerting.

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

Cisco IronPort S160

Chassis

Form Factor	1RU
Dimensions	1.75" (h) x 17.5" (w) x 21.5" (d)
Power Supply	750 watts, 100/240 volts
Redundant Power Supply	No

Processor, Memory and Disks

CPUs	1x2 (1 Dual Core) Pentium
Memory	4 GB
Disk Space	500 GB
Hot Swappable Hard Drives	No
RAID	RAID 1, battery-backed 256MB cache

Interfaces

Ethernet	6xGigabit NICs, RJ-45
Serial	1xRS-232 (DB-9) Serial
Fiber	No

Configuration, Logging and Monitoring

Web Interface	GUI-based (HTTP or HTTPS)
Command Line Interface	SSH or Telnet (Configuration Wizard or command-based)
Logging	Squid, Apache, syslog
Centralized Reporting	Supported
File Transfer	SCP, FTP
Configuration Files	XML-based
Centralized Configuration	Supported
Monitoring	SNMPv1-3, email alerts

SUMMARY

Industrial Strength Web Security

The challenge of securing and controlling 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 business downtime, productivity loss and resource strain on IT infrastructure. Businesses need control to understand when, where and how their employees are using the Internet. Additionally, even branch and remote office locations run 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.

The best place to control and protect against these risks posed by web traffic is right at the gateway. The Cisco IronPort S160 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 Web Usage Controls enforce acceptable use policy, while 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 S160 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.

The Cisco IronPort S160 provides the same powerful protection demanded by the world's largest enterprises – available in a size that's just right for your business. With threats becoming more complex and sophisticated, web security has never been better, or easier to deploy. Cisco enables your company to do business effectively and safely.

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.