Cisco IronPort S-Series Web Security Appliances

The industry's best secure web gateway for acceptable use policy enforcement, malware protection, data security, and application visibility and control.

Introduction

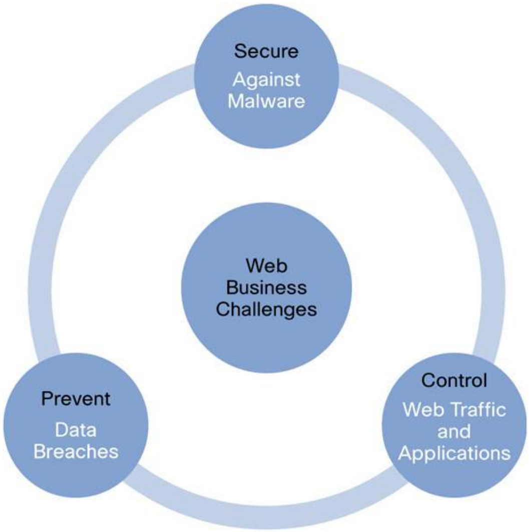
The web has become the ubiquitous platform for application delivery in the enterprise, whether that is browser-based application platforms such as Salesforce.com or Google Apps, or rich-media applications such as Apple iTunes or Cisco WebEx® meeting applications using web protocols as a widely available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

Threat writers, attracted by this ubiquitous access, have shifted malware attacks largely to the web, resulting in near-epidemic threat levels. Traditional defenses are proving to be inadequate against rapidly changing web-based malware, leaving corporate networks exposed to the inherent danger posed by these threats and emphasizing the importance of a robust, secure platform to protect the enterprise network perimeter from such threats.

Increasing employee mobility - largely enabled by web-based applications - offers productivity benefits for businesses and flexibility for users. However, this has also introduced significant security challenges, as organizations must find ways to extend security and policy enforcement to mobile users.

The Cisco IronPort® S-Series Web Security Appliance is the industry's first and only secure web gateway (Figure 1) to combine acceptable-use-policy (AUP) controls, reputation filtering, malware filtering, data security, and application visibility and control on a single platform to address these growing risks. By combining innovative technologies, the Cisco IronPort S-Series helps organizations address the growing challenges of both securing and controlling web traffic whether their employees are tethered to a corporate LAN or sitting in an airport on their smartphones.

Figure 1. Secure Web Gateway: A Comprehensive Security Solution to the Business Challenges of the Web



Customers enjoy low total cost of ownership (TCO), because 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.

The Cisco 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. Built for security and deployed at the gateway to protect the world's most important networks, these products enable a powerful perimeter defense.

By taking advantage of Cisco® Security Intelligence Operations (SIO) intelligence and global threat correlation, Cisco IronPort appliances are smarter and faster. Their advanced technology enables organizations to improve their security and transparently protect users from the latest Internet threats.

Features

Innovative Security Platform That Delivers Protection, 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, Adaptive Scanning, multiple antimalware scanning engines, and the Layer 4 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 AUP enforcement on the Cisco IronPort S-Series. It allows for comprehensive content analysis, which is critical to accurately detect 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 networks.

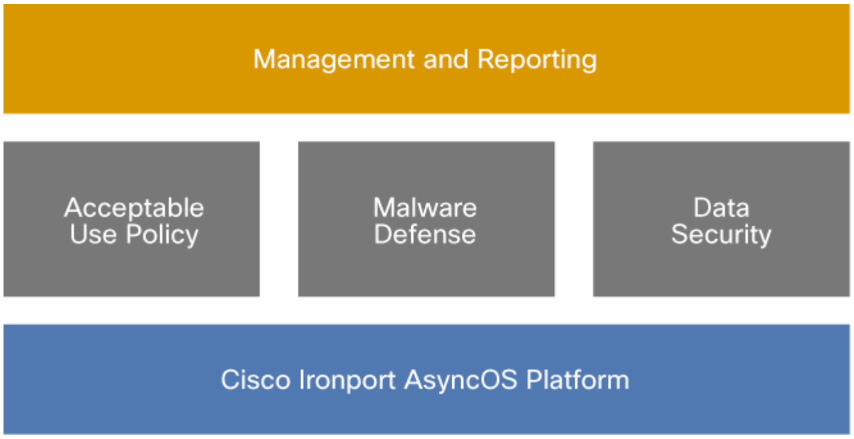
Industry-Leading Acceptable Use Enforcement

Cisco IronPort Web Usage Controls, available on all Cisco IronPort S-Series 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 innovative solution is powered by Cisco SIO, which uses global Internet traffic visibility and analysis to target categorization efforts and provide timely updates, maximizing URL list-based efficacy.

Cisco IronPort Web Usage Controls include both the category of the content and the application in use as part of the policy controls available to administrators. In addition to simply blocking or allowing applications by type or individually, administrators can apply deeper controls to particular application types. For instance, administrators can control the “safe search” settings on major search engines such as Google or Bing, as well as user-generated content sites such as YouTube or Flickr. Or limit bandwidth consumed by streaming-media applications to control congestion. Or allow chat through web instant messenger, but disallow file sharing.

Category, application, and protocol control are facilitated at a granular level, regardless of the protocol or application flowing through the network perimeter. 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 (Figure 2).

Figure 2. The Cisco IronPort S-Series Combines Revolutionary Technologies to Provide Multilayered Web Security on a Single Appliance



Multilayer, Multivendor Malware Defense in Depth

Cisco Security Intelligence Operation (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 SIO is a sophisticated security ecosystem consisting of three components:

- Cisco Sensor Base: The world’s largest threat-monitoring network captures global threat telemetry data from a massive footprint of Cisco devices.
- Threat Operations Center: A global team of security analysts and automated systems extracts 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 most accurate web reputation filters provide a powerful outer layer of malware defense.

Using the intelligence gained from Cisco SIO, Cisco IronPort Web Reputation Filters analyze more than 200 different web traffic-and network-related parameters to accurately evaluate the trustworthiness of a URL or IP address. Cisco IronPort Web Reputation Filters examine every request the browser makes (from the initial HTML request to all subsequent data requests) - including live data, which may be fed from different domains. This comprehensive examination gives these filters a unique advantage over those of other 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 botnet protection, URL outbreak detection, and exploit filtering - protecting users from exploits delivered through cross-site scripting (XSS), cross-site request forgery, Structured Query Language (SQL) injections, or invisible iFrames. The power behind this revolutionary reputation technology comes from the pattern-based assessment techniques and per-object scanning capabilities of the system.

Cisco IronPort Adaptive Scanning is a new content scanning logic feature on the Cisco IronPort S-Series. This new security feature greatly increases the catch rate for malware embedded in images and in JavaScript, text, and Flash files. Adaptive Scanning intelligently selects scanners after analyzing content type and risk profile, resulting in up to 50% higher efficacy in blocking malware.

Adaptive Scanning is an additional layer of security on top of Cisco IronPort Web Reputation Filters, which analyze more than 20 billion web transactions daily. Cisco IronPort Web Reputation Filters examine over 150 different characteristics (such as domain registration information, use of dynamic IPs, traffic volumes, and patterns in the URL being requested) to determine the risk profile of a given URL and assign a web reputation score.

Cisco IronPort's antimalware capabilities give the Cisco IronPort S-Series the distinction of being the first solution on the market to offer multiple antimalware 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 takes advantage of verdict engines from Sophos, Webroot, and McAfee to provide best-of-class protection against the widest variety of web-based threats, ranging from adware, browser hijackers, phishing, and pharming attacks to more malicious threats such as rootkits, Trojan horses, worms, system monitors, and keyloggers.

These engines from Sophos, Webroot, and McAfee are fully integrated into the Cisco IronPort Web Security Appliances. Sophos offers award-winning protection against known and unknown threats using its Genotype and Behavioral Genotype Protection. The Sophos Genotype virus-detection technology proactively blocks families of viruses, and Behavioral Genotype Protection automatically guards against zero-day threats by analyzing the behavior of the code before it executes - offering protection from new and existing viruses, Trojan horses, worms, spyware, and other adware. 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- and heuristics-based scanning.

Cisco IronPort S-Series Web Security Appliances provide an integrated, single-appliance solution with multiple antimalware scanning engines from different vendors. The appliances employ sophisticated object parsing and streaming techniques to enforce AUPs and security features for web traffic, and simultaneously use hardware optimizations (such as multicore scanning) to distribute these parallel operations and take full advantage of the system resources. The result is a tenfold 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 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, or is blocked outright. With this ability, administrators no longer have to sacrifice security for privacy.

Even with the best defenses in place, it is inevitable that some threats will still be present in the network. That is why the S-Series includes an integrated Layer 4 Traffic Monitor, which scans all ports at wire speed, detecting and blocking spyware phone-home activity. By tracking all 65,535 network ports, the Layer 4 Traffic Monitor effectively stops malware that attempts to bypass port 80. In addition, the Layer 4 Traffic Monitor can 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 Layer 4 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.

Powerful Data Security Enforcement

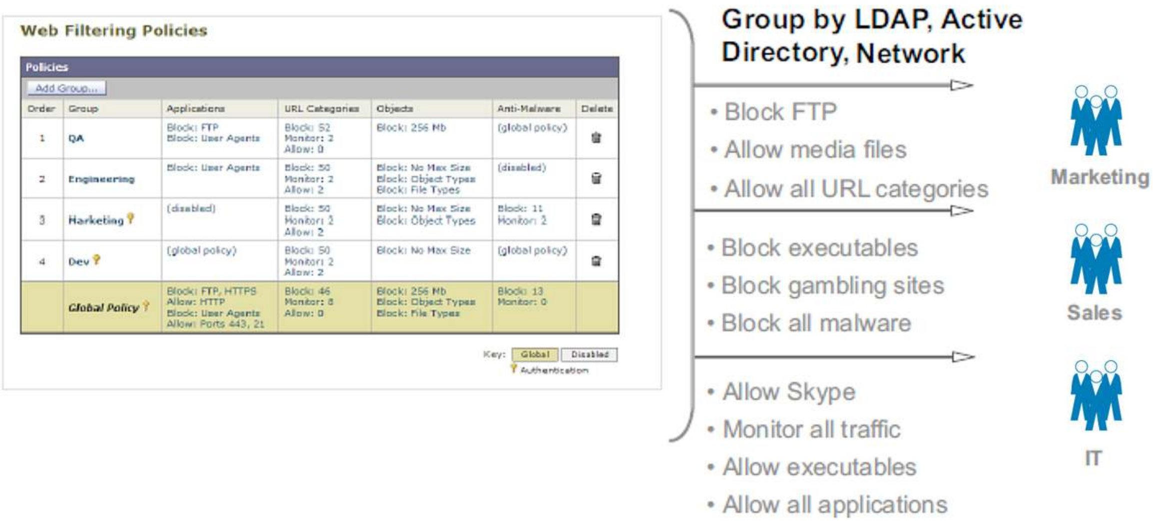
Data security and data-loss prevention (DLP) empower organizations to take quick, easy steps to enforce commonsense data security policies; for example, preventing engineers from sending design files by webmail, blocking uploads by finance staff of Microsoft Excel spreadsheets larger than 100 KB, or preventing posts of content to blogs or social networking sites. These simple data security policies can be created for outbound HTTP, HTTPS, and FTP traffic.

For enterprises that have already invested in special-purpose DLP systems, the Cisco IronPort S-Series offers an option to interoperate with DLP vendors through the Internet Content Adaptation Protocol (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 scenario also enables deep content inspection for regulatory compliance and intellectual property protection, incident severity definition, case management, and performance optimization.

Native FTP protection allows Cisco IronPort S-Series 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 the ability to allow or block FTP connections, perform active-passive FTP mediation, restrict users or groups, control uploads and downloads, and restrict sent and received files to certain types or sizes.

Additionally, S-Series appliances can use Cisco IronPort Web Reputation Filters to score FTP servers and scan downloaded content for malware and spyware payloads. This FTP protection enforces simple, commonsense data security policies based on file metadata, user, URL category, and reputation (Figure 4). Alternately, FTP traffic can be passed to an external DLP solution for additional, more granular, scanning.

Figure 3. Cisco IronPort Web Security Manager Makes It Easy to Create Different Sets of Policies for Each Group of Users

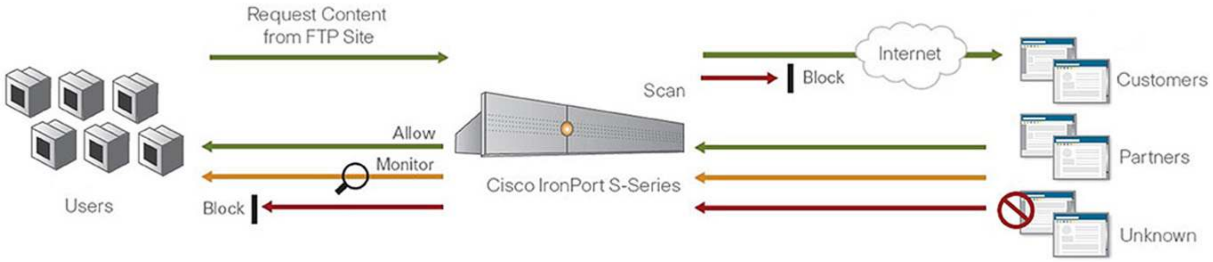


Web Filtering Policies

Policies

Order	Group	Applications	URL Categories	Objects	Anti-Malware	Delete
1	QA	Block: FTP Block: User Agents	Block: 52 Monitor: 2 Allow: 0	Block: 256 Mb	(global policy)	🗑
2	Engineering	Block: User Agents	Block: 50 Monitor: 2 Allow: 2	Block: No Max Size Block: Object Types Block: File Types	(disabled)	🗑
3	Marketing	(disabled)	Block: 50 Monitor: 2 Allow: 2	Block: No Max Size Block: Object Types	Block: 11 Monitor: 2	🗑
4	Dev	(global policy)	Block: 50 Monitor: 2 Allow: 2	Block: No Max Size	(global policy)	🗑
	Global Policy	Block: FTP, HTTPS Allow: HTTP Block: User Agents Allow: Ports 443, 21	Block: 46 Monitor: 8 Allow: 0	Block: 256 Mb Block: Object Types Block: File Types	Block: 13 Monitor: 0	

Figure 4. Native FTP Protection Enables Complete Visibility into FTP Usage - Enforcing Acceptable Use and Data Security Policies, and Preventing Malware Infections



Cisco AnyConnect Secure Mobility for Borderless Networks

The Cisco Borderless Network Architecture integrates security into the distributed network to address today's security requirements. This approach takes advantage of exceptional threat intelligence, a broad solution portfolio, and strategic partnerships and services to extend security to the right people, devices, and locations, enabling customers to build solutions to meet evolving business challenges.

One important component of this architecture is Cisco AnyConnect™ Secure Mobility. This solution combines the next-generation remote access capabilities of Cisco AnyConnect with the web security capabilities of the S-Series to provide mobile users with always-on, secure access to corporate resources while ensuring constant malware protection and policy enforcement.

The Cisco IronPort S-Series includes support for Cisco AnyConnect Secure Mobility. Employees connecting with the 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 to Software-as-a-Service Applications

In addition to users moving outside the traditional enterprise security boundary, critical business applications are increasingly being served from external servers. Enterprises are adopting software-as-a-service (SaaS) at high rates, whether it is collaboration services such as Cisco WebEx meeting applications or online application suites such as Google Apps or Zoho.

A major challenge with adoption of these services is managing user authentication and entitlements. Administrators want to control which users have access to which services, and control their access rights within each service. They also want the ability to revoke access in a timely fashion when a user leaves the organization. Employees need to remember multiple usernames and passwords, a problem they often solve by writing down the credentials in clear text, compromising security. These problems become especially difficult as the SaaS services proliferate.

The Cisco IronPort S-Series includes a standards-based authentication mechanism to bring this under control. The appliance signs onto the target website on behalf of the employee, using the Security Assertion Markup Language (SAML) 2.0 standard. This process uses the employee's credentials and access rights stored in the corporate user directory, either Active Directory or Lightweight Directory Access Protocol (LDAP).

Administrators retain control over access rights, and employees get a transparent experience by using the corporate username and password for accessing all applications. The Cisco IronPort S-Series also offers transparent user identification for Active Directory, which allows increased flexibility for identifying end users in environments using Active Directory for end-user authentication.

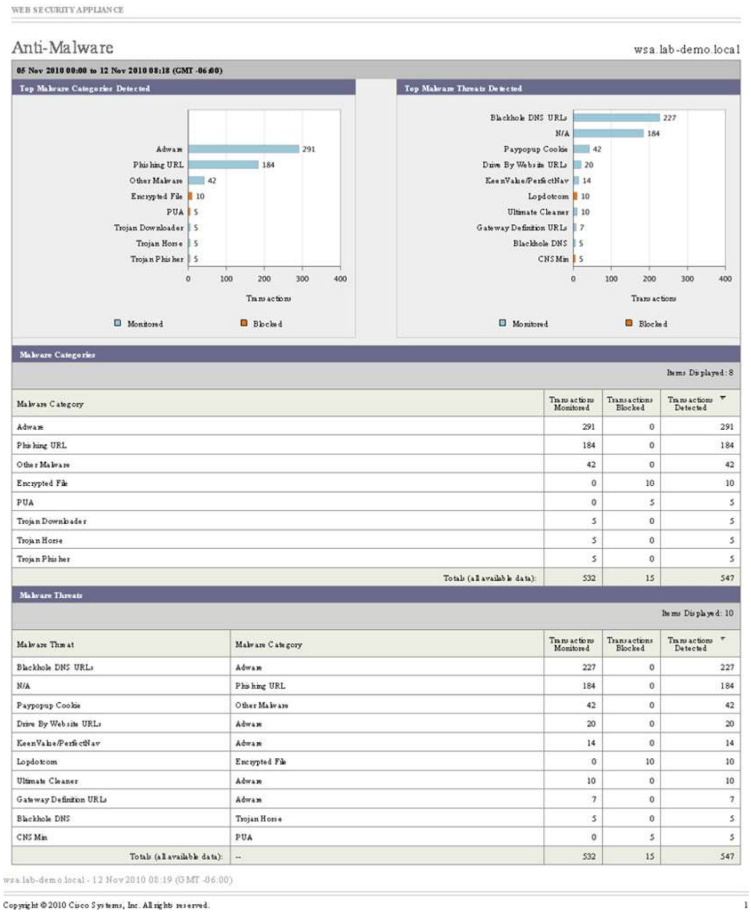
When combined with Cisco AnyConnect Secure Mobility, this capability gives your employees anytime, anywhere access to corporate resources - whether hosted within the organization or on external servers - without sacrificing control or security. SaaS applications are accessible only through the corporate infrastructure, regardless of device or location.

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 webaccess 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 (for example, client IP address, authenticated username, etc.) and destination-based criteria (for example, URL, URL category, proxy port, etc.) to flexibly determine when each set of policies is applied.

On-box web reports offer valuable insight into overall web activity within corporate networks, as well as threat identification and prevention. These reports provide actionable information in realtime, as well as historical trends (Figure 5). Enhanced reporting gives enterprises visibility into policy and security violations.

Figure 5. Native FTP Protection Enables Complete Visibility into FTP Usage - Enforcing Acceptable Use and Data Security Policies, and Preventing Malware Infections



WEB SECURITY APPLIANCE

Anti-Malware

wsa.lab-demo.local

05 Nov 2010 00:00 to 12 Nov 2010 08:18 (GMT -06:00)

Top Malware Categories Detected

Top Malware Threats Detected

Malware Categories

Items Displayed: 8

Malware Category	Transactions Monitored	Transactions Blocked	Transactions Detected
Adware	291	0	291
Phishing URL	184	0	184
Other Malware	42	0	42
Encrypted File	0	10	10
PUA	0	5	5
Trojan Downloader	5	0	5
Trojan Horse	5	0	5
Trojan Phisher	5	0	5
Totals (all available data):	532	15	547

Malware Threats

Items Displayed: 10

Malware Threat	Malware Category	Transactions Monitored	Transactions Blocked	Transactions Detected
Blackhole DNS URLs	Adware	227	0	227
N/A	Phishing URL	184	0	184
Paypopup Cookie	Other Malware	42	0	42
Drive By Website URLs	Adware	20	0	20
KeenValue/PerfectNav	Adware	14	0	14
Lopdotcom	Encrypted File	0	10	10
Ultimate Cleaner	Adware	10	0	10
Gateway Definition URLs	Adware	7	0	7
Blackhole DNS	Trojan Horse	5	0	5
CNS Min	PUA	0	5	5
Totals (all available data):	--	532	15	547

wsa.lab-demo.local - 12 Nov 2010 08:19 (GMT -06:00)

Copyright © 2010 Cisco Systems, Inc. All rights reserved.

1

Multiple deployment modes enable flexibility within a corporate network. Modes include deployment as an explicit forward proxy for the network or transparent deployment of a Layer 4 switch or a Web Cache Communications Protocol (WCCP) router within the network. Each Cisco IronPort S-Series Web Security Appliance can be configured as a standalone proxy or it can coexist with other proxies (such as in a proxy hierarchy for conditional routing, failover, and load balancing).

Enterprise-grade Simple Network Management Protocol (SNMP) facilitates hands-off monitoring and alerting for keysystem metrics, including hardware, performance, and availability. Support for SNMPv1, 2, and 3, along with a comprehensive enterprise-class alert engine, helps ensure oversight for all system parameters - including hardware, security, performance, and availability.

Integrated authentication through standard directories (such as LDAP or Active Directory) and the ability to implement multiple authentication schemes (such as Windows NT LAN Manager [NTLM]) lets enterprises deploy the Cisco IronPort S-Series transparently, while taking advantage of preexisting authentication and access control policies within their networks. Features such as multirealm authentication (which enables authentication against multiple authentication domains) provide flexible failover scenarios and multiorganization deployments.

Cisco IronPort S-Series Web Security Appliances also enable coaching to allow the organization to educate employees on corporate acceptable use and security policies, restricted guest access for visitors, and reauthentication for privilege override in real time. 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.

Extensive logging allows enterprises to keep track of all web traffic, whether benign or malicious. Standard log formats, such as Apache or Squid, provide 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 World Wide Web Consortium (W3C)-standard Extended Log File Format (ELFF). This format 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, human resources, 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.

Mitigation of Malware Risks and Costs: With malware infecting approximately 75 percent of corporate desktops, overhead for managing infected desktops, ensuring minimal downtime to employees, and minimizing the risk of information leakage is considerable. The Cisco Ironport S-Series mitigates this risk by significantly reducing, if not altogether eliminating, malware from the enterprise.

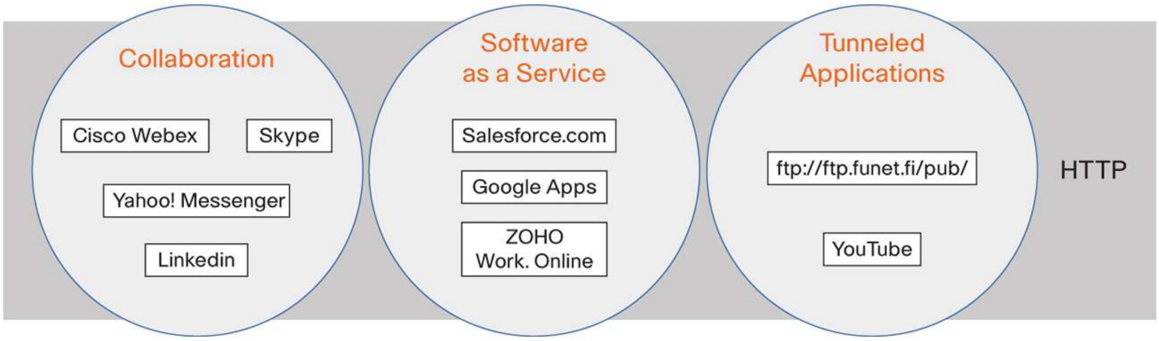
Reduced Administrative Costs: By stopping these threats at the network perimeter with the Cisco IronPort S-Series, enterprises can significantly reduce the administrative costs, prevent attacker phone-home activity on networks, reduce support calls, enhance worker productivity, and also eliminate the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

Complete, Accurate Protection: Cisco IronPort S-Series appliances are designed to address the broadest range of web-based malware threats, including those from the use of FTP and dynamic Web 2.0 sites. A multilayered defense that includes Cisco SIO, Cisco IronPort Web Usage Controls, Cisco IronPort Web Reputation Filters, and Cisco IronPort Adaptive Scanning helps ensure industry-leading accuracy.

This multilayered protection is based on a comprehensive 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 one of the industry's most secure web gateways.

Enforcement of Acceptable Use Policies: By implementing acceptable use web policies, enterprises can both conserve resources for work-related web usage and inform employees to help shape web access behavior over time (Figure 6). Enterprises can increase the amount of time that employees spend on business-oriented activities, reducing misuse of enterprise networks and bandwidth.

Figure 6. The Cisco IronPort S-Series Layers Additional Capabilities on Top of URL Filtering to Provide Richer Controls for Web Application Usage



Simplified Data Security: The data-loss problem extends well beyond malware. Employees can easily use webmail to send a message containing 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 employees to take advantage of the full power of the Internet - is an important and challenging problem to solve.

Cisco IronPort S-Series Web Security Appliances enable organizations to take quick, easy steps to enforce commonsense data security policies for outbound HTTP, HTTPS, and FTP traffic, as well as enabling simple interoperability with major dedicated DLP solutions.

Mobile Security Across Borderless Networks: The Cisco AnyConnect Secure Mobility solution supports a wide range of desktops and mobile devices, helping ensure that web security continues to be enforced as employees change the devices they use. By using a standardized security solution for employees whether they are in the office or mobile, IT can also streamline security operations for a compelling TCO.

SaaS Access Controls: The Cisco IronPort S-Series uses a standards-based authentication mechanism to bring sign-on under the control of your enterprise. Referencing the employee credentials and access rights stored in the corporate user directory, administrators retain control over access rights, and employees get a transparent experience using their corporate username and password to access all applications.

Reporting Visibility: 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 factors such as policy and security violations as they occur. Historical reports allow administrators to identify trends and report on efficacy and return on investment (ROI).

Enterprise-Scale Performance: The Cisco IronPort S-Series scales to meet the unique scanning needs of web traffic, thereby helping ensure that the employee's experience is maintained. Cisco offers industry-leading performance through its proprietary AsyncOS platform, an enterprise-grade web proxy and cache file system, and an intelligent, multicore engine for rapid content scanning.

Consequently, the Cisco IronPort S-Series can address the capacity requirements of even the largest of enterprises.

Low TCO: Traditional 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 S-Series Web Security Appliances offer easy setup and management with an intuitive GUI, support for automated updates, and comprehensive monitoring and alerting. The solution is easy to deploy and can be configured to match corporate-specific policies.

Product Line

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

Cisco IronPort S670: For organizations above 10,000 users.

Cisco IronPort S370: For organizations with 1,000 to 10,000 users.

Cisco IronPort S170: For small businesses and organizations with up to 1,000 users.

Table 1. Model-Dependent Specifications for the Cisco IronPort S-Series Web Security Appliance

	Cisco IronPort S670	Cisco IronPort S370	Cisco IronPort S170
Chassis			
Form Factor	2U	2U	1RU
Dimensions (H x W x D)	3.5 x 17.5 x 26.8 in.	3.5 x 17.5 x 26.8 in.	1.75 x 17.5 x 21.5 in.
Power Supply	870W, 100/240V	870W, 100/240V	345W, 100/240V
Redundant Power Supply	Yes	Yes	No
Processor Memory and Disks			
CPUs	2x4 (2 Quad Cores)	1x4 (1 Quad Core)	1x2 (1 Dual Core)
RAID Level & Controller	RAID 10, Hardware	RAID 10, Hardware	RAID 1, Software
Memory	8 GB	4 GB	4 GB

	Cisco IronPort S670	Cisco IronPort S370	Cisco IronPort S170
Disk Space	2.7 TB	1.8 TB	500 GB
Hot Swappable Hard Disk	Yes	Yes	Yes
Interfaces			
Ethernet	5 Gigabit NICSs, RJ-45	5 Gigabit NICSs, RJ-45	5 Gigabit NICSs, RJ-45
Speed (mbps)	10/100/1000, Auto-Negotiate	10/100/1000, Auto-Negotiate	10/100/1000, Auto-Negotiate
Duplex	Half or Full, Auto-Negotiate	Half or Full, Auto-Negotiate	Half or Full, Auto-Negotiate
Serial	1xRS-232 (DB-9) Serial	1xRS-232 (DB-9) Serial	1xRS-232 (DB-9) Serial
Fiber	Optional	No	No
USB	0	0	2
Configuration, Logging, and Monitoring			
Web Interface	GUI-based (HTTPS)	GUI-based (HTTPS)	GUI-based (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
Environmental Operating Ranges			
Total Current (A)	4	2.5	4.85 (max)
Input Voltage (V)	100 to 240 VACF	100 to 240 VAC	100 to 240 VAC
Operating Power (W)	427.1	267.3	400W (max)
Total Heat Dissipation (BTU/hr)	1,928.5	1,471	432.6
Leakage Current (mA)	3.5	3.5	3.5
Fan Exhaust Volume (CFM)	43.1	37.4	Idle at 24℃: 12.3 Full fan speed: 34.4
Ambient Noise (Bels)	6.3	6.1	Idle: 41.3 dBa Stress: 64.2 dBa max.
Effective MTBF (Hours)	94,400	94,400	107,356
Operating			
Temperature (℃)	10℃ to 35℃	10℃ to 35℃	-5℃ to 45℃
Relative Humidity (%)	20% to 80% (noncondensing)	20% to 80% (noncondensing)	20% to 80% (noncondensing)
Altitude (m)	3,048	3,048	3,000
Vibration	0.26 Grms at 5-350Hz	0.26 Grms at 5-350Hz	0.41Grms, at 3Hz-500Hz
Non-Operating			
Temperature (℃)	-40℃ to 65℃	-40℃ to 65℃	-25℃ to 70℃
Relative Humidity (%)	5% to 95% (noncondensing)	5% to 95% (noncondensing)	5% to 95% (noncondensing)
Altitude (m)	10,600	10,600	4,570
Vibration	1.54 Grms at 10-250Hz	1.54 Grms at 10-250Hz	1.12Grms at 3Hz-500Hz
Industry Certifications			
RoHS	Yes	Yes	Yes
Other Certifications			Safety: cULus, CB, CCC, BSMI EMC:CE, FCC, VCCI, C-TICK, KC

Summary

The Ultimate Web Security System

The challenge of securing and controlling enterprise web traffic is continually evolving. 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 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 its networks are compromised. 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 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 Web Usage Controls enforce AUP, while Cisco Security Intelligence Operations, Cisco IronPort Web Reputation Filters, and the Cisco IronPort Anti-Malware System—with simultaneous scanning by Sophos, 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 Layer 4 Traffic Monitor detects and blocks phone-home malware activity that attempts to circumvent port 80 security features. With threats becoming more complex and sophisticated, the Cisco IronPort S-Series offers one of the industry’s most comprehensive web security solutions while ensuring enterprise-class performance.

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.**

Printed in USA C78-702070-02 05/12