

Cisco IronPort URL Filters

FAST, ACCURATE CONTENT FILTERING
FOR ACCEPTABLE USE POLICY ENFORCEMENT



In today's business environment, the Internet is a valuable resource that gives organizations the means to facilitate communication, while offering instant access to virtually limitless amounts of information. At the same time, when access goes unmonitored, it can result in misuse, productivity issues and unforeseen legal risks.

IDC estimates that nearly forty percent of a corporation's Internet traffic is non-business related. This represents a very real and significant drain to employee productivity and network resources, as well as potential violations of these corporations' acceptable use policies. In addition to simply hurting productivity, this kind of activity potentially exposes organizations to unnecessary legal risks.

Cisco® IronPort URL Filters address these concerns by uniquely combining a high-performance scanning engine with the industry's broadest web database to provide a fast and accurate content filtering solution for all of your HTTP and HTTPS traffic. A key component of the acceptable use policy framework on the Cisco IronPort S-Series web security appliance, Cisco IronPort URL Filters rapidly scan employee browsing requests and evaluate them against corporate-specific policies – leveraging a highly accurate database of scored websites. Additionally, these filters leverage the HTTPS decryption capabilities of the Cisco IronPort S-Series. This allows the enforcement of your acceptable use policies to span across HTTPS traffic, eliminating a potential blind spot. By preventing employees from accessing sites that violate policies, organizations can now harness the benefits of the Internet while minimizing the associated productivity, resource and legal risks.

The Cisco IronPort S-Series is the only solution to combine Cisco IronPort URL Filters with Cisco IronPort Web Reputation Filters and the Cisco IronPort Anti-Malware System to provide a single, integrated solution that ensures that a corporation's web traffic is accurately scanned for both acceptable use violations and security threats.

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

Accuracy

Powered by one of the industry’s largest web databases, Cisco IronPort URL Filters provide administrators with over 50 content categories and more than 20 million websites (corresponding to over 3.5 billion webpages), across 70 languages and 200 countries.

The highest quality database drives Cisco IronPort URL Filters. This database is sourced through automated web crawling and classification technologies, combined with the human oversight provided by a global team of professional researchers. Periodic, automated ageing out of unused domains and sites, along with daily updates of millions of new URLs, helps maintain the industry’s highest quality web filtering database.

Broad international coverage ensures that Cisco IronPort URL Filters can accurately block websites, regardless of where the destination URL points. Today, an increasing number of websites hosting inappropriate content – adult, gaming, gambling and more – are set up using international domains to thwart URL filters.

Granular classification of websites means greater flexibility for organizations in defining and enforcing acceptable use policies. Support for unlimited custom categories (based on IP addresses, subnets, CIDR ranges, URLs, domains and regular expressions) provide additional agility in responding to violations.

Automatic, incremental web database updates add more than 100,000 new sites and 10 million new URLs weekly to ensure ongoing accuracy. Administrators configure the update schedule to check for new rules as frequently every five minutes.

Policy Control

Powerful and flexible authentication ensures seamless integration with corporate environments. Administrators can create policies based on existing LDAP-based or Active Directory-based directory structures. Single sign-on capabilities provide a seamless end-user experience while surfing the web. Administrators can also create authentication exemptions based on source or destination traffic profiles. Guest functionality allows restricted access without having to add the user to the AD or LDAP database, or if they fail authentication. Lastly, the system allows for re-authentication to temporarily enable access to restricted content by someone with higher privileges.

Granular policy creation using Cisco IronPort Web Security Manager allows administrators to create and manage policies on a per-user and per-group basis. Additionally, thanks to the HTTPS decryption capabilities of the Cisco IronPort S-Series, decrypting decisions can be tied to Cisco IronPort URL Filters and web reputation – providing tremendous flexibility and control. Cisco IronPort Web Security Manager enables automatic sync-up with existing authentication directories to provide a list of active groups. This enables administrators to further refine pre-existing LDAP-based or Active Directory-based groups. Administrators can define groups using network segments, IP addresses, subnet or CIDR ranges, as well as combine multiple network segments or separate groups into a single unit.

Consolidated policy management with Cisco IronPort Web Security Manager unifies security policies implemented across logical business groups. This tool is flexible and easy-to-use, allowing administrators to manage URL filtering policies from a single GUI.

Category	Use Global Settings	Override Global Settings		
		Allow	Monitor	Block
Adult/Sexually Explicit	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Advertisements & Popups	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alcohol & Tobacco	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Arts	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Category	Use Global Settings	Override Global Settings		
		Allow	Monitor	Block
IT Safe URLs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Partner URLs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Blacklist	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Whitelist	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Blogs & Forums	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pre-defined and unlimited custom URL categories provide granularity, flexibility and control in implementing enterprise policies.



FEATURES (CONTINUED)



Understand at-a-glance the web traffic blocked versus allowed, on a per-category basis.

Comprehensive application, object and protocol filtering

enables administrators to configure per-user and per-group controls, which apply to all HTTP and HTTPS traffic. Administrators can choose to block or allow applications such as instant messenger (IM) or Skype traffic tunneled through HTTP. Additionally, object filtering (based on “true type”) accurately recognizes objects to restrict object and file downloads that present security and/or compliance risks. Warn/continue pages can also be implemented for soft blocking of URL categories, enabling organizations to educate users on corporate acceptable use and security policies.

Customized and localized notifications automatically alert end-users to policy violations that impact their Internet browsing activity. Administrators choose system-determined notifications across more than 25 trigger events or redirect to a separate customizable internal policy page. The ability to customize allows administrators to maximize the educational opportunity of a blocked web request. End-user notifications can be selected in ten different languages, to ensure compliance with local regulations and business requirements. Available languages include English, French, German, Japanese, Spanish, Korean, Portuguese, Thai, Traditional Chinese and Simplified Chinese.

Visibility

Easy-to-understand reports provide extensive information on overall web traffic. At-a-glance reports indicate a corporation’s current web traffic usage, with more granular reports detailing top resources in use, on a per-user and per-category basis. Reports assist in identifying the top users within the network that comply or violate corporate acceptable use policy. Reports also provide detailed and summary information on bandwidth saved as a result of URL filtering. Administrators can use pre-defined reports or develop custom reports and notifications.

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

Comprehensive alerting, included with every Cisco IronPort S-Series appliance, supports Cisco IronPort URL Filters. Administrators can set up individual alert subscriptions, based on severity levels. Alerts are calibrated in three categories: informational, warning and critical. This provides administrators with clear visibility into the application and enables them to take appropriate and timely action, if required.



BENEFITS

Maintain Focus on Core Business Activities The Internet provides nearly unlimited distraction opportunities. Cisco IronPort URL Filters allow organizations to implement corporate-specific policies to keep employees focused on core business activities using granular, user and group-based policies that are applied dynamically. In addition, it allows organizations to maintain better control over resource costs, such as network bandwidth and IT staff time.

Control Legal Liabilities By instituting appropriate Internet usage guidelines, corporations using Cisco IronPort URL Filters can improve compliance – eliminating inappropriate web traffic, reducing inroads for illegal “phone-home” activity (which steals mission-critical and confidential data from within the network), and providing a concrete implementation of critical corporate acceptable use policies.

Ensure Accuracy Cisco IronPort URL Filters leverage the industry’s leading URL database in terms of quantity, quality and breadth. Automated, incremental updates ensure the ongoing accuracy of the database while eliminating the need for manual intervention.

Comprehensive Visibility Cisco IronPort Web Security Monitor reports help administrators quickly identify and investigate issues. Real-time reports help locate and track issues as they occur. Historical reports allow administrators to observe trends and report on efficacy and Return on Investment (ROI). These actionable reports minimize the time wasted on forensics – letting administrators focus efforts on education and awareness.

Reduced Total Cost of Ownership (TCO) Cisco IronPort URL Filters are integrated into the Cisco IronPort S-Series, a single appliance solution that addresses all web security requirements. This revolutionary system provides a single platform that addresses both acceptable use and security concerns which, when combined with comprehensive management and reporting support, significantly reduces initial and ongoing TCO.

Preserve the End-user Browsing Experience Powered by Cisco’s next-generation IronPort AsyncOS architecture, Cisco IronPort URL Filters scale to meet the unique scanning needs of web traffic – ensuring that the end-user experience is maintained.

URL Filtering Categories

Adult/Sexually Explicit	Hacking	Proxies & Translators
Advertisements & Pop-Ups	Health & Medicine	Real Estate
Alcohol & Tobacco	Hobbies & Recreation	Reference
Arts	Hosting Sites	Religion
Blogs & Forums	Illegal Drugs	Ringtones/Mobile Phone
Business	Infrastructure	Downloads
Chat	Intimate Apparel & Swimwear	Search Engines
Computing & Internet	Intolerance & Hate	Sex Education
Criminal Activity	Job Search & Career	Shopping
Downloads	Development	Society & Culture
Education	Kid’s Sites	Sports
Entertainment	Motor Vehicles	Streaming Media
Fashion & Beauty	News	Tasteless & Offensive
Finance & Investment	Peer-to-Peer	Threat & Fraud URLs
Food & Dining	Personals and Dating	Travel
Gambling	Philanthropic & Professional	Violence
Games	Photo Searches	Weapons
Government	Politics	Web-based Email



SUMMARY

Only Cisco offers URL filtering, combined on a single appliance with Cisco IronPort Web Reputation Filters and the Cisco IronPort Anti-Malware System, to ensure that a corporation's web traffic is accurately scanned for both acceptable use violations and security threats. Utilizing a high-performance scanning engine with the industry's broadest web database, Cisco provides a fast and accurate content filtering solution. Cisco IronPort URL Filters rapidly scan web traffic requests to evaluate against corporate-specific policies – helping organizations harness the benefits of the Internet while minimizing the associated productivity, resource and legal risks.

CONTACT US

Cisco sales representatives, channel partners and system engineers are ready to help you evaluate how Cisco IronPort products can make your 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) 435-0222-3 4/09