

Cisco IronPort Web Usage Controls

Industry-leading visibility and enforcement of acceptable web use policies

Improper web use costs businesses billions of dollars in lost productivity and resource misuse each year, and introduces the risk of compliance violations and legal liability. Traditional approaches to managing this challenge—using static lists of categorized URLs—have become decreasingly effective in the face of an increasingly dynamic and growing Internet. More than 1 billion new webpages are added every day, a staggering tribute to the success of Web 2.0 and the popularity of user-generated content. This content explosion, combined with rapid content churn—more than 30 percent of the domains change on an annual basis—has created a vast “dark web,” with more than 80 percent of content uncategorized by legacy solutions. The dark web exposes organizations to the same risks and costs that URL filtering was meant to address.

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 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.

List-based URL filtering alone cannot solve the dark web challenge. To overcome this limitation, Cisco IronPort Web Usage Controls include a dynamic content analysis engine, which categorizes up to 90 percent of objectionable dark web content and increases overall coverage on the most commonly blocked content by up to 50 percent.

“The source of web content on high-traffic pages is progressively more unknown. Social networking sites, blogs, wikis and other interactive websites are the second most-popular form of content on the web. . . Failure to secure the web will have a chilling effect on an organization’s capability to benefit from the Web 2.0 evolution.”

– Gartner, Inc. “Why Malware Filtering Is Necessary in the Web Gateway”
by Peter Firstbrook, August 26, 2008



THE CISCO IRONPORT DIFFERENCE

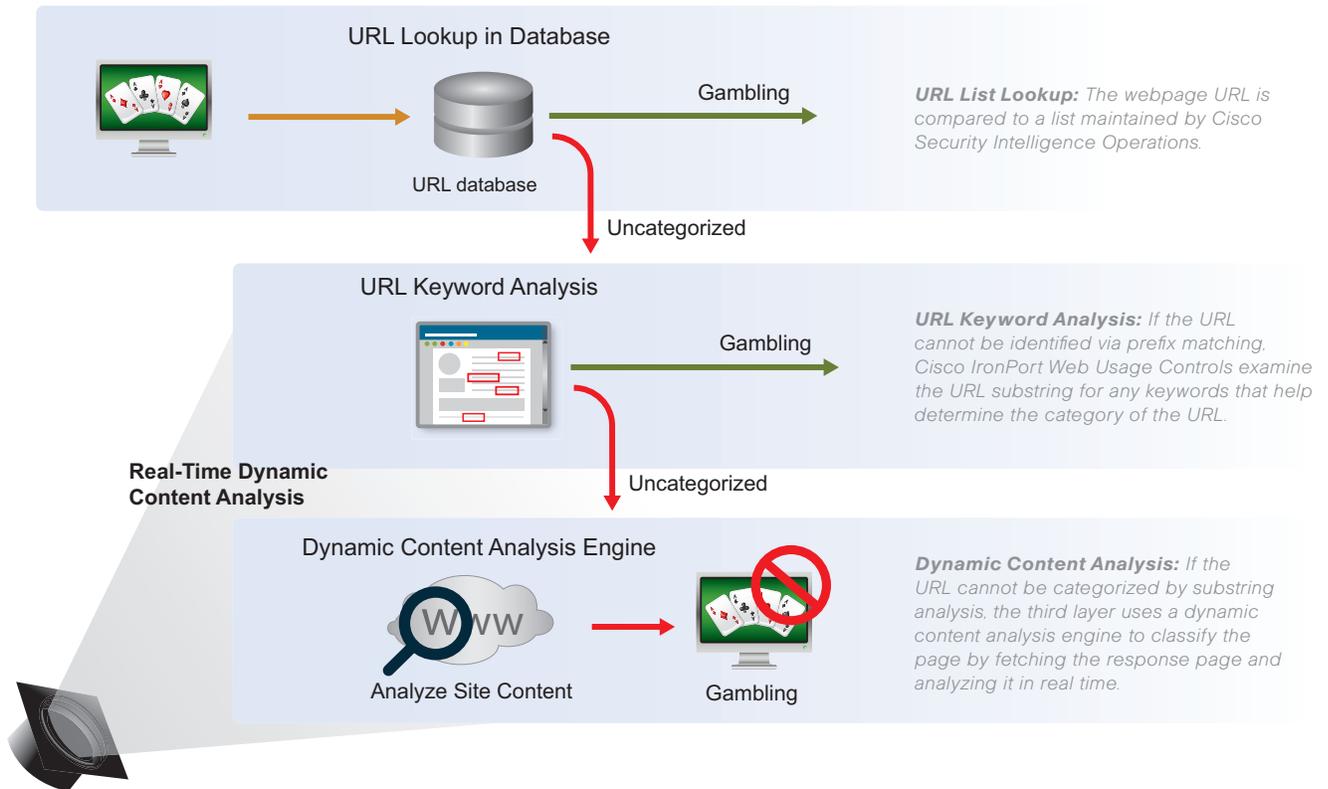
Cisco IronPort email and web security products are high-performance, easy-to-use, and technically innovative solutions, designed to secure organizations of all sizes. Purpose-built for security and deployed at the gateway to protect the world’s most important networks, these products enable a powerful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

Leveraging Cisco SIO and global threat correlation technology help to increase the intelligence and speed of Cisco IronPort appliances. This advanced technology enables organizations to improve their security and transparently protect users from the latest Internet threats.

FEATURES

Industry-Leading Efficacy

Cisco IronPort Web Usage Controls use multiple layers for URL categorization to provide the highest levels of efficacy and coverage for the web, including the dark web. The solution provides 65 URL categories and a comprehensive URL database that encompasses sites in more than 190 countries and more than 50 languages.



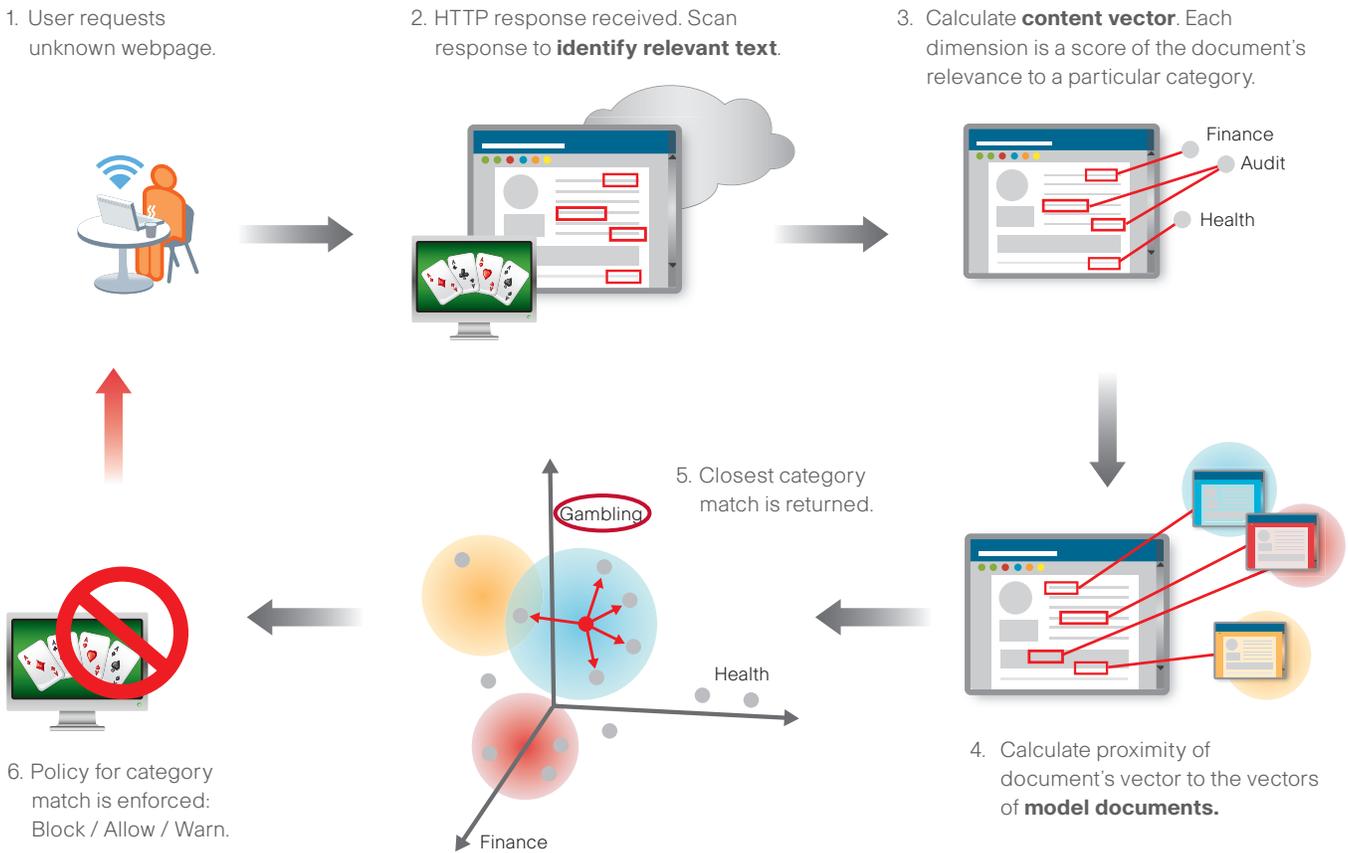
FEATURES (CONTINUED)

Cisco SIO updates the database every five minutes, taking advantage of its visibility into more than a third of global Internet traffic to provide customers with the most effective and timely coverage. URL updates are sourced from automated web crawling and classification technologies, combined with manual classification from Cisco’s global categorization team of professional researchers. Periodic, automated aging out of unused domains and sites, along with regular updates of millions of new URLs, helps maintain the industry’s highest-quality web filtering database.

In addition, data from thousands of participating Cisco IronPort web security appliances (deployed globally) is delivered to the Cisco SIO to classify uncategorized URLs. Any miscategorization requests are responded to promptly, often within minutes.

Dynamic Categorization: In Real Time and On-Box

The dynamic content analysis engine evaluates all uncategorized web content—even content hidden in an SSL tunnel—to make real-time categorization decisions. Advanced heuristics are used to calculate a concept vector, which is compared with an extensive library of model documents to quickly and accurately determine the content category. The engine is tuned to maximize catch rates for the most commonly blocked objectionable content, minimizing the liability and compliance violation risks for customers while maintaining a low false-positive rate.



Content analysis occurs in real time, before the user sees the requested webpage. Because the content is analyzed in just a few milliseconds, and since the technology is included on the appliance, there is no perceptible latency for the end user.



FEATURES (CONTINUED)

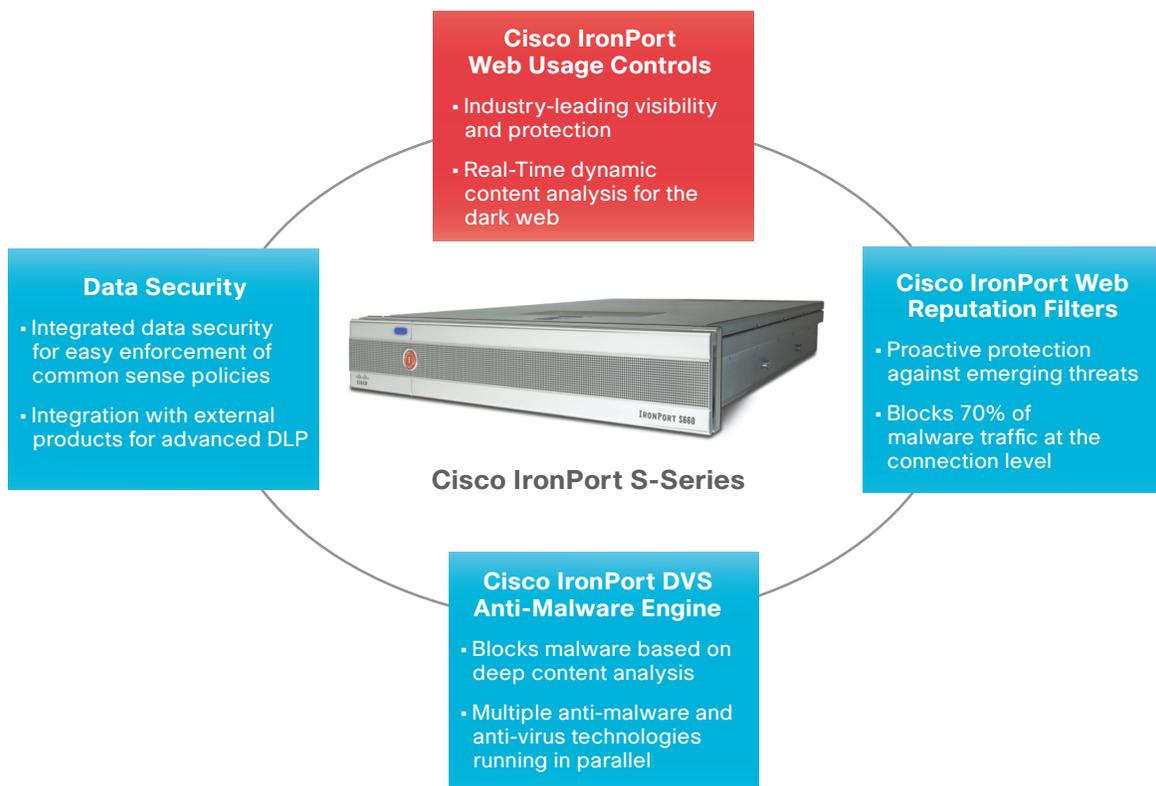
Rich Policy Controls and Comprehensive Reporting

Cisco IronPort Web Usage Controls provide rich policy features to control access to the web. Controls available at the URL category level include Block, Allow, Warn, and Monitor, along with time-of-day-based controls. Integration with existing AD or LDAP directories allows for user- and group-level policies. Custom categories with support for regular expressions allow flexibility in creating a virtually unlimited number of custom white and black lists.

The solution provides comprehensive reporting, both on-box and off-box. The reports are fully interactive, allowing an administrator to start by looking at high-level summaries, such as how many users are being blocked by policy. With a single click, the administrator can drill down and see what policies are being hit—or which users are being blocked the most. With another click, the administrator can see all of the traffic for a single user that may have been hitting a given policy. This reporting system allows administrators to quickly identify problems, and either adjust policy or take other appropriate actions. Logs can be exported for further analysis and forensics. Also included in the solution is comprehensive alerting for enterprise class support.

Fully Integrated Web Security

Cisco IronPort Web Usage Controls are fully integrated into the Cisco IronPort S-Series web security appliance, 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.



By combining innovative technologies, the Cisco IronPort S-Series helps organizations address the growing challenges of both securing and controlling web traffic.



URL Filtering Categories

Cisco IronPort Web Usage Controls provide 65 URL categories, and coverage for sites in more than 190 countries and more than 50 languages. The URL categories are:

Adult	Health and Nutrition	Science and Technology
Advertisements	Illegal Activities	Search Engines and Portals
Alcohol and Tobacco	Illegal Drugs	Sex Education and Abortion
Arts and Entertainment	Infrastructure	Shopping
Business and Industry	Instant Messaging	Social Networking
Cheating and Plagiarism	Internet Telephony	Social Science
Child Pornography	Job Search	Society and Culture
Computer Security	Lingerie and Swimsuits	Software Updates
Computers and Internet	Lottery and Sweepstakes	Spiritual Healing
Cults	Mobile Phones	Sports and Recreation
Dating	Nature	Streaming Media
Dining and Drinking	News	Tasteless or Obscene
Education	Non-sexual Nudity	Tattoos
File Transfer Services	Online Communities	Transportation
Filter Avoidance	Online Storage and Backup	Travel
Finance	Online Trading	Violence
Freeware and Shareware	Paranormal and Occult	Weapons
Gambling	Peer File Transfer	Web Hosting
Games	Pornography	Webpage Translation
Government and Law	Real Estate	Web-based Chat
Hacking	Reference	Web-based Email
Hate Speech	Safe for Kids	

SUMMARY

Cisco IronPort Web Usage Controls are the industry-leading solution for enforcing acceptable-use policies for web access, improving visibility into web traffic and raising employee productivity. This powerful solution combines the most accurate URL database with the widest coverage in the industry and real-time dynamic categorization to identify objectionable content hidden in the dark web. The solution is supported by Cisco SIO, which provides unparalleled visibility into global network traffic to provide the most relevant and continuous updates to the URL database. Cisco IronPort Web Usage Controls provide rich policy control and comprehensive reporting. It is integrated into the Cisco IronPort S-Series to provide a complete secure web gateway solution with malware security, rich acceptable use controls, and data security.

CONTACT US

Cisco sales representatives, channel partners, and systems 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 online 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, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco-Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLynx, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

P/N 435-0263-1 10/09