

Cisco IOS Content Filtering

Product Overview

Cisco IOS Content Filtering is a Web security solution that helps organizations protect against known and new Internet threats, improve employee productivity, and enforce business policies for regulatory compliance.

Cisco IOS Content Filtering is ideally suited for small medium businesses and enterprise branch offices that need a scalable, low-maintenance solution.

As employees surf the internet, they expose themselves to websites that are known to give out malware, adware, spyware, and phishing. This not only causes downtime, but also revenue losses. According to an Infonetics Research (2006), nearly 2 percent of revenue losses and 51 percent of downtime costs are due to security costs.

Deployed on Cisco® integrated services routers, Cisco IOS Content Filtering offers category-based productivity and security ratings. Content-aware security ratings protect against malware, malicious code, phishing attacks, and spyware. URL and keyword blocking help to ensure that employees are productive when accessing the Internet. This is a subscription-based hosted solution that leverages Trend Micro's global TrendLabs™ threat database, and is closely integrated with Cisco IOS.

Key Benefits

The Cisco IOS Content Filtering solution reduces network complexity by eliminating the need for a standalone content filtering product. Cisco ISR customers are not required to purchase and manage additional hardware for web filtering which reduces both capital and operational expenses for the organization.

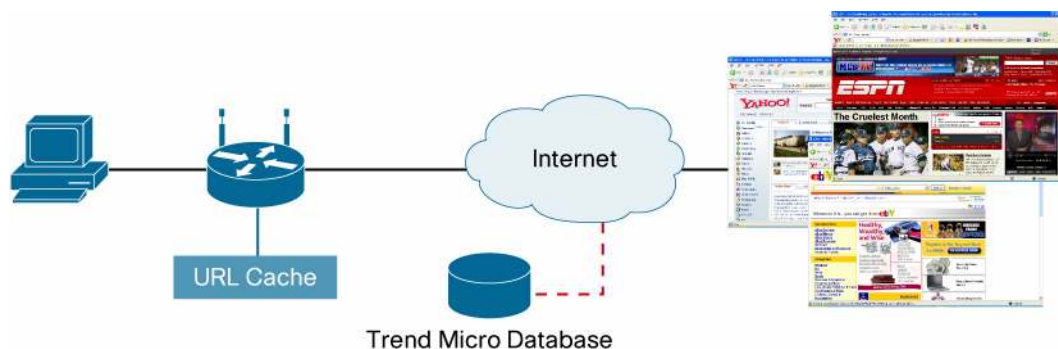
It interoperates with other Cisco IOS Software components such as Cisco IOS Firewall, Cisco IOS IPS, VPN functions, and per-user authentication and authorization to provide outstanding value and benefits:

- Improves employee productivity and reduces organizational risk: Cisco IOS Content Filtering helps organizations restrict Internet use that exposes them to risks such as inappropriate use of company resources, legal liability, and productivity losses.
- Prevents malware exposure: Cisco IOS Content Filtering blocks users from accessing Websites that are known to dispense malicious code (key loggers, adware, Trojans, spyware, phishing, etc.).
- Enforces compliance: Regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), and Children's Internet Protection Act (CIPA) mandate reliable content filtering. Cisco IOS Content Filtering uses industry-leading technology validated by TrendMicro's TrendLabs™, a global network of research centers committed to constant threat surveillance and attack prevention.

- Conserves network resources: Cisco IOS Content Filtering enables an organization to set security policies that limit Internet access. This prevents bandwidth-intensive applications and malware from being downloaded, thereby protecting network resources.
- Eases provisioning and management: Easy-to-use Web-based Cisco Configuration Professional enables rapid deployment of Cisco IOS Content Filtering registration and policies.

Figure 1 shows the components of IOS Content Filtering

Figure 1. IOS Content Filtering Components



Features

Table 1 lists the features and benefits of Cisco IOS Content Filtering.

Table 1. Cisco IOS Content Filtering Features and Benefits

Feature	Benefits
Subscription-Based	Easy-to-renew 1-, 2-, or 3-year subscription-based service is associated to the router platform; no individual user licenses are required. Subscription provides access to Trend Micro's database, with content filtering policies set on the router.
Security-Ratings	Offers protection against a variety of web-based threats, including zero-day attacks. Assesses the security risk posed by a Web site based on analysis from Trend Micro's TrendLabs™. Helps combat phishing and guards against spyware that may send confidential information to hackers and cybercriminals. TrendLabs provides the Security Rating for a given URL based on a combination of past behavior and current exposure to malware, adware, phishing, spyware, and hacking.
Category-Based URL Classification Over 70+ Categories Available	Content-based classification of URLs helps restrict access to objectionable or productivity-affecting Websites (sites focusing on gambling or weapons, for example). Categories for reputation-based blocking (spyware and keylogging, for example) are also available.
Keyword Blocking	Allows blocking of Websites based on selected keywords that occur in the URL.
Black and White List Support	Supports 100 black and 100 white URLs. For example, trusted Websites can be added to a white list.
Management Provisioning	Easy to use and deploy. It is managed through Cisco Configuration Professional, a Web-based router management tool.
Caching	Stores URL categories and their policy decisions (permit or deny) locally on the router, ensuring quick response time to access the Internet. Administrators can configure the cache duration on the router.

Orderability

Support for Cisco IOS Content Filtering begins in Cisco IOS Software Release 12.4(15)XZ. The Content Filtering subscriptions are available in 1-, 2-, or 3-year licenses. A 30-day free trial license is also available. The recommended number of users on Cisco 800 Series Routers is 20. Table 2 lists the available SKUs.

Table 2. SKU Information

Product Number	Description
SL-CNFIL-88x-1Y	1-year Cisco IOS Content Filtering subscription for Cisco 881/888 Routers (URL/Phishing)
SL-CNFIL-8xx-2Y	2-year Cisco IOS Content Filtering subscription for Cisco 881/888 Routers (URL/Phishing)
SL-CNFIL-8xx-3Y	3-year Cisco IOS Content Filtering subscription for Cisco 881/888 Routers (URL/Phishing)
SL-CNFIL-8xx-TRI	30-day free trial license

Platform Support

Table 3 provides platform support information for Cisco IOS Content Filtering.

Platform Support

Product Family	Platforms Supported	Cisco IOS Software Image	Availability
Cisco 800 Series	881, 888	Advanced IP Services	Now
Cisco 800 Series	886, 887, 871, 878, 891, 892	Advanced IP Services	Q3CY08
Cisco 1800 Series	1801, 1802, 1803, 1811, 1812, 1841	Advanced Security or higher	Q3CY08
Cisco 2800 Series	2801, 2811, 2821, 2851	Advanced Security or higher	Q3CY08
Cisco 3800 Series	3825, 3845	Advanced Security or higher	Q3CY08

To Download the Software

Visit the [Cisco Software Center](#) download Cisco IOS Software.

For More Information

For more information about Cisco IOS Content Filtering, visit

<http://www.cisco.com/go/IOSContentFiltering> or contact your local account representative.

For more on Router Security, please visit <http://www.cisco.com/go/routersecurity/>



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.

CCDF, CCVP, Cisco, Cisco StadiumField, the Cisco logo, CSE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play and Learn is a service mark; and Access Registrar, Altran, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCS, 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, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browser, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS IPPhone, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuickStudy, IronPort, the IronPort logo, Lightspeed, Linksys, MediaTone, MeetingPlace, MIM, 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. ©2008