Router-Based Web Filtering

Value-Added Security Services in Cisco IOS Software

At-A-Glance

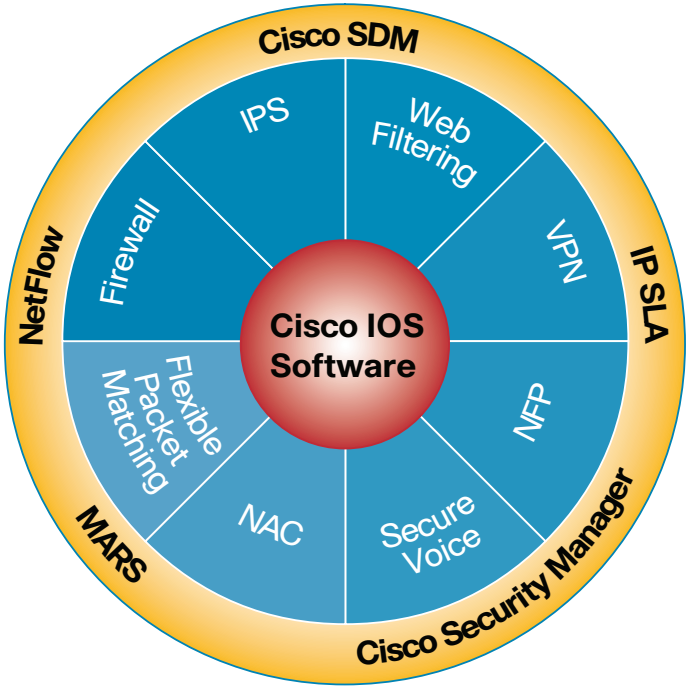
Integrated Router Security Solutions

Comprehensive network security features in Cisco routers help companies protect their infrastructures, devices, and important information, while reducing costs.

Use Cisco IOS® URL Filtering to block access to unwanted URLs in your organization.

For many businesses, Internet surfing is a critical part of conducting business to meet their organizational goals. However, unrestricted Internet usage opens up many risks such as inappropriate use of company resources, exposure to legal liability, and productivity losses. A sizeable number of employees access shopping, gambling, pornography, and auction Websites during work hours, causing unnecessary use of corporate bandwidth. This compels organizations to block access to various Websites, or to restrict access to only Websites that are needed for day-to-day functions.

The Cisco IOS URL Filtering solution monitors and regulates all Internet activities by blocking specific Websites or restricting access to Websites. Cisco IOS URL Filtering is simple and easy to deploy. It is scalable, stable, and fully integrated with Cisco IOS Software.



- Secure filtering capabilities to stop unwanted traffic before it traverses the WAN
- Works with third-party Web filtering servers such as Websense and SmartFilter
- Ease of use: Simplified configuration and URL management using Cisco Router and Security Device Manager (SDM)
- Take advantage of easily available black and white lists from the Internet and use them in Cisco IOS Software as static lists for filtering
- Supports more than 250 allowed and denied URLs within Cisco IOS Software that can be statically configured

Business Challenges	The Cisco Solution
Low Cost of Ownership	Can use existing Cisco integrated services routers in the branch to layer security features and eliminate point products.
Flexibility in Deployment	Can use black and white lists or external filtering servers. Flexible management and deployment with Cisco SDM and Cisco Security Manager.
Service Integration at the Branch	Cisco IOS Software offers numerous services that run on integrated services routers with minimal impact on performance.
Legal and Productivity Issues	Restrict Internet usage with an easy-to-use and deploy URL Filtering Solution

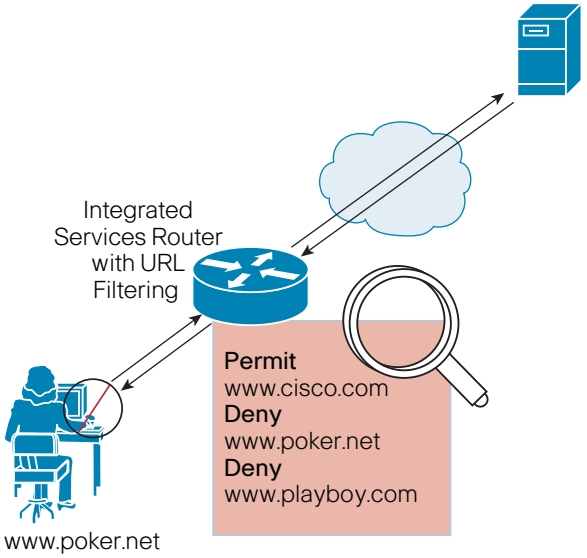
Router-Based Web Filtering

Value-Added Security Services in Cisco IOS Software

Small Office/Home Office Deployment

Cisco IOS URL Filtering is ideal for small branch offices and home offices. A static list of "good" and "bad" URLs can be pushed to a small office/home office router that can monitor Internet activity and allow or disallow access to Websites. Typically, companies disallow access to gaming, pornography, and "hate"-type Websites. Cisco IOS URL Filtering is useful in a split-tunneling scenario where all Internet traffic is sent in the clear and only corporate traffic is encrypted. If company policy is such that all traffic out of the small office/home office is encrypted, Cisco IOS URL Filtering can also be of value—before WAN links are filled up with unwanted traffic, the requests to disallow URLs are dropped at the small office/home office location.

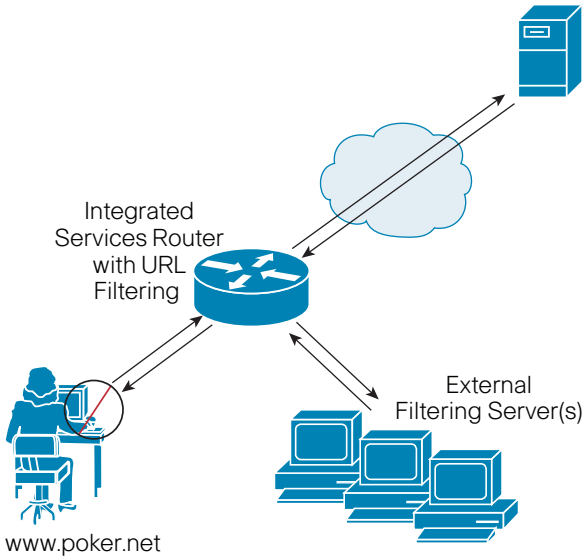
Figure 1. Medium-Sized Branch Office Deployment



Medium Sized Branch Office Deployment

The Cisco IOS URL Filtering engine works with third-party URL filtering servers such as Websense and SmartFilter. Traffic is redirected from the router to a customer-hosted server that runs the Web filtering software, makes Web access grant/deny decisions, and sends them back to the router. The administrator is responsible for the server, the software, and the associated management of the solution.

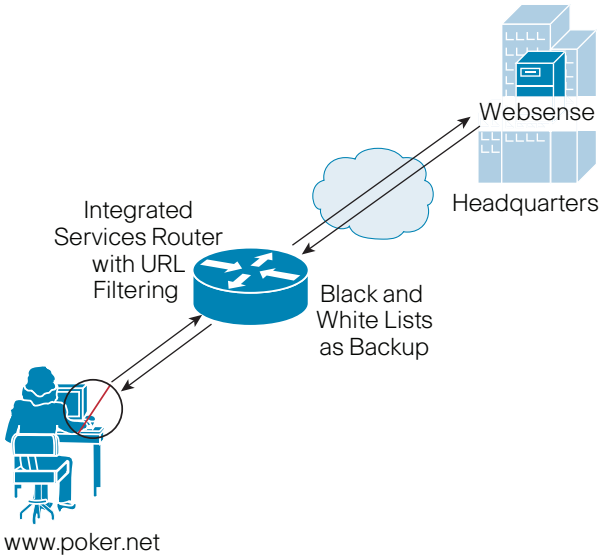
Figure 2. Medium Sized Branch Office Deployment



URL Filtering for the Branch at the Headquarters

Cisco IOS URL Filtering can act as a backup or as a failover mechanism if the third-party URL filtering server is unavailable or unreachable. A third-party URL filtering server such as Websense or N2H2 is present at the headquarters location. Each branch office points to this server at the headquarters for its URL filtering needs. The requests can be cached at the branch itself using Cisco IOS URL Filtering. Additionally, if the URL filtering server is unreachable, the Cisco IOS URL Filtering static list will act as a backup filtering mechanism.

Figure 3. URL Filtering for the Branch at the Headquarters



C45-395549-00 4/07