

Content Filtering

With Integrated Websense for Blue Coat[™] Software



High Performance URL Filtering Solutions for the Enterprise

Countless Internet-based distractions now compete for employee time in the workplace. Non-work related activities including online games, Internet shopping, stock trading, Internet radio, streaming media and MP3 downloads tempt users away from work. Organizations need to minimize legal liability and increase productivity by preventing inappropriate content from being available in the work environment. Schools need to protect children from pornographic or violent content while conserving precious bandwidth resources.

Since 1998, Blue Coat Systems and Websense have partnered to enable organizations to manage, secure and accelerate Web based content. Today, the joint solution integrates the scalability, performance, and protection of award-winning Web security platforms from Blue Coat with high quality URL databases from Websense. The joint solution allows organizations to effectively manage Internet access, reduce costs and ensure availability of Web-based applications. And, because it's an integrated appliance, it is far easier to deploy and manage compared to software products deployed on general purpose servers.

Contact Blue Coat Systems
1.866.30.BCOAT
408.220.2200 Direct
408.220.2250 Fax
www.bluecoat.com

“Blue Coat security appliances combine proxy caching with fine-grained control over Web, Secure Sockets Layer and streaming media traffic. This performance and ease-of-use made it worthy of our World-class award.” - Network World



Websense for Blue Coat[™] enables organizations to:

- Implement effective, accurate URL filtering based on the industry leading database from Websense
- Increase filtering performance and scalability by utilizing an optimized appliance to manage, block and restrict user access to the Web
- Simplify installation, management and administration associated with content filtering applications
- Select between “On-box” and “Off-box” implementations based on the unique needs of the organization
- Implement granular Web access policy based on any combination of users, groups, time of day, location, network address, user agent, and other attributes to meet unique business requirements
- Obtain comprehensive visibility and reporting on Web access throughout the organization via integrated reporting software

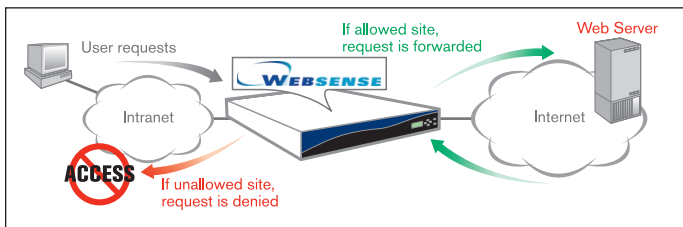
Content Filtering

With Integrated Websense Software

The Web Security Authority.™

Solution Overview

Unlike other content filtering products, the Blue Coat solution is built specifically to manage and filter access to Web content. The foundations of the Web Security Appliance are the patented proxy caching technology and Policy Processing Engine™ - a powerful combination for achieving optimal performance and enforcing granular Web access policies in any enterprise environment. With the integrated Websense for Blue Coat™ software, every Web request is processed using the Websense Master Database – capable of running natively on the Blue Coat security appliance or on a stand-alone server. Comprised of the most frequently accessed sites on the Web, the database includes sites in 44 languages, including English, French, German, Spanish and Japanese. The Master Database contains more than 4 million site postings, representing more than 900 million Web pages. These sites are organized into one of 30 categories allowing for greater customization of an organization's Internet filtering policy. An average of 25,000 additional sites are posted every week. Updates to the Master Database are automatically downloaded on a daily basis, including additions, changes and deletions, so customers are sure the latest database is being used at all times.



The solution allows for granular control and enforcement of Web access policy. For example, an organization may decide all Web sites in category “gambling” should be completely blocked for everyone, while job posting sites may be allowed for only users in the Human Resources department. Additionally, users can be prompted with the corporate use policy each day they access the network and can optionally be allowed access to specified categories only after confirming that they recognize that it is a restricted site and that user-based logs will be maintained. Software-only filtering solutions cannot provide this level of granularity along with the necessary performance, often forcing customers to choose between best-practices policy and acceptable network throughput.

Key Features of Websense for Blue Coat™:

High-quality URL Filtering – Allows organizations to manage, restrict and log access to URL's or content categories through integrated, subscription-based solutions from Websense™.

Policy Processing Engine – Patent-pending system enables sophisticated security policies based on any combination of individual users, groups of users, time of day, location, protocol, user agent, content type and much more.

Visual Policy Manager – Enables point-and-click configuration of URL filtering policies. Administrators can set policies based on user or group information, content type, URL categorization, time of day, location, subnet, user domain and other factors.

Centralized Management – Provides centralized configuration, monitoring and upgrading of Blue Coat appliances throughout the organization.

Coaching – Educate users through customized splash pages that communicate the company's Internet access policy.

Comprehensive Logging and Reporting – Provides complete visibility and reporting to network and security administrators detailing information and all events managed and monitored by the Blue Coat appliances.

Comprehensive Authentication – Supports proxied and transparent user authentication to multiple, diverse back-end authentication directories. Support includes RADIUS, LDAP and NTLM. Network level authentication enables identification of users based on IP address or subnet.

Extensibility – URL filtering deployment can be extended to manage user authentication, streaming bandwidth management, user-based logging, caching, Web virus scanning and content security.