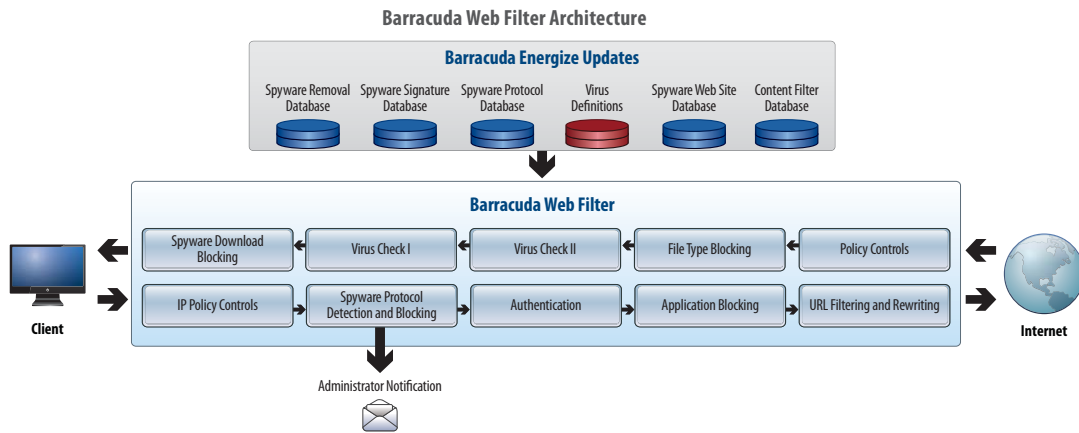




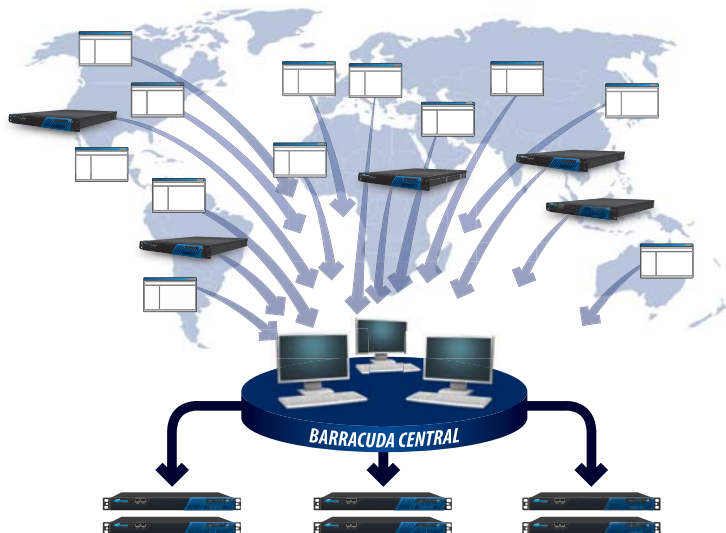
Barracuda Networks Web Filter Technology

The Barracuda Web Filter combines preventative, reactive and proactive measures to form a complete content filtering and anti-malware solution for businesses of all sizes. The Barracuda Web Filter is designed to enforce acceptable Internet usage policies by blocking access to objectionable content and unauthorized Internet applications. At the same time, the Barracuda Web Filter's award-winning feature set enables the Barracuda Web Filter to block spyware downloads, prevent viruses and stop access to spyware Web sites. Barracuda Networks has continually introduced pioneering technology to provide you with the best Web filtering technology at the best value. As a comprehensive solution, the Barracuda Web Filter incorporates award-winning spyware and virus protection with a powerful policy and reporting engine. To ease deployment, the Barracuda Web Filter seamlessly integrates with existing network components and user authentication systems. With industry-leading capabilities and no per user licensing fees, the Barracuda Web Filter provides the most cost-effective defense capabilities in the industry for Web filtering in an easy-to-use appliance.



Comprehensive Web Filtering

Layered Approach: Barracuda Networks' multilayered approach to Web filtering includes a variety of technologies to regulate Web usage and protect against malware. The Barracuda Web Filter gives administrators granular control to manage bandwidth usage, visits to Web sites and use of Internet applications to enforce corporate Internet usage policy. Several layers of defense protect against all forms of harmful traffic between internal clients and the Internet, including HTTP, HTTPS, FTP and application protocols. The measures include: IP-based policy controls, Spyware Protocol Detection and Blocking, User Authentication, Application Protocol Blocking, URL filtering, User/Group-based policy controls, early detection and deep content inspection for Virus Checking, File Type Blocking, Spyware Download Blocking and Desktop Spyware Protection.



Barracuda Central monitors data 24x7 from tens of thousands of collection points and more than 50,000 Barracuda Networks products in over 80 countries and 17 languages. As new threats emerge, Barracuda Central quickly responds to outbreaks and delivers the latest definitions through automatic Barracuda Energize Updates.

Barracuda Central: All Barracuda Networks products are supported by Barracuda Central, a 24x7 advanced security operations center that works continuously to monitor and block the latest Internet threats. Barracuda Central collects emails, URLs and other data from tens of thousands of collection points located in more than 80 countries. In addition, Barracuda Central collects data contributions from more than 50,000 Barracuda Networks customers and analyzes the data collected to develop defenses, rules and signatures to defend your network.

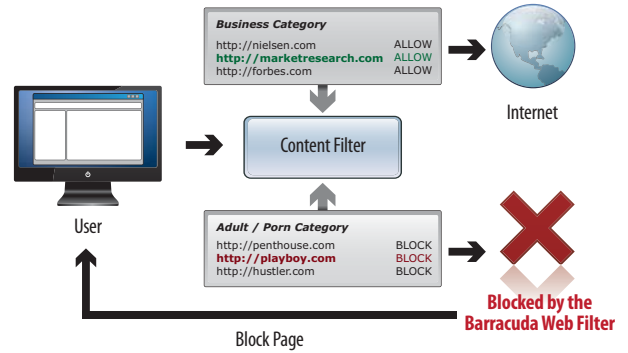
As new threats emerge, Barracuda Central is quick to respond to early outbreaks and delivers the latest definitions through Barracuda Energize Updates. These updates require zero administration and ensure that the Barracuda Web Filter provides comprehensive and accurate protection against the latest Internet threats.

BARRACUDA WEB FILTER

Barracuda Networks Web Filter Technology: A Look Inside

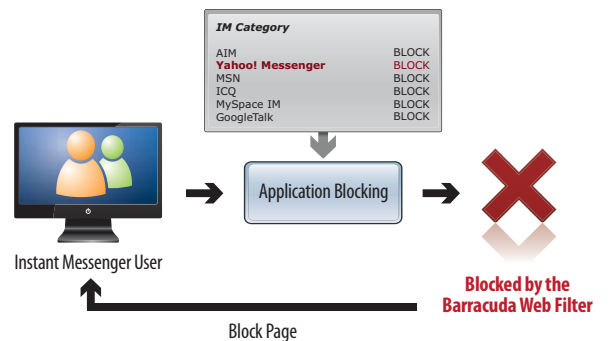
CONTENT FILTERING

Recreational Web browsing adversely impacts employee productivity and exposes the network to malware threats. Barracuda Central maintains a comprehensive database of Web domains organized in 58 categories, that is delivered through Energize Updates. This comprehensive database covers over 99.95% of all Web visits across Barracuda Web Filters worldwide. Administrators can choose to block, accept, warn or monitor access to these domains based on corporate policies. The Barracuda Web Filter can also leverage “safe search” filtering capabilities built into image search engines and automatically rewrite URLs for image searches to restrict objectionable content. These measures enable organizations to boost productivity, optimize bandwidth usage, secure the network and minimize exposure to inappropriate online content.



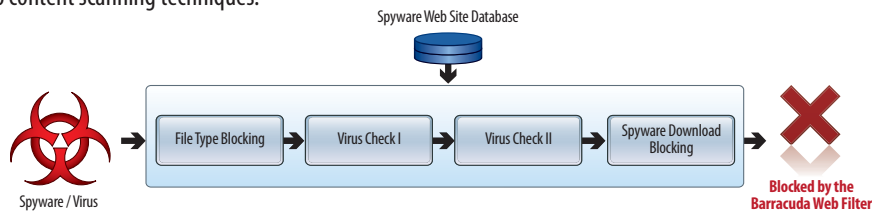
APPLICATION FILTERING

P2P, IM and streaming media applications can be used to spread malware. More effective than a standard HTTP proxy, the Barracuda Web Filter regulates the Internet application usage for public IM clients, Internet music applications, software updaters, Skype and SkypeOut and popular browser toolbars. The Barracuda Web Filter controls most applications by profiling the ports and destination IP addresses used. However, P2P applications, such as Skype, communicate with other peers at varied IP addresses rather than centralized servers and utilize fallback ports used for other protocols, including HTTP and HTTPS. To handle this, the Barracuda Web Filter uses real-time deep packet inspection technology to analyze protocols independent of their port or destination servers. By integrating layer 7 protocol analysis with policy controls, the Barracuda Web Filter enables complete control over application usage.



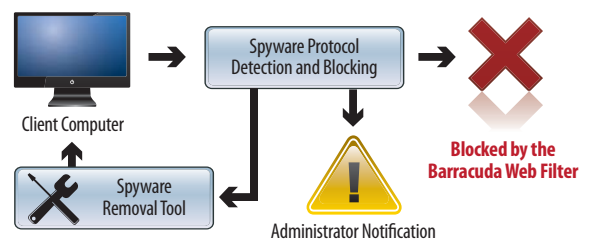
GATEWAY MALWARE PROTECTION

Barracuda Central maintains reputation data on domains associated with spam, phishing and malware. The Barracuda Web Filter's spyware protection engines can detect and block access to and from these sites through a database lookup. Spyware and viruses can also be found in downloads from legitimate sites over HTTP or FTP. The Barracuda Web Filter unpacks and examines individual files within 17 different types of archives for viruses and spyware. It can also be configured to block password-protected archives that may contain harmful payloads. The Barracuda Web Filter scans inbound traffic for spyware, such as keyloggers, Browser Helper Objects, data miners, as well as adware, trojans and viruses. The Barracuda Web Filter's virus engines utilize both signature-based early detection and deep content scanning techniques.



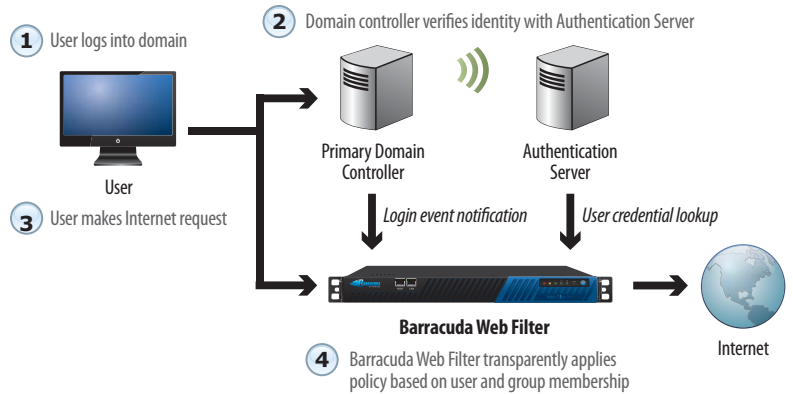
INTEGRATED DESKTOP SPYWARE PROTECTION

From inside the network, the Barracuda Web Filter identifies and blocks communications from infected systems to the Internet. By monitoring traffic at layer 4, the Barracuda Web Filter detects and blocks outbound spyware activity, like phone home or botnets, across all protocols and ports. Once an infected machine is identified, the Barracuda Web Filter intercepts Web browsing sessions and presents the user with the Barracuda Spyware Removal Tool in the form of an ActiveX control. By integrating powerful gateway and desktop spyware protection strategies, the Barracuda Web Filter provides complete security without the need to install client software on each workstation.



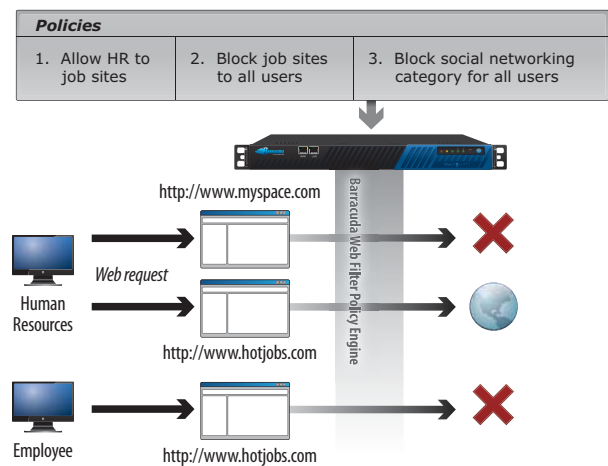
TRANSPARENT USER AUTHENTICATION

By automatically detecting user login events and gathering credentials, the Barracuda Web Filter applies Web filtering policies in real time. The Barracuda Web Filter transparently authenticates domain users by integrating with existing LDAP or NTLM based authentication servers. The Barracuda Web Filter integrates with popular LDAP directory servers, including Microsoft Active Directory, Novell eDirectory and IBM Lotus Domino Directory. By joining the Barracuda Web Filter to an NTLM domain as an authorized host, NTLM users are transparently authenticated to the Barracuda Web Filter using their Microsoft Windows credentials. This is particularly useful in terminal services, Network Address Translation (NAT) or other thin client environments, such as Citrix where multiple client computers share a single IP address.



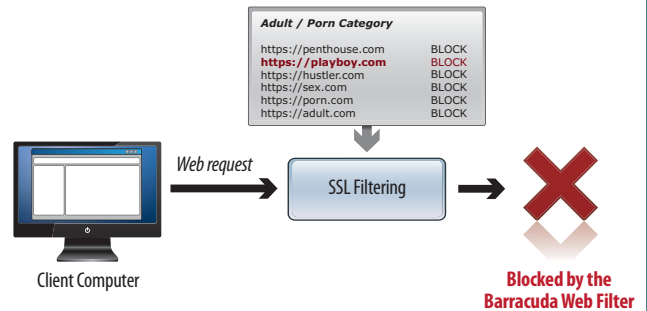
POLICY MANAGEMENT

The Barracuda Web Filter includes a powerful policy engine that supports granular policies by user, group, IP address ranges or time. Separate policies can be applied to domain users (authenticated) and guests (unauthenticated). In addition to built-in content and application categories, the Barracuda Web Filter allows for creation of allow lists ("whitelists") and block lists ("blacklists") to control access to specific domains. Administrators can specify URL patterns using the UNIX regular expression (regex) syntax and restrict downloading files from the Internet based on MIME types, such as executables, streaming media or videos. Administrators can also control Internet access from specific client machines or external servers and applications based on source or destination IP address and ports. In addition, exception rules can be created to override global policies.



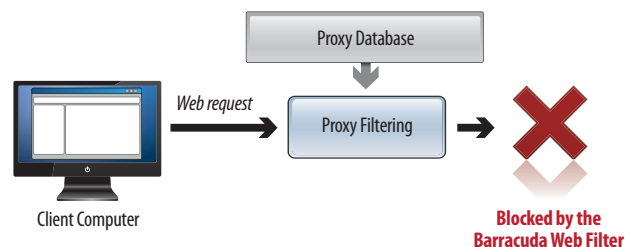
SSL FILTERING

Unlike traditional content filtering techniques that depend on reading URL data, the Barracuda Web Filter can block encrypted SSL traffic at layer 3. Access to HTTP over SSL (HTTPS) Web sites is subject to the same filtering rules and policies applied to HTTP traffic. The Barracuda Web Filter monitors Domain Name System (DNS) traffic generated by HTTPS requests and stores an internal database that maps IP addresses to domain names. Using this database, the Barracuda Web Filter can apply policies based on the IP addresses without the need to actually decrypt the traffic to identify domain names. Since secure content is not decrypted for inspection, this technique ensures that the Barracuda Web Filter does not expose any sensitive data to risk of theft or corruption.



PROXY FILTERING

Anonymous proxies attempt to hide client computer identities and make Internet activity untraceable. Barracuda Central maintains an extensive database of proxy sites that allow anonymous browsing to circumvent content filtering. The Barracuda Web Filter blocks access to these Web sites as part of its content filtering capabilities. In addition the Barracuda Web Filter also blocks anonymous proxy tools as part of its application filtering capabilities.





BARRACUDA WEB FILTER

Barracuda Web Filter Core Technologies



Hardened Operating System: Based on the popular Linux open source kernel that has stood up to scrutiny among security researchers, the Barracuda Web Filter operating system is hardened for maximum security and stability. In addition to internal testing, Barracuda Networks credits the “white hat” research community who continually work with security vendors to uncover and resolve potential vulnerabilities in both the Linux operating system and its associated utilities. While the vast majority of technology in the Barracuda Web Filter is proprietary, Barracuda Networks does leverage secure and functional open source alternatives whenever possible.



Security: Barracuda Central leverages Web crawling technologies, its network of spam collection points and feedback from Barracuda Networks installed base of more than 50,000 customers, to build the most effective database of malware definitions and URLs. With spyware and virus protection at the gateway combined with content and application filtering, the Barracuda Web Filter effectively shields against network threats and helps customers implement security strategies.



Policy: The Barracuda Web Filter is designed to satisfy the diverse needs of small and medium businesses, enterprises, educational institutions and government agencies. The policy management engine of the Barracuda Web Filter supports granular policy at several user levels. It can control Internet access by individuals, groups or machines within the organization based on a combination of criteria. Access lists, IP-based policies and exception rules can be combined and customized to provide maximum flexibility to administrators.



Reporting: The Barracuda Web Filter includes a reporting engine that supports more than 30 types of reports. Unlike solutions that require dedicated reporting clients or database servers, the Barracuda Web Filter reports are generated natively without the need for additional software management. Barracuda Web Filter reports provide comprehensive details about all Web filtering and spyware detection activity. Reports are available on demand or can be scheduled for automatic delivery on a daily, weekly or monthly basis. Besides reports, the Barracuda Web Filter also provides real-time views of content and application filtering activity. The Barracuda Web Filter also records each Web traffic request processed in syslog messages. Syslog messages can be directed to a remote syslog server for further processing.



Clustering and Scalability: The Barracuda Web Filter supports clustering of multiple units for both management and scalability. For centralized management, Barracuda Web Filters link together to share configuration and policy across the cluster and administrators can change policy across the cluster from any unit. Clustered systems can be geographically dispersed and do not need to be collocated on the same network. Barracuda Web Filters can be placed on redundant network paths for High Availability deployments. Barracuda Web Filters also supports the Web Cache Communication Protocol (WCCP). WCCP provides for load balancing, fault tolerance and linear scalability across multiple Barracuda Web Filters. Through these features, the Barracuda Web Filter is equipped to handle needs of the largest enterprise environments.

Barracuda Networks Commitment to Innovation

Barracuda Networks is committed to providing you with the most advanced and comprehensive Web filtering and anti-spyware technology. Through Barracuda Networks proven multilayered approach backed by the dedicated and constant vigilance of the highly-trained engineers at Barracuda Central, the Barracuda Web Filter offers the most sophisticated and effective Web Filtering technology in the industry. For additional information on the technologies outlined here, along with Barracuda Networks latest innovations, visit www.barracuda.com/technology.