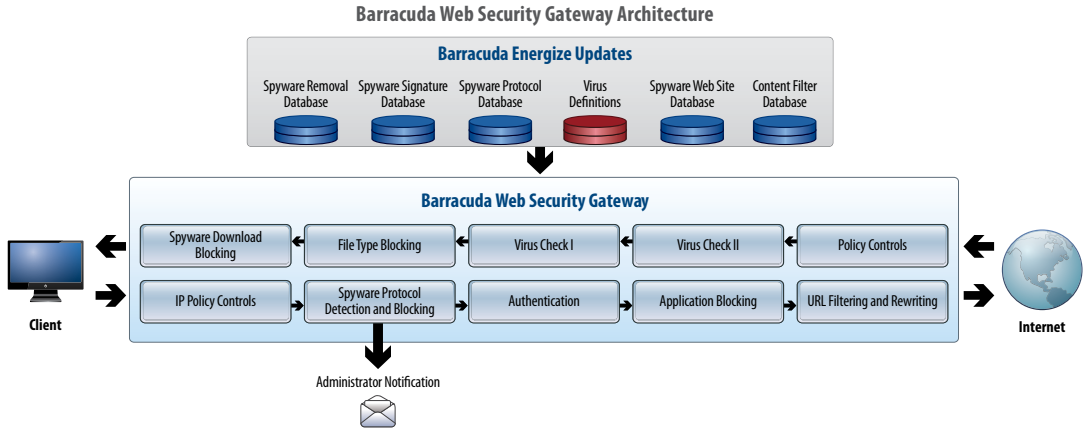
Barracuda

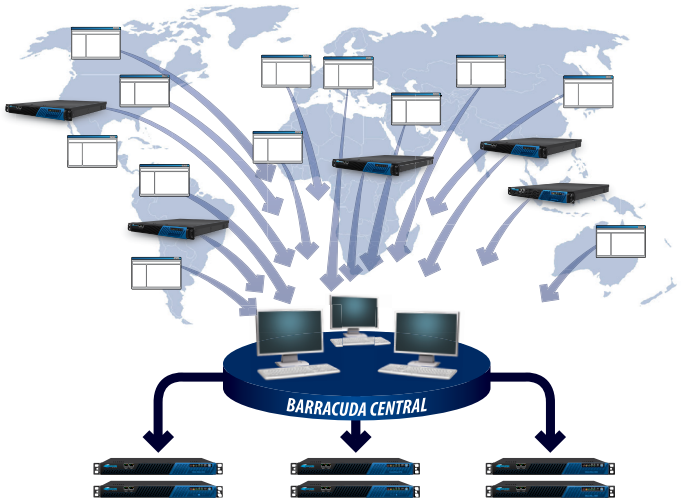
Barracuda Web Security Gateway Technology

The Barracuda Web Security Gateway combines preventative, reactive, and proactive measures to form a complete content filtering and anti-malware solution for businesses of all sizes. The Barracuda Web Security Gateway enforces Internet usage policies by blocking access to objectionable content and unauthorized Internet applications, while its award-winning anti-malware technology blocks spyware downloads, prevents viruses, and blocks requests to malicious websites. To ease deployment, Barracuda Web Security Gateway seamlessly integrates with existing network components and user authentication systems. Web-based threats evolve swiftly, so as new requirements emerge—e.g., social-networking control—the Barracuda Web Security Gateway is automatically updated with new capabilities to meet those requirements, at no extra charge. With industry-leading capabilities and no per-user licensing fees, the Barracuda Web Security Gateway is the most cost-effective solution in the industry.



Comprehensive Web Security Gatewaying

Layered Approach: Barracuda multilayered approach to Web Security Gatewaying includes a variety of technologies to regulate web usage and protect against malware. The Barracuda Web Security Gateway gives administrators granular control to manage bandwidth usage, visits to websites, 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 more than 150,000 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.

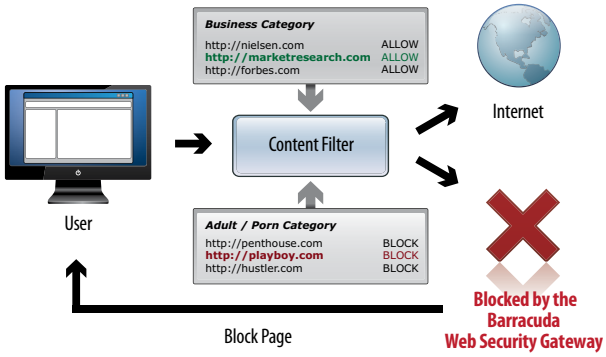
Barracuda Central: All Barracuda Networks products are supported by Barracuda Central, a 24x7 advanced security operations center that works continuously to monitor and block the latest Internet threats. Barracuda Central collects email, URLs, and other data from tens of thousands of collection points located in more than 80 countries. In addition, Barracuda Central gets data contributions from more than 150,000 collection points 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 Security Gateway provides comprehensive and accurate protection against the latest Internet threats.

BARRACUDA WEB SECURITY GATEWAY

Barracuda Networks Web Security Gateway Technology: A Look Inside

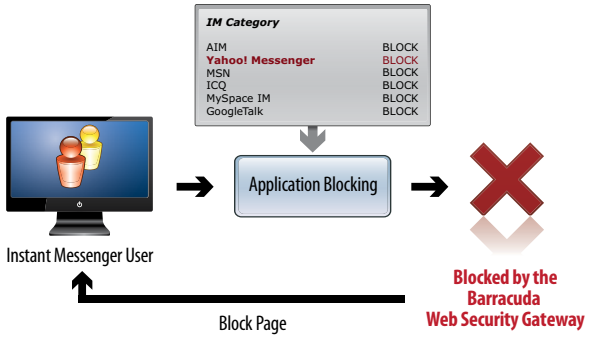
CONTENT FILTERING

Recreational web browsing adversely impacts employee productivity and exposes the network to malware threats. With Barracuda Web Security Gateway, administrators can create policies that control user access to websites using multiple methods, including URL content categories, URL by domain or pattern, and file type blocking. Administrators can choose to block, allow, warn, or monitor access to these domains based on corporate policies.



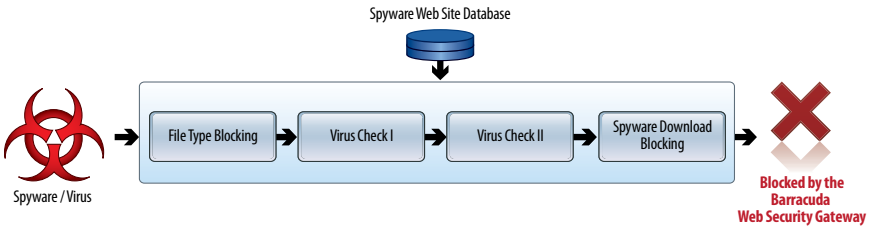
APPLICATION FILTERING

The Barracuda Web Security Gateway provides extremely granular control over Web 2.0 sites and applications, which allows administrators to limit access based on activity type within the same portal. For example, an organization may want to use Facebook or Twitter for viral marketing campaigns but prevent employees from playing games on Facebook or leaking confidential information through Twitter. (Traditional content filtering solutions either completely block or allow unrestricted access to these types of content and web applications.) In addition, administrators can configure the Barracuda Web Security Gateway to archive outbound social media communications, like Facebook posts, tweets, and web-based email, to a message archive solution like the Barracuda Message Archiver. These messages can be searched to comply with HR or litigation requests. This level of functionality allows organizations to provide mission-critical access to Web 2.0 sites while restricting time and bandwidth wasting actions and applications.



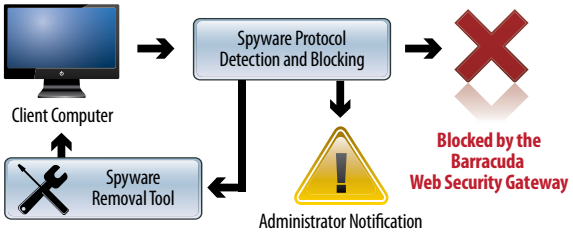
GATEWAY MALWARE PROTECTION

The Barracuda Web Application Filter's spyware protection engine blocks access to blacklisted sites in the extensive, up to date Barracuda Central Database. It also unpacks and examines individual files within 17 different types of archives for viruses and spyware. It can be configured to block password-protected archives that may contain harmful payloads. And, it scans inbound traffic for spyware, adware, trojans, and viruses.



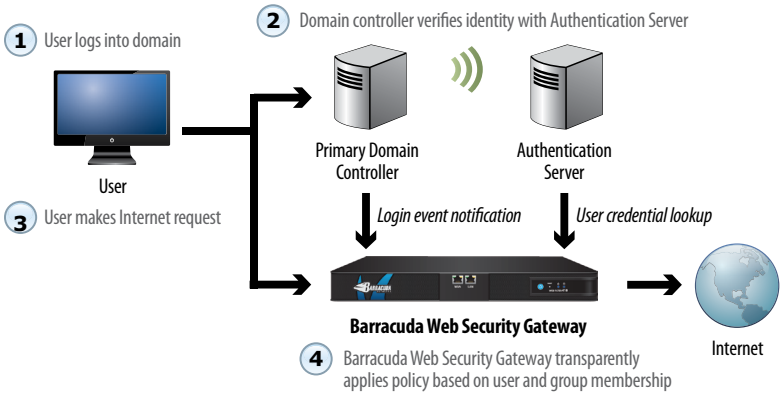
INTEGRATED DESKTOP SPYWARE PROTECTION

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



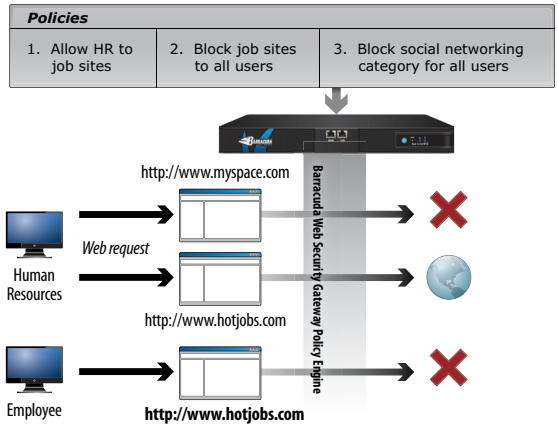
TRANSPARENT USER AUTHENTICATION

The Barracuda Web Security Gateway integrates with popular LDAP servers including Microsoft Active Directory, Novell eDirectory, and IBM Lotus Domino Directory. It transparently authenticates workers using their Windows credentials over NTLM or Kerberos when IP-based authentication is not feasible. This is useful in terminal services, Network Address Translation (NAT), or other thin client environments such as Citrix, where multiple clients share one IP address.



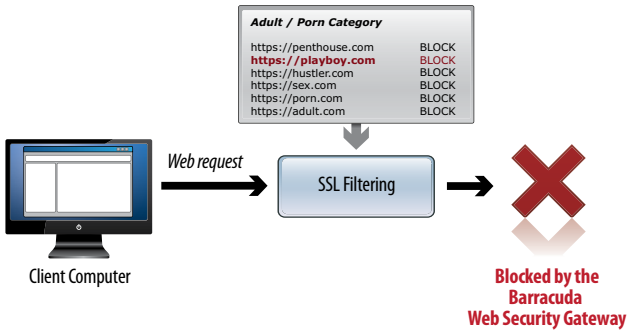
POLICY MANAGEMENT

A powerful policy engine supports granular policies by user, group, IP address ranges, or time. The Barracuda Web Security Gateway allows custom creation of allow and block lists, specification of URL patterns, and restriction of Internet downloads based on MIME type, e.g., executables, streaming media, or videos. Administrators can control Internet access from specific client machines or external servers based on source or destination IP address and ports. In addition, exception rules can be created to override global policies and further refine Internet access policy.



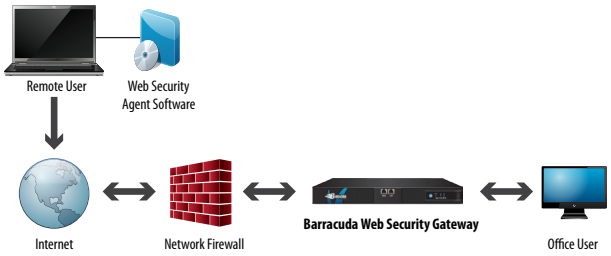
SSL VISIBILITY

The combination of SSL Filtering and SSL Inspection lets customers filter SSL (HTTPS) websites subject to the same filtering rules and policies applied to HTTP traffic. With SSL Filtering, the Barracuda Web Security Gateway 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 Security Gateway can apply policies based on the IP addresses without actually decrypting the traffic to identify domain names. Also, if users require more of granular control, SSL Inspection would decrypt and scan user HTTPS web requests, enabling malware detection and web policy enforcement. It does this by acting as a secure intermediary between user HTTPS web requests and the destination web server (i.e., Facebook, YouTube). After processing, this HTTPS traffic will be re-encrypted on the fly by the Barracuda Web Security Gateway and routed to the destination web server.



REMOTE FILTERING

The Barracuda Web Security Gateway extends protection beyond the network perimeter with the Barracuda Web Security Agent (WSA) and the Barracuda Safe Browser (BSB). The WSA is a tamper-proof client software for off-network Windows and Mac OS X computers, while the BSB is a fully-functional mobile browser for iOS-based devices. In both cases, web traffic from remote clients is filtered through a central Barracuda Web Security Gateway to apply the same web policies to users on and off the network. Both the WSA and the BSB can be centrally configured from the administrator interface. Together, these powerful solutions let organizations implement a consistent web policy across local and distributed workforces without purchasing additional tools.



BARRACUDA WEB SECURITY GATEWAY

Barracuda Web Security Gateway 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 Security Gateway 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 Security Gateway is proprietary, Barracuda Networks does leverage secure and proven 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 150,000 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 Security Gateway effectively shields against network threats and helps customers implement security strategies.

Management: The Barracuda Web Security Gateway is designed to satisfy the diverse needs of small and medium businesses, enterprises, educational institutions, and government agencies. Administrators manage the device through a simple web-based interface. The Barracuda Web Security Gateway's policy management engine 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. The Barracuda Web Security Gateway supports role-based administration through which multiple administrative user accounts can be delegated to specific roles and assigned control over specific users and groups. These user accounts can be restricted to only generating reports or creating policies for specific users or groups of users. Role-based administration lets IT administrators maintain system-level control for security and to delegate policy definition and enforcement to individual departments.

Reporting: The Barracuda Web Security Gateway includes a reporting engine that supports more than 30 types of reports. Unlike solutions that require dedicated reporting clients or database servers, Barracuda Web Security Gateway reports are generated natively without the need for additional software management. These reports provide comprehensive details about all Web Security Gateweying 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 Security Gateway also provides real-time views of content and application filtering activity. Each web traffic request processed is also recorded in syslog messages, which can be directed to a remote syslog server for further processing.

Clustering and Scalability: The Barracuda Web Security Gateway supports clustering of multiple units for both management and scalability. For centralized management, Barracuda Web Security Gateways 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 co-located on the same network. Barracuda Web Security Gateways can be placed on redundant network paths for high availability deployments. Barracuda Web Security Gateway also supports the Web Cache Communication Protocol (WCCP). WCCP provides for load balancing, fault tolerance, and linear scalability across multiple Barracuda Web Security Gateways. Through these features, it's equipped to handle the 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 Security Gatewaying 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 Security Gateway offers the most sophisticated and effective Web Security Gatewaying technology in the industry.

For more information about the Barracuda Web Security Gateway, visit http://www.barracuda.com//products/websecuritygateway