Barracuda Web Security Service Technology

Barracuda Web Security Service is a cloud solution that protects organizations against web-based malware, filters web content and provides visibility about web activity through features for monitoring and reporting. It provides these capabilities through a cloud platform that was purpose-engineered for web security and policy enforcement in highly distributed network environments. Barracuda Web Security Service enforces Internet usage policies by blocking access to undesirable web content and Internet applications while protecting networks against spyware downloads, spyware websites and viruses. By leveraging the cloud, Barracuda Web Security Service provides central management of security and policies for all users regardless of their locations on and off the network including remote locations and mobile users. Barracuda Web Security Service gives administrators clear visibility into web use and security issues then gives them the powerful policy enforcement tools needed to isolate users from Internet threats, conserve network bandwidth and filter web content for compliance and productivity. With award-winning features and a simple pricing model, Barracuda Web Security Service is the easy, affordable way for organizations to provide uniform web security to all users and locations.

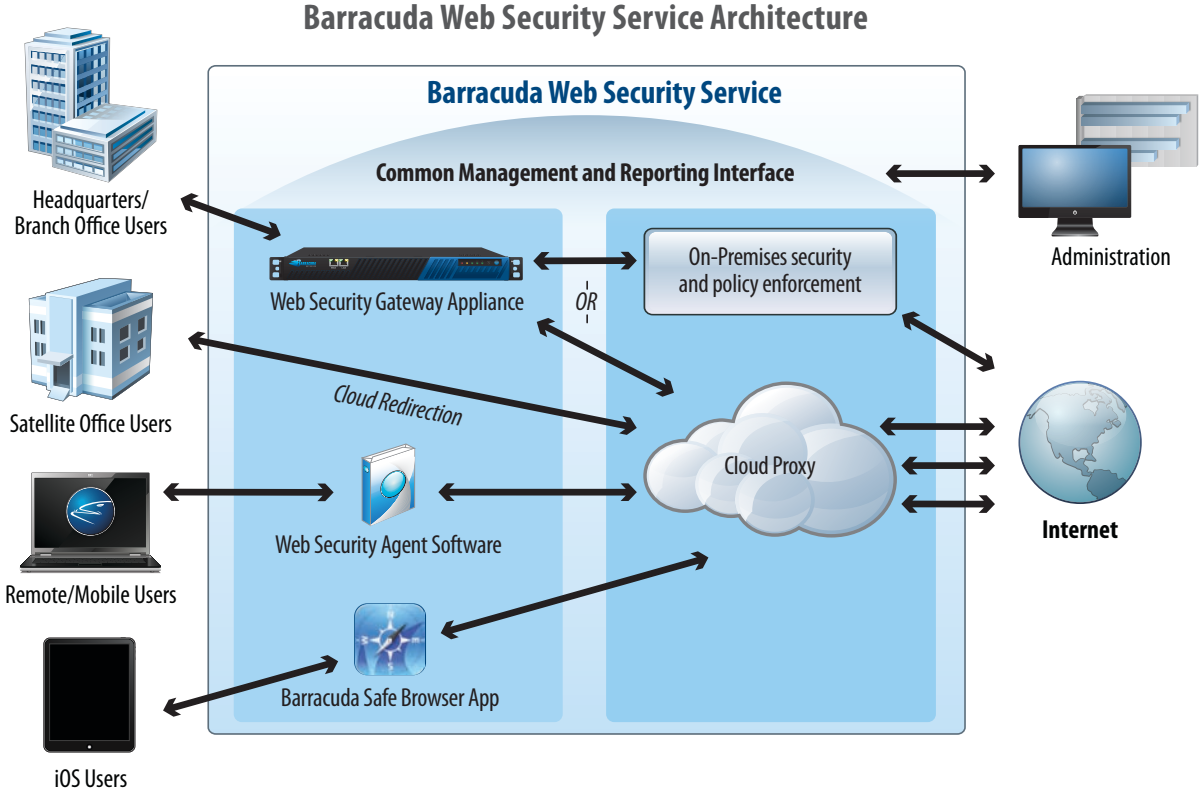
Flexible Deployment

Primarily a cloud service, Barracuda Web Security Service offers a variety of deployment options to perfectly customize web filtering to any network environment. Web traffic can be forwarded directly to the cloud proxy with minimal configuration. Remote users can be filtered using software agents and the new Barracuda Safe Browser app for iPhones and iPads that transparently redirect web traffic to the cloud proxy. Gateway appliances can be optionally deployed to complement the cloud service by providing advanced application control, caching and granular identity management. Barracuda Web Security Service can be deployed using combinations of the cloud service, apps, and gateways with administrators managing all deployment options through a unified management portal in the cloud.

Centralized Management and Reporting

Barracuda Web Security Service's intuitive cloud portal provides centralized control over all aspects of the service. From the portal, administrators can configure web access policies, monitor web use and generate aggregated reports across any number of sites and users. All deployment options are managed through the portal as well. For more granular control, administration can be delegated to users with specific roles (like report generation and policy management) and assigned control over specific users and groups. The cloud-based management framework makes it easy to implement a uniform web security policy in highly distributed environments.

Barracuda Web Security Service Architecture



BARRACUDA WEB SECURITY SERVICE

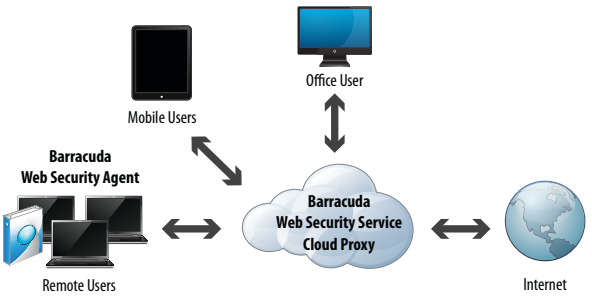
Barracuda Networks Web Security Service Technology: A Look Inside

REAL-TIME THREAT PROTECTION

Barracuda Web Security Service provides several ways to create and enforce granular policies for specific users and groups. Administrators can automatically upload user and group information from their directory servers using the Barracuda Directory Synch Tool or import user data in LDIF files. Domain and remote users can be transparently identified when enforcing policies. Barracuda Web Security Gateways transparently authenticate domain users by integrating with authentication servers on the network. Barracuda Web Security Service gateway appliances integrate with popular LDAP directory servers including Microsoft Active Directory, Novell eDirectory and IBM Lotus Domino Directory. Gateways also support NTLM and Kerberos schemes to authenticate users with their Microsoft Windows credentials. This is particularly useful in terminal services, Network Address Translation (NAT) and other thin client environments such as Citrix where multiple client computers share a single IP address. Also, the Barracuda Web Security Agent and the Barracuda Safe Browser app forward user credentials when redirecting traffic from remote computers to the cloud service. This enforces the same policies whether users are on or off the network.

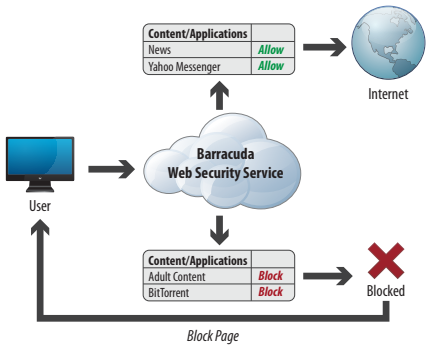
REMOTE AND MOBILE USER FILTERING

Barracuda Web Security Service extends protection to remote and mobile users through the Barracuda Web Security Agent (WSA), a downloadable client installed on off-network Windows and Mac computers. With the WSA installed, web traffic from off-network client computers is transparently filtered through the Barracuda Web Security Service. Web browsing policies applied to users on the network are also enforced on off-network users. In addition to forwarding web traffic, the WSA also provides local control over applications. The WSA can be centrally configured through the cloud portal. It is tamper-proof once installed on client computers. For iPhones and iPads, users can download the Barracuda Safe Browser app. It is a full-featured mobile browser. It enforces policies for user access to web content while providing a secure Internet browsing environment.



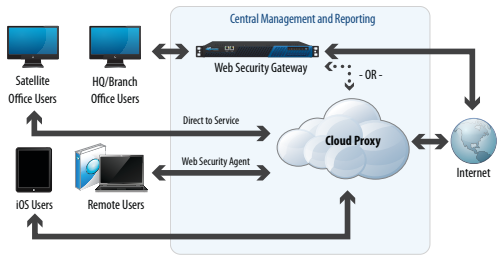
CONTENT FILTERING

Recreational web browsing can degrade employee productivity and expose the network to malware. Barracuda Web Security Service lets administrators regulate access to websites using 95 content categories. Administrators can block, accept, warn or log access to domains based on an organization's policies. Barracuda Web Security Service can use the "safe search" filtering features built into image search engines and automatically rewrite URLs for image searches to restrict objectionable content. Barracuda Web Security Service also regulates access to over 50 web applications such as communication and instant messaging clients, P2P and file-sharing software and streaming media. This control lets organizations boost user productivity, optimize use of bandwidth, secure the network and block exposure to inappropriate content.



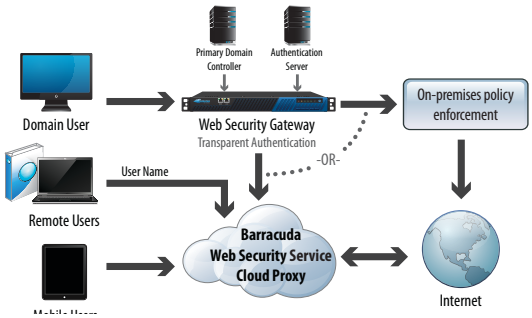
OPTION FOR ON-PREMISES PROTECTION

Barracuda Web Security Service sets the standard for deployment flexibility. Besides the cloud service and agents, it offers the Barracuda Web Security Gateway appliance as an option for on-premises web security. This appliance integrates with network directory services. It also locally caches web content to save bandwidth and provide advanced layer 7 application control. The gateway can provide local security and policy enforcement or forward traffic to the cloud proxy. Administrators manage and configure these gateway appliances through the same central cloud portal as the cloud service and the agents. Gateways can be deployed with the cloud service, safe browser apps and software agents for true hybrid web security.



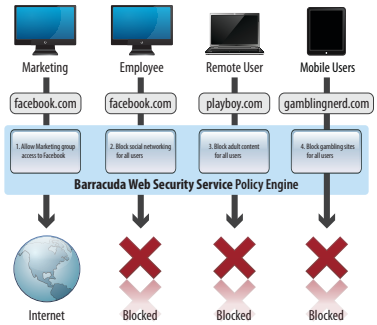
TRANSPARENT USER AUTHENTICATION

Barracuda Web Security Service provides several ways to create and enforce granular policies for specific users and groups. Administrators can automatically upload user and group information from their directory servers using the Barracuda Directory Synch Tool or import user data in LDIF files. Domain and remote users can be transparently identified when enforcing policies. Barracuda Web Security Gateways transparently authenticate domain users by integrating with authentication servers on the network. Barracuda Web Security Service gateway appliances integrate with popular LDAP directory servers including Microsoft Active Directory, Novell eDirectory and IBM Lotus Domino Directory. Gateways also support NTLM and Kerberos schemes to authenticate users with their Microsoft Windows credentials. This is particularly useful in terminal services, Network Address Translation (NAT) and other thin client environments such as Citrix where multiple client computers share a single IP address. Also, the Barracuda Web Security Agent forwards user credentials when redirecting traffic from remote computers to the cloud service. This enforces the same policies whether users are on or off the network.



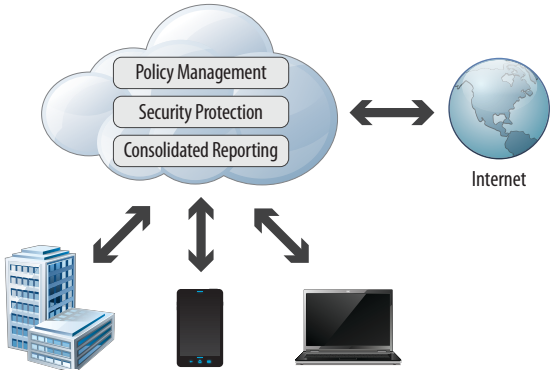
POLICY MANAGEMENT

Barracuda Web Security Service has a powerful policy engine that supports creating granular rules that can be applied to users, groups and IP address ranges. The policy engine's URL categories can be combined with allow lists (whitelists) and block lists (blacklists) to regulate access to websites. Administrators can fine tune access policies by creating complex rules to regulate upload and download of specific content types or file extensions on websites. For example, an administrator can let users access social networking sites, but restrict content uploads. In addition, thresholds for web use can be set based on time factors, connections and bandwidth. Administrators have full control over the rules' order of execution. Administrators can also individualize the user experience with custom block-page messages, email alerts and override passwords.



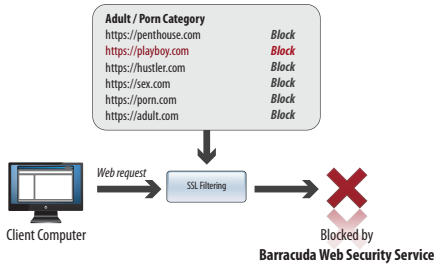
CLOUD-BASED REPORTING

Barracuda Web Security Service provides cloud-based monitoring and reporting for clear visibility into web and threat activity. An interactive dashboard in the cloud UI provides a high-level overview of web use and security across any number of locations and users protected by the service. From the dashboard, administrators can quickly drill down to detailed real-time forensic information about the web activity of specific users. In addition to real-time visibility, Barracuda Web Security Service provides over 50 different reports on all aspects of web use including user activity, time spent, bandwidth and security. Reports can be viewed ad-hoc or scheduled for recurring automatic email delivery. By storing all report and log data securely in the cloud, Barracuda Web Security Service makes it fast and easy to view Internet use aggregated across locations and remote users without any added software or hardware or performing any database administration.



SSL FILTERING

Barracuda Web Security Service filters content in SSL traffic without decrypting it and exposing it to security risks. HTTPS traffic directly proxied to the service is filtered using information in the web request. Alternately, the Barracuda Web Security Gateway monitors Domain Name System (DNS) traffic generated by HTTPS requests and stores an internal database mapping IP addresses to domain names. Using this database, the gateway can apply policies based on the IP address without decrypting the traffic to identify domain names.



BARRACUDA WEB SECURITY SERVICE

Cloud Infrastructure

Barracuda Web Security Service is purpose built as a true SaaS solution on a global, multi-tenant platform that delivers high-performance, high-availability services to users.

1. High Availability

With processing centers on six continents, Barracuda Web Security Service handles billions of web requests every month from customers in more than 50 countries. Barracuda Web Security Service's network infrastructure has redundant, high-speed connections to major Internet backbones for unmatched reliability. The platform includes intelligent route-optimization technology that dynamically identifies the best paths for web traffic. The Barracuda network operations center continuously monitors traffic to and from our data centers as well as the data flow within the data centers. Barracuda Web Security Service's data centers are SAS 70 compliant facilities designed for redundancy, fast disaster recovery and the highest throughputs available.

2. Low Latency

Barracuda Web Security Service's massively scalable, multi-tenant service infrastructure ensures users don't experience delays while web browsing. A blend of traffic processing centers and processing nodes around the world ensure the fastest, most reliable performance in the industry. The processing nodes provide proxies and security scanning while traffic processing centers separately handle reporting and archival logs ensuring high-speed throughput. When users connect to Barracuda Web Security Service, the globally load-balanced architecture automatically routes them to the fastest processing node based on distance and network latency.

3. Data Security

In addition to high availability and low latency, the Barracuda Web Security Service cloud infrastructure provides the highest level of privacy and security. Network and application security is seamlessly integrated into the platform architecture and software. All server-to-server data communications are encrypted with industry standard technologies including secure HTTP and SSL. Data communications between the service and end users can also be SSL protected using certificates signed by industry standard root authorities. The data centers are secured by robust 24x7 physical security.

Barracuda Networks Commitment to Innovation

Barracuda Networks provides the broadest array of web-security technology in the industry with solutions available as dedicated hardware appliances (the Barracuda Web Filter), virtual appliances (the Barracuda Web Filter Vx) as a cloud service (Barracuda Web Security Service) and as a web filter feature integrated with the Barracuda NG Firewall. Barracuda Networks backs these solutions with the industry-leading threat research team at Barracuda Central. Barracuda Networks web security provides the most comprehensive protection against web-based threats for organizations of all sizes. For more information on the technologies outlined here, along with Barracuda Networks latest innovations, visit www.barracuda.com.