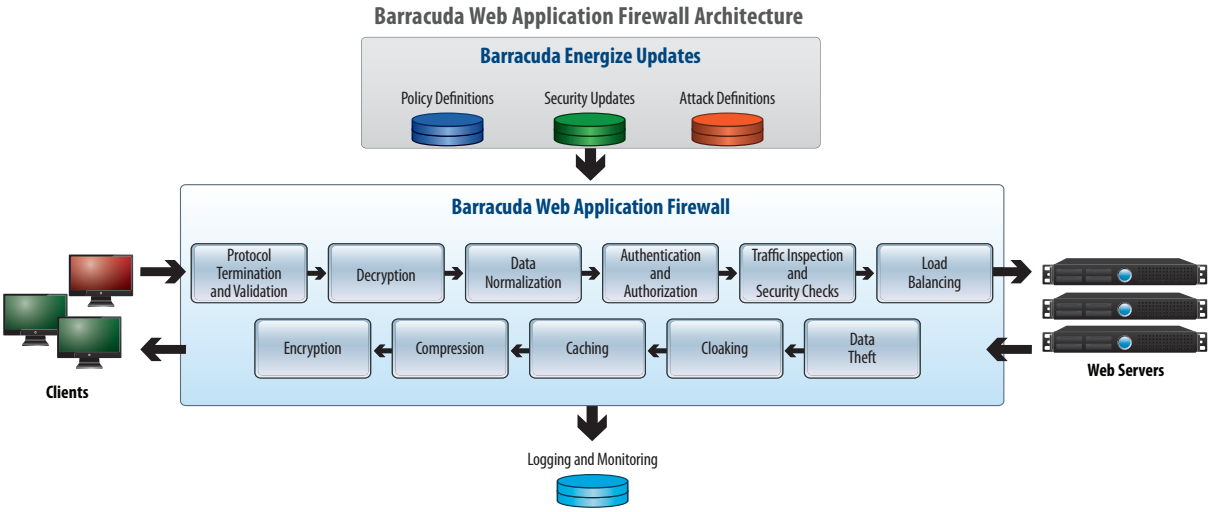
Introduction

The Barracuda Web Application Firewall integrates security, scalability and acceleration technologies to create the next generation application deployment platform for delivering highly secure and scalable Web applications. The application-layer firewall protects Web applications against existing and emerging Layer 7 threats such as Cross Site Scripting, SQL injections and Cross Site Request Forgery. The integrated access control engine enables administrators to deploy their internal applications on the Internet behind a protective layer of security without having to change the application to add additional authentication capabilities. Furthermore, as organizations grow, their deployments can scale by utilizing the built-in traffic distribution capabilities with the help of Layer 4 or Layer 7 load balancing. Beyond load balancing, the Barracuda Web Application Firewall also integrates caching and compression to ensure faster delivery of the Web application content. In addition, the Barracuda Web Application Firewall provides extensive visibility into deployed applications, enabling integration teams to secure and fine-tune the delivery of the application.

Available in five models, the Barracuda Web Application Firewall can be used to securely deploy medium to large applications.



Next Generation Application Delivery Platform

Deployment best practices: The Barracuda Web Application Firewall offers multiple deployment options for maximum flexibility while ensuring complete security. The appliance can be deployed in full reverse proxy, one-armed proxy or bridge modes.

Installing a reverse proxy in front of a server farm is an industry standard best practice for secure application deployment. The Barracuda Web Application Firewall is built on a strong reverse proxy foundation. This deployment enables a clear separation between the network edge and the server farm while ensuring that the internal network is not visible to the external world. In proxy deployments, the Barracuda Web Application Firewall offers multiple application acceleration capabilities such as SSL offloading, which enables servers to process more application logic.

Comprehensive security: As a next generation application delivery platform, the Barracuda Web Application Firewall encompasses all important aspects of application delivery, including security, scalability, availability, acceleration and visibility. The security capabilities of the Barracuda Web Application Firewall are augmented by an extensive network of more than 50,000 sensors that are deployed worldwide and feed into the research being done at Barracuda Labs. This wide array of sensors monitors all threat vectors such as email and Web traffic. The sensors provide valuable data to the security research team to not only build relevant security rules and capabilities, but also to monitor and map threat vectors such as botnets to provide comprehensive security against emerging threats.

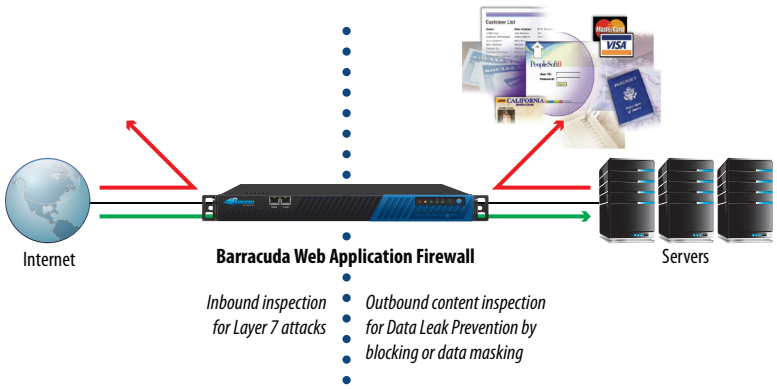
Centralized control with Barracuda Control Center: The Barracuda Control Center is the centralized management platform for all Barracuda Networks products. The Barracuda Control Center acts as the centralized policy *decision* point, while the Barracuda Web Application Firewall acts as the policy *enforcement* point.

The Barracuda Control Center also enables administrators to have an aggregated view of the distributed network via a centralized console. This console can provide aggregated reporting based on data from all of the enforcement endpoints.

Application-Layer Security

Input validation: Lack of proper input validation is one of the prime culprits in Layer 7 security vulnerabilities. The Barracuda Web Application Firewall provides a layered approach to enforcing validation on client side inputs. It decrypts all encrypted traffic and normalizes the inputs to ensure that all data can be inspected and that invalid content in not smuggled to the servers using different encoding techniques. The Barracuda Web Application Firewall provides secures applications using HTTP, HTTPS or FTP protocols.

Tampering protection: Modifying form parameters marked as read-only or hidden parameters or cookies is one more way of attacking an application. The Barracuda Web Application Firewall can encrypt or digitally sign application cookies to protect them from client side modification. Form parameters marked as 'read-only' or 'hidden' can also be protected using digital signing techniques to protect them from being modified by the client.



Anti-virus and malware protection: Web applications that allow files to be uploaded can also utilize the built-in anti-virus and anti-malware scanner to ensure that infected files are not uploaded to the Web application.

Brute Force protection: Guessing passwords to gain access is a very old hacking technique, yet many applications do not provide security against this type of attack. The Barracuda Web Application Firewall tracks user access to restricted resources and blocks clients if the server does not accept the supplied credentials.

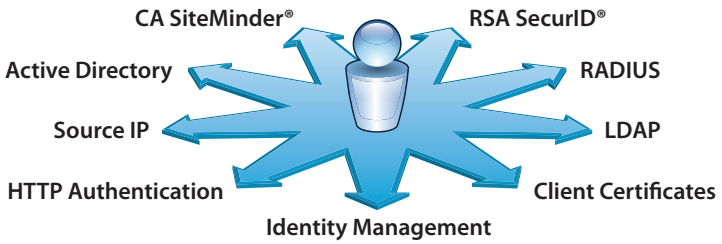
XML / Web Services protection: Service Oriented Architectures (SOA) with Web Services are used to build large, distributed and scalable applications. These applications, along with many Web 2.0 based applications, use XML for transferring data between servers and between clients and servers. The XML firewall built into the Barracuda Web Application Firewall provides protection for such XML data transfer between servers or between client and servers. The Barracuda Web Application Firewall enforces structure on Web services and XML data interchange using WSDL and XML Schema.

Outbound content inspection: In addition to inbound content inspection, the Barracuda Web Application Firewall also offers outbound content inspection. The Barracuda Web Application Firewall cloaking capability strips out all server related information such as server headers and server banners. Denying information about the server infrastructure restricts the attacker's ability to tune their attacks based on the type of Web servers or databases being used. The Barracuda Web Application Firewall can also prevent data leakage by either completely blocking responses containing sensitive information such as credit card numbers or by masking the sensitive information.

Access Control

Authentication: In many cases, authentication is required before a client is given access to an application. This authentication can either be built into the application itself or this functionality can be offloaded on to the Barracuda Web Application Firewall.

The Barracuda Web Application Firewall integrates with any user database using LDAP or RADIUS to authenticate a user's credentials before granting access to the secured resources.



Authorization: Authenticated users can be granted different access privileges by applying access control rules. These privileges can be based on a user's accounts or on the group to which the user belongs.

Two-factor authentication: Password-based security can be augmented by using client certificates or security tokens. The Barracuda Web Application Firewall integrates with RSA SecurID and client certificates to provide this extended layer of security.

Single Sign On (SSO): For a group of applications that need client authentication before granting access, single sign on is used to provide clients with one seamless authentication system, whereby the client logs in once and their identity is propagated to all applications in the group. The Barracuda Web Application Firewall integrates with CA SiteMinder to enable administrators to build a single sign on portal for all of their Web applications.

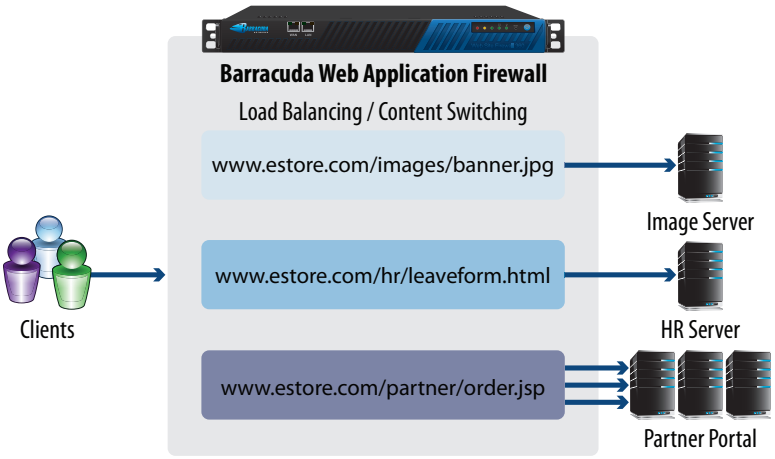
Scaling the Application Infrastructure

The Barracuda Web Application Firewall provides significant capabilities that enable organizations to scale their application deployment infrastructure.

Load balancing: Availability of multiple servers is monitored with the help of an integrated application monitoring module. The built-in load balancing module distributes incoming traffic across the available servers using one of many available algorithms, such as Weighted Round Robin or Least Connections. Traffic can be distributed at Layer 4 or at Layer 7.

Layer 7 content routing: The Barracuda Web Application Firewall provides enormous flexibility while deploying large applications in which each application module can be deployed on multiple servers. Requested content such as the URL of the module, HTTP Headers and parameters, is used to route content to the correct set of servers.

SSL offloading: Web servers hosting HTTPS Web sites require a significant amount of processing power in handling SSL encryption / decryption, as compared to actually serving Web pages or processing Web forms. The Barracuda Web Application Firewall provides SSL offloading capabilities, thereby freeing up the processing power of the servers and making them more efficient.



Instant SSL: As the work force becomes distributed, organizations find the need to expose their internal applications via the Web. Most of these applications are not deployed securely. Using the Instant SSL capability of the Barracuda Web Application Firewall, deployment teams can convert their HTTP based applications to HTTPS with having to touch the application code.

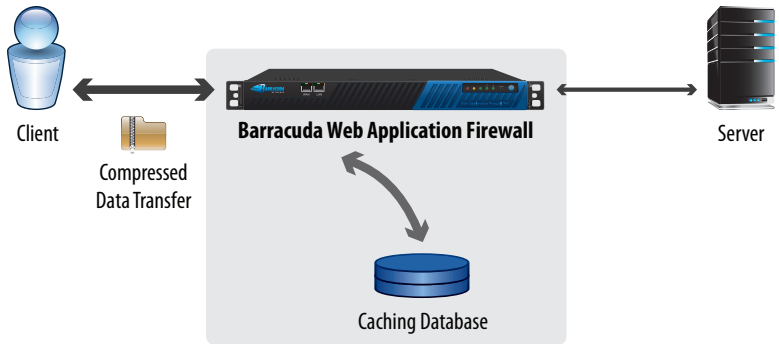
Rate control: The magnitude of threats faced by Internet facing Web applications is compounded due to the distributed nature of some attacks. In this environment, it is important that Web applications protect themselves against rate-based attacks which overwhelm applications, resulting in denial of service (DOS). The Barracuda Web Application Firewall can control the number of application sessions being created or how many times a client can access a given resource. These measures, in conjunction with other rate control techniques such as client queuing, protect Web applications from application-level denial of service attacks.

Accelerating application delivery

Caching: The Barracuda Web Application Firewall speeds up application response time by caching static content and using it to respond to repeated requests for the same content. Caching rules can be tuned based on URL space, file size or file type.

Compression: The integrated compression engine in the Barracuda Web Application Firewall compresses data as it is sent out to the client. This capability is extremely useful in low bandwidth situations and makes application delivery faster.

Protocol tuning: The Barracuda Web Application firewall employs multiple techniques such as connection-pooling and TCP multiplexing to optimize protocol performance. Connection pooling techniques enable Barracuda Web Application Firewall to cut down the overhead associated with creating and terminating connections, thereby cutting the time it takes to respond to client requests.



BARRACUDA WEB APPLICATION FIREWALL

Barracuda Web Application Firewall Core Technologies

Hardened operating system: Based on the Linux open source kernel, which has stood up to the scrutiny of security researchers over time, the Barracuda Web Application Firewall 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 Barracuda Web Application Firewall technology is proprietary, Barracuda Networks does leverage secure and functional open source alternatives whenever possible.

Security: Barracuda Labs maintains a large network of proxy honey pots to gather information about botnets and emerging Web threats worldwide. In addition, customers of other Barracuda Networks products can "opt-in" to report threat data to create a large and distributed data collection network. The data collected from this global network of sensors is applied to tune security policies and also to track and secure against evolving attacks.

Granular control: Starting with baseline security, the Barracuda Web Application Firewall allows administrators to tune the configuration settings at different levels of granularity. The administrators can configure rules that affect the entire application, a section of the application or even a specific URL. These granular rules can be created utilizing the extremely flexible content matching algorithms with an extensive list of security controls.

Logging and reporting: The Barracuda Web Application Firewall's extensive logging and reporting capability empowers administrators and Web application teams to tune and secure their Web applications. The built in reporting engine provides summarized reports on various aspects of the deployments such as traffic statistics, attack reports and compliance related reports. The logs can be exported out to external logging systems and are completely documented to ease the integration with available SIEM products.

Adaptive profiling: The built-in profiling engine continuously evaluates traffic passing through the Barracuda Web Application Firewall. The profiler can create a complete application profile consisting of all URLs, forms and parameters to ensure a comprehensive positive security model. In addition, the Barracuda Web Application Firewall also profiles traffic violations triggered by the configured rule set and uses the heuristics-driven exception profiling engine to create recommendations for tuning the existing rule set. This heuristics-driven model creates a very tight feedback mechanism for tuning security policies.

Role-based administration: Barracuda Web Application Firewall management tasks can be delegated with role-based administration. The system ships with multiple built-in roles such as administrator, auditor, network manager and application manager. These roles can be customized or others can be added to meet the requirements of the organization.

For questions about the Barracuda Web Application Firewall, please visit http://www.barracuda.com/waf or call Barracuda Networks for a free 30-day evaluation at 1-888-ANTI-SPAM or +1 408-342-5400. For more information on our other security and productivity solutions, please visit http://www.barracuda.com/products.

US 1.0