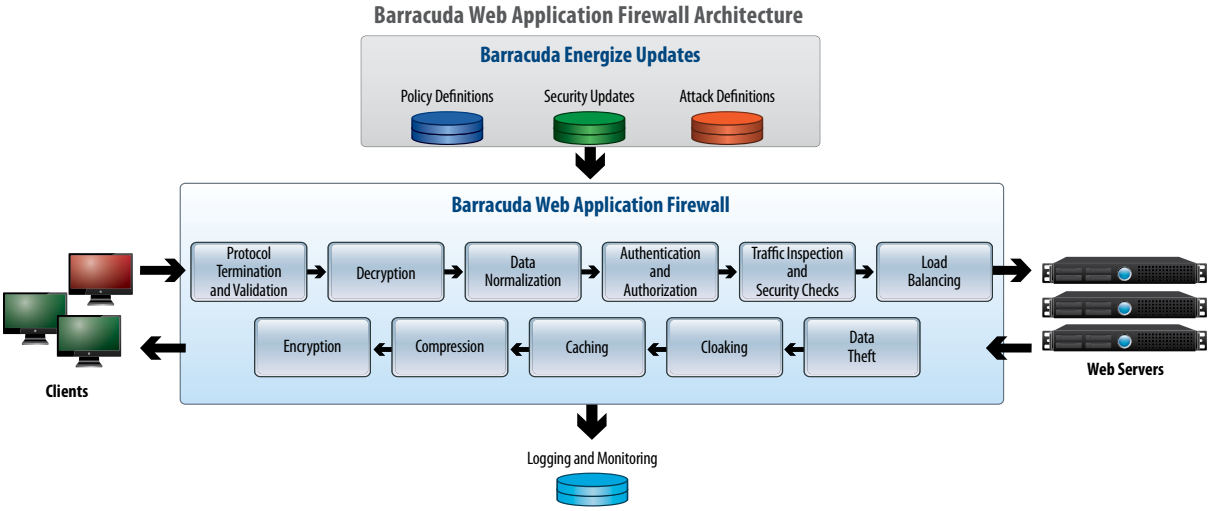
Barracuda

Introduction

The Barracuda Web Application Firewall integrates security, scalability and application acceleration into a next generation Application Delivery Controller (ADC) platform for highly secure and scalable web applications. Its **application-layer firewall** protects web applications against existing and emerging Layer 7 threats such as Cross Site Scripting (XSS), SQL injections (SQLi) and Cross Site Request Forgery (CSRF). The **integrated access control engine** enables administrators to create granular access control policies for Authentication Authorization & Accounting (AAA) without having to change the application. The onboard **L4/L7 Load Balancing** capabilities enable organizations to quickly add backend servers to scale deployments as they grow. Its **application acceleration** capabilities like SSL Offloading, caching, compression, and connection pooling to ensure faster application delivery of the web application content.

Available in five models, the Barracuda Web Application Firewall can be used to securely deploy applications of any size.



Value Proposition

Web Application Security
- Inbound Attack Protection
- Outbound Data Theft Protection
- Integrated Anti-Virus Scanning

Application Delivery
- L4/L7 Load Balancing
- SSL Offloading
- HTTP Caching & Compression

Authentication, Authorization, Accounting (AAA)
- LDAP, RADIUS integration
- Single Sign On (SSO)
- Two-Factor Authentication

Mature Product
- 10+ Years of WAF Experience
- Thousands of customer deployments Worldwide
- Built Ground Up for Security & architected for Reverse-Proxy Deployment

Next Generation Application Delivery Platform

Flexible Deployment: The Barracuda Web Application Firewall offers multiple deployment options for maximum flexibility while ensuring complete security. Built ground up for full reverse proxy deployments, the Barracuda Web Application Firewall insures maximum security and application acceleration in the industry accepted best practice for secure application deployment. In addition to reverse proxy, the appliance can be deployed in one-armed proxy or bridge modes. An inbuilt FIPS 140-2 Level 2 HSM model provides regulatory compliance in the strictest environments.

IPv6/IPv4 Capable: The Barracuda Web Applications Firewall is IPv6 ready, offering easy integration into IPv6 or mixed IPv4/IPv6 environments. This gives organizations the flexibility to use the Barracuda Web Application Firewall as an IPv6 gateway while keeping it internal servers on IPv4 until it is ready for full end-to-end IPv6 networks.

BARRACUDA WEB APPLICATION FIREWALL

Comprehensive security: The Barracuda Web Application Firewall provides unparalleled application security to help organizations secure critical web assets. The security capabilities of the Barracuda Web Application Firewall are further augmented by an extensive network of more than 150,000 sensors that are deployed worldwide and feed into Barracuda Labs. The sensors provide valuable data to the security research team to build new security definitions and automatically update Barracuda Web Application Firewalls in the field.

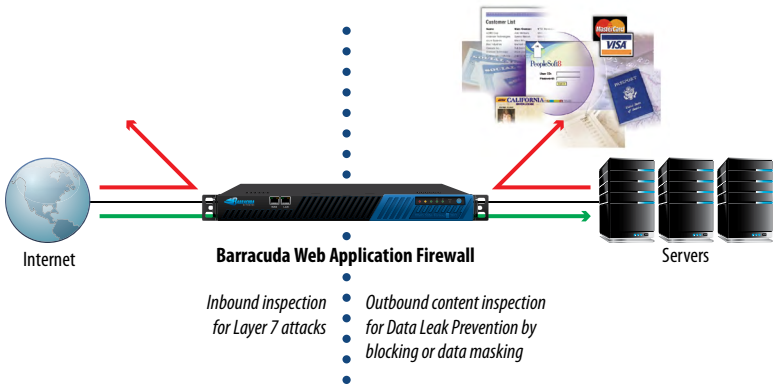
Centralized control with Barracuda Control Center: The Barracuda Control Center is the centralized management platform for all Barracuda Networks products. The Barracuda Control Center acts as the centralized policy decision point, while the Barracuda Web Application Firewall acts as the policy enforcement 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 decrypts all encrypted traffic and normalizes inputs to ensure that all data is inspected and validated against known attack patterns before sending to the backend servers. Protocol Validation allows administrators to enforce protocol versions or verbs for HTTP, HTTPS, FTP or FTPS.

Cloaking: 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, Operating System, or databases being used.

Session Tampering Protection: Most applications use cookies or hidden, read-only parameters for application session state and other sensitive information. The Barracuda Web Application Firewall can encrypt or sign these tokens to prevent third party impersonation attacks.



Session Riding and Clickjacking Protection: Third party sites can employ malicious JavaScript that exploits the servers trust with the user's browser. The Barracuda Web Application Firewall blocks such attacks by generating unique tokens or injection anti-UI redressing measures to prevent malicious JavaScript from attacks like Session Riding or Clickjacking.

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.

Layer 7 DDoS Protection: Distributed Denial of Service attacks (DDoS) attacks have moved to the application layer as they provide higher impact compared to network layer DDoS. Due to its complete visibility into application layer constructs, the Barracuda Web Application Firewall can intelligently fingerprint and throttle these attacks and ensure that the protected web applications continue to service genuine users.

Brute Force protection: The Barracuda Web Application Firewall tracks user access to restricted resources and blocks clients if the server does not accept the supplied credentials. Additional rate controlling mechanisms in the Barracuda Web Application Firewall provide additional layer of security against brute force attempts.

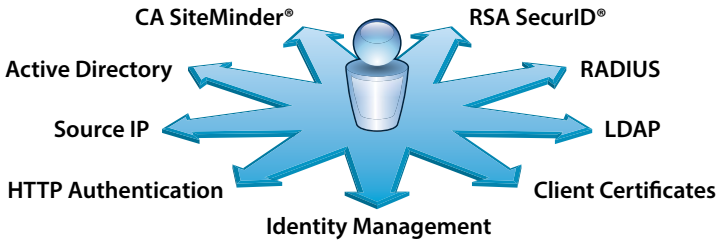
XML / Web Services protection: Service Oriented Architectures (SOA) with web services is used to build large, distributed and scalable applications. These applications, along with many Web 2.0 based applications, use XML for transferring data between servers and between clients and servers. The XML Firewall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

Data Loss Protection: In addition to inbound content inspection, the Barracuda Web Application Firewall also offers outbound content inspection for Data Loss Prevention. The Barracuda Web Application Firewall prevents data leakage by either masking or blocking responses containing sensitive information such as credit card numbers or any other custom data patterns.

Access Control

Authentication: 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. This allows administrators to add an authentication layer or to offload an existing application authentication policy to the Barracuda Web Application Firewall.

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.

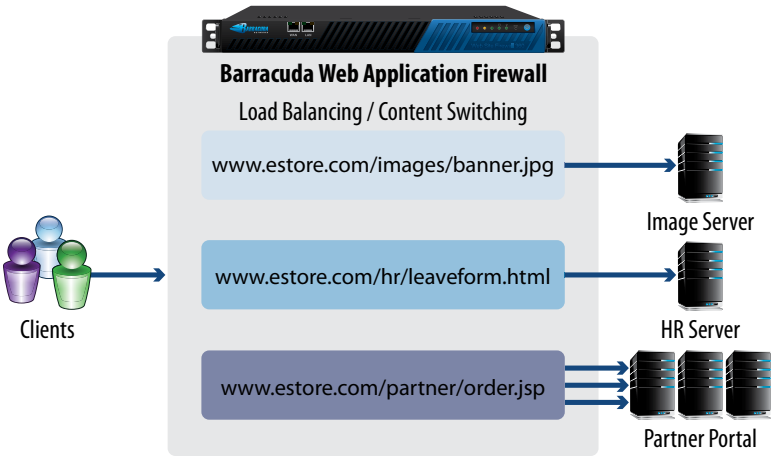
Single Sign On (SSO): For a group of applications that need client authentication before granting access, single sign on is used to provide clients with one seamless authentication system, whereby the client logs in once and their identity is propagated to all applications in the group. The Barracuda 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: 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. Availability of multiple servers is monitored with the help of an integrated application monitoring module. 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 websites require a significant amount of processing power in handling SSL encryption / decryption. 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: Using the Instant SSL capability of the Barracuda Web Application Firewall, deployment teams can convert their HTTP based applications to HTTPS without having to touch the application code.

Rate control: The Barracuda Web Application Firewall can control the number of application sessions being created and/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 (DoS) 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.

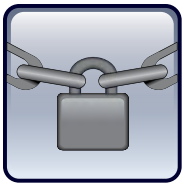
Compression: The integrated compression engine in the Barracuda Web Application Firewall compresses data as it is sent out to the client. This capability is extremely useful in low bandwidth situations and makes application delivery faster.

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.