



The Barracuda Web Application
Firewall Advantages

White Paper

#1 Web Application Firewall Solution

The Barracuda Web Application Firewall is the industry's most highly rated, security-focused Application Delivery Controller (ADC) platform. Gartner cites the Barracuda Web Application Firewall's strong security-focused capabilities and affordable pricing as a key differentiator in their 2010 ADC Magic Quadrant vendor profile. SC Magazine rates the Barracuda Web Application Firewall as the 2011 Best Buy.

Value Proposition

Comprehensive Protection <ul style="list-style-type: none">• Extensive inbound protection• Outbound Data Theft Protection• Integrated Anti-Virus Scanning• Integrated Authentication, Authorization	Easy Management & Administration <ul style="list-style-type: none">• Up and running in less than a couple of days• Centralized management via Barracuda Control Center (BCC)• Automated updates from Barracuda Central
Enhanced Application Delivery <ul style="list-style-type: none">• Load Balancing• SSL Offloading• Application Acceleration	Barracuda Advantage <ul style="list-style-type: none">• Mature Product w/ 10+ Years of R&D• Thousands of customer deployments Worldwide• No additional server or license fees

Key Features

<ul style="list-style-type: none">• Built Ground Up for Security & architected for Reverse-Proxy Deployment• PCI-DSS Certified by ICSA Labs• FIPS 140-2 compliant Model 963• HTTP/HTTPS/FTP Protocol Validation• OWASP Top Ten Protection• Distributed Denial of Service (DDoS) Protection• L4/L7 Load Balancing	<ul style="list-style-type: none">• Integrated Anti-Virus Scanning on file uploads• Vulnerability Scanning Integration• LDAP/RADIUS integration• Two-factor authentication with RSA SecurID or client certificates• XML Firewall• HTTP Caching & Compression• Granular logging, Monitoring & Reporting
--	--

Feature Insights

Comprehensive Protection

Barracuda Web Application Firewalls provide an extensive set of functionality to protect Web applications from attacks. These include:

- **Code injection protection:** The Barracuda Web Application Firewall inspects each input parameter to ensure that the submitted data does not contain SQL injection, OS commands, directory traversal code, malicious scripts or any other code injection patterns.
- **Form input protection:** Administrators can set detailed rules to control user input. These include the ability to validate parameter types, input sizes, input characters and other form input values. This protects against SQL injection attacks, overflow attacks, and other attacks that target form inputs.
- **Server cloaking:** Most attackers start by gathering information about the underlying infrastructure used by the target Web site to find weakness. The Barracuda Web Application Firewall suppresses identifiable server information in web application responses, thereby cloaking backend servers from external inquiry.
- **Data theft protection:** For applications that work with sensitive data like credit card information or social security numbers, the Barracuda Web Application Firewall can be configured to inspect outgoing data and to either mask sensitive information or to block the entire response. This helps prevent data leakage and ensures compliance with regulations such as PCI-DSS or HIPAA.
- **Request forgery protection:** The Barracuda Web Application Firewall prevents cross-site request forgery (CSRF) and other forgery attacks by adding randomized tokens to web forms. It can also limit requests to sensitive pages based on referring Web pages. Together these help identify and block unsolicited requests from spoofing clients.
- **Denial of Service Protection:** The Barracuda Web Application Firewall has session monitoring capabilities that can identify and protect against Denial of Service attacks. Administrators can limit the number of sessions originating from a particular client IP address to prevent attackers from overwhelming Web applications with bogus requests.

- **IP Reputation:** The Barracuda Web Application Firewall can leverage historical and contextual information about the clients to apply security policies as required. It provides geo-awareness, integrates with Barracuda Reputation Blocklist, can identify requests coming from Anonymous Proxies, Satellite ISPs as well as TOR nodes.
- **Client fingerprinting and CAPTCHA Integration:** Malicious clients and bots attempting to DoS the applications can be fingerprinted using client side scripting and controls. Suspicious clients are challenged with a CAPTCHA to prove that they are human and not automated bots.
- **Tampering protection:** The Barracuda Web Application Firewall can set form parameters as 'read-only' or 'hidden' to protect against unauthorized alteration. It can also encrypt or digitally sign cookies to protect them from modification. This protects applications like online shopping or net banking applications from unauthorized tampering.
- **Brute force protection:** Attackers often use brute-force dictionary attacks to guess passwords. The Barracuda Web Application Firewall protects against brute force attacks by blocking offending client or limiting the number of retries per amount of time.
- **XML Web service protection:** The Barracuda Web Application Firewall provides XML firewalling capabilities that protect Web application from malicious XML traffic. The Web Application Firewall can validate XML traffic against XML schemas. In the case of web services, Web Application Firewall will also validate the request against WSDL associated with the Web Services.
- **File upload protection:** The Barracuda Web Application Firewall allows administrators to control file types that can be uploaded by clients to the Web servers. It also performs Anti-Virus scans on all uploaded files for malware to ensure file safety.
- **Instant SSL:** The Barracuda Web Application Firewall can automatically convert an insecure HTTP Web application into an encrypted HTTPS application without having to rewrite any code. The Barracuda Web Application Firewall handles SSL encryption on behalf of the Web Application and rewrite traffic in real time to use the secure HTTPS protocol.
- **Authentication and Authorization:** The Barracuda Web Application Firewall provides out-of-box integration with LDAP, RADIUS and KERBEROS authentication services. It is integrated with CA SiteMinder for Single-Sign On (SSO) and it supports two factor authentication using RSA SecurID or client certificates. These allow administrators to create granular Access Control (ACL) rules to control access to different parts of the Web application, ensuring that only authorized users or roles can view protected pages.

Enhanced Application Delivery

Beyond Web application security, the Barracuda Web Application Firewalls provides a complete application delivery platform that accelerates content delivery:

- **Load balancing:** The Barracuda Web Application Firewall has a built-in load balancer that can distribute L4/L7 traffic to multiple backend servers. It can monitor server health and intelligently reroute traffic based on back on availability. This ensures that Web applications are highly available and can scale as needed.
- **SSL Offloading:** SSL encryption / decryption are resource intensive operations that utilize significant amounts of processing power. The Barracuda Web Application Firewall can encrypt/decrypt on behalf of the Web Server, freeing up server resources.
- **Content Routing:** Barracuda Web Application Firewalls provide content routing capabilities that allow administrators to map URL domains to different backend servers. For example images or media files can be served by a dedicated media server different from the main Web application server. This improves scalability by offloading portions of the Web application to different servers and also provides a layer of security by shielding internal server configurations from the external world.
- **Application acceleration:** Barracuda Web Application Firewalls provide integrated file caching, traffic compression and connection pooling capabilities. This improves content delivery while decreasing backend server load.
- **High Availability:** The Barracuda Web Application Firewall provides a number high availability capabilities that help keep mission-critical Web Applications online. In the event of web server failure, the Barracuda Web Application Firewall can detect primary failure and redirect traffic to a back up web server. The Barracuda Web Application Firewall itself can be configured in a HA pair for added availability.

Easy Management & Administration

The Barracuda Web Application Firewall provides a number of easy-to-use tools to aid the development of application specific security policies.

- **Centralized Management via Barracuda Control Center (BCC):** The Barracuda Web Application Firewall is integrated with BCC which allows organizations to manage all their Barracuda Web Application Firewall from a single interface. This gives administrators a global view of all of their devices and ensures that all devices have the latest firmware, definitions, and security policies.
- **Easy Tuning:** By default, all new policies are configured as "Passive" policies, where violations are simply logged. This useful non-invasive state that allows administrators to test security policies before actively applying them against live traffic. After the completion of testing, administrators can turn on new policy by setting it to the "Active" state where the Web Application Firewall actively blocks the violating traffic.
- **Exception profiling:** The Barracuda Web Application Firewall allows heuristics-based tuning of the existing firewall rules. Based on violations, the Barracuda Web Application Firewall provides the administrator with a proposed recommendation on tuning the configuration.
- **Adaptive profiling:** The Barracuda Web Application Firewall can analyze the incoming and outgoing traffic to build a profile of the Web application that contains all accessed URLs and allowed form parameters. This profile can then used to enforce strict security positive security model for the Web application.
- **Comprehensive Logging and Reporting:** All client requests, administrator modifications, and firewall actions are logged. This provides a comprehensive audit log for compliance and security policy tuning. Data from the logs are used by the Web Application Firewall to build graphical reports on attacks, web traffic, compliance or a number of other analytical reports. Logs can also be exported to 3rd party analytics suite via Syslog or FTP.
- **Alerts:** Notifications of system alerts are sent out via SNMP traps or email. This allows administrators to be well informed about the security status of their applications.
- **Barracuda Central updates:** The Barracuda Networks' security analysis team keeps abreast with all emerging threats and all updates are automatically sent to the Barracuda Web Application Firewalls in the field.

The Barracuda Advantage

- **Models:** The Barracuda Web Application Firewalls are available in five models that can handle any sized deployments. A FIPS 140-2 HSM model is also available for customers requiring FIPS compliance.
- **No software license or per server fees:** All features listed for the Barracuda Web Application Firewall models are included with the appliance and do not require any additional software license or server fees.

To learn more about Barracuda's web security solutions, please visit www.barracuda.com/products or call Barracuda for a free 30-day evaluation at 1-408-342-5400 or 1-888-268-4772 (US & Canada).

About Barracuda Networks, Inc.

Protecting users, applications, and data for more than 150,000 organizations worldwide, Barracuda Networks has developed a global reputation as the go-to leader for powerful, easy-to-use, affordable IT solutions. The company's proven customer-centric business model focuses on delivering high-value, subscription-based IT solutions for security and data protection. For additional information, please visit www.barracuda.com.



Barracuda Networks

3175 S. Winchester Boulevard

Campbell, CA 95008

United States

408-342-5400

888-268-4772 (US & Canada)

www.barracuda.com

info@barracuda.com