Overview

The Barracuda Web Application Firewall blocks an ever-expanding list of sophisticated web-based intrusions and attacks that target applications hosted on web servers and in the cloud. The Barracuda Web Application Firewall scans all inbound web traffic to block attacks, and inspects the HTTP responses from the configured back-end servers for Data Loss Prevention (DLP). The integrated access control engine enables administrators to create granular access control policies for Authentication, Authorization & Accounting (AAA) without requiring application changes. The onboard L4/L7 Load Balancing capabilities enable organizations to add back-end servers quickly to scale deployments as they grow. Its application acceleration capabilities like SSL Offloading, caching, compression, and connection pooling ensure faster application delivery of the web application content.

The Barracuda Web Application Firewall is available in multiple models and can be used to securely deploy applications of any size. For information on available models, refer to Barracuda Web Application Firewall Datasheet's .

Where to Start

Learn about your Deployment Options. Also, refer to Deployment Best Practices.

If you have the Barracuda Web Application Firewall Vx virtual machine, start here: Virtual Deployment .

If you have the Barracuda Web Application Firewall appliance, start here: Getting Started.

Alternatively, you can download the Barracuda Web Application Firewall Quick Start Guide.

Key Features

- Protection from common, high-visibility attacks – SQL injection, Cross Site Scripting, Command injection, CSRF, XML attacks, Antivirus Protection, Adaptive Profiling
- Protection from attacks based on session state – Session Hijacking, Cookie Tampering, Clickjacking
- Brute Force Attack Prevention
- Application denial of service (DoS) protection – Slow Client Attack, DDoS Prevention using CAPTCHA, IP Reputation Filter
- Protection from volumetric and application DDoS attacks using Barracuda Active DDoS Prevention.
- Data Theft Protection – Deep inspects all server responses to prevent leakage of sensitive information using provided default patterns (credit card data, social security numbers, etc.) or User Defined Patterns (Custom Patterns).
- Website Cloaking – Strips identifying banners and version numbers from web server software and provides customizable HTTP error handling to defeat server fingerprinting attacks (suppressing error codes and filtering headers).
- Access Control – Form and Basic Authentication and Single Sign On with integrations into LDAP, RADIUS, CA SiteMinder, RSA SecurID, Kerberos, SMS Passcode
- Application Delivery – Load Balancing, Caching and Compression, SSL Offloading, Rate Control
- Logging, Reporting and Monitoring – Inbuilt reporting module, Web Firewall Logs, Access Logs, Audit Logs, Configuring Syslog

Additional Resources

- Barracuda Web Application Firewall REST API Guide
- Configuring Syslog and other Logs
- System Log Messages
- Mitigating Website Vulnerabilities using Vulnerability Scanners