



# Barracuda Web Application Firewall

Protect Applications and Data from Advanced Threats



The Barracuda Web Application Firewall **blocks an ever-expanding list of sophisticated web-based intrusions and attacks** that target the applications hosted on your web servers—and the sensitive or confidential data to which they have access.

- Security
- Storage
- Application Delivery

## The Barracuda Advantage

- State-of-the-art security utilizing full reverse-proxy architecture
- Malware protection for collaborative web applications
- Employs IP Reputation intelligence to defeat DDoS attacks
- No user-based or module-based licensing
- Designed to make it easier for organizations to comply with regulations such as PCI DSS and HIPAA

## Product Spotlight

- Comprehensive inbound attack protection including the OWASP Top 10
- Built-in caching, compression, and TCP pooling ensure security without performance impacts
- Identity-based user access control for web applications
- Built-in data loss prevention
- ICSA certified



### Constant Protection from Evolving Threats

The Barracuda Web Application Firewall provides superior protection against data loss, DDoS, and all known application-layer attack modalities. Automatic updates provide defense against new threats as they appear. As new types of threats emerge, it will acquire new capabilities to block them.



### Identity and Access Management

The Barracuda Web Application Firewall has strong authentication and access control capabilities that ensure security and privacy by restricting access to sensitive applications or data to authorized users.



### Affordable and Easy to Use

Pre-built security templates and intuitive web interface provide immediate security without the need for time-consuming tuning or application learning. Integration with security vulnerability scanners and SIEM tools automates the assessment, monitoring, and mitigation process.

**Protect servers, applications, and data from web-based attacks.**



Internet



Barracuda Web Application Firewall



Servers



Inbound inspection for Layer 7 attacks



Outbound inspection to protect against data theft

*With the Barracuda Web Application Firewall in place, we are demonstrating to our customers and partners that we are serious about the security of their data. It lets our staff to worry less about backend security and concentrate more on providing quality services to our partners and customers.*

*Michael Fainshtein  
Chief Technology Officer  
CredoRax.*

## Technical Specs

### Web Application Security

- OWASP top 10 protection
- Protection against common attacks
  - SQL injection
  - Cross-site scripting
  - Cookie or forms tampering
- Form field meta-data validation
- Adaptive security
- Website cloaking
- Response control
- Outbound data theft protection
  - Credit card numbers
  - Custom pattern matching (regex)
- Granular policies to HTML elements
- Protocol limit checks
- File upload control
- Protection against Distributed Denial of Service (DDoS)
- Client IP Reputation
- Geo IP location
  - Anonymous Proxy

### Supported Web Protocols

- HTTP/S 0.9/1.0/1.1
- FTP/S
- XML
- IPv4/IPv6

### Authentication & Authorization

- LDAP/RADIUS/local user database
- Client certificates
- Single Sign-On
- RSA SecurID
- CA SiteMinder
- SMS Passcode

## Support Options

### Instant Replacement Service

- Replacement unit shipped next business day
- 24x7 technical support
- Hardware refresh every four years

### Logging, Monitoring & Reporting

- System log
- Web Firewall log
- Access log
- Audit log

### SIEM Integrations

- ArcSight
- RSA enVision
- Splunk
- Symantec
- Custom

## Hardware Options

- FIPS 140-2 HSM Model Available
- Optional Ethernet Bypass

### Application Delivery & Acceleration

- High availability
- SSL offloading
- Load balancing
- Content routing

### XML Firewall

- XML DOS protection
- Schema/WSDL enforcement
- WS-I conformance checks

### Networking

- VLAN, NAT
- Network ACLs

## Management Features

- Customizable role-based administration
- Vulnerability scanner integration
- Trusted host exception

| MODEL COMPARISON                  | 360             | 460             | 660               | 860                  | 960                    |
|-----------------------------------|-----------------|-----------------|-------------------|----------------------|------------------------|
| <b>CAPACITY</b>                   |                 |                 |                   |                      |                        |
| Backend Servers Supported         | 1-5             | 5-10            | 10-25             | 25-150               | 150-300                |
| Throughput                        | 25 Mbps         | 50 Mbps         | 200 Mbps          | 1 Gbps               | 4 Gbps                 |
| <b>HARDWARE</b>                   |                 |                 |                   |                      |                        |
| Form Factor                       | 1U Mini         | 1U Mini         | 1U Fullsize       | 2U Fullsize          | 2U Fullsize            |
| Dimensions (in)                   | 16.8 x 1.7 x 14 | 16.8 x 1.7 x 14 | 16.8 x 1.7 x 22.6 | 17.4 x 3.5 x 25.5    | 17.4 x 3.5 x 25.5      |
| Weight (lb)                       | 12              | 12              | 26                | 46                   | 52                     |
| Data Path Ports                   | 2 x 10/100      | 2 x GbE         | 2 x GbE           | 2 x GbE <sup>1</sup> | 2 x 10GbE <sup>1</sup> |
| Management Port                   | 1 x 10/100      | 1 x 10/100      | 1 x 10/100/1000   | 1 x 10/100/1000      | 1 x 10/100/1000        |
| AC Input Current (amps)           | 1.2             | 1.4             | 1.8               | 4.1                  | 5.4                    |
| ECC Memory                        |                 |                 | ●                 | ●                    | ●                      |
| <b>FEATURES</b>                   |                 |                 |                   |                      |                        |
| Response Control                  | ●               | ●               | ●                 | ●                    | ●                      |
| Outbound Data Theft Protection    | ●               | ●               | ●                 | ●                    | ●                      |
| File Upload Control               | ●               | ●               | ●                 | ●                    | ●                      |
| SSL Offloading                    | ●               | ●               | ●                 | ●                    | ●                      |
| Authentication and Authorization  | ●               | ●               | ●                 | ●                    | ●                      |
| Vulnerability Scanner Integration | ●               | ●               | ●                 | ●                    | ●                      |
| Protection Against DDoS Attacks   | ●               | ●               | ●                 | ●                    | ●                      |
| Network Firewall                  | ●               | ●               | ●                 | ●                    | ●                      |
| High Availability                 | Active/Passive  | Active/Passive  | Active/Active     | Active/Active        | Active/Active          |
| Caching and Compression           |                 | ●               | ●                 | ●                    | ●                      |
| LDAP/RADIUS Integration           |                 | ●               | ●                 | ●                    | ●                      |
| Load Balancing                    |                 | ●               | ●                 | ●                    | ●                      |
| Content Routing                   |                 | ●               | ●                 | ●                    | ●                      |
| Advanced Routing                  |                 |                 | ●                 | ●                    | ●                      |
| Adaptive Profiling                |                 |                 | ●                 | ●                    | ●                      |
| Antivirus for File Uploads        |                 |                 | ●                 | ●                    | ●                      |
| XML Firewall                      |                 |                 | ●                 | ●                    | ●                      |

<sup>1</sup> Fiber NIC and Ethernet hard bypass options available.

Specifications subject to change without notice.