Barracuda **Web Application Firewall**

Protect your web applications by extending your security with VMware®

The Barracuda Web Application Firewall integrates into VMware Service to block an ever-expanding list of sophisticated web-based intrusions and attacks that target your applications on premises or in the cloud.

☑ **Security**
□ Storage
□ Application Delivery
□ Productivity

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, NSS recommended
- Protection against Application DDoS attacks

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.

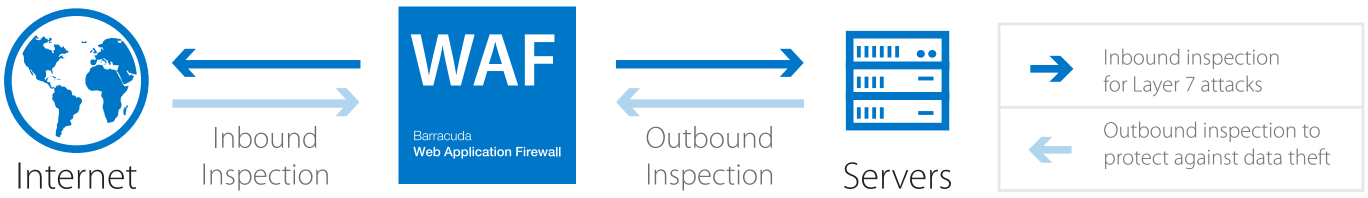
Identity and Access Management

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

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



> *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

DDoS Protection

- Barracuda IP Reputation Database
- Heuristic Fingerprinting
- CAPTCHA challenges
- Slow Client protection
- Geo IP
- Anonymous Proxy
- ToR exit nodes
- Barracuda Blacklist

Supported Web Protocols

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

Authentication & Authorization

- LDAP/RADIUS/local user database
- SAML 2.0
- Client certificates
- Single Sign-On
- Azure AD
- RSA SecurID
- CA SiteMinder
- SMS PASSCODE

SIEM Integrations

- ArcSight
- RSA enVision
- Splunk
- Symantec
- Custom

XML Firewall

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

Networking

- VLAN, NAT
- Network ACLs
- Advanced routing

Management Features

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

Logging, Monitoring & Reporting

- System log
- Web Firewall log
- Access log
- Audit log
- Network firewall log
- On-demand and scheduled reports

Centralized Management

- Monitor and configure multiple Barracuda products from a single interface
  - Check health and run reports
  - Assign roles with varied permissions
  - Available from anywhere

MODEL COMPARISON	V360	V460	V660
CAPACITY			
Backend Servers Supported	1-5	5-10	150-300
Throughput	25 Mbps	50 Mbps	4 Gbps
Number of Cores Supported	2	3	4+
FEATURES			
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
Caching and Compression		●	●
LDAP/RADIUS Integration		●	●
Load Balancing		●	●
Content Routing		●	●
Advanced Routing			●
Adaptive Profiling			●
Antivirus for File Uploads			●
XML Firewall			●

*Additional cores available for increased throughput

Specifications subject to change without notice.