Barracuda **Web Application Firewall Vx**

Protect Applications and Data from Advanced Threats

- ☑ **Security**
- ☐ Data Protection
- ☑ **Application Delivery**

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.

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
- Cloud-based scan with Barracuda Vulnerability Manager
- Automatic vulnerability remediation

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
- 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.

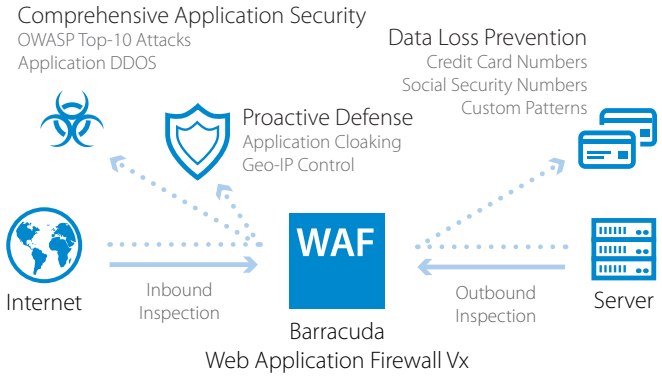
Identity and Access Management

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
- XML firewall
- JSON payload inspection
- Web scraping protection
- Outbound data theft protection
  - Credit card numbers
  - Custom pattern matching (regex)
- Granular policies to HTML elements
- Protocol limit checks
- File upload control

Hypervisor Support
- VMware ESX/ESXi
- VMware Server/Fusion/Workstation/Player
- Citrix Xenserver
- Oracle VirtualBox
- Microsoft Hyper-V

DDoS Protection
- Barracuda IP Reputation Database
- Integration with Barracuda Next-Gen Firewall to block malicious IP's
- Heuristic Fingerprinting
- CAPTCHA challenges
- Slow Client protection
- Layer 3 and Layer 7 Geo IP
- Anonymous Proxy
- ToR exit nodes
- Barracuda Blacklist

Supported Web Protocols
- HTTP/S 0.9/1.0/1.1/ 2.0
- WebSocket
- FTP/S
- XML
- IPv4/IPv6

Authentication
- LDAP/RADIUS
- Client Certificates
- SMS Passcode
- Single Sign-On
- Multi-Domain SSO

Advanced Authentication (660VX & above)
- Kerberos v5
- SAML
- Azure AD
- RSA SecurID

Application Delivery and Acceleration
- High availability
- SSL offloading
- Load balancing
- Content routing

SIEM Integrations
- HPE ArcSight
- RSA enVision
- Splunk
- Symantec
- Microsoft Azure Event Hub
- Custom

Support Options

Barracuda Energize Updates
- Standard technical support
- Firmware and capability updates as required
- Automatic application definitions updates

Management Features
- Customizable role-based administration
- Vulnerability scanner integration
- Trusted host exception
- REST API
- Custom Templates

Logging, Monitoring and 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	360VX	460VX	660VX	760VX	860VX	960VX
CAPACITY						
Backend Servers Supported	1-5	5-10	10-25	25-50	50-150	150-300
Number of Cores Supported	2	4	6	8	10	12
Throughput	25Mbps	50Mbps	200Mbps	500Mbps	1Gbps	5Gbps
FEATURES						
SSL Offloading	●	●	●	●	●	●
Response Control	●	●	●	●	●	●
Outbound Data Theft Protection	●	●	●	●	●	●
File Upload Control	●	●	●	●	●	●
Antivirus for File Uploads			●	●	●	●
Advanced Threat Protection[1]			●	●	●	●
Authentication and Authorization	●	●	●	●	●	●
Basic AAA		●	●	●	●	●
Advanced AAA			●	●	●	●
Protection Against DDoS Attacks[2]	●	●	●	●	●	●
Web Scraping Protection	●	●	●	●	●	●
Network Firewall	●	●	●	●	●	●
High Availability	Active/Passive	Active/Passive	Active/Active	Active/Active	Active/Active	Active/Active
XML Firewall			●	●	●	●
URL Encryption		●	●	●	●	●
Adaptive Profiling		●	●	●	●	●
Vulnerability Scanner Integration	●	●	●	●	●	●
Load Balancing		●	●	●	●	●
Caching and Compression		●	●	●	●	●
Content Routing		●	●	●	●	●
Advanced Routing			●	●	●	●

[1] Requires active Advanced Threat Protection subscription. [2] Volumetric DDoS protection requires subscription.

Specifications subject to change without notice.