The Barracuda Web Application Firewall blocks application layer DDoS and other attack vectors, directed at online applications hosted in Microsoft Azure. Simultaneously, it provides superior protection against data loss. It also has strong authentication and access control capabilities for restricting access to sensitive applications and data.

### The Barracuda Advantage
- Barracuda Central Operations Center keeps track of emerging threats
- State-of-the-art security utilizing full reverse-proxy architecture
- Malware protection for collaborative web applications
- Employing IP Reputation intelligence to defeat DDoS attacks
- 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 vectors. 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 user interface provide immediate security without the need for time-consuming tuning or application learning. Integration with vulnerability scanners and SIEM tools automates the assessment, monitoring, and mitigation process.
## Technical Specs

### Web Application Security
- OWASP top 10 protection
- Protection against common attacks
  - SQL injection
  - Cross-site scripting
  - Cookie or form tampering
  - Form field meta-data validation
  - Adaptive security
  - Website cloaking
  - URL encryption
  - 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

### XML Firewall
- XML DOS protection
- Schema/WSL enforcement
- WS-I conformance checks

### Networking
- VLAN, NAT
- Network ACLs
- Advanced routing

### SQL injection
- Level 10

### Cookie or forms tampering
- Level 5

### Cross-site scripting
- Level 15

### Credit card numbers
- Level 15

### Specifications subject to change without notice.

---

## BARRACUDA WEB APPLICATION FIREWALL

### 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
- Adaptive profiling for learning
- Exception profiling for tuning

### Logging, Monitoring & Reporting
- System log
- Web firewall log
- Access log
- Audit log
- Network firewall log
- On-demand and scheduled comprehensive 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

---

### BARRACUDA WEB APPLICATION FIREWALL

<table>
<thead>
<tr>
<th>CAPABILITIES</th>
<th>SMALL (A1)</th>
<th>MICROSOFT AZURE - COMPUTE INSTANCE NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Level 1</td>
<td>Level 5</td>
</tr>
<tr>
<td>Virtual Cores</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Throughput</td>
<td>100 Mbps</td>
<td>200 Mbps</td>
</tr>
<tr>
<td>HTTP Connections per Second</td>
<td>5,000</td>
<td>7,000</td>
</tr>
<tr>
<td>HTTPS Requests per Second</td>
<td>5,000</td>
<td>7,000</td>
</tr>
</tbody>
</table>

### 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
- Caching and Compression
- LDAP/RADIUS/Kerberos/Local User DB Integration
- Load Balancing
- Content Routing
- Advanced Routing
- Adaptive Profiling
- Antivirus for File Uploads
- XML Firewall
- Premium Support

1. Clustering enables synchronization of configuration between multiple instances. Azure Load Balancer may be used to distribute the traffic to multiple nodes.

2. Premium Support ensures that an organization's network is running at its peak performance by providing the highest level of 24x7 technical support for mission-critical environments.

For more information please visit https://www.barracuda.com/support/premium.

Specifications subject to change without notice.