The Barracuda Web Application Firewall blocks application layer DDoS and other attack vectors directed at web-facing applications hosted in Amazon Web Services, while providing superior protection against data loss. It also has strong authentication and access control capabilities for restricting access to sensitive applications and data, along with the ability to autoscale inside your VPC.

**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
- Employs 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
- Ability to bootstrap and autoscale with automated and clustered deployments using CloudFormation templates
- Available on the AWS marketplace as a single AMI or as a CloudFormation template
- Integration with Cloudwatch, S3 and IAM Roles
- AWS Security Competency 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 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.
## 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
- REST API
- Custom Templates

## 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
- URL encryption
- Response control

### DDoS Protection
- Barracuda IP Reputation Database
- Heuristic Fingerprinting
- CAPTCHA challenges
- Slow Client protection
- Geo IP
- Anonymous Proxy
- Tor exit nodes
- Barracuda Blacklist

### Authentication & Authorization
- LDAP/RADIUS/Kerberos/
  - local user database
- SAML 2.0
- Client certificates
- Single Sign-On
- CA SiteMinder
- CA
- SMS PASSCODE

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

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

### AWS Integrations/Support for
- ELB / VPC
- CloudWatch
- CloudFormation / Bootstrapping
- Auto/Dynamic Scaling
- IAM/S3
- MIT Clustering Support
- Amazon Short Notification Service

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

## SIEM Integrations
- ArcSight
- RSA enVision
- Splunk
- Symantec
- Custom

## Capabilities

<table>
<thead>
<tr>
<th>Feature</th>
<th>M3.MEDIUM</th>
<th>M3.LARGE</th>
<th>M3.XLARGE</th>
<th>M3.2XLARGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPABILITIES</td>
<td>Level 1</td>
<td>Level 5</td>
<td>Level 10</td>
<td>Level 15</td>
</tr>
<tr>
<td>Virtual Cores</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Throughput</td>
<td>100 Mbps</td>
<td>200 Mbps</td>
<td>400 Mbps</td>
<td>750 Mbps</td>
</tr>
<tr>
<td>HTTP Connections per Second</td>
<td>5,000</td>
<td>7,000</td>
<td>10,000</td>
<td>14,000</td>
</tr>
<tr>
<td>HTTPS Requests per Second</td>
<td>5,000</td>
<td>7,000</td>
<td>10,000</td>
<td>14,000</td>
</tr>
<tr>
<td>FEATURES</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Response Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outbound Data Theft Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Upload Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL Offloading</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication and Authorization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL Offloading</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Scanner Integration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection Against DDoS Attacks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Scraping Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Firewall</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clustering</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Caching and Compression</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP/RADIUS/Kerberos/Local User DB Integration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Load Balancing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content Routing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced Routing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adaptive Profiling</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URL Encryption</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antivirus for File Uploads</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XML Firewall</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JSON Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Premium Support
- Optional

---

1. 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](https://www.barracuda.com/support/premium)

Specifications subject to change without notice.

Datasheet US 1.7 • Copyright 2015-2016 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772 (US & Canada) • barracuda.com

Barracuda Networks and the Barracuda Networks logo are registered trademarks of Barracuda Networks, Inc. in the United States. All other names are the property of their respective owners.