The Barracuda CloudGen WAF 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
- 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
- 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

**Constant Protection from Evolving Threats**

The Barracuda CloudGen WAF 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 CloudGen WAF 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.
**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
- 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

**DDoS Protection**
- Barracuda IP reputation database
- Integration with Barracuda Next-Gen Firewall to block malicious IPs
- 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/1.0/1.1/1.2
- WebSocket
- FTP/S
- XML

**Authentication**
- LDAP/RADIUS
  - Client Certificates
  - SMS Passcode
  - Single sign-On
  - Multi-domain SSO

**Advanced Authentication**
- 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
- Adaptive profiling for learning
- Exception profiling for tuning
- 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

---

**BARRACUDA CLOUDGEN WAF FOR AZURE**

<table>
<thead>
<tr>
<th>CAPABILITIES</th>
<th>SMALL (D1)</th>
<th>MICROSOFT AZURE - COMPUTE INSTANCE NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Cores</td>
<td>LEVEL 1</td>
<td>LEVEL 5</td>
</tr>
<tr>
<td>Throughput</td>
<td>100 Mbps</td>
<td>200 Mbps</td>
</tr>
<tr>
<td>HTTP Requests 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>

<table>
<thead>
<tr>
<th>FEATURES</th>
<th>SMALL (D1)</th>
<th>MICROSOFT AZURE - COMPUTE INSTANCE NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response Control</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Advanced Threat Protection</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Outbound Data Theft Protection</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>File Upload Control</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>SSL Offloading</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Authentication and Authorization</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Network Firewall</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Web Scrapping Protection</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Clustering</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Caching and Compression</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Basic AAA</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Advanced AAA</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Content Routing</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Adaptive Profiling</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>URL Encryption</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Antivirus for File Uploads</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>XML Firewall</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>JSON Security</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>

**Management Features**

- Customizable role-based administration
- Vulnerability scanner integration
- Trusted host exception
- Adaptive profiling for learning
- Exception profiling for tuning
- REST API
- Custom Templates

**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

---

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.
3 Requires active Advanced Threat Protection subscription. Available on 810 models only.
4 Volumetric DDoS protection requires subscription. For more information please visit [https://www.barracuda.com/support/premium](https://www.barracuda.com/support/premium)

Specifications subject to change without notice.