Barracuda **CloudGen WAF for Azure**

Securing Applications and Data in Microsoft Azure

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

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

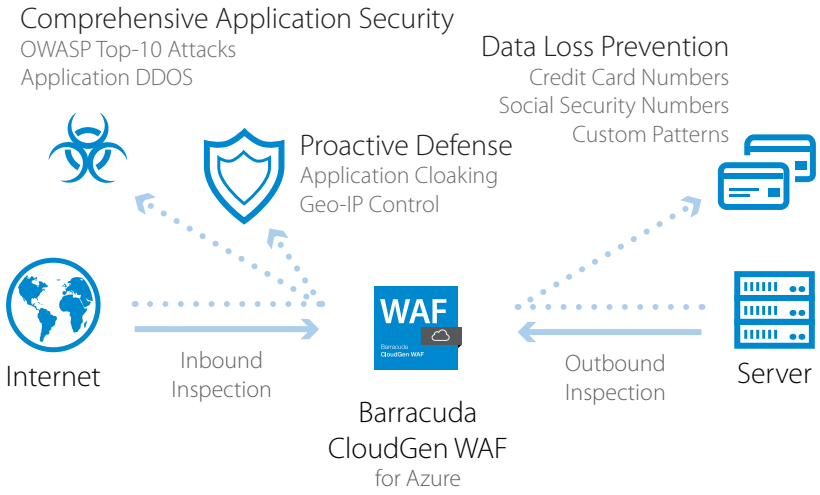
The Barracuda CloudGen WAF provides superior protection against data loss, DDoS, and all known application-layer attack modalities. Automatic updates provide defense against new threats as they appear. As new types of threats emerge, it will acquire new capabilities to block them.

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.



NSS LABS RECOMMENDED

ICSA labs CERTIFIED WEB APPLICATION FIREWALL

Microsoft Azure Certified

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 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

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	MICROSOFT AZURE - COMPUTE INSTANCE NAME			
	SMALL (D1)	MEDIUM (D2)	LARGE (D3)	EXTRA LARGE (D4)
CAPABILITIES	**LEVEL 1**	**LEVEL 5**	**LEVEL 10**	**LEVEL 15**
Virtual Cores	1	2	4	8
Throughput	100 Mbps	200 Mbps	400 Mbps	750 Mbps
HTTP Connections per Second	5,000	7,000	10,000	14,000
HTTPS Requests per Second	5,000	7,000	10,000	14,000
FEATURES				
Response Control	●	●	●	●
Advanced Threat Protection[3]		●	●	●
Outbound Data Theft Protection	●	●	●	●
File Upload Control	●	●	●	●
SSL Offloading	●	●	●	●
Authentication and Authorization	●	●	●	●
Vulnerability Scanner Integration	●	●	●	●
Protection Against DDoS Attacks[4]	●	●	●	●
Network Firewall	●	●	●	●
Web Scraping Protection	●	●	●	●
Clustering	Config Sync	Config Sync	Config Sync	Config Sync
Caching and Compression	●	●	●	●
Basic AAA	●	●	●	●
Advanced AAA	●	●	●	●
Load Balancing	●	●	●	●
Content Routing	●	●	●	●
Adaptive Profiling	●	●	●	●
URL Encryption	●	●	●	●
Antivirus for File Uploads		●	●	●
XML Firewall	●	●	●	●
JSON Security	●	●	●	●
Premium Support [2]	Optional	Optional	Optional	Optional

[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 BYoL models only.

[4] Volumetric DDoS protection requires subscription. For more information please visit https://www.barracuda.com/support/premium.

Specifications subject to change without notice.