Barracuda CloudGen WAF for GCP

Securing applications and data in Google Cloud Platform.

Barracuda CloudGen WAF blocks an ever-expanding list of sophisticated web-based intrusions and attacks that target the applications hosted on Google Cloud Platform (GCP) and the sensitive or confidential data to which they have access. Deployed within your GCP infrastructure, Barracuda CloudGen WAF scans all inbound web traffic to block attacks, and scans outbound traffic to provide highly effective data loss prevention.

Barracuda CloudGen WAF simplifies application security so you can focus on your business. Its comprehensive feature set, versatile deployment options, and ease of use lets you automate many application security tasks.

Constant protection from evolving threats

Barracuda CloudGen WAF provides superior protection against all application-layer attacks, including the OWASP Top 10, application DDoS, and more. Automatic updates provide defense against new threats as they appear. Powerful application learning provides positive security capabilities against advanced attacks, while XML and JSON Firewalls protect API-based applications.

Identity and access management

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 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
- JSON payload inspection
- XML firewall
- 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

SIEM integrations

- HPE ArcSight
- RSA enVision
- Splunk
- Symantec
- Custom
- VLAN, NAT
- Network ACLs

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

Advanced Bot Protection

- Detects "low-and-slow" bots
- Minimizes false positives
- Allows human and good-crawler activity

DDoS protection

- Integration with Barracuda NextGen Firewall
  to block malicious IPs
- Barracuda IP Reputation Database
- Heuristic Fingerprinting
- CAPTCHA challenges
- Slow Client protection
- Layer 3 and Layer 7 Geo IP
- Anonymous proxy
- ToR exit nodes
- Barracuda block list

Supported web protocols

- HTTP/S 0.9/1.0/1.1/2.0
- WebSocket
- FTP/S
- XML
- ABP

Application delivery and acceleration

- High availability
- SSL offloading
- Load balancing
- Content routing

Basic AAA

- LDAP/RADIUS
- Client certificates
- SMS passcode
- Single sign-on
- Multi-domain SSO

AAA

- Kerberos v5
- SAML
- RSA SecurID
- OpenID Connect
- JSON Web Tokens

Management features

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

Model Comparison

CAPABILITIES	GOOGLE CLOUD PLATFORM - COMPUTE INSTANCE SIZES			
	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				
SSL offloading	✓	✓	✓	✓
Smart signatures	✓	✓	✓	✓
Response control	✓	✓	✓	✓
Advanced Threat Protection[2]	-	✓	✓	✓
Advanced Bot Protection[4]	✓	✓	✓	✓
Client-Side Protection[4]	✓	✓	✓	✓
Advanced Bot Protection[4]	✓	✓	✓	✓
Outbound data theft protection	✓	✓	✓	✓
File upload control	✓	✓	✓	✓
Authentication and authorization	✓	✓	✓	✓
Vulnerability scanner integration	✓	✓	✓	✓
Protection against DDoS attacks[3]	✓	✓	✓	✓
Web scraping protection	✓	✓	✓	✓
Network firewall	✓	✓	✓	✓
Clustering	Config sync	Config sync	Config sync	Config sync
Caching and compression	✓	✓	✓	✓
Basic AAA	✓	✓	✓	✓
Advanced AAA	✓	✓	✓	✓
Load balancing	✓	✓	✓	✓
Content routing	✓	✓	✓	✓
Adaptive profiling	✓	✓	✓	✓
Auto-Configuration Engine (Requires ABP Subscription)	✓	✓	✓	✓
URL encryption	✓	✓	✓	✓
Antivirus for file uploads	-	✓	✓	✓
XML firewall	✓	✓	✓	✓
JSON security	✓	✓	✓	✓
Premium support[1]	Optional	Optional	Optional	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.*

[2] *Requires active Advanced Threat Protection subscription. Available on BYoL models only.*

[3] *Volumetric DDoS protection requires the ADP subscription. Available on BYoL models only.*

[4] *Requires active Advanced Bot Protection subscription. Available on BYoL models only.*

Barracuda.
Your journey, secured.