

# Barracuda CloudGen Firewall für AWS

## Schutz Ihrer digitalen Assets in Amazon Web Services

Das Wachstum der Cloud Computing-Fähigkeiten und -Services hat dazu geführt, dass mehr Daten an Orte gelangen, an die traditionelle IT-Sicherheitsmaßnahmen nicht gelangen können - in Rechenzentren, die nicht im Besitz Ihrer IT-Unternehmensgruppe sind. Neben den leistungsstarken Netzwerk-Firewall-, IPS- und VPN-Technologien integriert die Barracuda CloudGen Firewall Next-Generation-Firewall-Technologien, wie Funktionen für Application Control, Verfügbarkeit und Quality of Services (QoS).



### Granulare Application Control

Barracuda CloudGen Firewall ermöglicht Administratoren granulare Kontrolle über Applikationen. Dabei können sie Regeln zur Weiterleitung des Datenverkehrs über die jeweils besten Übertragungskanäle je nach Applikationstyp, Benutzer, Inhalt, Tageszeit und geografischem Standort festlegen. Mit Barracuda CloudGen Firewall können Organisationen Datenverkehr priorisieren, indem sie den Zugriff auf nicht-geschäftsrelevante Applikationen und den damit verbundenen Netzwerkverkehr begrenzen oder einschränken, selbst wenn dieser Verkehr verschlüsselt ist.

### Integrierte Sicherheit und Konnektivität der neuen Generation

Die Intrusion Detection und das Prevention System (IDS/IPS) der Barracuda CloudGen Firewall verbessern die Netzwerksicherheit, indem sie vollständigen und umfassenden Echtzeit-Netzwerkschutz gegen eine große Bandbreite von Netzwerkbedrohungen, Schwachstellen, Sicherheitslücken und Lücken in Betriebssystemen, Anwendungen und Datenbanken bereitstellen, und so unter anderem SQL-Injektionen und das Ausführen von beliebigem Code verhindern.

### Cloud-Automatisierung

Der große Vorteil des Cloud-Betriebs geht über Kosteneinsparungen hinaus, in Richtung größerer Agilität und Flexibilität. Das erlaubt wiederum die Einführung einer DevOps/Agile-Methodik, Cloud-nativen Architekturen und Automatisierung ermöglicht. Alle Komponenten, einschließlich der Infrastruktur für Sicherheit und Konnektivität, müssen sich dabei über API oder Skripting an die Funktionsweise in der Public Cloud anpassen.

Barracuda CloudGen Firewall bietet vollautomatischen Schutz bei Multi-Cloud-Bereitstellungen, einschließlich VPN-Automatisierung.

## Technische Spezifikationen

### Firewall

- Stateful Packet Inspection und Forwarding
- Volle User-Identity Awareness
- Intrusion Detection und Prevention (IDS/IPS)
- Application Control und granulares Application Enforcement
- Abfangen und entschlüsseln von SSL/TLS verschlüsselten Anwendungen
- Antivirus und Web-Filtering im Single-Pass Modus
- Email-Security
- SafeSearch-Enforcement
- Google-Accounts-Enforcement
- Denial-of-Service Schutz (DoS/DDoS)
- Spoofing und Flooding Schutz
- Schutz vor ARP Spoofing u. Trashing
- DNS Reputation Filter
- TCP Stream Reassembly
- Transparentes Proxying (TCP)
- NAT (SNAT, DNAT), PAT
- Dynamische Regeln/zeitbasierte Trigger
- Einzelobjekt-Orientiertes Regelwerk für Routing, Bridging und Routed-Bridging
- Virtuelle Regeltestumgebung

### Infrastructure Services

- DHCP-Server, Relay
- SIP- und HTTP-Proxies
- SMTP-Gateway & IPFIX Unterstützung
- JSON Lifecycle-Automatisierungs-API
- Auto VPN über API / Script Control
- DNS Cache
- Integrierte Unterstützung für Azure Virtual WAN

### VPN

- VPN-Tunnel-Konfiguration per Drag-and-Drop
- Network Access Control
- VPN-Unterstützung für Mobilgeräte mit iOS und Android
- Zwei-Faktor Authentisierung mittels Time-based One-Time Passwords (TOTP), Radius, oder RSA MFA (erfordert eine aktive Advanced Remote Access Subscription) für VPN und NAC Clients
- Multi-Faktor Authentisierung für SSL VPN und CudaLaunch

### Advanced Threat Protection

- Dynamische, „on-demand“ Analyse von Malware (Sandboxing)
- Dynamische Analyse von Dokumenten mit eingebetteten Exploits (PDF, Office, usw.)
- Detaillierte Forensik für Malware Binaries und Web-Bedrohungen
- Botnet- und Spyware-Schutz
- TypoSquatting und Link- Protection für E-Mail

### Intrusion Detection und Prevention

- Schutz vor Exploits, Bedrohungen und Schwachstellen
- Schutz vor Packet Anomaly und Fragmentation
- Fortschrittlichste Anti-Evasion und Obfuscation-Techniken

### Unterstützte Protokolle

- IPv4, IPv6
- BGP/OSPF/RIP
- VoIP (H.323, SIP, SCCP [skinny])
- RPC-Protokolle (ONC-, DCE-RPC)
- 802.1q VLAN

### Zentrale Management-Optionen über Barracuda Firewall Control Center

- Administration für unlimitierte Zahl an Firewalls
- Mandantenfähig
- Multi-Administrator & RCS
- Enterprise/MSP Lizenzierung
- Template & Repository-basiertes Management
- REST API

### Traffic Intelligence & SD-WAN

- Optimierte Internet-Uplink-Auswahl
- VPN-basiertes SD-WAN
- FIPS 140-2 zert. Verschlüsselung
- On-demand VPN-Tunnel-Erstellung zwischen entfernten Spoke-Standorten basierend auf dem Anwendungstyp
- Dynamische Bandbreitenerkennung
- Performance-basierte Transportauswahl
- Anwendungsorientiertes Traffic-Routing (VPN, Direct Connect)
- Adaptives Session-Balancing über mehrere Uplinks hinweg
- Traffic-Replikation (vorwärts gerichtete Fehlerkorrektur)
- App-based Provider Selection
- Traffic-Shaping und QoS
- Integrierte Datenduplizierung
- Automatische Signatur Updates

## Support Optionen

### Barracuda Energize Updates

- Standardmäßiger techn. Support
- Firmware-Updates
- IPS-Signaturen-Updates
- Application-Control Definition-Updates
- Web-Filter-Updates

## Unterstützung von AWS Funktionen

- Volle AWS Direct Connect Unterstützung
- Auto-Scaling Cluster
- Cold-Standby Cluster
- Log-File Streaming und Custom-Metrics für AWS CloudWatch

## Verfügbare Optionen

### Barracuda Firewall Insights

Konsolidiert Informationen zu Sicherheit, Datenfluss der Applikationen und Konnektivität Hunderter oder sogar Tausender von Firewalls im erweiterten Wide Area Network - unabhängig davon, ob es sich um Hardware-, virtuelle oder cloud-übergreifende Implementierungen handelt.

### Advanced Threat Protection

Schützt vor Network-Breaches, erkennt Zero-Day-Malware-Angriffe, gezielte Angriffe, erweiterte persistente Bedrohungen und andere fortschrittliche Malware.

### Malware Protection

Bietet Gateway-basierten Schutz vor Malware, Viren, Spyware und anderen unerwünschten Programmen im SMTP/S-, HTTP/S- und FTP/S-Verkehr.

### Advanced Remote Access

Bietet ein anpassbares und benutzerfreundliches portalbasiertes SSL-VPN sowie anspruchsvolle Network Access Control (NAC)-Funktionalität und CudaLaunch-Unterstützung.

	BRING-YOUR-OWN-LICENSE				PAY-AS-YOU-GO LICENSE	
LEISTUNGSMERKMALE	LEVEL 2	LEVEL 4	LEVEL 6	LEVEL 8	NACH ZEIT	NACH VOLUMEN
Geschützte IP Adressen	Unlimitiert	Unlimitiert	Unlimitiert	Unlimitiert	Unlimitiert	Unlimitiert
Virtuelle Kerne	1	2	4	8	Nicht zutreffend	Nicht zutreffend
Max. Anzahl an Interfaces	2	2	4	4	Nicht zutreffend	Nicht zutreffend
FUNKTIONEN						
Firewall inkl. IPS	✓	✓	✓	✓	✓	✓
Application Control	✓	✓	✓	✓	✓	✓
Site-to-Site und Client-to-Site VPN	✓	✓	✓	✓	✓	✓
Network Access Control für Client-to-Site VPN	✓	✓	✓	✓	✓	✓
SD-WAN	✓	✓	✓	✓	✓	✓
SSL Interception	✓	✓	✓	✓	✓	✓
Energize Updates	✓	✓	✓	✓	✓	✓
Barracuda Firewall Insights	Optional	Optional	Optional	Optional	✓	✓
Malware Protection <sup>1</sup>	Optional	Optional	Optional	Optional	-	-
Advanced Threat Protection <sup>1</sup>	Optional	Optional	Optional	Optional	-	-
Advanced Remote Access	Optional	Optional	Optional	Optional	✓	✓
Premium Support <sup>2</sup>	Optional	Optional	Optional	Optional	-	-



<sup>1</sup> Inklusive FTP, E-Mail- und Web-Protokolle

<sup>2</sup> Mit dem Premium Support wird die maximale Performance für das Netzwerk einer Organisation gewährleistet – dank technischem Support für betriebskritische Umgebungen rund um die Uhr.

Weitere Informationen finden Sie unter <https://www.barracuda.com/support/premium>.

Diese Angaben können sich ohne Ankündigung ändern.