

Aufgrund der wachsenden Cloud Computing-Funktionen und –Services befinden sich immer mehr Daten an Stellen, wo herkömmliche IT-Sicherheitsmaßnahmen nicht mehr greifen: genauer gesagt in Datenzentren, die nicht zur IT-Gruppe Ihres Unternehmens gehören.

Barracuda CloudGen Firewall bietet **zentrale Verwaltung und hoch sicheren, verschlüsselten Datenverkehr zu, von und innerhalb des Google Cloud Platform (GCP)-Deployments.**

- ☑ Security
- ☐ Data Protection
- ☐ Application Delivery

## Der Barracuda-Vorteil

- Eine echte Cloud-Generation Firewall: flexible Deployment-Möglichkeiten und integrierte GCP-spezifische Funktionen und Lizenzmodelle sorgen für reibungslosen Geschäftsverkehr
- Einfache Bedienung, Integration von On-Premises- und Cloud-Sicherheit in einer einzigen Oberfläche
- Sichere und zuverlässige Konnektivität zwischen standortbasierten und GCP-Bereitstellungen
- Zentrale Verwaltung aller Funktionen sowohl für On-premise als auch für GCP-Installationen
- Einzigartige Quality of Service-Funktionen

## Produktmerkmale

- Volle User-/Group-Awareness
- Volle Application-Visibility und granulare Application-Control
- Advanced Threat Protection (inkl. Sandboxing)
- Integrierte Web-Security und IDS/IPS
- Integrierte SD-WAN Funktionalität
- Application-Based Provider Selection
- Echte Flexibilität in Sachen Lizenzierung: Bring-Your-Own-License oder Pay-as-You-Go (zeit-basiert)



### Sichere Konnektivität

Eine optimale GCP-Installation muss unbedingt auf sichere und zuverlässige Art gestartet werden. Durch die Installation einer Barracuda CloudGen Firewall in GCP erhalten Sie umfassende, sichere Konnektivitätsfunktionen, beginnend mit leistungsstarken TINA-VPN-Tunneln für Site- to-Site- und Client-to-Site-Verbindungen. Die Bereitstellung umfasst bewährte WAN-Optimierungsfunktionen, um die höchstmögliche Quality of Service zu erhalten.



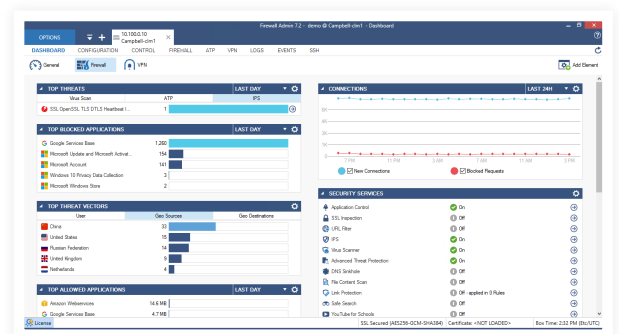
### Integrierte Next-Generation Sicherheit

Die Barracuda CloudGen Firewall wurde von Grund auf für umfassende Next-Generation Firewall-Funktionalität ausgelegt und zugeschnitten. Die Barracuda CloudGen Firewall basiert auf Application Visibility, User Identity, Intrusion Prevention und zentraler Verwaltung und ist somit die ideale Lösung für moderne, dynamische Unternehmen, die GCP in ihr Unternehmensnetzwerk einbinden.



### Zentrale Verwaltung

Benutzer der Barracuda CloudGen Firewall profitieren von derselben transparenten zentralen Verwaltung, die auch bei On-Premise Installation eingesetzt wird. Damit können die sicheren VPN-Verbindungen zu, von und innerhalb von GCP sowie die Barracuda CloudGen Firewall selbst verwaltet werden.



Das Dashboard der Barracuda CloudGen Firewall bietet Echtzeitinformationen und Zusammenfassungen aller Prozesse in einem Unternehmensnetzwerk.



Google Cloud Platform und Barracuda CloudGen Firewall helfen uns dabei, unsere primäre Mission zu erfüllen: Menschen dabei zu helfen, finanziell stabil zu werden, um ihr Leben zu verbessern.

Kishore Venkat  
IT Solutions Lead  
Opportunity Fund

## Technische Spezifikationen

### Firewall

- Stateful Packet Inspection und Forwarding
- IP-lose Konfiguration mittels Named-Networks
- 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 und 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
- REST API

### Unterstützte Protokolle

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

### Intrusion Detection und Prevention

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

### 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 (Exploits)
- Unterstützung für mehrere Betriebssysteme (Windows, Android, usw.)
- Botnet- und Spyware-Schutz
- TypoSquatting und Link- Protection für E-Mail

### 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

### Infrastructure Services

- DHCP-Server, Relay
- SIP-, HTTP-, SSH-, FTP-Proxies
- SMTP-Gateway & IPFIX Unterstützung
- DNS Cache

### Traffic Intelligence & SD-WAN

- Zertifizierte Verschlüsselung (FIPS 140-2)
- Automatische VPN-Tunnel-Erstellung zwischen entfernten Spoke-Standorten basierend auf dem Anwendungstyp
- Dynamische Bandbreitenerkennung
- Performance-basierte Transportauswahl
- Adaptive Session-Balancing über mehrere Uplinks hinweg
- Traffic-Replikation (vorwärts gerichtete Fehlerkorrektur)
- Application-based Provider Selection
- Anwendungsorientiertes Traffic-Routing (VPN)
- Traffic-Shaping und QoS
- Integrierte Datenduplizierung

### VPN

- VPN-Tunnel-Konfiguration per Drag-and-Drop
- Network Access Control
- VPN-Unterstützung für Mobilgeräte mit iOS und Android
- Multi-Faktor Authentisierung für SSL VPN und CudaLaunch

### Barracuda Energize Updates

- Standardmäßiger technischer Support
- Firmware-Updates
- IPS-Signaturen-Updates
- Application-Control Definition-Updates
- Online Web Filter

BARRACUDA CLOUDGEN FIREWALL	BRING-YOUR-OWN-LICENSE					PAY-AS-YOU-GO LICENSE (ZEIT-BASIERT)
LEISTUNGSMERKMALE	Level 1	Level 2	Level 4	Level 6	Level 8	
Virtuelle Kerne	1	1	2	4	8	nicht eingeschränkt
Geschützte IP Adressen	10	unlimitiert	unlimitiert	unlimitiert	unlimitiert	unlimitiert
FUNKTIONEN						
Firewall	•	•	•	•	•	•
Application Control	•	•	•	•	•	•
IPS	•	•	•	•	•	•
VPN (Site-to-Site und Client-to-Site)	•	•	•	•	•	•
SSL Interception	•	•	•	•	•	•
WAN Compression	•	•	•	•	•	•
Network Access Control für VPN Client-to-Site-Verbindungen	•	•	•	•	•	•
Energize Updates	•	•	•	•	•	•
Malware Protection <sup>1</sup>	Optional	Optional	Optional	Optional	Optional	-
Advanced Threat Protection <sup>1</sup>	Optional	Optional	Optional	Optional	Optional	-
Advanced Remote Access	Optional	Optional	Optional	Optional	Optional	•
Premium Support <sup>2</sup>	Optional	Optional	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>.

## Sicherheitsoptionen

- **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-Verkehr.
- **Advanced Remote Access** bietet ein anpassbares und benutzerfreundliches portalbasiertes SSL-VPN sowie anspruchsvolle Network Access Control (NAC)-Funktionalität und CudaLaunch-Unterstützung.

Diese Angaben können sich ohne Ankündigung ändern.