Barracuda **CloudGen Firewall für AWS**

Schutz Ihrer digitalen Assets in Amazon Web Services

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

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

aws partner network
Advanced Technology Partner
Security Competency
GovCloud (US) Skill Partner
Public Sector Partner
Marketplace Seller

aws competency

Der Barracuda-Vorteil

- Eine echte Cloud-Generation Firewall: flexible Deployment-Möglichkeiten und integrierte AWS-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 Amazon Web Services-Bereitstellungen
- Zentrale Verwaltung aller Funktionen sowohl für On-premise als auch für Amazon Web Services-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
- Volle Unterstützung von AWS Direct Connect
- Echte Flexibilität in Sachen Lizensierung: Bring-Your-Own-License oder Pay-as-You-Go (zeit- oder volumen-basiert)

Granulare Application Control

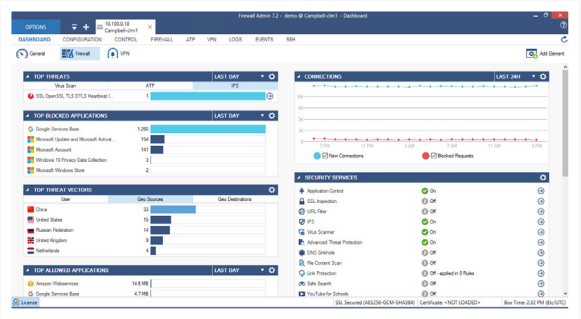
Barracuda CloudGen Firewall ermöglicht Administratoren granulare Kontrolle über Applikationen. Dabei können sie Regeln zur Weiterleitung des Datenverkehrs über die jeweils besten Übertragungskanäle je nach Applikationstyp, Benutzer, Inhalt, Tageszeit und geografischem Standort festlegen. Mit Barracuda 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.
Barracuda CloudGen Firewall enthält moderne Site-to-Site- und Client-to-Site-VPN-Funktionen, die sowohl SSL- als auch IPsec-Protokolle verwenden, um zu gewährleisten, dass Remote-Benutzer einfach und sicher auf Netzwerkressourcen zugreifen können, ohne dass eine komplexe Client-Konfiguration und -Verwaltung erforderlich ist.

Zentrale Verwaltung

Barracuda CloudGen Firewall profitiert vom selben branchenführenden transparenten zentralen Management, das auch bei standortbasierten Bereitstellungen eingesetzt wird. Damit können die sicheren VPN-Verbindungen zu, von und innerhalb von Amazon Web Services sowie die Barracuda CloudGen Firewall selbst gemanagt werden.



Das Dashboard der Barracuda CloudGen Firewall bietet Informationen in Echtzeit und Zusammenfassungen über Vorgänge im Netzwerk.

BARRACUDA NETWORKS NEXT GENERATION FIREWALL NSS RECOMMENDED

ICSA labs CERTIFIED ENTERPRISE

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

FIPS VALIDATED 140-2

Wir verwenden Barracuda CloudGen Firewalls, die über den AWS Marketplace bereitgestellt werden, um unsere Anwendung effektiv vor webbasierten Angriffen und Angriffen auf die Anwendungsebene zu schützen. Die Barracuda-Lösung fügt sich nahtlos in unsere AWS-Umgebung ein und erfüllt ihre Aufgabe, die Angriffsfläche zu minimieren und unseren Kunden dabei zu helfen, die Daten der Club-Mitgliederkarteninhaber zu schützen.

Max Longin
Gründungspartner
Club Automation

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

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.)
- Detailierte 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 Lizensierung
- Template & Repository-basiertes Management
- REST API

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
- Anwendungsorientiertes Traffic-Routing
- Adaptives Session-Balancing über mehrere Uplinks hinweg
- Traffic-Replikation (vorwärts gerichtete Fehlerkorrektur)
- Application-based Provider Selection
- Anwendungsorientiertes Traffic-Routing (VPN, Direct Connect)
- Traffic-Shaping und QoS
- Integrierte Datendeduplizierung

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
- Web-Filter-Updates

BARRACUDA CLOUDGEN FIREWALL	BRING-YOUR-OWN-LICENSE					PAY-AS-YOU-GO LICENSE	
						ZEIT-BASIERT	VOLUMEN-BASIERT
LEISTUNGSMERKMALE	**Level 1**	**Level 2**	**Level 4**	**Level 6**	**Level 8**	nicht eingeschränkt	nicht eingeschränkt
Geschützte IP Addressen	10	unlimitiert	unlimitiert	unlimitiert	unlimitiert	unlimitiert	unlimitiert
Virtuelle Kerne	1	1	2	4	8	nicht zutreffend	nicht zutreffend
Max. Anzahl an Interfaces	2	2	2	4	4	nicht zutreffend	nicht zutreffend
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 [1]	Optional	Optional	Optional	Optional	Optional	-	-
Advanced Threat Protection [1]	Optional	Optional	Optional	Optional	Optional	-	-
Advanced Remote Access	Optional	Optional	Optional	Optional	Optional	●	●
Premium Support [2]	Optional	Optional	Optional	Optional	Optional	-	-

[1] Inklusive FTP, E-Mail- und Web-Protokolle

[2] 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.