

Barracuda CloudGen Firewall



Schutz von Cloud-verbundenen Benutzern, Netzwerken, Workloads und Geräten – wo auch immer sie sich befinden.

Immer mehr Unternehmen machen die Public Cloud zu einem Bestandteil ihrer Netzwerke. Dadurch wandeln sich Firewalls vom reinen Perimeterschutz hin zum Dreh- und Angelpunkt der IT Kommunikation. Die Barracuda CloudGen Firewall wurde speziell für die Optimierung der Leistung, Sicherheit und Verfügbarkeit moderner, verteilter Unternehmens-SD-WANs entwickelt.

Barracuda CloudGen Firewall kombiniert Next-Generation Security, leistungsstarke SD-WAN-Funktionen und einfache zentrale Verwaltung für Hunderte oder Tausende von Firewalls. Zero-Touch Deployment und native Cloud-Integration ermöglichen die schnelle und einfache Inbetriebnahme in jeder Umgebung.

Kompromisslose Sicherheit

Barracuda CloudGen Firewall schützt das gesamte Unternehmensnetzwerk. Firewalling, IPS, URL-Filtering, dualer Virenschutz und Applikationskontrolle erfolgt verzögerungslos direkt im Datenfluss. Ressourcenintensivere Schutzmechanismen zur Abwehr von Ransomware durch Sandboxing erfolgen nahtlos integriert in der Cloud. Der Schutzbereich ist über alle Plattformen und Modelltypen identisch - egal ob Aussenstellen- oder High-End Modelle - maximale Sicherheit bleibt gewährleistet.

Sichere SD-WAN-Konnektivität

Das Cloud-Zeitalter stellt Unternehmen vor die Anforderung jede Niederlassung direkt und sicher mit der Cloud zu verbinden. Eine solche Verbindung über ein einziges, zentrales Gateway ist kostspielig und macht Cloud-basierte Anwendungen durch erhöhte Latenz unbenutzbar. Eine optimierte Internet-Uplink-Auswahl sorgt für schnelle SaaS-Anwendungen. Barracuda CloudGen Firewall nutzt bis zu 24 Breitbandanschlüsse pro SD-WAN Verbindung für bestmögliche Performance und Redundanz.

Cloud-Automatisierung

Der große Vorteil des Wechsels in die Cloud liegt in mehr Agilität und Flexibilität. Dies erfordert einen hohen Grad an Automatisierung. Alle Komponenten, einschließlich der Infrastruktur für Sicherheit und Konnektivität, müssen sich an die Funktionsweise anpassen. CloudGen Firewall bietet vollautomatischen Schutz für Multi-Cloud-Deployments, einschließlich SD-WAN-Automatisierung bei mehreren Cloud-Anbietern, vor Ort und virtuell.

Technische Angaben

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 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
- Network Security Orchestrierung mit tufin SecureTrack

Unterstützte Protokolle

- IPv4, IPv6
- BGP/OSPF/RIP
- VoIP (H.323, SIP, SCCP [skinny])
- RPC-Protokolle (ONC, DCE)
- 802.1q VLAN
- Industrielle Protokolle und deren Unterprotokolle (S7, S7+, IEC 60870-5-104, IEC 61850, MODBUS, DNP3)

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

Zentrale Management-Optionen über Firewall Control Center

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

Remote und Zero Trust Access

- VPN-Tunnel-Konfiguration per Drag-and-Drop
- Network Access Control
- Unterstützung für Mobilgeräte mit iOS und Android
- Zwei-Faktor Authentisierung mittels Time-based One-Time Passwords (TOTP), Radius, oder RSA MFA (erfordert eine gültige Advanced Remote Access Subscription) für Remote Access Clients
- Multi-Faktor Authentisierung für browser gestützten Remote Access und CudaLaunch
- ZTNA Funktionalität mittels Barracuda SecureEdge Access Agent Unterstützung

Infrastructure Services

- DHCP-Server, Relay
- SIP- und HTTP-Proxies
- SMTP-Gateway & IPFIX Unterstützung
- JSON Lifecycle-Automatisierungs-API
- Auto VPN über API / Script Control
- Autoritative DNS Server
- DNS Server
- DNS Cache
- WLAN (802.11n)-Access Point für ausgewählte Modelle
- Integrierte Unterstützung für Azure Virtual WAN

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

High Availability

- Aktiv-Passiv
- Transparentes Failover ohne Session-Verlust
- Verschlüsselte HA-Kommunikation

Self-Healing SD-WAN

- Optimierte Internet-Uplink-Auswahl
- Optimierte Internet Uplinks (Forward Error Correction)
- Gleichzeitige Nutzung mehrerer Uplinks (Transports) pro SD-WAN Verbindung
- Zertifizierte Verschlüsselung (FIPS 140-2)
- On-demand Verbindungsaufbau zwischen entfernten Spoke-Standorten basierend auf dem Anwendungstyp
- Dynamische Bandbreitenerkennung
- Performance-basierte Transportauswahl
- Anwendungsorientiertes Traffic-Routing
- Adaptive Session-Balancing über mehrere Uplinks hinweg
- Applikationsbasierte Providerwahl
- Traffic-Shaping und QoS
- Integrierte Datenduplizierung

Support Optionen

Barracuda Energize Updates

- Standardmäßiger technischer Support
- Firmware-Updates
- IPS-Signature-Updates
- App Control Definitionupdates
- Web-Filter-Updates

Instant Replacement Service

- Austauschgeräteversand innerhalb eines Werktags
- Technischer 24-Stunden-Support
- Alle vier Jahre gratis Hardware Refresh

Verfügbare Subscriptions

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.

Malware Protection

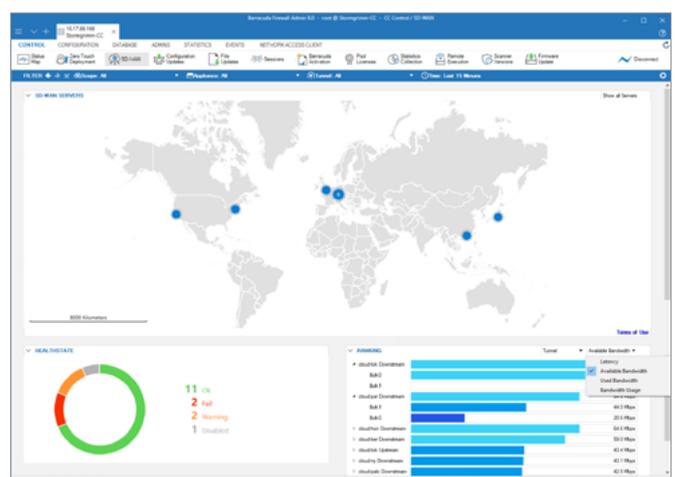
Schützt Gateway-gestützt vor Schadsoftware, Viren und anderen unerwünschten Programmen in SMTP/S-, HTTP/S- und FTP/S-Datenverkehr.

Advanced Threat Protection

Schützt vor Sicherheitslücken im Netzwerk, identifiziert Zero-Day-Malware-Angriffe, gezielte Angriffe, fortgeschrittene persistente Bedrohungen und andere fortschrittliche Malware.

Advanced Remote Access

Bietet anpassbaren und benutzerfreundlichen browser-gestützten Remote Access sowie anspruchsvolle Network Access Control (NAC)-Funktionalität und CudaLaunch-Unterstützung.



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

Grundfunktionen

	EINSTIEGS- UND BRANCH OFFICE / RUGGED MODELLE	MID-RANGE MODELLE	HIGH-END MODELLE
Firewall inkl. IPS	✓	✓	✓
Application Control	✓	✓	✓
Dynamic Routing	✓	✓	✓
Application-based Provider Selection	✓	✓	✓
TLS Inspection	✓	✓	✓
Secure SD-WAN	✓	✓	✓
Automatisierung der Cloud-Konnektivität mit Azure Virtual WAN	✓	✓	✓
Web Filter	✓	✓	✓
Zero-Touch Deployment	✓	✓	✓
Remote Access	✓	✓	✓

Optionale Funktionen

	EINSTIEGS- UND BRANCH OFFICE / RUGGED MODELLE	MID-RANGE MODELLE	HIGH-END MODELLE
Firewall Insights	Optional	Optional	Optional
Advanced Threat Protection	Optional	Optional	Optional
Malware Protection	Optional ¹	Optional	Optional
Advanced Remote Access	Optional ²	Optional	Optional

Einstiegs- und Branch Office / Rugged Modelle

	EINSTIEGS- UND BRANCH OFFICE MODELLE					RUGGED MODELLE	
	F12A	F18B	F80B	F180B	F280C	F93A.R	F193A.R
DURCHSATZ / LEISTUNG							
Firewall ³	1.2 Gbps	2.0 Gbps	2.0 Gbps	3.2 Gbps	4.8 Gbps	1.5 Gbps	2.1 Gbps
SD-WAN ⁴	220 Mbps	720 Mbps	720 Mbps	800 Mbps	1.5 Gbps	240 Mbps	320 Mbps
IPS ⁵	400 Mbps	600 Mbps	600 Mbps	1.0 Gbps	2.0 Gbps	400 Mbps	790 Mbps
NGFW ⁶	250 Mbps	400 Mbps	400 Mbps	1.2 Gbps	1.6 Gbps	400 Mbps	800 Mbps
Threat Protection ⁷	230 Mbps	380 Mbps	380 Mbps	1.0 Gbps	1.5 Gbps	380 Mbps	700 Mbps
Gleichzeitige Sessions	80,000	80,000	80,000	150,000	300,000	80,000	100,000
Neue Sessions/s	8,000	12,000	12,000	12,000	12,000	8,000	9,000
HARDWARE							
Formfaktor	Kompakt	Desktop	Desktop	Desktop	Desktop	Kompakt, Hutschiene	Kompakt, Hutschiene
Kupfer-Ethernet NICs [1 GbE]	5x	5x	5x	12x	12x	2x	5x
Glasfaser-Ethernet SFP NICs [1 GbE]	-	-	-	4x	4x	1x	2x
WLAN Access Point	-	-	✓	✓	✓	-	-
Stromversorgung	Einfach, extern	Einfach, extern	Einfach, extern	Einfach, extern	Einfach, extern	Phoenix 4-pin oder Dual, extern	Phoenix 4-pin oder Dual, extern

Mid-Range Modelle

	F380B	F400C MODELLE		F600D MODELLE				
		STD	F20	C10	C20	F10	F20	E20
DURCHSATZ / LEISTUNG								
Firewall ³	8.5 Gbps	13 Gbps	13 Gbps	15 Gbps		15 Gbps		20 Gbps
SD-WAN ⁴	2.1 Gbps	3.6 Gbps	3.6 Gbps	3.8 Gbps		3.8 Gbps		6.8 Gbps
IPS ⁵	2.5 Gbps	4.2 Gbps	4.2 Gbps	4.8 Gbps		4.8 Gbps		8.0 Gbps
NGFW ⁶	2.0 Gbps	3.7 Gbps	3.7 Gbps	4.2 Gbps		4.2 Gbps		6.4 Gbps
Threat Protection ⁷	1.7 Gbps	3.1 Gbps	3.1 Gbps	4.0 Gbps		4.0 Gbps		5.8 Gbps
Gleichzeitige Sessions	400,000	500,000	500,000	2,100,000		2,100,000		2,100,000
Neue Sessions/s	15,000	20,000	20,000	115,000		115,000		115,000
HARDWARE								
Formfaktor	1U rack mount	1U rack mount		1U rack mount				
Kupfer-Ethernet NICs [1 GbE]	8x	8x	8x	18x	18x	10x	10x	10x
Glasfaser-Ethernet SFP NICs [1 GbE]	-	-	4x	-	-	8x	8x	8x
Glasfaser-Ethernet SFP+ NICs [10 GbE]	2x	2x	2x	-	-	-	-	2x
Stromversorgung	Einfach, intern	Einfach, intern	Dual, hot swap	Einfach, intern	Dual, hot swap	Einfach, intern	Dual, hot swap	Dual, hot swap

High-End Modelle

	F800C MODELLE			F900B MODELLE				F1000B MODELLE				
	CCC	CCF	CCE	CCC	CCE	CFE	CFEQ	CE0	CE2	CFE	CFEQ	
DURCHSATZ / LEISTUNG												
Firewall ³	34.5 Gbps			43 Gbps				54 Gbps	52 Gbps			
SD-WAN ⁴	9 Gbps			12.1 Gbps				17.6 Gbps	15.8 Gbps			
IPS ⁵	10 Gbps			13.8 Gbps				15.6 Gbps	16 Gbps			
NGFW ⁶	8.1 Gbps			10 Gbps				14.4 Gbps	14.8 Gbps			
Threat Protection ⁷	8 Gbps			9.6 Gbps				13.8 Gbps	13.5 Gbps			
Gleichzeitige Sessions	2,500,000			4,000,000				4,000,000	10,000,000			
Neue Sessions/s	180,000			190,000				190,000	250,000			
HARDWARE												
Formfaktor	1U rack mount			1U rack mount				2U rack mount				
Kupfer-Ethernet NICs [1 GbE]	24x	16x	16x	32x	16x	8x	8x	16x	32x	16x	16x	
Glasfaser-Ethernet SFP NICs [1 GbE]	-	8x	-	-	-	8x	8x	-	-	16x	16x	
Glasfaser-Ethernet SFP+ NICs [10 GbE]	-	-	4x	-	8x	8x	4x	4x	8x	8x	6x	
Glasfaser-Ethernet QSFP+ NICs [40 GbE]	-	-	-	-	-	-	2x	-	-	-	2x	
Stromversorgung	Dual, Hot Swap			Dual, Hot Swap				Dual, Hot Swap				

Alle Performance-Zahlen werden unter optimierten Bedingungen gemessen, sind als "bis zu" Werte zu betrachten und können je nach Systemkonfiguration und Infrastruktur variieren:

¹ Für das Model F12A ist Malware Protection durch Cloud-basierte Malware Protection im Zuge einer aktiven Advanced Threat Protection Subscription gegeben.

² Für das Model F12A ist diese Funktion nicht verfügbar.

³ Firewall-Durchsatz gemessen mit großen UDP-Paketen (MTU1500), bidirektional über mehrere Ports.

⁴ SD-WAN-Durchsatz basiert auf 1415 Byte UDP-Paketen, bidirektional mit BreakingPoint-Traffic-Generator.

⁵ IPS-Durchsatz gemessen mit großen UDP-Paketen (MTU1500) und über mehrere Ports.

⁶ NGFW-Durchsatz wird mit aktivem IPS, Application Control und Web Filter, basierend auf BreakingPoint Realworld-IPS-Enterprise-Traffic-Mix, bidirektional über mehrere Ports hinweg gemessen.

⁷ Threat-Protection-Durchsatz wird mit aktivem IPS, Application Control, Web Filter, Antivirus und TLS-Inspection, basierend auf

BreakingPoint Realworld-IPS-Enterprise-Traffic-Mix, bidirektional über mehrere Ports hinweg gemessen.

Angaben können sich ohne Ankündigung ändern.

