

Durch die Integration des "Internet der Dinge" (Internet of Things) werden Unternehmensnetzwerke jeden Tag größer und komplexer – und haben immer mehr Einfluss auf das Kerngeschäft vieler Unternehmen. Barracuda Cloud Generations sind ein wichtiges Tool für die **Leistungsoptimierung, Sicherheit und Verfügbarkeit für die verzweigten Unternehmens-WANs der heutigen Zeit.**

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

Der Barracuda-Vorteil

- Schnelle Bereitstellung
- Umfassendes Reporting
- Hoch skalierbar
- Vollständig kompatibel mit Microsoft Azure, Amazon Web Services und Google Cloud Platform

Produktmerkmale

- Leistungsstarke Next-Generation Netzwerk-Firewall
- Advanced Threat Protection (inkl. Sandboxing)
- Integrierte Web-Security und IDS/IPS
- Vollständige Anwendungstransparenz und detaillierte Steuerung
- Linux-Container für anwenderspezifische Applikationen (Edge Computing)
- Zentralisiertes Management aller Funktionen
- Vorlagen- und rollenbasierte Konfiguration
- Zero-Touch Deployment (für Secure Connector 2.x-Modelle)



Ein sicheres Internet der Dinge

Barracuda Cloud Generation Firewalls wurden speziell als eine umfassende Next-Generation Sicherheitslösung entwickelt, die einfach in der Bereitstellung und Wartung sowie hoch skalierbar ist. Benötigen Sie eine Verbindung von kleinen Zweigstellen, Verkaufsstellen und Maschine-zu-Maschine? Dann sind Barracuda Cloud Generation Firewalls genau das Richtige für Sie.



Machine Access Security Broker

Der Secure Access Controller fungiert als Knotenpunkt für die Konnektivität und die Sicherheit des Datenstroms. Der Secure Access Controller bietet die volle Next-Generation Firewall-Funktionalität und kann auf VMware-, Hyper-V-, XenServer- oder KVM-Umgebungen sowie direkt in Microsoft Azure, Amazon Web Services und Google Cloud Platform ausgeführt werden.



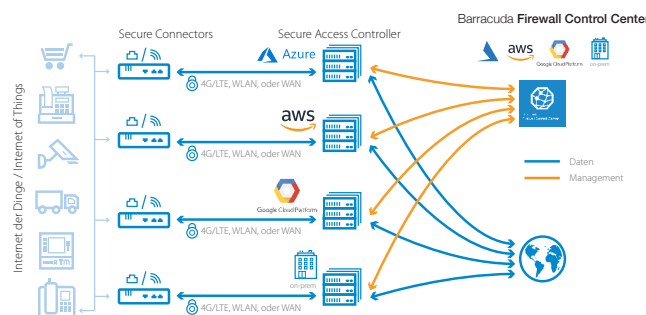
Einfache Einrichtung und Wartung – Secure Connector

Der Barracuda Secure Connector ist eine Purpose-Built Hardware-Appliance, die vor Ort als Verbindungsgerät fungiert und dadurch die leistungsstarke und manipulationssichere VPN-Verbindung sicherstellt, wodurch der Datenverkehr geschützt und gleichzeitig eine unterbrechungsfreie Datenverbindung sichergestellt wird.



Wächst mit den Anforderungen

Die Integration in die Barracuda Firewall Control Center-Architektur stellt sicher, dass Sie Ihre Bereitstellung an Ihre wachsenden Anforderungen anpassen können, ohne das technische oder finanzielle Nachsehen zu haben. Die Vorlagen-basierte Konfiguration garantiert eine einfache Bereitstellung von zusätzlichen Geräten und unterstützt die Einhaltung von Compliance-Anforderungen.



Mit den Barracuda Secure Connectors sind die Wi-Fi Access Points in den öffentlichen Bussen sicher, immer mit dem Rechenzentrum verbunden und die zentrale Verwaltung ist kein Thema mehr.

Frank van Tuyl
Consultant
ICT Vision B.V.

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
- SafeSearch enforcement
- Google Account 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

VPN

- Sicheres Site-to-Site VPN
- Unterstützt AES-128/256, 3DES, DES, Blowfish, CAST, Null

Hypervisor- & Public-Cloud

Unterstützung (für Secure Access Controller und Firewall Control Center)

- VMware
- Hyper-V
- XenServer
- KVM
- Microsoft Azure
- Amazon Web Services
- Google Cloud Platform

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.)
- Flexible Malware Analyse in der Cloud

High Availability (HA)

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

Zentrales Management

- Barracuda Firewall Control Center
 - Unbegrenzte Secure Access Controller und Secure Connector
 - Mandantenfähig
 - Multi-Administrator und RCS

Protokollunterstützung

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

Support-Optionen

Barracuda Energize Updates

- Technischer Standardsupport
- Firmware-Updates
- IPS-Signaturen-Updates
- Application Control Definitionupdates
- Web-Filter Updates

SECURE CONNECTOR	SC1	SC2.0	SC2.1	SC2.2	SC2.3
INTERFACES					
WAN Kupfer NICs (PoE-Recipient) ¹	1x1 GbE	1x1 GbE	1x1 GbE	1x1 GbE	1x1 GbE
LAN Kupfer NICs (Switch) ¹	1x1 GbE	3x1 GbE	3x1 GbE	3x1 GbE	3x1 GbE
USB 2.0	1	1	1	1	1
Micro-USB OTG	1	1	1	1	1
WiFi (Access Point / Client Mode)	●	-	●	-	●
3G / UMTS Unterstützung	-	-	-	●	●
LEISTUNG					
Firewall Durchsatz (UDP)	300 Mbps	300 Mbps	300 Mbps	300 Mbps	300 Mbps
WiFi AP Durchsatz (UDP)	80 Mbps	-	80 Mbps	-	80 Mbps
VPN Durchsatz (AES-128, SHA)	30 Mbps	30 Mbps	30 Mbps	30 Mbps	30 Mbps
SPEICHER					
RAM [GB]	1	1	1	1	1
MASSENSPEICHER					
Typ	Micro SD	Micro SD	Micro SD	Micro SD	Micro SD
Grösse [GB]	16	16	16	16	16
GEWICHT, ABMESSUNGEN					
Gewicht [kg]	0.16	0.55	0.6	0.6	0.65
Abmessungen (BxTxH) [mm]	28.3 x 132 x 94.7		37 x 140 x 150		
Formfaktor	Pocket Size		Compact, Hutschienenmontage		
HARDWARE					
Kühlung	Lüfterlos	Lüfterlos	Lüfterlos	Lüfterlos	Lüfterlos
Stromversorgung	●	Optional (PCB Connector, 12V-57V)			

SAC - VERSIONEN ²	SAC400	SAC610	SAC820
Anzahl der geschützten IPs	unlimited	unlimited	unlimited
Unterstützte Kerne	2	4	8
Max. Anzahl an VPN-Verbindungen	500	1,200	2,500
Firewall	●	●	●
Application Control ³	●	●	●
IPS ³	●	●	●
Dynamisches Routing	●	●	●
VPN ⁴	●	●	●
SSL Interception	●	●	●
Web Filter	●	●	●
Malware Protection ⁵	Optional	Optional	Optional
Advanced Threat Protection ⁵	Optional	Optional	Optional

Barracuda Secure Access Controller

Images sind verfügbar für:



¹ Die Funktionen "PoE-Recipient" und "Switch" sind nur auf SC2.x Modellen verfügbar.

² Das virtuelle Image des Barracuda Secure Access Controller umfasst alle Versionen.

³ Erfordert ein gültiges Energize Updates-Abonnement.

⁴ Die in den Barracuda Secure Access Controller-Versionen enthaltenen VPN-Lizenzen entsprechen der Anzahl der geschützten IPs. VPN-Clients mit einer aktiven Verbindung werden zur Begrenzung der geschützten IPs dazugezählt.

⁵ Inkludiert FTP, E-Mail und Web-Protokolle.

Änderungen vorbehalten.