Barracuda **NextGen Firewall S**

Skalierbare Sicherheit für das Internet der Dinge

- ☑ **Security**
- ☐ Storage
- ☐ Application Delivery
- ☐ Productivity

Unternehmensnetzwerke werden jeden Tag größer und komplexer – und haben immer mehr Einfluss auf das Kerngeschäft vieler Unternehmen. Die Barracuda NextGen Firewall S-Serie – Secure Connector 1 (SC1) und Secure Access Concentrator (SAC) – ist ein wichtiges Tool für die **Leistungsoptimierung, Sicherheit und Verfügbarkeit für die verzweigten Unternehmens-WANs der heutigen Zeit.**

Der Barracuda-Vorteil

- Schnelle Bereitstellung
- Umfassendes Reporting
- Hoch skalierbar
- Vollständig kompatibel mit Microsoft Azure

Produktmerkmale

- Leistungsstarke Netzwerk-Firewall der nächsten Generation
- Advanced Threat Detection
- Integrierte Web-Security und IDS/IPS
- Vollständige Anwendungstransparenz und detaillierte Steuerung
- Zentralisiertes Management aller Funktionen
- Vorlagen- und rollenbasierte Konfiguration
- **Verfügbar für VMware, XenServer, KVM, Hyper-V und Microsoft Azure**

Ein sicheres Internet der Dinge

Die Barracuda NextGen Firewall S-Serie wurde 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 ist die S-Serie genau das Richtige für Sie.

Bündelung des Datenverkehrs – SAC

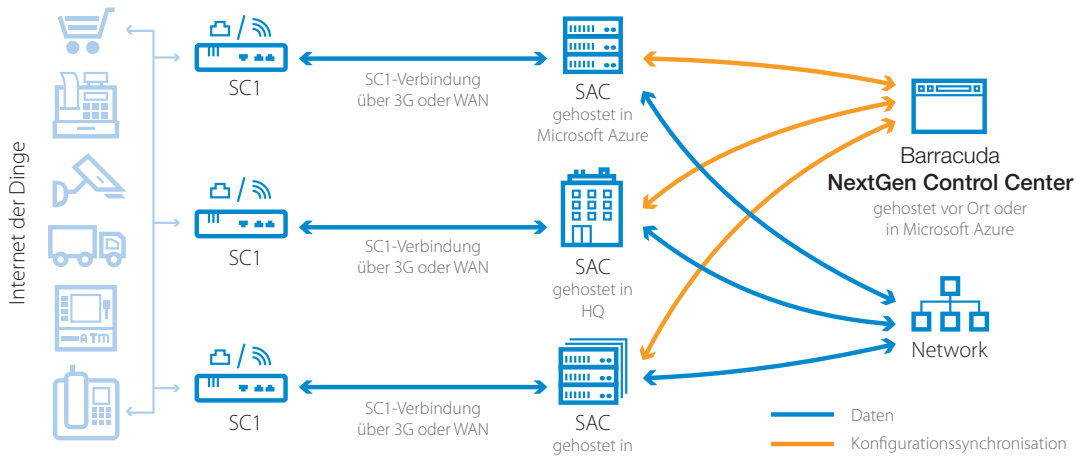
Beim Secure Access Concentrator wird der Datenverkehr gebündelt. Diese eigenständige NextGen Firewall agiert als VPN-Gateway für die SC1-Bereitstellungen. SACs können auf VMware-, Hyper-V-, XenServer- oder KVM-Umgebungen sowie direkt in Microsoft Azure ausgeführt werden.

Einfache Einrichtung und Wartung – SC1

Secure Connector (SC1) 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 NextGen 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



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
- YouTube for Schools Unterstützung
- 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

Hypervisor- & Public-Cloud Unterstützung (für SAC und NextGen Control Center)

- VMware
- Hyper-V
- XenServer
- KVM
- Microsoft Azure

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 Detection

- 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.)
- Flexible Malware Analyse in der Cloud

VPN

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

High Availability (HA)

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

Zentrales Management

- Barracuda NextGen Control Center
  - Unbegrenzte SACs und SC1s
  - Mandantenfähig
  - Multi-Administrator & RCS

Protokollunterstützung

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

Support-Optionen

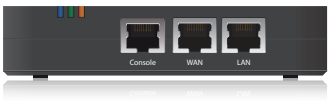
Barracuda Energize Updates

- Technischer Standardsupport
- Firmware-Updates
- IPS-Signaturen-Updates
- Application Control Definitionsupdates
- Online-Webfilter

Security-Optionen

- Advanced Threat Detection
- Malware Protection

Frontansicht einer Barracuda NextGen Firewall SC1.



Rückansicht einer Barracuda NextGen Firewall SC1.

SC1 - FAKTEN	
HARDWARE	
Dimensions (BxTxH) [mm]	132 x 94,7 x 28,3
Gewicht [kg]	0,16
1 GbE Kupfer	2
USB	1x Micro-USB OTG
	1x USB 2.0
RAM [GB]	1
Massenspeicher [Typ / GB]	MicroSD / 16
Stromversorgung	Einzeln (extern über Micro-USB)
WLAN Access Point	2.4 Ghz b/g
MERKMALE	
Management	Zentral über NextGen Control Center
	über Gerät via web-basierte Oberfläche
Firewall	Zonenregeln
	NAT (Source, Destination, Mapping)
	Zonen-basierter Service-Zugriff
Unterstützte Netzwerkdienste	NTP, SSH, DNS, DHCP, Wi-Fi Access Point
Unterstützte Uplink-Verbindung	Wi-Fi Client, DHCP Client, Static IP
Unterstützte VPN-Protokolle	TINA

SAC - VERSIONEN [1]	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 & VPN Throughput	1 Gbit/s	2 Gbit/s	4 Gbit/s
Firewall	•	•	•
Application Control [2]	•	•	•
IPS [2]	•	•	•
Dynamisches Routing	•	•	•
VPN [3]	•	•	•
SSL Interception	•	•	•
Web Filter	•	•	•
Malware Protection [4]	Optional	Optional	Optional
Advanced Threat Detection [4, 5]	Optional	Optional	Optional

[1] Das virtuelle Image des Barracuda NextGen Firewall S-Series SAC umfasst alle Versionen.
[2] Erfordert ein gültiges Energize Updates-Abonnement.
[3] Die in den Barracuda NextGen Firewall S-Serie SAC-Versionen enthaltenen VPN-Lizenzen entsprechen der Anzahl der geschützten IPs. VPN-Clients mit einer aktiven Verbindung zum Barracuda NextGen Firewall S-Serie SAC werden zur Begrenzung der geschützten IPs dazugezählt.
[4] Inkludiert FTP, E-Mail und Web-Protokolle
[5] Erfordert ein gültiges Malware Protection-Abonnement.

Änderungen vorbehalten.