Barracuda **NextGen Firewall S**

Scalable Security for the Internet of Things

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

Enterprise networks grow larger and more complex every day, thus becoming more critical to key business operations. The Barracuda NextGen Firewall S-Series—Secure Connector 1 (SC1) and Secure Access Concentrator (SAC)—is an essential tool for **optimizing the performance, security and availability of today's dispersed enterprise WANs.**

The Barracuda Advantage

- Quick rollout
- Comprehensive reporting
- Highly scalable
- Fully compatible with Microsoft Azure

Product Spotlight

- Powerful next-generation network firewall
- Advanced Threat Detection
- Built-in web security and IDS/IPS
- Full application visibility and granular controls
- Centralized management of all functionalities
- Template-based and role-based configuration
- **Available for VMware, XenServer, KVM, Hyper-V, and Microsoft Azure**

Securing the Internet of Things

The Barracuda NextGen Firewall S-Series is designed and built from the ground up to provide comprehensive, next-generation security while being simple to deploy and maintain, and highly scalable. Need to connect micro-offices, point of sales and machine-to-machine business? With the S-Series you're all set!

Bundling the data stream: SAC

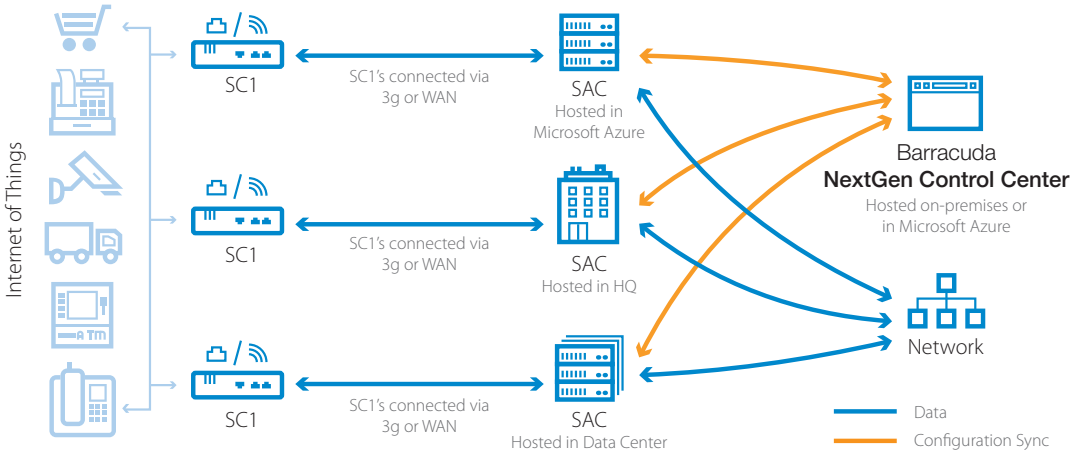
The Secure Access Concentrator is the collecting point for the data stream. This fully fledged NextGen Firewall acts as VPN gateway for the SC1 deployments. SACs can be run on VMware, Hyper-V, XenServer, or KVM environments as well as directly in Microsoft Azure.

Easy to setup and maintain: SC1

The Secure Connector (SC1) is a hardware appliance purpose-built to be an on-premises connectivity device that ensures high-performance and tamper-proof VPN connections to protect the data flow and, thus, guarantee data continuity.

Grows with your needs

Integration within the Barracuda NextGen Control Center architecture ensures that your deployment can grow with your needs without technical or financial trapdoors. The template-based configuration ensures easy rollout of additional devices and maintain compliance.



Technical Specs

Firewall

- Stateful packet inspection and forwarding
- Full user-identity awareness
- Intrusion Detection and Prevention System (IDS/IPS)
- Application control and granular application enforcement
- Interception and decryption of SSL/TLS encrypted applications
- Antivirus and web filtering in single pass mode
- SafeSearch enforcement
- YouTube for Schools support
- Denial of Service protection (DoS/DDoS)
- Spoofing and flooding protection
- ARP spoofing and trashing protection
- DNS reputation filtering
- TCP stream reassembly
- NAT (SNAT, DNAT), PAT
- Dynamic rules / timer triggers
- Single object-oriented rule-set for routing, bridging, and routed bridging
- Virtual rule test environment

Hypervisor and Public Support (for SAC and NextGen Control Center)

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

Intrusion Detection & Prevention

- Protection against exploits, threats and vulnerabilities
- Packet anomaly and fragmentation protection
- Advanced anti-evasion and obfuscation techniques
- Automatic signature updates

Advanced Threat Detection

- Dynamic, on-demand analysis of malware programs (sandboxing)
- Dynamic analysis of documents with embedded exploits (PDF, Office, etc.)
- Detailed forensics for both malware binaries and web threats (exploits)
- Support for multiple operating systems (Windows, Android, etc.)
- Flexible malware analysis in the cloud

VPN

- Secure site-to-site
- Supports AES-128/256, 3DES, DES, Blowfish, CAST, null ciphers

High Availability

- Active-passive
- Transparent failover without session loss
- Network notification of failover
- Encrypted HA communication

Central Management Options

- Barracuda NextGen Control Center
  - Unlimited SACs and SC1s
  - Support for multi-tenancy
  - Multi-administrator support & RCS

Protocol Support

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

Support Options

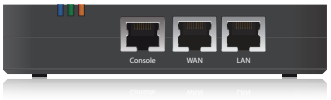
Barracuda Energize Updates

- Standard technical support
- Firmware updates
- IPS signature updates
- Application control definition updates
- Online web filter

Security Options

- Advanced Threat Detection
- Malware Protection

Front view of a Barracuda NextGen Firewall SC1.



Rear view of a Barracuda NextGen Firewall SC1.

SC1 - KEY FEATURES	
HARDWARE	
Dimensions (WxDxH) [mm / in]	132 x 94,7 x 28,3 / 5.2 x 3.73 x 1.11
Weight [kg / lbs]	0,16 / 0.35
1 GbE Copper	2
USB	1x Micro-USB OTG
	1x USB 2.0
RAM [GB]	1
Storage [Type / GB]	MicroSD / 16
Power Supply	Single (external via Micro USB)
Wi-Fi Access Point	2.4 Ghz b/g
FEATURES	
Management	Central via NextGen Control Center
	per Device via web-based user interface
Firewall	Zone rules
	NAT (source, destination, mapping)
	Zone-based service access
Supported Network Services	NTP, SSH, DNS, DHCP, Wi-Fi Access Point
Supported Uplink Connection	Wi-Fi Client, DHCP Client, Static IP
Supported VPN protocols	TINA

SAC - EDITIONS [1]	SAC400	SAC610	SAC820
Number of Protected IPs	unlimited	unlimited	unlimited
Allowed Cores	2	4	8
Max. number of VPN Connections	500	1,200	2,500
Firewall & VPN Throughput	1 Gbit/s	2 Gbit/s	4 Gbit/s
Firewall	●	●	●
Application Control [2]	●	●	●
IPS [2]	●	●	●
Dynamic Routing	●	●	●
VPN [3]	●	●	●
SSL Interception	●	●	●
Web Filter	●	●	●
Malware Protection [4]	Optional	Optional	Optional
Advanced Threat Detection [4, 5]	Optional	Optional	Optional

[1] The Barracuda NextGen Firewall S-Series SAC virtual image covers all editions.
[2] Requires a valid Energize Updates subscription.
[3] Barracuda NextGen Firewall S-Series SAC editions include as many VPN licenses as the number of protected IPs. VPN clients with an active connection to the Barracuda NextGen Firewall S-Series SAC are counted towards the protected IP limits.
[4] Including FTP, mail and Web protocols.
[5] Requires a valid Malware Protection subscription.

Specifications subject to change without notice.