Barracuda **Cloud Generation Firewalls**

Scalable Security for Internet of Things Connectivity

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

Properly managing enterprise networks is critical to key business operations as more businesses adopt Internet of Things. As these networks grow larger and more complex, it's important to implement robust security and performance of endpoint devices. Barracuda Cloud Generation Firewalls are 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, Amazon Web Services, and Google Cloud Platform

Product Spotlight

- Powerful next-generation network firewall
- Advanced Threat Protection (incl. sandboxing)
- Built-in web security and IDS/IPS
- Full application visibility and granular controls
- Linux container for custom edge computing
- Centralized management of all functionalities
- Template-based and role-based configuration
- Zero-Touch Deployment (for Secure Connector 2.x models)

Securing the Internet of Things

Barracuda Cloud Generation Firewalls are 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 Barracuda Cloud Generation Firewalls you're all set!

Machine Access Security Broker

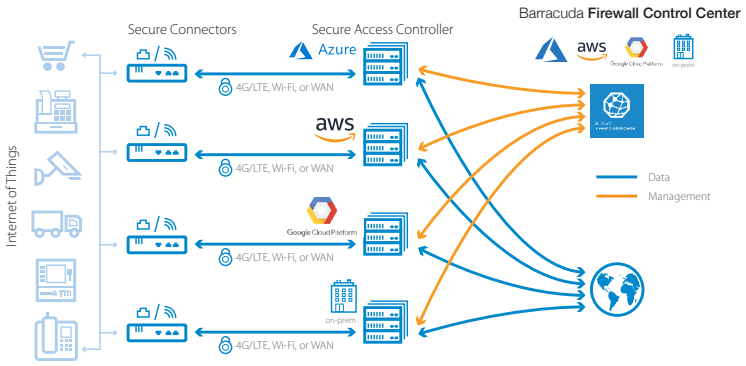
The Secure Access Controller acts as the connectivity and security enforcement hub for the data stream. The Secure Access Controller provides full next-generation firewall functionality and can be run on VMware, Hyper-V, XenServer, or KVM environments as well as directly in Microsoft Azure, Amazon Web Services, and Google Cloud Platform.

Easy to Setup and Maintain: Secure Connector

The Barracuda Secure Connector 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 Firewall 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.



With the Barracuda Secure Connectors the Wi-Fi access points on the public buses are secure, always connected to the datacenter and central management is no longer an issue.

Frank van Tuyl
Consultant
ICT Vision B.V.

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
- Google accounts enforcement
- 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

Central Management Options

- Barracuda Firewall Control Center
  - Unlimited Secure Access Controller and Secure Connectors
  - Support for multi-tenancy
  - Multi-administrator support and RCS

Hypervisor and Public Cloud Support (for Secure Access Controller and Firewall Control Center)

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

Intrusion Detection and Prevention

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

Advanced Threat Protection

- 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

High Availability

- Active-passive
- Transparent failover without session loss
- Encrypted HA communication

VPN

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

Protocol Support

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

Support Options

Barracuda Energize Updates

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

SECURE CONNECTOR	SC1	SC2.0	SC2.1	SC2.2	SC2.3
INTERFACES					
WAN Copper NICs (PoE-recipient) [1]	1x1 GbE	1x1 GbE	1x1 GbE	1x1 GbE	1x1 GbE
LAN Copper 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 support	-	-	-	●	●
PERFORMANCE					
Firewall throughput (UDP)	300 Mbps	300 Mbps	300 Mbps	300 Mbps	300 Mbps
WiFi AP throughput (UDP)	80 Mbps	-	80 Mbps	-	80 Mbps
VPN throughput (AES-128, SHA)	30 Mbps	30 Mbps	30 Mbps	30 Mbps	30 Mbps
MEMORY					
RAM [GB]	1	1	1	1	1
MASS STORAGE					
Type	Micro SD	Micro SD	Micro SD	Micro SD	Micro SD
Size [GB]	16	16	16	16	16
SIZE, WEIGHT, DIMENSIONS					
Weight appliance [lbs]	0.35	1.21	1.32	1.32	1.43
Weight appliance [kg]	0.16	0.55	0.6	0.6	0.65
Appliance size (WxDxH) [in]	1.11 x 5.2 x 3.73	1.5 x 5.5 x 5.9			
Appliance size (WxDxH) [mm]	28.3 x 132 x 94.7	37 x 140 x 150			
Form factor	Pocket Size	Compact, Din rail			
HARDWARE					
Cooling	Fanless	Fanless	Fanless	Fanless	Fanless
Power supply	●	optional (PCB Connector, 12V-57V)			

SAC - EDITIONS [2]	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	●	●	●
Application Control [3]	●	●	●
IPS [3]	●	●	●
Dynamic 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 are available for:

vmware · Microsoft Hyper-V · KVM · Citrix XenServer · aws · Azure · Google Cloud Platform

[1] Notations "PoE-recipient" and "Switch" apply for SC2.x models only.
[2] Barracuda Secure Access Controller virtual image covers all editions.
[3] Requires a valid Energize Updates subscription.
[4] Barracuda Secure Access Controller editions include as many VPN licenses as the number of protected IPs. VPN clients with an active connection to the SAC are counted towards the protected IP limits.
[5] Including FTP, mail and Web protocols.

Specifications subject to change without notice.