Barracuda Secure Connector

FIPS VALIDATED 140-2

Securing the industrial internet of things

Properly managing enterprise networks is critical to key business operations as more businesses adopt industrial internet of things (IIoT). As these networks grow larger and more complex, it's important to implement robust security and performance of endpoint devices. Barracuda Secure Connector appliances are an essential tool for optimizing the performance, security and availability of IIoT deployments.

Securing the industrial internet of things

Barracuda Secure Connector appliances 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 Secure Connector you're all set.

Easy to setup and maintain: Secure Connector

The 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.

Next-generation security and connectivity enforcement

Depending on the size of your Secure-Connector deployment, either a Barracuda CloudGen Firewall (when operating up to 250 Secure Connector units) or a dedicated Secure Access Controller (above 250 Secure Connector deployments) can act as the connectivity and security enforcement hub for the data stream. Both CloudGen Firewall and Secure Access Controller provide 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.

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 in combination with zero-touch deployment ensures easy rollout of additional devices and maintain compliance without the need of trained IT personnel on the ground.

Technical Specs

Secure Connector

- Policy-based firewall for TCP and UDP traffic
- Linux container for 3rd party software
- Wi-Fi (802.11n) on selected models

Firewall Control Center

- Administration for unlimited SACs/SCs
- Distribution, maintenance, and installation of Linux container
- Support for multi-tenancy
- Multi-administrator support & RCS
- Zero-touch deployment
- Enterprise/MSP licensing
- Template & repository-based management
- REST API

Secure Access Controller

Firewall

- Stateful packet inspection and forwarding
- Full user-identity awareness
- Application control and granular application enforcement
- Interception and decryption of SSL/TLS encrypted applications
- Denial of service protection (DoS/DDoS)
- Spoofing and flooding protection
- ARP spoofing and trashing protection
- DNS reputation filtering
- NAT (SNAT, DNAT), PAT
- Dynamic rules / timer triggers
- Single object-oriented rule set for routing, bridging, and routed bridging
- Virtual rule test environment
- Network security orchestration with tufin SecureTrack

Protocol support

- IPv4, IPv6
- BGP/OSPF/RIP
- VoIP (H.323, SIP, SCCP [skinny])
- RPC protocols (ONC-RPC, DCE-RPC)
- 802.1q VLAN
- Industrial protocols and subprotocols (S7, S7+,
  IEC 60870-5-104, IEC 61850,
  MODBUS, DNP3)

Self-Healing SD-WAN

- FIPS 140-2 certified cryptography
- Dynamic bandwidth detection
- Application-aware traffic routing
- Traffic shaping and QoS
- Built-in data deduplication

Infrastructure services

- DHCP server, relay
- SIP and HTTP proxies
- SNMP and IPFIX support
- JSON lifecycle automation API
- Auto VPN via API and script control
- DNS cache

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)
- Detailed forensic analysis
- Botnet and spyware protection

Models

	SC20	SC21	SC22	SC23	SC24 [1]	SC25 [1]	SC26 [2]	SC27 [2]	SC28 [3]	SC29 [3]
INTERFACES										
WAN copper NICs (PoE-recipient)	1x1 GbE	1x1 GbE	1x1 GbE	1x1 GbE	1x1 GbE	1x1 GbE	1x1 GbE	1x1 GbE	1x1 GbE	1x1 GbE
LAN copper NICs (Switch)	3x1 GbE	3x1 GbE	3x1 GbE	3x1 GbE	3x1 GbE	3x1 GbE	3x1 GbE	3x1 GbE	3x1 GbE	3x1 GbE
USB 2.0	1	1	1	1	1	1	1	1	1	1
Micro-USB OTG	1	1	1	1	1	1	1	1	1	1
WiFi (Access point / client)	-	✓	-	✓	-	✓	-	✓	-	✓
3G / UMTS support	-	-	✓	✓	✓	✓	✓	✓	✓	✓
4G / LTE support	-	-	-	-	✓	✓	✓	✓	✓	✓
PERFORMANCE										
Firewall throughput (UDP) [Mbps]	300	300	300	300	300	300	300	300	300	300
WiFi AP throughput (UDP) [Mbps]	-	80	-	80	-	80	-	80	-	80
VPN throughput (AES-128, SHA) [Mbps]	30	30	30	30	30	30	30	30	30	30
HARDWARE										
Form factor	Pocket size		Pocket size		Pocket size		Pocket size		Pocket size	
Appliance size (w x d x h) [in]	1.5 x 5.5 x 5.9		1.5 x 5.5 x 5.9		1.5 x 5.5 x 5.9		1.5 x 5.5 x 5.9		1.5 x 5.5 x 5.9	
Cooling	Fanless		Fanless		Fanless		Fanless		Fanless	
Power supply	PCB connector, 12V-57V		PCB connector, 12V-57V		PCB connector, 12V-57V		PCB connector, 12V-57V		PCB connector, 12V-57V	
Operating temperature [°F]	+30 to +105		+30 to +105		+30 to +105		+30 to +105		+30 to +105	
Operating humidity	5% to 95%		5% to 95%		5% to 95%		5% to 95%		5% to 95%	
Max. power draw [W]	40	40	40	40	40	40	40	40	40	40
Max. power draw @ 12V [A]	3.33	3.33	3.33	3.33	3.33	3.33	3.33	3.33	3.33	3.33

[1] Available in EMEA

[2] Available in US/CA

[3] Available in US/CA for deployments utilizing Verizon

Specifications subject to change without notice.

Barracuda®
Your journey, secured.