Barracuda CloudGen Firewall Rugged

Securing operational technology and industrial control systems.

Operating industrial control systems (ICS) in a secure way and integrating operational technology (OT) adds new challenges to the current standard means of protection and security management.
Barracuda CloudGen Firewall rugged appliances are the perfect fit for special requirements in regards to usability and operating concepts for industrial and harsh environments.

Full next-generation security

Barracuda CloudGen Firewall is designed and built from the ground up to provide comprehensive, next-generation firewall protection. Firewalling, IPS, dual antivirus and application control (including industrial protocols and subprotocols) take place directly in the data path.

More resource-intensive tasks like sandboxing —required for protecting against ransomware—are seamlessly integrated in the cloud. All CloudGen Firewall platforms and models provide the same level of security, maintaining maximum security for micro-segmentation for Operational Technology with local enforcement of highest security levels.

Security meets OT

ICS/OT security projects have to combine two operating concepts: while the individual firewall is part of hundreds to thousands of other similar firewalls that follow similar policies and ensure that all security components function in a traceable and controllable manner, the very same firewall is one of many different components of a system that has to be integrated into operation and maintenance concepts.

Just think about remote access for maintenance purposes. Remote access is predefined by the firewall administrator while it is activated on-demand and for a limited amount of time by the maintenance technician. Or imagine the replacement of equipment by the maintenance personal according to a simple procedure. However, the IT component in this simple process has to be prepared in such a way that it fits into the maintenance concept of the remaining machine components.

CloudGen Firewall enables OT to manage firewall deployments and remote connections as required in cooperation with the IT department.

Secure remote access for OT

For operational technology protected by CloudGen Firewall, secure remote access capabilities make it extremely convenient to grant secure, temporary VPN access to sensitive parts of manufacturing assets for third-party-maintenance providers.

Technical specs

Firewall

- Stateful packet inspection and forwarding
- Full user-identity awareness
- IDS/IPS
- Application control and granular application enforcement
- Interception and decryption of SSL/TLS encrypted applications
- Antivirus in single pass mode
- 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)

Advanced threat protection

- Dynamic, on-demand analysis of malware programs (sandboxing)
- Detailed forensic analysis
- Botnet and spyware protection

Infrastructure services

- DHCP server, relay
- JSON lifecycle automation API
- Auto VPN via API and script control
- DNS cache
- Built-in support for Azure Virtual WAN

Remote and Zero Trust Access

- Network access control
- iOS and Android mobile device support for remote access
- Two-factor authentication via timebased one-time passwords (TOTP), Radius, or RSA MFA (requires an active Advanced Remote Access subscription) for remote access clients
- Multi-factor authentication for CudaLaunch
- Barracuda CloudGen Access support - CloudGen Access Proxy service included with every CloudGen Firewall for quick Zero-Trust-Access rollout

Intrusion detection and prevention

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

Central management options via Barracuda Firewall Control Center

- Administration for unlimited firewalls
- Support for multi-tenancy
- Multi-administrator support & RCS
- Zero-touch deployment
- Enterprise/MSP licensing
- Template & repository-based mgmt.
- REST API

Self-Healing SD-WAN

- FIPS 140-2 certified cryptography
- Drag & drop tunnel configuration
- Dynamic bandwidth detection
- Performance-based transport selection
- Application-aware traffic routing
- Traffic shaping and QoS
- Built-in data deduplication

Support options

Barracuda Energize Updates

- Standard technical support
- Firmware updates
- IPS signature updates
- Application control definition updates
- Barracuda CloudGen Access support

Instant Replacement Service

- Replacement unit shipped next business day
- 24/7 technical support
- Free hardware refresh every four years

Available subscriptions

Barracuda Firewall Insights

Consolidates security, application flow, and connectivity information from hundreds or even thousands of firewalls on the extended wide area network – regardless of whether they are hardware, virtual, or cross-cloud-based deployments.

Malware Protection

Provides gateway-based protection against malware, viruses, spyware, and other unwanted programs inside SMTP/S, HTTP/S, and FTP/S traffic.

Advanced Threat Protection

Prevents from network breaches, identifies zero-day malware exploits, targeted attacks, advanced persistent threats and other advanced malware.

Advanced Remote Access

Provides a customizable and easy-to-use browser-based remote access as well as sophisticated network access control (NAC) functionality and CudaLaunch support.

	F93A.R	F193A.R
THROUGHPUT		
Firewall [1]	1.5 Gbps	2.1 Gbps
SD-WAN [2]	240 Mbps	320 Mbps
IPS [3]	400 Mbps	790 Mbps
NGFW [4]	400 Mbps	800 Mbps
Threat protection [5]	380 Mbps	700 Mbps
HARDWARE		
Form factor	Compact, DIN rail	
Copper NICs [1 GbE]	2x	5x
Fiber NICs (SFP) [1 GbE]	1x	2x
Power supply	Phoenix 4-pin	Phoenix 4-pin
Power type	DC	DC
Max power draw [W]	60	60
Max power draw @ 24V [Amps]	2.5	2.5
Operation temperature [°F]	-40 to +167	-40 to +167
Operating humidity	5% to 95%	5% to 95%
Magnetic isolation protection	1.5KV built-in	1.5KV built-in
Appliance size (w x d x h) [in]	2.04 x 5.9 x 5.11	2.67 x 5.9 x 5.11
Cooling	Fanless	Fanless
CERTIFICATIONS AND COMPLIANCE		
CE emissions	✓	✓
CE electrical safety	✓	✓
FCC emissions	✓	✓
ROHS compliant	✓	✓
Shock and vibration resistance	IEC 60068/60950/61000, ISTA 2A	
Protection classification	IP 20	IP 20

All performance values are measured under optimized conditions and are to be considered as "up to" values and may vary depending on system configuration and infrastructure:

[1] *Firewall throughput measured with large UDP packets (MTU1500), bi-directional across multiple ports, utilizing highest available port density.*

[2] *SD-WAN performance is based on 1415 Byte UDP packets, bidirectional using BreakingPoint traffic generator.*

[3] *IPS throughput is measured using large UDP packets (MTU1500) and across multiple ports, utilizing highest available port density.*

[4] *NGFW throughput is measured with IPS, application control, and web filter enabled, based on BreakingPoint Realworld-IPS-Enterprise-Traffic-Mix, bidirectional across multiple ports, utilizing highest available port density.*

[5] *Threat protection throughput is measured with IPS, application control, web filter, antivirus, and SSL inspection enabled, based on BreakingPoint Realworld-IPS-Enterprise-Traffic-Mix, bidirectional across multiple ports.*

Specifications subject to change without notice.

Barracuda®
Your journey, secured.