Barracuda CloudGen Firewall F-Series 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 F-Series 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 tracing 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

Protocol support
- IPv4, IPv6
- BGP/OSPF/IRP
- VoIP (H.323, SIP, SCCP [skinny])
- RPC protocols (ONC-RPC, DCE-RPC)
- 802.1q VLAN
- Industrial protocols and subprotocols (57, 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

VPN
- Drag & drop VPN tunnel configuration
- Network access control
- iOS and Android mobile device support
- Two-factor authentication via time based one-time passwords (TOTP), Radius, or RSA MFA (requires an active Advanced Remote Access subscription) for VPN and NAC clients

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

Traffic intelligence and SD-WAN
- VPN-based SD-WAN
- FIPS 140-2 certified cryptography
- Dynamic bandwidth detection
- Performance-based transport selection
- Application-aware traffic routing (VPN)
- Traffic shaping and QoS
- Built-in data deduplication

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 portal based SSL VPN as well as sophisticated network access control (NAC) functionality and CudaLaunch support.

Support options

Barracuda Energize Updates
- Standard technical support
- Firmware updates
- IPS signature updates
- Application control definition updates

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

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 is measured with large packets (MTU1500) UDP packets, bidirectional across multiple ports, utilizing highest available port density
2 VPN performance is based on 4KB byte UDP packets, bidirectional using BreakPoint traffic generator.
3 IPS throughput is measured using large packets (MTU1500) UDP traffic and across multiple ports, utilizing highest available port density
4 NGFW throughput is measured with IPS, application control, and web filter enabled, based on Barracuda 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 Barracuda Realworld-IPS-Enterprise-Traffic-Mix, bidirectional across multiple ports.

Specifications subject to change without notice.