Barracuda CloudGen Firewall F-Series Rugged

Absichern von Operational Technology und Industrial Control Systems.

Der sichere Betrieb von Industrial Control Systems (ICS) und die Integration von Operational Technology (OT; Betriebstechnik) stellen neue Herausforderungen für das heutige Schutz- und Sicherheitsmanagement dar. Barracuda CloudGen Firewall F-Series Rugged Appliances sind die perfekte Lösung für spezielle Anforderungen in Bezug auf Benutzerfreundlichkeit und Bedienkonzepte in industriellen und rauen Umgebungen.

Full Next-Generation Security

Barracuda CloudGen Firewalls schützen das gesamte Unternehmensnetzwerk. Firewalling, IPS, dualer Virenschutz und Applikationskontrolle (inklusive industrieller Protokolle und deren Unterprotokollen) erfolgen verzögerungslos direkt im Datenfluss.

Ressourcenintensivere Schutzmechanismen zur Abwehr von Ransomware durch Sandboxing erfolgen nahtlos integriert in der Cloud. Alle CloudGen Firewall-Plattformen und -Modelle bieten das gleiche Sicherheitsniveau und sorgen für maximale Sicherheit bei der Mikrosegmentierung für Operational Technology mit lokaler Durchsetzung höchster Sicherheitsstufen.

Sicherer Fernzugriff für OT

Barracuda CloudGen Firewalls bieten mit Secure Remote Access-Funktionen eine einfache und komfortable Möglichkeit, Drittanbietern einen sicheren, temporären VPN-Zugriff auf sensible Teile von Produktionsanlagen zu gewähren.

Security für die Betriebstechnik

ICS/OT-Sicherheitsprojekte müssen zwei Betriebskonzepte kombinieren: Während die einzelne Firewall Teil eines Verbundes Hunderten bis Tausenden anderer ähnlicher Firewalls ist, die ähnliche Richtlinien befolgen und sicherstellen, dass alle Sicherheitskomponenten nachvollziehbar und kontrollierbar funktionieren, ist die gleiche Firewall eine von vielen verschiedenen Komponenten eines Systems, die in Betriebs- und Wartungskonzepte integriert werden müssen.

Denken Sie nur an Fernzugriff zu Wartungszwecken. Der Fernzugriff wird vom Firewall-Administrator vordefiniert, während der Zugriff von Aussen bei Bedarf und für einen begrenzten Zeitraum vom Wartungstechniker aktiviert wird. Oder stellen Sie sich den Austausch von Geräten durch das Wartungspersonal nach einem einfachen Verfahren vor. Allerdings muss die IT-Komponente dafür von der Firewall IT so vorbereitet werden, dass sie in das Wartungskonzept der übrigen Maschinenkomponenten passt.

Die Barracuda CloudGen Firewall ermöglicht es OT, in Zusammenarbeit mit der IT-Abteilung, Firewallbereitstellungen und Remote-Verbindungen nach Bedarf zu verwalten.

Technische Angaben

Firewall

- Stateful Packet Inspection und Forwarding
- Volle User-Identity Awareness
- Intrusion Detection und Prevention (IDS/IPS)
- Application Control und granulares Application Enforcement
- Abfangen und entschlüsseln von SSL/TLS verschlüsselten Anwendungen
- Antivirus im Single-Pass Modus
- Denial-of-Service Schutz (DoS/DDoS)
- Spoofing und Flooding Schutz
- Schutz vor ARP Spoofing / Trashing
- DNS Reputation Filter
- TCP Stream Reassembly
- Transparentes Proxying (TCP)
- NAT (SNAT, DNAT), PAT
- Dynamische Regeln/zeitbasierte Trigger
- Einzelobjekt-Orientiertes Regelwerk für Routing, Bridging und Routed-Bridging
- Virtuelle Regeltestumgebung

Unterstützte Protokolle

- IPv4, IPv6
- BGP/OSPF/RIP
- VoIP (H.323, SIP, SCCP [skinny])
- RPC-Protokolle (ONC-, DCE-RPC)
- 802.1q VLAN
- Industrielle Protokolle und deren Unterprotokolle (S7, IEC 60870-5-104, IEC 61850, MODBUS, DNP3)

Advanced Threat Protection

- Dynamische, „on-demand“ Analyse von Malware (Sandboxing)
- Detailierte Forensik für Malware Binaries und Web-Bedrohungen (Exploits)
- Unterstützung für mehrere Betriebssysteme (Windows, Android, usw.)
- Botnet- und Spyware-Schutz

Infrastructure Services

- DHCP-Server, Relay
- JSON Lifecycle-Automatisierungs-API
- Auto VPN über API / Script Control
- DNS cache
- Integrierte Unterstützung für Azure Virtual WAN

Intrusion Detection und Prevention

- Schutz vor Exploits, Bedrohungen und Schwachstellen
- Schutz vor Packet Anomaly und Fragmentation
- Fortschrittlichste Anti-Evasion und Obfuscation Techniken
- Automatische Signatur Updates

Zentrale Management-Optionen über Firewall Control Center

- Administration für unlimitierte Zahl an Firewalls
- Mandantenfähig
- Multi-Administrator & RCS
- Zero-Touch Deployment
- Enterprise/MSP Lizensierung
- Template & Repository-basiertes Management
- REST API

Traffic Intelligence & SD-WAN

- VPN-basiertes SD-WAN
- FIPS 140-2 zertif. Verschlüsselung
- Dynamische Bandbreitenerkennung
- Performance-basierte Transportauswahl
- Anwendungsorientiertes Traffic-Routing (VPN)
- Traffic-Shaping und QoS
- Integrierte Datendeduplizierung

VPN

- VPN-Tunnel-Konfiguration per Drag-and-Drop
- Network Access Control
- VPN-Unterstützung für Mobilgeräte mit iOS und Android
- Zwei-Faktor Authentisierung mittels Time-based One-Time Passwords (TOTP), Radius, oder RSA MFA (erfordert eine gültige Advanced Remote Access Subscription) für VPN und NAC Clients
- Multi-Faktor Authentisierung für SSL VPN und CudaLaunch

Alle Performance-Zahlen werden unter optimierten Bedingungen gemessen, sind als “bis zu” Werte zu betrachten und können je nach Systemkonfiguration und Infrastruktur variieren:

[1] *Firewall-Durchsatz gemessen mit großen UDP-Paketen (MTU1500), bidirektional über mehrere Ports.*

[2] *VPN-Performance basiert auf 1415 Byte UDP-Paketen, bidirektional mit BreakingPoint-Traffic-Generator.*

[3] *IPS-Durchsatz gemessen mit großen UDP-Paketen (MTU1500) und über mehrere Ports.*

[4] *NGFW-Durchsatz wird mit aktivem IPS, Application Control und Web Filter, basierend auf BreakingPoint Realworld-IPS-Enterprise-Traffic-Mix, bidirektional über mehrere Ports hinweg gemessen.*

[5] *Threat-Protection-Durchsatz wird mit aktivem IPS, Application Control, Web Filter, Antivirus und SSL Inspection, basierend auf BreakingPoint Realworld-IPS-Enterprise-Traffic-Mix, bidirektional über mehrere Ports hinweg gemessen.*

Angaben können sich ohne Ankündigung ändern.

Barracuda
Your journey, secured.

Support Optionen

Barracuda Energize Updates

- Standardmäßiger techn. Support
- Firmware-Updates
- IPS-Signaturen-Updates
- Application Control Definitionsupdates

Instant Replacement Service

- Austauschgeräteversand innerhalb eines Werktags
- Technischer 24-Stunden-Support
- Alle vier Jahre gratis Hardware Refresh

Malware Protection

Schützt Gateway-gestützt vor Schadsoftware, Viren und anderen unerwünschten Programmen in SMTP/S-, HTTP/S- und FTP/S-Datenverkehr.

Advanced Threat Protection

Schützt vor Sicherheitslücken im Netzwerk, identifiziert Zero-Day Malware-Angriffe, gezielte Angriffe, fortgeschrittene persistente Bedrohungen und andere fortschrittliche Malware.

Advanced Remote Access

Bietet ein anpassbares und benutzerfreundliches portalbasiertes SSL-VPN sowie anspruchsvolle Network Access Control (NAC)-Funktionalität und CudaLaunch-Unterstützung.

Verfügbare Subscriptions

Barracuda Firewall Insights

Konsolidiert Informationen zu Sicherheit, Datenfluss der Applikationen und Konnektivität Hunderter oder sogar Tausender von Firewalls im erweiterten Wide Area Network - unabhängig davon, ob es sich um Hardware-, virtuelle oder cloud-übergreifende Implementierungen handelt.

	F183R
LEISTUNG	
Firewall Durchsatz [1]	2.1 Gbps
VPN Durchsatz [2]	320 Mbps
IPS Durchsatz [3]	790 Mbps
NGFW Durchsatz [4]	800 Mbps
Threat Protection Durchsatz [5]	700 Mbps
HARDWARE	
Formfaktor	Kompakt, Hutschienenmontage
Kupfer-Ethernet NICs [GbE]	5x1
Glasfaser-SFP NICs [GbE]	2x1
Stromversorgung	Phoenix 6-Pin
Stromart	DC
Max. Leistungsaufnahme [W]	60
Max. Leistungsaufnahme bei 24V [A]	2.5
Betriebstemperatur [°C]	-40 to +75
Zulässige Luftfeuchtigkeit	5% to 95%
Magnetic Isolation Protection	1.5KV built-in
Abmessungen (BxTxH) [mm]	78 x 127 x 146
Kühlung	Lüfterlos
ZERTIFIZIERUNGEN	
CE Emissions	✓
CE Electrical Safety	✓
FCC Emissions	✓
ROHS Compliant	✓
IP-Schutzklassen	Standard: IP 20; IP 30 mit E/A Gummiabdeckungen und Stromversorgung mit Phoenix 6-Pin