Barracuda CloudGen Firewall

Protect cloud-connected users, network workloads, and devices wherever they reside.

As you integrate public-cloud platforms and environments into your network, your firewalls must go beyond perimeter security and serve as the linchpins of your IT communications flow, ensuring reliable, cost-effective connections. Barracuda CloudGen Firewall was designed to optimize the performance, security, and availability of today's dispersed enterprise SD-WANs.

Barracuda CloudGen Firewall combines a complete security stack, powerful SD-WAN capabilities, and simple centralized management for hundreds or thousands of firewalls. Zero-touch hardware deployment and native cloud integration get you up and running quickly and easily in any environment.

Full next-generation security

Barracuda CloudGen Firewall is built to provide comprehensive, next-generation firewall protection. Firewalling, IPS, URL filtering, dual antivirus, and application control take place in the data path. Sandboxing and other resource-intensive tasks are offloaded seamlessly to the cloud. All platforms and models include the same comprehensive security feature-set.

Secure SD-WAN connectivity

In the cloud era, you need to connect branch offices with the cloud directly and securely. Connecting through a single, central gateway is costly and renders cloud based applications unresponsive. Optimized direct internet uplink selection ensures fast cloud-hosted SaaS applications. CloudGen Firewall lets you replace costly MPLS connections with up to 24 bonded broadband uplinks per SD-WAN connection for increased application performance and built-in redundancy.

Cloud automation

The big advantage of going to the cloud is greater agility and flexibility. This requires high degrees of automation. All components, including the infrastructure for security and connectivity, need to adapt to the way this works. CloudGen Firewall provides fully automated protection across multi-cloud deployments, including SD-WAN automation across multiple cloud providers, on-site and virtual.

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 and web filtering in single pass mode
- Email security
- SafeSearch enforcement
- Google Accounts Enforcement
- 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/Multicast
- 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)

Intrusion detection and prevention

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

Infrastructure services

- DHCP server, relay
- SIP and HTTP proxies
- SNMP, IPFIX, and LLDP support
- JSON lifecycle automation API
- Auto VPN via API and script control
- Authoritative DNS server
- DNS server
- DNS cache
- Wi-Fi (802.11n) on selected models
- Built-in support for Azure Virtual WAN

Remote and Zero Trust Access

- 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 remote access clients
- Multi-factor authentication for browser-based remote access and CudaLaunch
- ZTNA access and enforcement via Barracuda SecureEdge Access Agents

Advanced threat protection

- Dynamic, on-demand analysis of malware programs (sandboxing)
- Dynamic analysis of documents with embedded exploits (PDF, Office, etc.)
- Detailed forensic analysis
- Botnet and spyware protection
- TypoSquatting and link protection for email

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 management
- REST API
- Edge computing deployments

High Availability

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

Edge Computing

- Support for OCI-compliant applications
- Example use cases
  - Anomaly detection and asset discovery
  - Secure access and access control
  - Securing legacy systems and optimizing data formats
  - Harness the power of AI and edge computing for smarter data processing

Self-Healing SD-WAN

- Drag & drop configuration
- Optimized direct internet uplink selection
- Internet uplink optimization (forward error correction)
- Simultaneous use of multiple uplinks (transports) per SD-WAN connection
- FIPS 140-2 certified cryptography
- On-demand direct connection creation between remote spoke locations based on application type
- Dynamic bandwidth detection
- Performance-based transport selection
- Application-aware traffic routing
- Adaptive session balancing across multiple uplinks
- Application-based provider selection
- Traffic shaping and QoS
- Built-in data deduplication

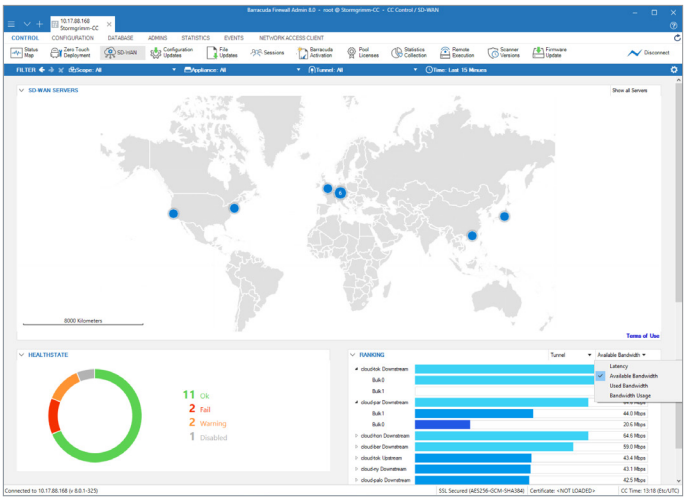
Support options

Barracuda Energize Updates

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

Instant Replacement Service

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



Barracuda CloudGen Firewall's SD-WAN dashboard provides real-time information and summaries of what is going on in an organization's network.

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.

BASIC FEATURES	ENTRY AND BRANCH OFFICE / RUGGED	MID-RANGE	HIGH-END
Firewall incl. IPS	✓	✓	✓
Application control	✓	✓	✓
Dynamic routing	✓	✓	✓
Application-based provider selection	✓	✓	✓
TLS inspection	✓	✓	✓
Secure SD-WAN	✓	✓	✓
Cloud connectivity automation with Azure Virtual WAN	✓	✓	✓
Web filter	✓	✓	✓
Zero-touch deployment	✓	✓	✓
Remote access	✓	✓	✓
Edge computing	✓	✓	✓

OPTIONAL FEATURES	ENTRY AND BRANCH OFFICE / RUGGED	MID-RANGE	HIGH-END
Firewall Insights	Optional	Optional	Optional
Advanced threat protection	Optional	Optional	Optional
Malware protection	Optional [1]	Optional	Optional
Advanced remote access	Optional [2]	Optional	Optional

ENTRY & BRANCH OFFICE / RUGGED MODELS	ENTRY AND BRANCH OFFICE					RUGGED	
	F12A	F18B	F80B	F180B	F280C	F93A.R	F193A.R
THROUGHPUT / PERFORMANCE							
Firewall [3]	1.2 Gbps	3.0 Gbps	3.0 Gbps	3.2 Gbps	4.8 Gbps	1.5 Gbps	2.1 Gbps
SD-WAN [4]	220 Mbps	1.0 Gbps	1.0 Gbps	800 Mbps	1.5 Gbps	240 Mbps	320 Mbps
IPS [5]	400 Mbps	900 Mbps	900 Mbps	1.0 Gbps	2.0 Gbps	400 Mbps	790 Mbps
NGFW [6]	250 Mbps	670 Mbps	670 Mbps	1.2 Gbps	1.6 Gbps	400 Mbps	800 Mbps
Threat protection [7]	230 Mbps	630 Mbps	630 Mbps	1.0 Gbps	1.5 Gbps	380 Mbps	700 Mbps
Concurrent sessions	80,000	160,000	160,000	150,000	300,000	80,000	100,000
New sessions/s	8,000	15,000	15,000	12,000	12,000	8,000	9,000
HARDWARE							
Form factor	Compact	Desktop	Desktop	Desktop	Desktop	Compact, DIN rail	Compact, DIN rail
Copper ethernet NICs [1 GbE]	5x	5x	5x	12x	12x	2x	5x
Fiber ethernet NICs (SFP) [1 GbE]	-	-	-	4x	4x	1x	2x
Wi-Fi (access point & client mode)	-	-	✓	✓	✓	-	-
Power supply	Single, external	Single, external	Single, external	Single, external	Single, external	Phoenix 4-pin or dual, external	Phoenix 4-pin or dual, external

MID-RANGE MODELS	F380B	F400C SUBMODELS		F600D SUBMODELS				
		STD	F20	C10	C20	F10	F20	E20
THROUGHPUT / PERFORMANCE								
Firewall [3]	13 Gbps	17.1 Gbps	17.1 Gbps	15 Gbps		15 Gbps		20 Gbps
SD-WAN [4]	3.6 Gbps	4.7 Gbps	4.7 Gbps	3.8 Gbps		3.8 Gbps		6.8 Gbps
IPS [5]	4.2 Gbps	5.5 Gbps	5.5 Gbps	4.8 Gbps		4.8 Gbps		8.0 Gbps
NGFW [6]	3.7 Gbps	4.8 Gbps	4.8 Gbps	4.2 Gbps		4.2 Gbps		6.4 Gbps
Threat protection [7]	3.1 Gbps	4.2 Gbps	4.2 Gbps	4.0 Gbps		4.0 Gbps		5.8 Gbps
Concurrent sessions	500,000	600,000	600,000	2,100,000		2,100,000		2,100,000
New sessions/s	20,000	50,000	50,000	115,000		115,000		115,000
HARDWARE								
Form factor	1U rack mount	1U rack mount		1U rack mount				
Copper ethernet NICs [1 GbE]	8x	8x	8x	18x	18x	10x	10x	10x
Fiber ethernet NICs (SFP) [1 GbE]	4x	4x	4x	-	-	8x	8x	8x
Fiber ethernet NICs (SFP+) [10 GbE]	2x	2x	2x	-	-	-	-	2x
Power supply	Single, internal	Single, internal	Dual, hot swap	Single, internal	Dual, hot swap	Single, internal	Dual, hot swap	Dual, hot swap

HIGH-END MODELS	F800D SUBMODELS			F900C SUBMODELS				F1000B SUBMODELS				F2000A SUBMODELS	
	CCC	CCF	CCE	CCC	CCE	CFE	CFEQ	CE0	CE2	CFE	CFEQ	F2040A	F2100A
THROUGHPUT / PERFORMANCE													
Firewall [3]	42.0 Gbps			53.2 Gbps			63.0 Gbps	52 Gbps				80 Gbps	
SD-WAN [4]	11.5 Gbps			15.0 Gbps			20.0 Gbps	15.8 Gbps				40 Gbps	
IPS [5]	12.9 Gbps			16.9 Gbps			19.4 Gbps	16 Gbps				30 Gbps	
NGFW [6]	9.7 Gbps			13.0 Gbps			15.2 Gbps	14.8 Gbps				28 Gbps	
Threat protection [7]	9.3 Gbps			12.2 Gbps			14.1 Gbps	13.5 Gbps				25 Gbps	
Concurrent sessions	3,000,000			4,000,000			4,000,000	10,000,000				15,000,000	
New sessions/s	220,000			250,000			250,000	250,000				300,000	
HARDWARE													
Form factor	1U rack mount			1U rack mount				2U rack mount				2U rack mount	
Copper ethernet NICs [1 GbE]	24x	16x	16x	32x	16x	8x	8x	16x	32x	16x	16x	16x	16x
Fiber ethernet NICs (SFP) [1 GbE]	-	8x	-	-	-	8x	8x	-	-	16x	16x	16x	16x
Fiber ethernet NICs (SFP+) [10 GbE]	-	-	4x	-	8x	8x	4x	4x	8x	8x	6x	6x	8x
Fiber ethernet NICs (QSFP+) [40 GbE]	-	-	-	-	-	-	2x	-	-	-	2x	6x	2x
Fiber ethernet NICs (QSFP28) [100 GbE]	-	-	-	-	-	-	-	-	-	-	-	-	2x
Power supply	Dual, hot swap			Dual, hot swap				Dual, hot swap				Dual, hot swap	

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] *For model F12A, malware protection utilizes cloud-based malware protection as part of an active Advanced Threat Protection subscription.*

[2] *For model F12A, this feature is not available.*

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

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

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

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

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

Specifications subject to change without notice.

Barracuda®