

# Barracuda CloudGen Firewall for AWS

Protecting your digital assets in Amazon Web Services

The growth in cloud computing capabilities and services has driven more data into places where traditional IT security measures cannot reach - into data centers not owned by your corporate IT group. Beyond its powerful network firewall, IPS, and VPN technologies, Barracuda CloudGen Firewall integrates a comprehensive set of next-generation firewall technologies, including comprehensive application control, availability, and quality-of-services (QoS) features.

## Granular application control

Barracuda CloudGen Firewall gives administrators granular control over applications, allowing them to define rules for forwarding data traffic using the best respective transmission channels based on type of application, user, content, time of day, and geographical location. Barracuda CloudGen Firewall allows organizations to prioritize traffic by limiting or restricting access to non-business-related applications and network traffic, even when encrypted.

## Integrated next-generation security and connectivity

Barracuda CloudGen Firewall's intrusion detection and prevention system (IDS/IPS) strongly enhances network security by providing complete and comprehensive real-time network protection against a broad range of network threats, vulnerabilities, exploits, and exposures in operating systems, applications, and databases preventing network attacks such as SQL injections and arbitrary code executions.

Barracuda CloudGen Firewall incorporates advanced site-to-site and client-to-site VPN capabilities, using both SSL and IPsec protocols to ensure remote users can easily and securely access network resources without complex client configuration and management.

## Cloud automation

The big advantage of going to the cloud goes beyond cost savings but in greater agility and flexibility, enabling adoption of a DevOps/Agile methodology, and of cloud-native constructs and automation. Development and deployment processes in the cloud show drastic improvements over on-premises deployments and, thus, require high levels of automation and scripting. All of the components, including infrastructure for security and connectivity, need to adapt to the way this works in the public cloud via API or scripting.

Barracuda CloudGen Firewall provides fully automated protection across multi-cloud deployments, including VPN automation.



## 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

### 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

### Protocol support

- IPv4, IPv6
- BGP/OSPF/RIP
- VoIP (H.323, SIP, SCCP [skinny])
- RPC protocols (ONC-RPC, DCE-RPC)
- 802.1q VLAN

### 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

### VPN

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

### Intrusion detection and prevention

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

### Traffic intelligence & SD-WAN

- Optimized internet uplink selection
- VPN-based SD-WAN
- FIPS 140-2 certified cryptography
- On-demand direct VPN tunnel creation between remote spoke locations based on application type
- Dynamic bandwidth detection
- Performance-based transport selection
- Application-aware traffic routing (VPN, Direct Connect)
- Adaptive session balancing across multiple uplinks
- Traffic replication (forward error correction)
- Application-based provider selection
- 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
- Built-in support for Azure Virtual WAN

## Support options

### Barracuda Energize Updates

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

## Support for AWS specifics

- Full AWS Direct Connect support
- Auto-scaling cluster
- Cold-standby cluster
- Log file streaming and custom metrics for AWS CloudWatch

## Available options

### 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-cloudbased deployments.

### Advanced Threat Protection

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

### Malware Protection

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

### 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.

CAPABILITIES	BRING-YOUR-OWN-LICENSE				PAY-AS-YOU-GO LICENSE	
	LEVEL 2	LEVEL 4	LEVEL 6	LEVEL 8	TIME-BASED	VOLUME-BASED
Protected IP addresses	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Virtual cores	1	2	4	8	Does not apply	Does not apply
Max number of interfaces	2	2	4	4	Does not apply	Does not apply
FEATURES						
Firewall incl. IPS	✓	✓	✓	✓	✓	✓
Application control	✓	✓	✓	✓	✓	✓
Site-to-site and client-to-site VPN	✓	✓	✓	✓	✓	✓
Network access control for client-to-site VPN	✓	✓	✓	✓	✓	✓
SD-WAN	✓	✓	✓	✓	✓	✓
SSL interception	✓	✓	✓	✓	✓	✓
Energize Updates	✓	✓	✓	✓	✓	✓
Barracuda Firewall Insights	Optional	Optional	Optional	Optional	✓	✓
Malware Protection <sup>1</sup>	Optional	Optional	Optional	Optional	-	-
Advanced Threat Protection <sup>1</sup>	Optional	Optional	Optional	Optional	-	-
Advanced Remote Access	Optional	Optional	Optional	Optional	✓	✓
Premium Support <sup>2</sup>	Optional	Optional	Optional	Optional	-	-

<sup>1</sup> Including FTP, mail and web protocols.

<sup>2</sup> Premium Support ensures that an organization's network is running at its peak performance by providing the highest level of 24x7 technical support for mission-critical environments.

For more information please visit <https://www.barracuda.com/support/premium>

Specifications subject to change without notice.

