Barracuda

CloudGen Firewall for Azure

Protecting your digital assets in Microsoft Azure

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, remote access, and SD-WAN technologies, CloudGen Firewall integrates a comprehensive set of next-generation firewall technologies, including 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-businessrelated applications and network traffic, even when encrypted.

Fully integrated SD-WAN functionality makes use of dozens of physical uplinks, including Microsoft Azure ExpressRoute. This ensures connectivity to Microsoft 365 and applications hosted in Azure is never interrupted and always operating at peak performance. Barracuda CloudGen Firewall is the best choice for connectivity with Azure Virtual WAN. Tight integration into the automated management concept and zero touch deployment for unlimited remote locations enables connecting any number of branches to the cloud and to each other with throughput and scalability provided by the Microsoft Global Network.

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 SD-WAN and remote access 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 connectivity automation across multiple cloud providers, on-site and virtual.

NETWORK SECURITY

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

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 **Remote and Zero Trust Access**
- Network access control
- iOS and Android mobile device support
- 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 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

Intrusion detection and prevention

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

Self-Healing SD-WAN

- Drag & drop configuration
- Optimized direct internet uplink selection
- Internet uplink optimization (forward error correction)
- 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 (VPN, ExpressRoute)
- Adaptive session balancing across multiple uplinks
- Application-based provider selection
- Traffic shaping and QoS
- Built-in data deduplication

Protocol support

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

Support options

Barracuda Energize Updates

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

Support for Azure specifics

- Full Azure Virtual WAN support
- Log File Streaming to Azure OMS

Available subscription plans [1]

Threat Protection plan

This subscription plan bundles
- Energize Updates
- Advanced Threat Protection
- Firewall Insights

Total Threat Protection plan

This subscription plan bundles
- Energize Updates
- Advanced Threat Protection
- Firewall Insights
- Malware Protection
- Advanced Remote Access

CAPABILITIES	BRING-YOUR-OWN-LICENSE						PAY-AS-YOU-GO LICENSE
	VFC1	VFC2	VFC4	VFC8	VFC16	VFC48	
Protected IP addresses	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Virtual cores	1	2	4	8	16	48	Does not apply
FEATURES							
Firewall incl. IPS	✓	✓	✓	✓	✓	✓	✓
Application control	✓	✓	✓	✓	✓	✓	✓
Remote Access	✓	✓	✓	✓	✓	✓	✓
Network access control for remote access	✓	✓	✓	✓	✓	✓	✓
Secure SD-WAN	✓	✓	✓	✓	✓	✓	✓
TLS inspection	✓	✓	✓	✓	✓	✓	✓
Energize Updates	✓	✓	✓	✓	✓	✓	✓
Barracuda Firewall Insights	Optional	Optional	Optional	Optional	Optional	Optional	✓
Malware Protection [2]	Optional	Optional	Optional	Optional	Optional	Optional	-
Advanced Threat Protection [2]	Optional	Optional	Optional	Optional	Optional	Optional	-
Advanced Remote Access	Optional	Optional	Optional	Optional	Optional	Optional	✓
Premium Support [3]	Optional	Optional	Optional	Optional	Optional	Optional	-
Threat Protection plan	Optional	Optional	Optional	Optional	Optional	Optional	-
Total Threat Protection plan	Optional	Optional	Optional	Optional	Optional	Optional	-

[1] All subscriptions mentioned are also available "à la carte".

[2] Including FTP, mail and web protocols

[3] 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.

Barracuda.
Your journey, secured.

www.cobranetworks.lat
ventas@cobranetworks.lat
+52 (55) 5599-0691