Barracuda **NextGen Firewall F**

Protecting your Digital Assets in Microsoft Azure

- ☑ **Security**
- ☐ Storage
- ☐ Application Delivery
- ☐ Productivity

Growth in cloud computing capabilities and services has driven more data into places where traditional IT security measures cannot reach; specifically, data centers not owned by your corporate IT group. The Barracuda NextGen Firewall F-Series provides **centralized management and highly secure, encrypted traffic to, from, and within Microsoft Azure deployments.**

The Barracuda Advantage

- Secure and reliable connectivity between on-premises and Azure deployments as well as between Azure deployments
- Central management of all functionality for both, on-premises and Azure deployments
- Unrivaled Quality of Service capabilities
- Available as Bring-Your-Own-License and Pay-As-You-Go

Product Spotlight

- Powerful next-generation network firewall
- Advanced Threat Detection
- Built-in web security and IDS/IPS
- Client-to-Site VPN via browser (SSL VPN), mobile apps and desktop VPN clients
- Full application visibility and granular control
- Intelligent traffic regulation including application-based provider selection
- Tightly integrated Quality of Service (QoS) and link balancing
- Centralized management of all functionality
- Template-based and role-based configuration

Secure Connectivity

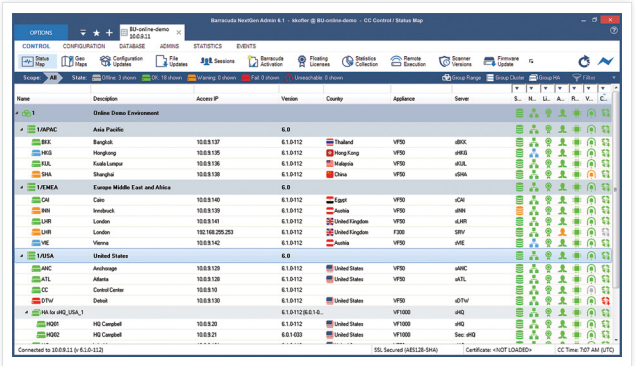
For an optimum Azure deployment, it is crucial to initiate the deployment in a highly secure and reliable way. Deploying a Barracuda NextGen Firewall F-Series in Microsoft Azure provides comprehensive, secure connectivity capabilities, starting with high-performance TINA VPN tunnels for site-to-site and client-to-site connections. Deployment includes robust WAN optimization features to maintain the highest quality of service possible.

Integrated Next-Generation Security

The Barracuda NextGen Firewall F-Series is designed and built from the ground up to provide comprehensive, next-generation firewall capabilities. Based on application visibility, user-identity awareness, intrusion prevention, and centralized management, the F-Series is the ideal solution for today's dynamic enterprises that are adding Microsoft Azure into their company network.

Central Management

The Barracuda NextGen Firewall F-Series benefits from the same industry-leading central management as on-premises deployments. Easily manage the secure VPN connections to, from, and within Microsoft Azure and the Barracuda NextGen Firewall F deployment itself.



Status overview of a centrally managed Barracuda NextGen Firewall F-Series deployment

ICSA labs CERTIFIED ENTERPRISE

NSS Labs TESTED

Microsoft Azure Certified

Technical Specs

Firewall

- Stateful packet inspection and forwarding
- Full user-identity awareness
- Intrusion Detection and Prevention System (IDS/IPS)
- Application control and granular application enforcement
- Interception and decryption of SSL/TLS encrypted applications
- Antivirus and web filtering in single pass mode
- SafeSearch enforcement
- YouTube for Schools support
- Denial of Service protection (DoS /DDoS)
- Spoofing and flooding protection
- ARP spoofing and trashing protection
- DNS reputation filtering
- TCP stream reassembly
- Transparent proxying (TCP)
- NAT (SNAT, DNAT), PAT
- Dynamic rules / timer triggers
- Single object-oriented rule set for routing, bridging, and routed bridging
- Virtual rule test environment

User Identity Awareness

- Terminal Server Agent
- Domain Controller Agent
- Authentication – supports x.509, NTLM, RADIUS, RSA SecurID, LDAP/LDAPS, Active Directory, TACACS+, SMS Passcode (VPN), local authentication database

Intrusion Detection & Prevention

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

Traffic Optimization

- Fully Azure ExpressRoute compatible traffic shaping and QoS
- On-the-fly flow reprioritization
- Stream and packet compression
- Byte-level data deduplication
- Protocol optimization (SMBv2)

VPN

- Drag & drop VPN tunnel configuration
- Secure site-to-site, client-to-site VPN
- Dynamic mesh site-to-site VPN
- Supports AES-128/256, 3DES, DES, Blowfish, CAST, null ciphers
- Private CA or external PKI
- VPNC certified (basic interoperability)
- Application-aware traffic routing
- IPsec VPN / SSL VPN / TINA VPN / L2TP / PPTP
- Dedicated VPN clients for Windows, MacOS, and Linux
- iOS and Android mobile device VPN support

Advanced Threat Detection

- Dynamic, on-demand analysis of malware programs (sandboxing)
- Dynamic analysis of documents with embedded exploits (PDF, Office, etc.)
- Detailed forensics for both, malware binaries and web threats (exploits)
- Support for multiple operating systems (Windows, Android, etc.)
- Flexible malware analysis in the cloud

Central Management Options

- Barracuda NextGen Control Center
  - Centrally administer unlimited Barracuda NextGen F-Series Firewalls
  - Support for multi-tenancy
  - Multi-administrator support & RCS

Infrastructure Services

- DHCP server, relay
- SIP, HTTP, SSH, FTP proxies
- SNMP and IPFIX support
- DNS Cache
- SMTP gateway and SPAM filter

Protocol Support

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

BARRACUDA NEXTGEN FIREWALL F-SERIES	MICROSOFT AZURE - COMPUTE INSTANCE NAME			
	SMALL	MEDIUM	LARGE	EXTRA LARGE
CAPABILITIES	**Level 2**	**Level 4**	**Level 6**	**Level 8**
Virtual Cores	1	2	4	8
Firewall Throughput	400 Mbps	2 Gbps	5 Gbps	9 Gbps
VPN Throughput	120 Mbps	500 Mbps	1 Gbps	1.5 Gbps
IPS Throughput	80 Mbps	900 Mbps	2.5 Gbps	3 Gbps
Concurrent Sessions	35,000	300,000	500,000	1,000,000
New Session/s	2,500	16,000	35,000	45,000
FEATURES				
Firewall	●	●	●	●
Application Control	●	●	●	●
IPS	●	●	●	●
VPN (site-to-site and client-to-site)	●	●	●	●
SSL Interception	●	●	●	●
WAN Optimization	●	●	●	●
Network Access Control for VPN client-to-site connections	●	●	●	●
Malware Protection	Optional	Optional	Optional	Optional
Advanced Threat Protection	Optional	Optional	Optional	Optional
Premium Remote Access [1]	Optional	Optional	Optional	Optional
Premium Support [2]	-	-	●	●

[1] Basic Remote Access is included in Energize Updates.
[2] 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.

Support Options

Barracuda Energize Updates

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