Protect Your Digital Assets in Microsoft Azure with the Barracuda CloudGen Firewall for Azure

Barracuda

FW

Barracuda
CloudGen Firewall

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.

The Barracuda CloudGen Firewall for Azure ensures highly secure, encrypted traffic within Microsoft Azure, provides secure remote and site-to-site access, and centralized management.

The Barracuda CloudGen Firewall fills the functional gaps between cloud infrastructure security and a defense-in-depth strategy by providing protection where the application and data reside, rather than solely where the connection terminates.

Because of the isolation between VMs, tenants, and virtual networks, the Barracuda CloudGen Firewall for Azure operates just as if it were a physical device bridging connections between application servers in a network DMZ and your ISP's router.

Since no traffic is allowed from the Microsoft Azure Fabric, host OS, or hypervisor to a tenant's virtual network or VMs, the F-Series can intercept all Layer 2 through 7 traffic and apply policy-based controls, authentication, filtering, and other capabilities. And as with its physical counterpart, the same traffic management and bandwidth optimizations can be used to make the environment more efficient, thereby using fewer billable cloud resources.

Beyond its powerful network firewall, high availability, and VPN technologies, the F-Series integrates a comprehensive set of next-generation firewall technologies, including Application Control, IPS, anti-malware, network access control enforcement, and comprehensive user awareness. The F-Series is fully compatible with Microsoft Azure for establishing site-to-site and/or client-to-site connections to its cloud services, and creating a virtual DMZ in Azure to implement an additional high-security layer.

The Barracuda CloudGen Firewall merges the worlds of on-premises data center network protection with cloud IT security needs, helping you close the gaps between native Microsoft Azure capabilities and traditional hardware-based application firewalls.

Deploying the Barracuda Cloudgen Firewall for Azure in the cloud is very similar to running local network firewalls, and provides the advantages of common policy enforcement and distributed security management in a hybrid-IT environment.
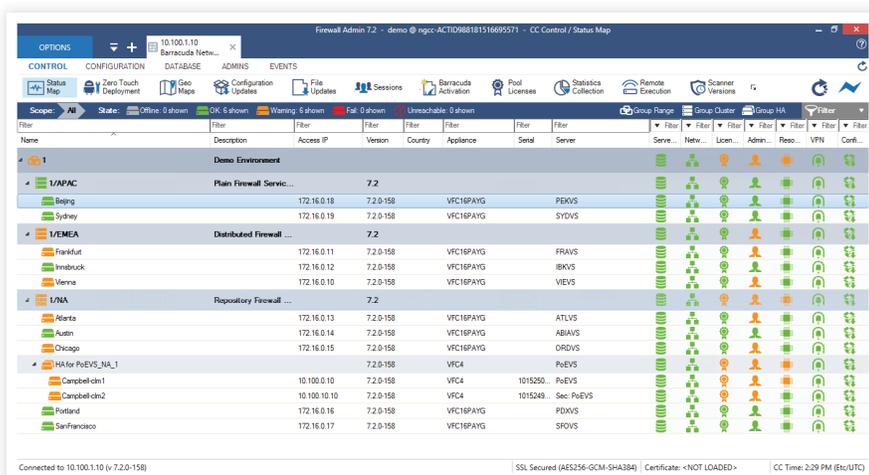

Status overview of a centrally managed Barracuda CloudGen Firewall deployment

Microsoft Azure

Certified

ICSAlabs CERTIFIED ENTERPRISE

NSS Labs TESTED

Secure Remote Access for Mobile Users

- Dedicated VPN clients available for Windows, Mac, Linux
- Clientless SSL VPN
- CudaLaunch app available for iOS and Android devices
- Supported protocols: TINA, IPsec, L2TP, PPTP
- Gateway probing
- Unlimited connections

Client-to-Site:
- Dedicated VPN Clients for
- Clientless SSL VPN
- CudaLaunch App for

Site-to-Site:
- On-premises Barracuda CloudGen Firewall F-Series
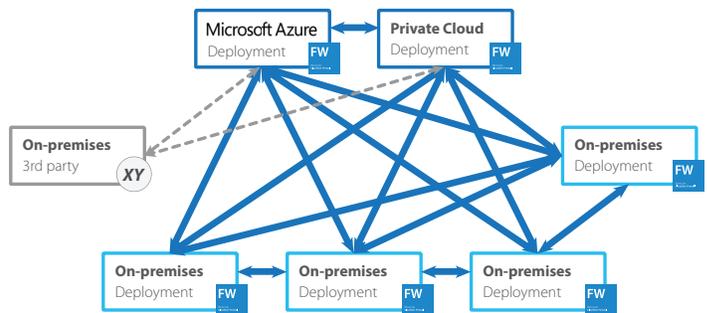
Microsoft Azure
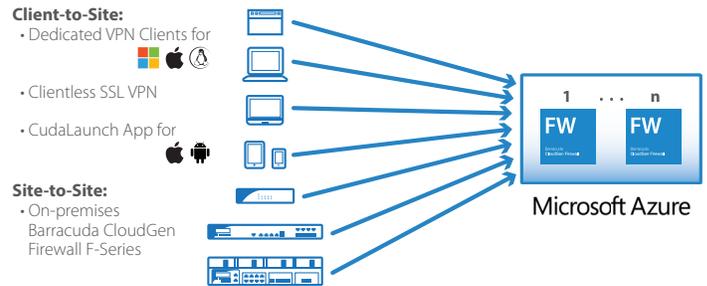
Multi-Tier Architecture Security Enforcement

- Internal and cross-region network segmentation
- Access control based on user and instance identity
- Instance OS health check
- Full traffic visibility and monitoring
- Support for Azure custom routing

Microsoft Azure

Location **A** — Zone **1** — Zone **4**

FW Barracuda CloudGen Firewall

Location **B** — Zone **2** — Zone **3**
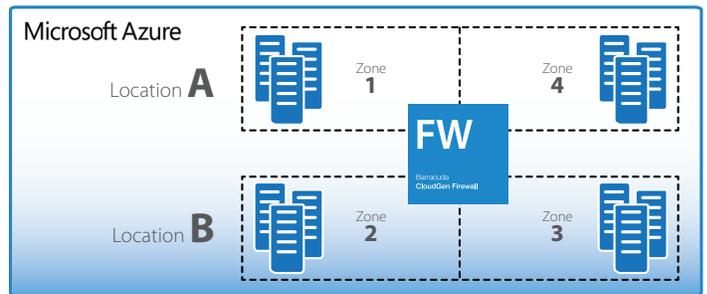
Multiple Site-to-Site Connectivity

- Vnet-to-Vnet connectivity
- Automatic user ID synchronization across sites
- Support for multiple ISPs
- Built-in WAN Optimization
- Full ExpressRoute support
- Unlimited sites
- High performance (>1Gbps)

Microsoft Azure Deployment **FW**

Private Cloud Deployment **FW**

On-premises 3rd party **XY**

On-premises Deployment **FW**

On-premises Deployment **FW**

On-premises Deployment **FW**

On-premises Deployment **FW**

About TINA (Transport Independent Network Architecture)

Due to the limitations that come with standard IPsec connections, Barracuda Networks created several powerful extensions to standard IPsec tunnel management. This core of the Firewall VPN engine is called TINA (Transport Independent Network Architecture).

The TINA protocol allows use of TCP, UDP, and ESP for high speed VPN connections which improves the VPN connectivity substantially by adding:

- Endpoint-to-Endpoint (not network-to-network) connectivity
- NAT friendliness
- Multiple physical transport paths for a logical tunnel
- Multiple tunnels between two locations
- HTTPS and SOCKS4/5 proxy compatibility
- Dynamic Address Support
- Tunnel heartbeat monitoring