FW

Barracuda
CloudGen Firewall

Barracuda CloudGen Firewall
Deploying Multi-Tier Architectures in Azure

Barracuda

Deploying Applications in the Cloud

When deploying applications within virtual machines in the cloud, the approach of not allowing any direct connections to the application provides additional layers of security. This best practice is especially relevant for modern IT infrastructures which are vulnerable to:

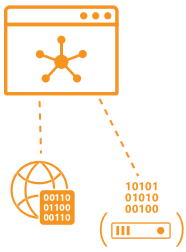
Mobile and BYOD Devices

Evasive Web 2.0 Applications

Remote Network Users

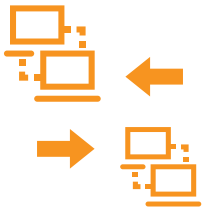
Best Practices for Multi-Tier Architectures

By separating the front end, application, database tiers, and securing, restricting, and monitoring the communication between these tiers, businesses limit the potential damage in the event of an attack.



Preventing direct connections protect applications

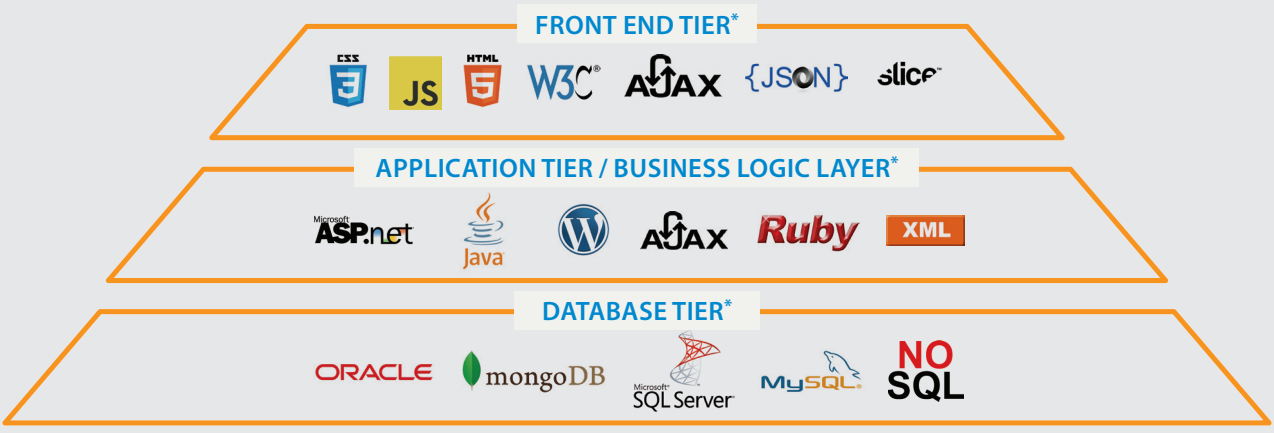
Through a reverse-proxy architecture, all connections are terminated at a proxy, decrypted, and then inspected for any malicious content or embedded attacks. Only after the traffic has been validated is it passed to the application.



Control traffic between VNETs

Using IP, port, application, or protocol, maintain full visibility into traffic, as well as the ability to control that traffic (block, allow, re-direct, etc.) between VNETs.

Multi-Tier Architecture



*Common applications deployed in each tier

 | www.barracuda.com/azure

Barracuda

Barracuda CloudGen Firewall

Benefits

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.

Secure remote access for mobile users

- Dedicated VPN clients available for Windows, Mac, and Linux
- Clientless SSL VPN
- Several supported protocols: TINA, IPsec, L2TP, PPTP

Multiple site-to-site connectivity

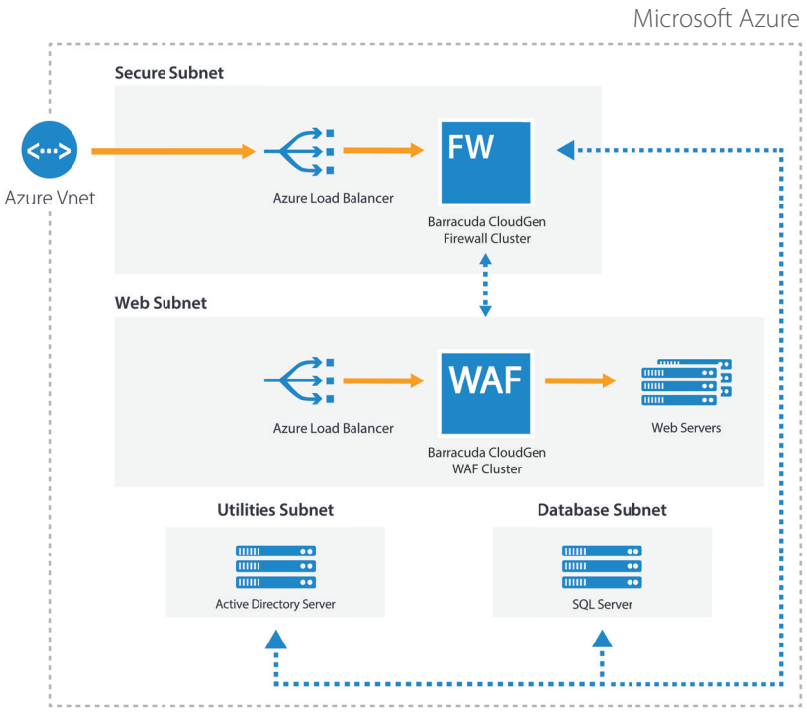
- VNET-to-VNET connectivity
- Automatic user ID synchronization across sites
- Support for multiple ISPs
- Built-in WAN optimization
- Full ExpressRoute support

Comprehensive security enforcement

- Internal and cross-region network segmentation
- Access control based on user and instance identity
- Full traffic visibility and monitoring

Overcome IPsec Limitations to Improve Connectivity

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) which was developed exclusively by Barracuda. The TINA protocol allows use of TCP, UDP, and ESP for high speed VPN connections which substantially improves the VPN connectivity.



Why Barracuda for Multi-Tier Architectures

The Barracuda CloudGen Firewall 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, Barracuda CloudGen Firewalls are the ideal solution for today's dynamic enterprises looking to protect themselves from vulnerabilities caused by the explosion of mobile and BYOD devices, evasive Web 2.0 applications, and remote network users.

Learn More

www.barracuda.com/azure
www.barracuda.com/programs/azure/network-security
www.barracuda.com/products/cloudgenfirewall-f

Learn About Barracuda CloudGen Firewall
Learn About Deploying Multi-Tier Architecture in Azure

Microsoft Azure Certified

Barracuda