Azure Virtual WAN

https://campus.barracuda.com/doc/79463435/

Barracuda CloudGen Firewalls support Microsoft's Azure Virtual WAN technology to allow fast, secure, and uninterrupted network availability to both your cloud-hosted or hybrid data center and your branch offices through Microsoft's global network. The CloudGen Firewall in combination with Virtual WAN fully enables automated, large-scale branch connectivity, selective traffic backhauling, unified networks and policy management, and optimized routing using the Microsoft global network.

Automated Connectivity to Azure Virtual WAN

Barracuda Networks' automated approach to interconnect branch offices or data centers with resources located in Azure virtual networks via Azure Virtual WAN hubs radically simplifies complex and time-consuming deployment and configuration tasks. An easy-to-use and fully automated connectivity configuration allows administrators to connect CloudGen Firewalls to Azure hubs with only a few clicks. Azure Virtual WAN can be configured both on CC-managed firewall devices and stand-alone devices. Every 30 minutes the Virtual WAN config is automatically synchronized.

For more information, see How to Configure Automatic Connectivity to Azure Virtual WAN and How to Create a Service Principal for Azure Virtual WAN.

Multi-Link Support

The Barracuda CloudGen Firewall supports up to four Internet Service Provider (ISP) links to Microsoft Azure Virtual WAN. You must have a static IPv4 public IP address with similar bandwidth and latency. For each link, two active-active IPsec IKEv2 VPN tunnels are automatically created if you use automated connectivity. BGP multi-path routing is used to route the traffic, and the configuration of BGP multi-path routing is likewise set up automatically when using automated connectivity. The firewall learns path information as set by the Virtual WAN hub, which results in better path affinity. In addition, BGP-based load balancing and automatic path failover are used for the best connection results.

High Availability Support

With CloudGen Firewall firmware 8.0.2 or higher, high availability is supported for Microsoft Azure Virtual WAN. In case of a failover, the last-known Virtual WAN configuration from the primary firewall is used for the connection to Microsoft Azure Virtual WAN. The synchronization of the Virtual WAN config every 30 minutes is available only if the primary firewall is running. For more information on high availability, see High Availability.

Manual Connectivity to Azure Virtual WAN

In addition to automated connectivity, CloudGen Firewalls also provide advanced manual configuration for adoption of hybrid cloud deployments already implemented with Microsoft Azure and CloudGen Firewalls.

For more information, see How to Configure BGP over IKEv2 IPsec Site-to-Site VPN to an Azure VPN Gateway (from Step 4 to the end).

Figures