CloudGen Firewall Active-Active Performance in Microsoft Azure

https://campus.barracuda.com/doc/29824/

Microsoft Azure allows you to deploy resources and to provision appliances based on demand in order to ensure uninterrupted computing and resource capacities, especially during workload peaks. The Microsoft Azure cloud supports horizontal scaling; in other words, it allows the service to increase or decrease the number of compute instances (VMs) within a zone in the Azure Network. The Barracuda CloudGen Firewall integrates with various Microsoft Azure services to provide load balancing capabilities that enable high availability in the form of active-active performance set deployments, based on individual networking demands.

Active-Active Performance Set Deployment in Azure

The Barracuda CloudGen Firewall provides the following deployment methods for active-active performance:

Active-Active Performance Setup with Symmetric Load Balancing

Barracuda CloudGen Firewall active-active deployment with symmetric load balancing (i.e., the enabling of HA ports in Azure) allows the seamless integration of Control Center-managed CloudGen Firewall instances in a network environment with User Defined Routing (UDR), without requiring NAT. With this straightforward approach, new instances are easily integrated into the back-end pool, and no other routing modifications are required.

For more information, see Active-Active Performance Setup with Symmetric Load Balancing.

Active-Active Performance Setup with Load Balancing and VPN Termination

Barracuda CloudGen Firewall active-active deployment with load balancing and VPN allows a load distribution across instances for external access in order to avoid session limitations caused by the underlying platform. This setup also allows the termination of VPN connections in an active-active architecture. In addition, Barracuda CloudGen Firewall SD-WAN features can be leveraged to distribute traffic across multiple instances.

For more information, see Active-Active Performance Setup with Load Balancing and VPN Termination.

Service Requirements

The following Microsoft Azure Services are required for active-active performance set deployment:

- Compute Virtual Machines
- Resource Group
- Azure Storage
- Azure Active Directory

You must have the following configured before deploying an active-active performance set:

- A VNET containing subnets.
- A subnet ID where you want to deploy the Barracuda CloudGen Firewall and protect your servers.
- A resource group. Ensure that the subnet is associated with the resource group where you want to deploy the Barracuda CloudGen Firewall.
- Service Principal Credentials generated for the user.

For instructions on how to create a resource group containing a VNET and a subnet, see How to Create a Resource Network in Azure.

This setup integrates the CloudGen Firewalls into the back-end pool as independent instances. Therefore, in order to keep the configuration of all involved units in sync, central management via Firewall Control Center is recommended.