Azure Networking

https://campus.barracuda.com/doc/96025981/

To use your firewall in Azure as you would with on-premises firewalls, you must configure routing and other networking features.

Default Routes in Azure

Azure automatically creates routes with an address prefix that corresponds to each address range defined within the address space of a virtual network. If the virtual network address space has multiple address ranges defined, Azure creates an individual route for each address range. Azure automatically routes traffic between subnets using the routes created for each address range. The default system routes always present in an Azure route table allow the following:

- Traffic within the virtual network
- Traffic to the Internet
- Traffic between different virtual networks using the Azure VPN gateway
- Traffic from the virtual network to networks connected via the Azure VPN gateway
- If peering is enabled, Traffic between the peered networks

User Defined Routes

Azure Route Tables, or User Defined Routes (UDRs), define the traffic flow in Azure. In order for traffic to be routed successfully to and from the Barracuda virtual appliance, the UDRs need to be configured correctly.

For more information, see User Defined Routing in Azure.

Azure Route Tables (UDR) Using Azure Web Portal

To use your firewall VM as the gateway for other VMs in your virtual network, you can configure a user-defined routing table in Azure. Route tables can also be used to route Control Center VIP networks and S-Series networks to the correct VM. HA clusters must be configured to rewrite the Azure routing table so that the backend VMs are always using the active firewall as the gateway.

For more information, see How to Configure Azure Route Tables (UDR) using Azure Portal and ARM.

Azure Route Tables (UDR) Using Azure PowerShell

Create a user-defined routing table to send traffic from the VMs in the backend subnets through the firewall using PowerShell.

For more information, see How to Configure Azure Route Tables (UDR) using PowerShell and ARM.

Azure Load Balancer for High Availability Clusters

For HA clusters, you need a load balancer in front of the two firewall VMs to forward incoming traffic to the active firewall. The load balancer handles all traffic that matches the load balancer rules you defined. The service is polled by a health probe every 4 seconds. After two failed health checks, the VM is marked as inactive and traffic is redirected to the now-active secondary firewall.

For more information, see How to Configure Azure Load Balancer for HA Clusters using PowerShell and ARM.

Azure Cloud Integration

Azure cloud integration allows the firewall to connect directly to the Azure service fabric to rewrite Azure user-defined routes and to monitor the IP Forwarding setting of the NIC of your firewall VM.

For more information, see How to Configure Azure Cloud Integration Using ARM.

VNET Peering

VNET peering allows you to connect virtual networks with a high-bandwidth, low-latency connection. The VNETs can be configured to use this peering connection to send all traffic through a pair of firewalls in a central VNET. This allows you to apply security policies to all traffic leaving your VNET in one central location. You can also forward traffic between VNETs that are not directly peered with each other by using the firewall as the next-hop device.

For more information, see How to Configure VNET Peering with the CloudGen Firewall.

Azure Accelerated Networking

Accelerated Networking provides single-root I/O virtualization (SR-IOV) technology to enable multiple virtual host operating systems to share PCI-e I/O devices. With Accelerated Networking, data packets are routed between virtual machines without traversing the virtual switch in order to increase network performance between Azure virtual machines. Accelerated Networking is enabled by default on CloudGen Firewalls with firmware 8.0.1 or higher when the size of the virtual machine meets the requirements for Accelerated Networking. Accelerated Networking creates, for each existing interface, a second interface for Accelerated Networking (one for the hv_netvsc driver, and one for Mellanox). Use only every second interface in boxnet (e.g., eth0, eth2, eth4). On devices with DHCP enabled, eth0 is replaced with the DHCP interface. On DHCP-enabled devices, as well, use only every second interface (e.g., eth0, eth2, eth4).

For more information, see How to Enable Azure Accelerated Networking.