Azure Networking

https://campus.barracuda.com/doc/48203335/

To use your firewall in Azure in a similar way as on-premise firewalls, you must configure routing and other networking features. Most features are available for both Azure Resource Manager (ARM) and Azure Service Manager (ASM), which is also known as "classic" deployment mode. Microsoft recommends using ARM for new deployments. Do not mix ASM and ARM resources.

Azure Resource Manager (ARM)

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 connections. 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 F-Series Firewall.

Azure Service Manager (ASM)

Azure route tables (UDR) using Azure PowerShell

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. 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) in Azure using PowerShell and ASM and How to Configure Azure Cloud Integration using ASM.

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 ASM.

Reserved, static, and public IP addresses

By default, the firewall in the cloud service is accessible by a dynamic IP address or static hostname assigned to the cloud service. The internal IP address is also dynamically assigned and can change on reboot. Azure offers static public and private IP addresses that can be configured for your firewall VM.

For more information, see Reserved, Static and Public IP Addresses in the Azure Cloud using ASM.