High Availability in Azure

https://campus.barracuda.com/doc/95259007/

Deploying a Barracuda CloudGen Firewall HA cluster in the Microsoft Azure Public Cloud requires a custom deployment and configuration to integrate the CloudGen Firewall with the Azure networking stack. Barracuda Firewall Control Centers in Azure do not support high availability configurations. For backend servers to be able to send traffic through the currently active unit, there are two high availability methods available for Azure:

- **Cloud Integration** – With this method, the Firewall can directly manipulate the Azure routing table so that routing entries always point to the active unit of the HA cluster. Due to the limitation of Azure networking, all active sessions will time out whenever a failover occurs.

or

- **Standard Load Balancer** – With this method, a new type of load balancer is used in Azure to be the destination for the route tables. The load balancer will monitor for the active firewall and direct traffic on all ports to the active unit.

Within Azure, IP addresses are fixed and non-transferable between VMs. Therefore, IP traffic must be redirected by either rewriting the UDR routes in Azure or by using a standard load balancer.

Azure Route Tables and Standard Load Balancers

The Azure Load Balancer polls a service that is reachable through the Forwarding Firewall service on the active firewall. The fastest failover method available within Azure is to use the new Standard Load Balancer product from Microsoft. The Standard Load Balancer actively probes the firewalls to determine which one is active; subnet route tables will point to an internal load balancer's IP. When the firewall service fails over to the other unit, the load balancer will follow with a latency of a couple of seconds, and change the active IP to the forwarding unit. Using the new rule type HA ports for health probes, the load balancer will actively redirect all traffic to the IP of the active firewall. This method is stateful and fails over as quickly as the load balancer probes can indicate failure. Note that Barracuda Session Sync is not supported with standard load balancers.

For more information, see: How to Configure a High Availability Cluster in Azure with the Standard Load Balancer.

> You cannot directly migrate between a Cloud Integration design and a Standard Load Balancer design because the load balancers and any public IPs used need to be built using a new Standard type. It is not possible to combine the old IPs, which are considered Basic, with any

Standard components.

Standard load balancer designs require a Network Security Group (NSG) to be present in order to pass any traffic. The NSG can permit Any inbound and Any outbound to allow the firewall to filter instead.

Choosing a Failover Method

Cloud Integration	Standard Load Balancers
No additional costs	Charges per rule and traffic volume
Slow failover as API calls	Fast failover as LB monitors
Non-stateful due to routes being rewritten	Stateful failover
Poor for multi-VNET designs	Best for multi-VNET designs

Azure Route Table Rewriting with Azure Cloud Integration

User-defined routing is limited to one VM as the gateway device when creating a route. When you are using a high availability cluster as the gateway, the VM that is used changes when the service fails over. Both firewalls are configured to access the Azure fabric and reconfigure the routing table when a failover occurs. For the firewall to rewrite the routes, you must configure Azure cloud integration.

For more information, see How to Deploy a High Availability Cluster with Cloud Integration from the Microsoft Azure Marketplace and How to Configure Azure Cloud Integration Using ARM.

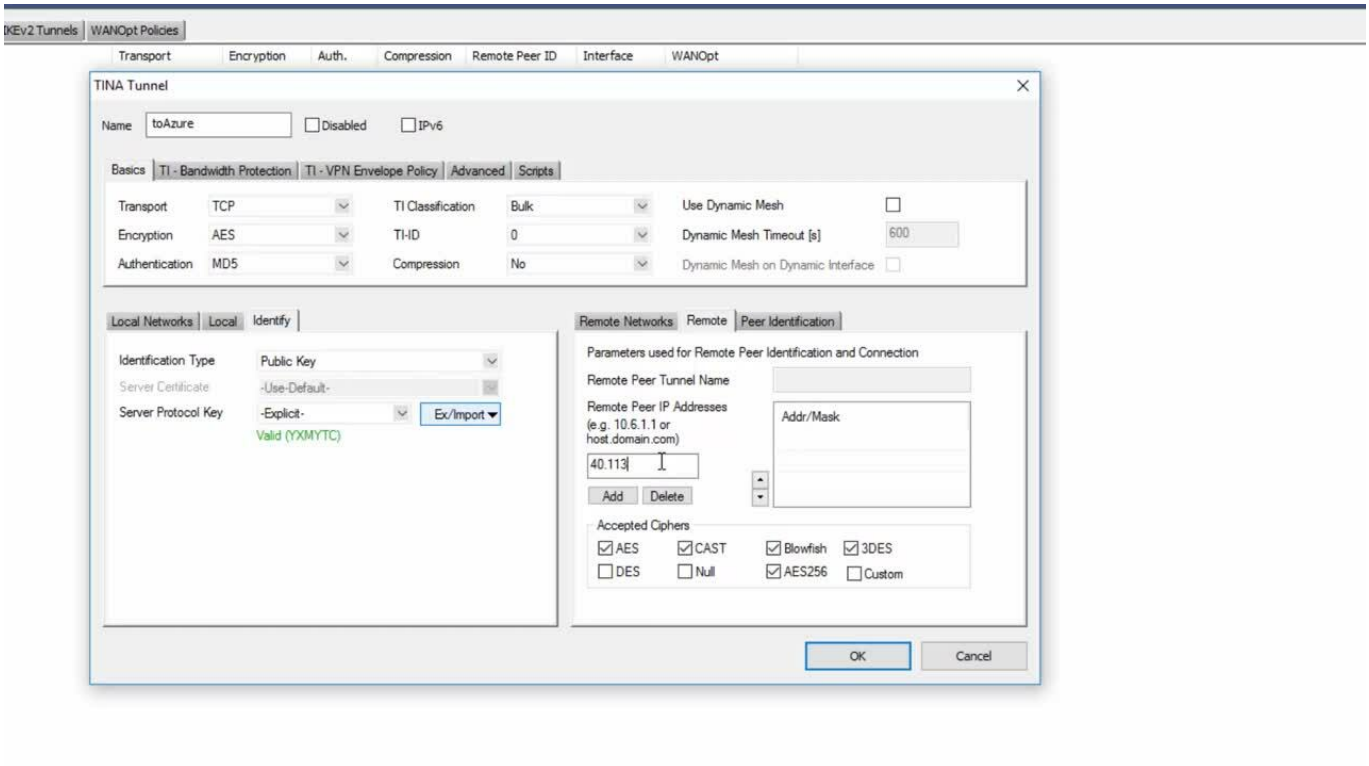
Deploy a High Availability Cluster

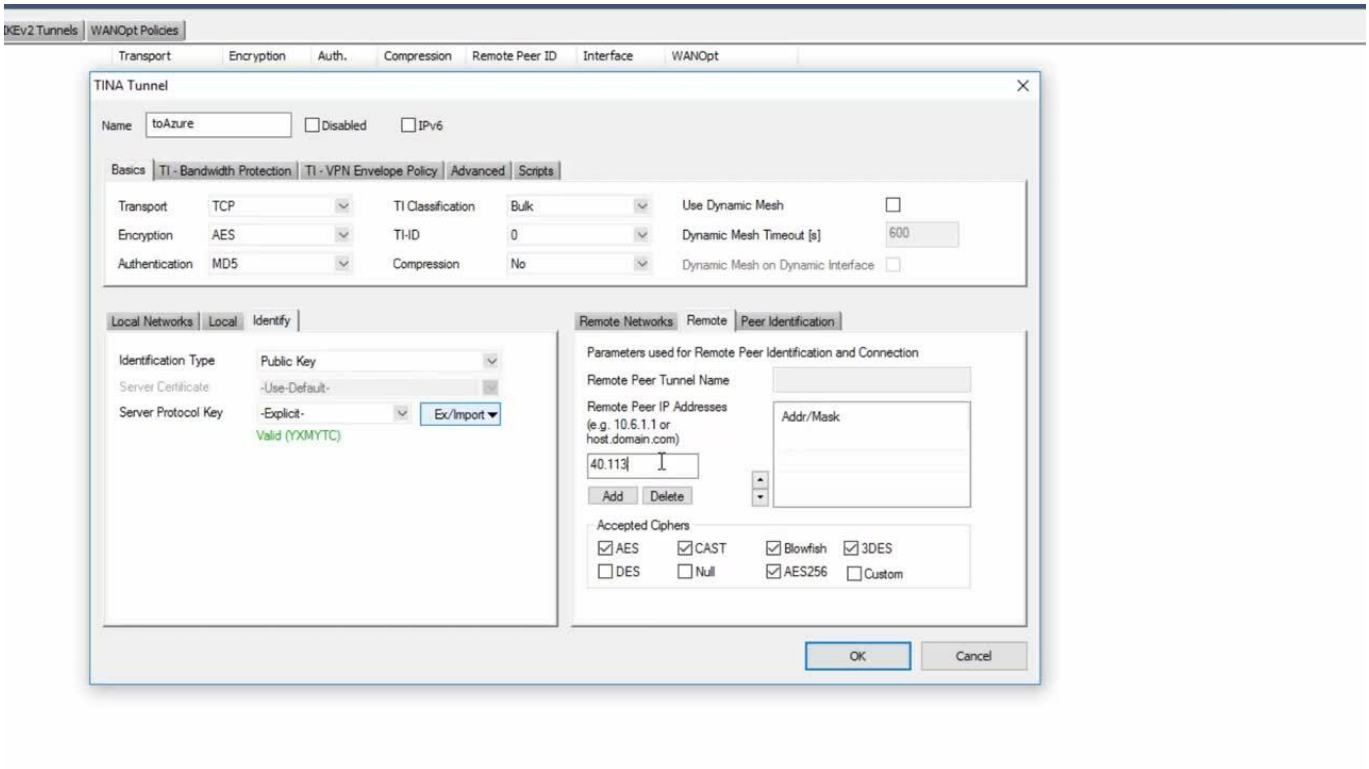
Create a high availability cluster by deploying two CloudGen Firewall VMs in the same subnet and availability zone. Incoming traffic is then forwarded to the active firewall by an Azure Load Balancer. User-defined routing and the rewriting of the routes by the active firewall ensure that the backend VMs always use the active firewall as the gateway device.

For more information, see How to Configure a High Availability Cluster in Azure using PowerShell and ARM.

Example Video

Watch the following video to see a high availability firewall cluster using SD-WAN for a hybrid cloud setup.





Videolink:

https://campus.barracuda.com/

Figures

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.