Microsoft

Microsoft Azure Networking

The Definitive Guide

Avinash Valiramani

Microsoft

Microsoft Azure Networking: The Definitive Guide

Avinash Valiramani

HIGHLY AVAILABLE VNET-TO-VNET

Similar to the full-mesh S2S HA in active-active mode, the vNET-to-vNET design supports an active-active gateway between two vNETs. (See Figure 3-8.) This allows for the establishment of four tunnels between the two VPN gateways connected to two vNETs to provide higher availability and resiliency. (Note that BGP is optional in this setup unless transit routing is required.)

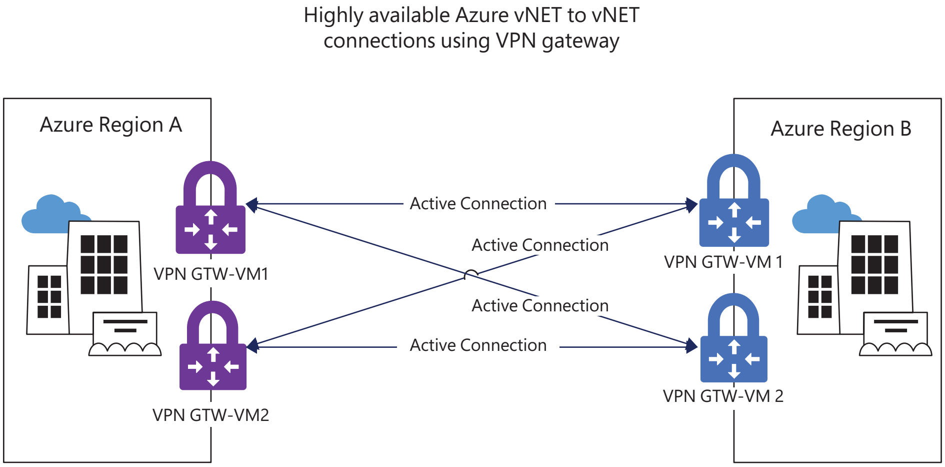


FIGURE 3-8 Highly available Azure vNET-to-vNET connections using VPN gateways.

ExpressRoute

This book does not discuss ExpressRoute in detail. Still, it is important to know that ExpressRoute is a connectivity option available for your environment, based on your use case. ExpressRoute allows you to extend your on-premises networks with the help of a connectivity provider directly into the Microsoft cloud over a private connection.

> ***NOTE*** **Connections to Microsoft cloud services are not limited to Microsoft Azure. Connectivity to other Microsoft services such as Microsoft 365 and Dynamics 365 is also allowed.**

With ExpressRoute, all connectivity occurs over a private network with the most stringent possible SLAs. This makes ExpressRoute connections more secure and reliable than S2S VPN connections. ExpressRoute also provides higher throughputs and lower latency, making it ideal for large organizations and for organizations whose security and compliance requirements call for its use.

ExpressRoute and site-to-site VPN gateways can co-exist on the same Azure vNET and can be implemented with an active-failover design, such that issues with ExpressRoute will result in an automated failback to the S2S VPN. The other option is to leverage S2S VPNs for sites that are not covered by ExpressRoute connections. It is important to be aware of this compatibility so that you can take it into account when designing for larger environments in which reliability and redundancy are critical for business.

Zonal and zone-redundant VPN gateways

Azure VPN gateway devices support deployment in Azure availability zones. This extends all the redundancy, scalability, and availability features of availability zones to the vNET gateway devices. When gateway devices are deployed in Azure availability zones, they are separated physically and logically within an Azure region to protect against zone-level failures.

There are two options for availability zones:

- **Zonal gateways** When a VPN gateway is deployed in an availability zone and the availability zone configuration is specified, all instances of the gateway are deployed in that same availability zone. These are called zonal gateways.
- **Zone-redundant gateways** If the availability zone configuration is set to automatic, the VPN gateway is deployed across availability zones, making them zone-redundant to provide higher resiliency.

> ***NOTE*** **The two VPN gateway instances will be deployed in any two out of the three availability zones in a region.**

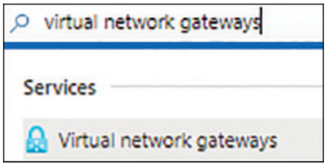
Azure VPN gateway walkthrough

The following sections walk you through the process of creating an Azure VPN gateway using the Azure Portal, Azure PowerShell, and the Azure CLI. If you are following along, be sure to select resources and resource names based on your environment, including a unique Azure VPN gateway name for each of your deployments. Also be sure to delete any unwanted resources after you have completed testing to reduce charges levied by Microsoft for these resources.

USING THE AZURE PORTAL

To create an Azure VPN gateway using the Azure Portal, follow these steps:

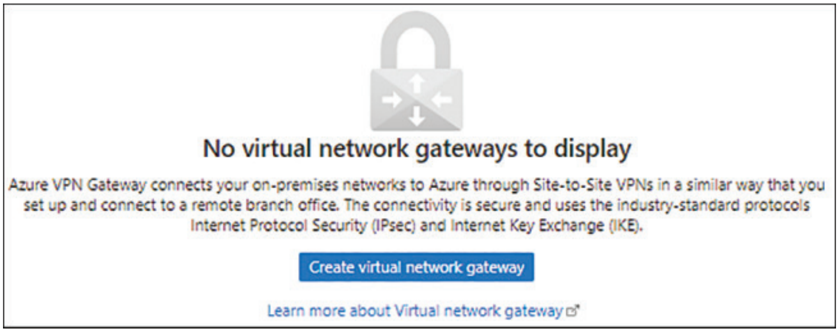
1. Log into the Azure Portal, type **virtual network gateway** in the search box to locate the service, and select it from the list that appears. (See Figure 3-9.)



virtual network gateways

FIGURE 3-9 Selecting the virtual network gateway in the Azure Portal.

2. Click **Create** or **Create Virtual Network Gateway** to start the Create Virtual Network Gateway wizard. (See Figure 3-10.)



No virtual network gateways to display

Azure VPN Gateway connects your on-premises networks to Azure through Site-to-Site VPNs in a similar way that you set up and connect to a remote branch office. The connectivity is secure and uses the industry-standard protocols Internet Protocol Security (IPsec) and Internet Key Exchange (IKE).

Create virtual network gateway
Learn more about Virtual network gateway

FIGURE 3-10 Creating the virtual network gateway.

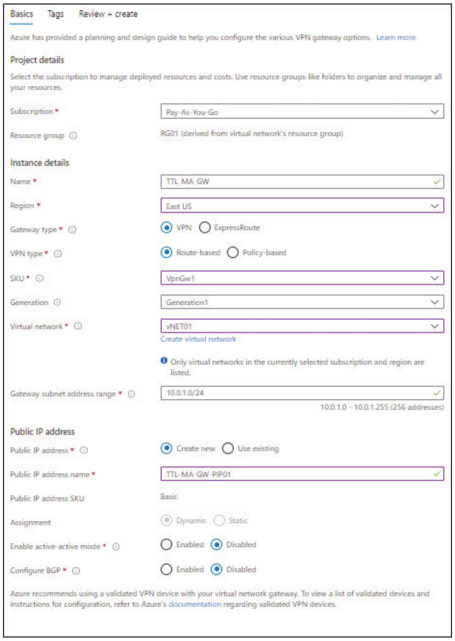
3. In the **Basics** tab of the Create Virtual Network Gateway wizard (see Figure 3-11), enter the following information and click **Next**:
   - **Subscription** Select the subscription to host the vNET gateway.
   - **Name** Type a name for the vNET gateway. If the name you type is already in use, the wizard will prompt you to enter a different name.
   - **Region** Select the Azure region in which you want to create the VPN gateway.

NOTE **Selecting an Azure region automatically populates the Resource Group setting.**

   - **Gateway Type** Select the **VPN** option button.
   - **VPN Type** Select the **Route-Based** option button.
   - **SKU** Choose the **VpnGw1** SKU. Alternatively, for higher throughput, choose a higher SKU.
   - **Generation** Select the SKU's generation. (The options available will depend on the SKU you choose.)
   - **Virtual Network** Select the virtual network you want to use to host the VPN gateway. Alternatively, click the Create New link and follow the prompts to create a new vNET.
   - **Gateway Subnet Address Range** Enter an address range for the gateway subnet. This will be used to assign a private IP address to your VPN gateway.
   - **Public IP Address** Select whether to create a new public IP address or use an existing one. If you want to select an existing IP, you will have to ensure that it is a static public IP on the Standard SKU.

NOTE **If you select the Create New option button, you'll need to add a unique name for the new public IP address in the Public IP Address Name box. If the name you type is already in use, the wizard will prompt you to enter a different one.**

- **Enable Active-Active Mode** Select the **Disabled** option button.
- **Configure BGP** Select the **Disabled** option button (unless BGP is required for the on-premises firewall that you will integrate).



Azure has provided a planning and design guide to help you configure the various VPN gateway options. Learn more.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	Pay-As-You-Go
Resource group ⓘ	RG01 (derived from virtual network's resource group)

Instance details

Name *	TTL MA GW ✓
Region *	East US
Gateway type * ⓘ	● VPN ○ ExpressRoute
VPN type * ⓘ	● Route-based ○ Policy-based
SKU * ⓘ	VpnGw1
Generation ⓘ	Generation1
Virtual network * ⓘ	vNET01 Create virtual network Only virtual networks in the currently selected subscription and region are listed.
Gateway subnet address range * ⓘ	10.0.1.0/24 ✓ 10.0.1.0 - 10.0.1.255 (256 addresses)

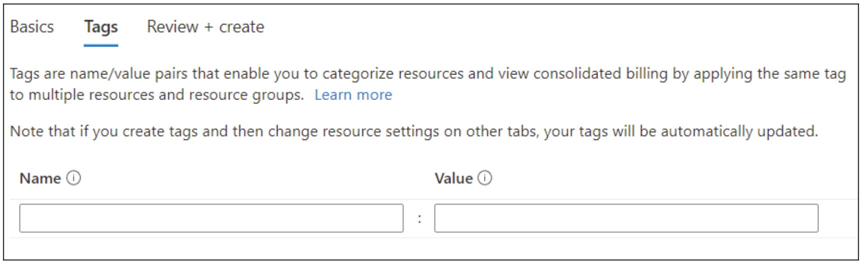
Public IP address

Public IP address * ⓘ	● Create new ○ Use existing
Public IP address name *	TTL-MA-GW-PIP01 ✓
Public IP address SKU	Basic
Assignment	● Dynamic ○ Static
Enable active-active mode * ⓘ	○ Enabled ● Disabled
Configure BGP * ⓘ	○ Enabled ● Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's documentation regarding validated VPN devices.

FIGURE 3-11 The Basics tab of the Create Virtual Network Gateway wizard.

4. In the **Tags** tab (see Figure 3-12), enter any tags required for the vNET gateway or leave the fields blank. Then click **Next: Review + Create**.



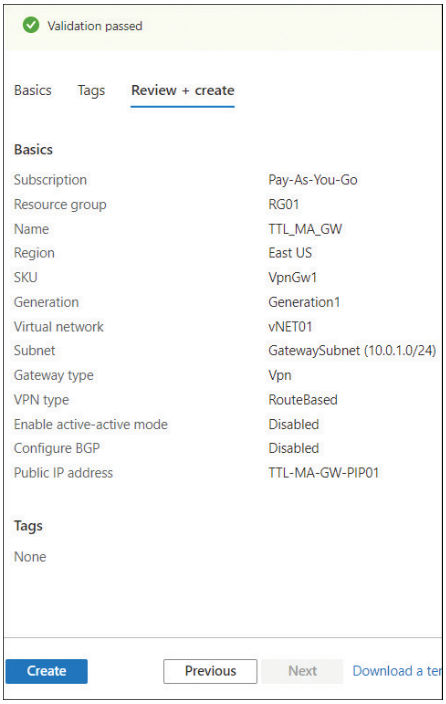
Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name ⓘ		Value ⓘ
	:	

FIGURE 3-12 The Tags tab of the Create Virtual Network Gateway wizard.

5. On the **Review + Create** tab (see Figure 3-13), review your settings and click **Create**.



Basics

Subscription	Pay-As-You-Go
Resource group	RG01
Name	TTL_MA_GW
Region	East US
SKU	VpnGw1
Generation	Generation1
Virtual network	vNET01
Subnet	GatewaySubnet (10.0.1.0/24)
Gateway type	Vpn
VPN type	RouteBased
Enable active-active mode	Disabled
Configure BGP	Disabled
Public IP address	TTL-MA-GW-PIP01

Tags

None

FIGURE 3-13 The Review + Create tab of the Create Virtual Network Gateway wizard in the Azure Portal.

Azure builds the new vNET gateway. Be aware that this can take 30 to 45 minutes.

6. After Azure builds the new vNET gateway, click **Go to Resource**.
7. In the left pane of the vNET gateway's configuration blade, click **Connections**. (See Figure 3-14.)

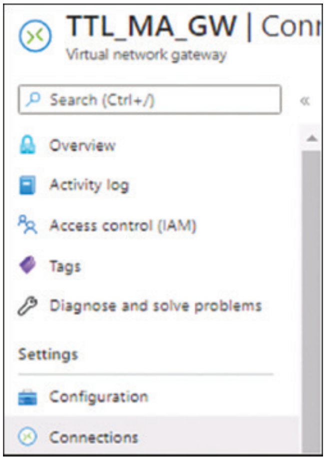
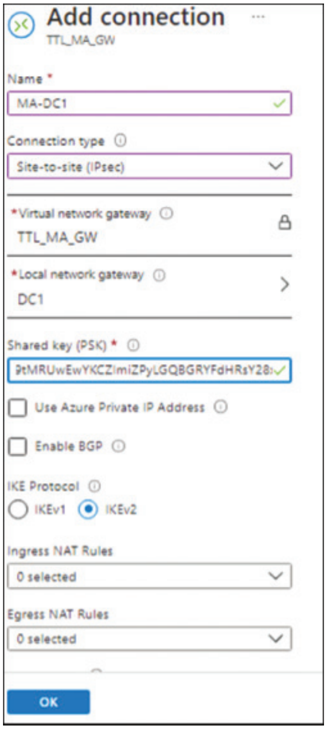


FIGURE 3-14 Creating connections in the vNET gateway.

8. Click **Add** to create a new site-to-site VPN tunnel.

   The Add Connection options open. (See Figure 3-15.)



Add connection

TTL_MA_GW

Name *

MA-DC1

Connection type

Site-to-site (IPsec)

*Virtual network gateway

TTL_MA_GW

*Local network gateway

DC1

Shared key (PSK) *

9tMRUwEwYKCZlmiZPyLGQBGRYFdHRsY28

□ Use Azure Private IP Address

□ Enable BGP

IKE Protocol

○ IKEv1 ● IKEv2

Ingress NAT Rules

0 selected

Egress NAT Rules

0 selected

FIGURE 3-15 The Add Connection options.

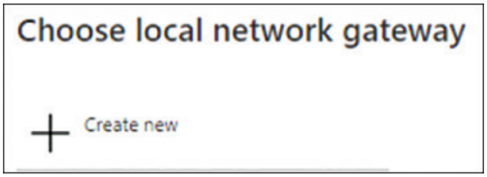
9. In the **Name** box, enter a unique name for the connection. If the name you type is already in use, the dialog box will prompt you to enter a different name.

10. Open the **Connection Type** drop-down list and select **Site-to-Site (IPsec)**.

    The Azure service automatically adds the vNET gateway. Now you need to create a new local network gateway to contain the details of your on-premises firewall.

11. In the Add Connection options, click **Local Network Gateway**.

12. Under **Choose Local Network Gateway**, click **Create New**. (See Figure 3-16.)



Choose local network gateway

FIGURE 3-16 Creating a new local network gateway.