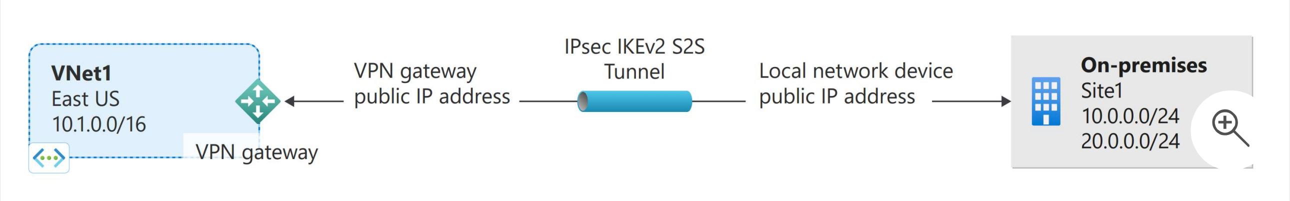
Tutorial: Create a site-to-site VPN connection in the Azure portal

Article • 10/05/2023

This tutorial shows you how to use the Azure portal to create a site-to-site VPN gateway connection between your on-premises network and a virtual network (VNet). You can also create this configuration using Azure PowerShell or Azure CLI.



In this tutorial, you learn how to:

- ✓ Create a virtual network
- ✓ Create a VPN gateway
- ✓ Create a local network gateway
- ✓ Create a VPN connection
- ✓ Verify the connection
- ✓ Connect to a virtual machine

Prerequisites

- An Azure account with an active subscription. If you don't have one, create one for free .
- Make sure you have a compatible VPN device and someone who is able to configure it. For more information about compatible VPN devices and device configuration, see About VPN Devices.
- Verify that you have an externally facing public IPv4 address for your VPN device.
- If you're unfamiliar with the IP address ranges located in your on-premises network configuration, you need to coordinate with someone who can provide those details for you. When you create this configuration, you must specify the IP address range prefixes that Azure will route to your on-premises location. None of the subnets of your on-premises network can over lap with the virtual network subnets that you want to connect to.

Create a virtual network

In this section, you'll create a virtual network (VNet) using the following values:

- **Resource group:** TestRG1
- **Name:** VNet1
- **Region:** (US) East US
- **IPv4 address space:** 10.1.0.0/16
- **Subnet name:** FrontEnd
- **Subnet address space:** 10.1.0.0/24

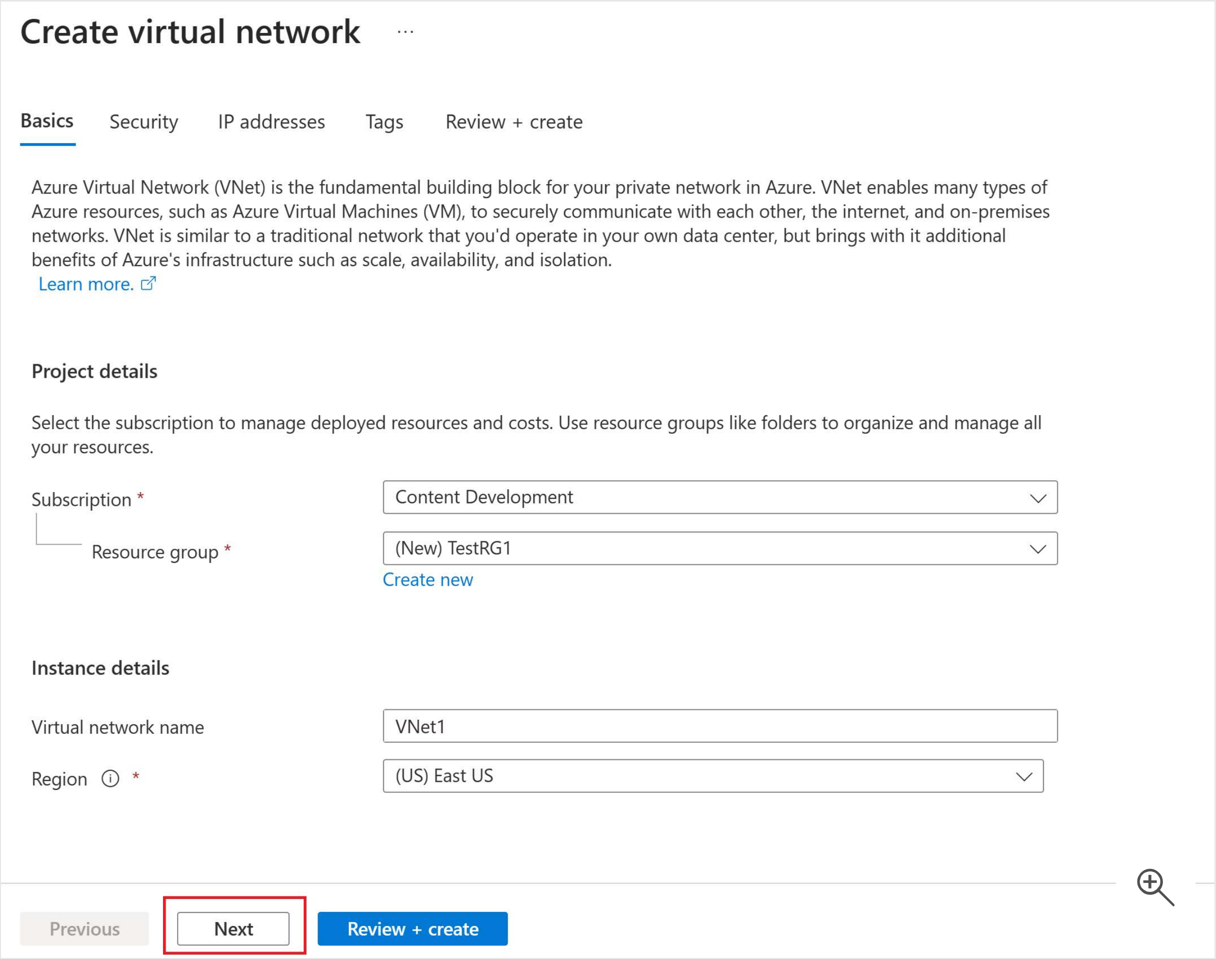
> ⓘ **Note**
>
> When using a virtual network as part of a cross-premises architecture, be sure to coordinate with your on-premises network administrator to carve out an IP address range that you can use specifically for this virtual network. If a duplicate address range exists on both sides of the VPN connection, traffic will route in an unexpected way. Additionally, if you want to connect this virtual network to another virtual network, the address space cannot overlap with the other virtual network. Plan your network configuration accordingly.

1. Sign in to the Azure portal .

2. In **Search resources, service, and docs (G+/)** at the top of the portal page, type ***virtual network***. Select **Virtual network** from the **Marketplace** results to open the **Virtual network** page.

3. On the **Virtual network** page, select **Create**. This opens the **Create virtual network** page.

4. On the **Basics** tab, configure the VNet settings for **Project details** and **Instance details**. You'll see a green check mark when the values you enter are validated. The values shown in the example can be adjusted according to the settings that you require.



Create virtual network ···

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.
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 * Content Development

Resource group * (New) TestRG1

Create new

Instance details

Virtual network name VNet1

Region * (US) East US

- **Subscription**: Verify that the subscription listed is the correct one. You can change subscriptions by using the drop-down.
- **Resource group**: Select an existing resource group, or select **Create new** to create a new one. For more information about resource groups, see Azure Resource Manager overview.
- **Name**: Enter the name for your virtual network.
- **Region**: Select the location for your VNet. The location determines where the resources that you deploy to this VNet will live.

5. Select **Next** or **Security** to advance to the Security tab. For this exercise, leave the default values for all the services on this page.

6. Select **IP Addresses** to advance to the IP Addresses tab. On the **IP Addresses** tab, configure the settings.

   - **IPv4 address space**: By default, an address space is automatically created. You can select the address space and adjust it to reflect your own values. You can also add a different address space and remove the default that was automatically created. For example, you can specify the starting address as **10.1.0.0** and specify the address space size as **/16**, then **Add** that address space.

- **+ Add subnet**: If you use the default address space, a default subnet is created automatically. If you change the address space, add a new subnet within that address space. Select **+ Add subnet** to open the **Add subnet** window. Configure the following settings, then select **Add** at the bottom of the page to add the values.
  - **Subnet name**: Example: **FrontEnd**.
  - **Subnet address range**: The address range for this subnet. For example, **10.1.0.0** and **/24**.

7. Review the **IP addresses** page and remove any address spaces or subnets that you don't need.

8. Select **Review + create** to validate the virtual network settings.

9. After the settings have been validated, select **Create** to create the virtual network.

Create a VPN gateway

In this step, you create the virtual network gateway for your VNet. Creating a gateway can often take 45 minutes or more, depending on the selected gateway SKU.

About the gateway subnet

The virtual network gateway uses specific subnet called the gateway subnet. The gateway subnet is part of the virtual network IP address range that you specify when configuring your virtual network. It contains the IP addresses that the virtual network gateway resources and services use.

When you create the gateway subnet, you specify the number of IP addresses that the subnet contains. The number of IP addresses needed depends on the VPN gateway configuration that you want to create. Some configurations require more IP addresses than others. It's best to specify /27 or larger (/26,/25 etc.) for your gateway subnet.

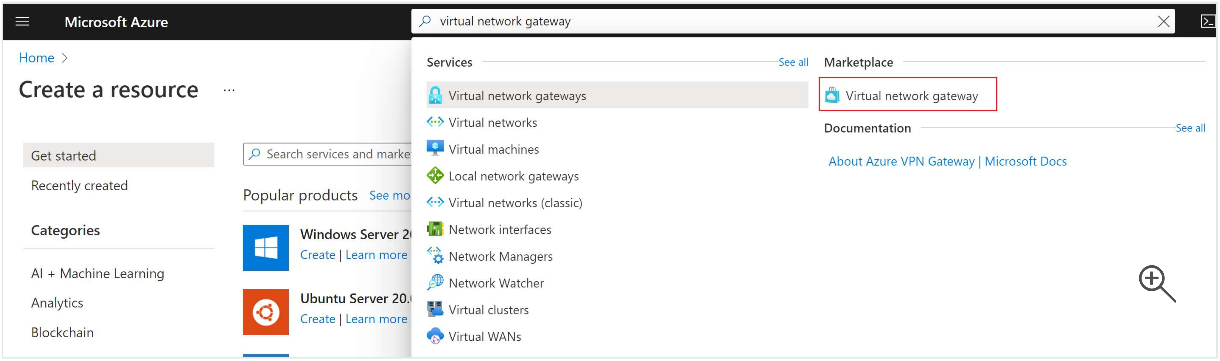
If you see an error that specifies that the address space overlaps with a subnet, or that the subnet isn't contained within the address space for your virtual network, check your VNet address range. You may not have enough IP addresses available in the address range you created for your virtual network. For example, if your default subnet encompasses the entire address range, there are no IP addresses left to create additional subnets. You can either adjust your subnets within the existing address space to free up IP addresses, or specify an additional address range and create the gateway subnet there.

Create the gateway

Create a virtual network gateway (VPN gateway) using the following values:

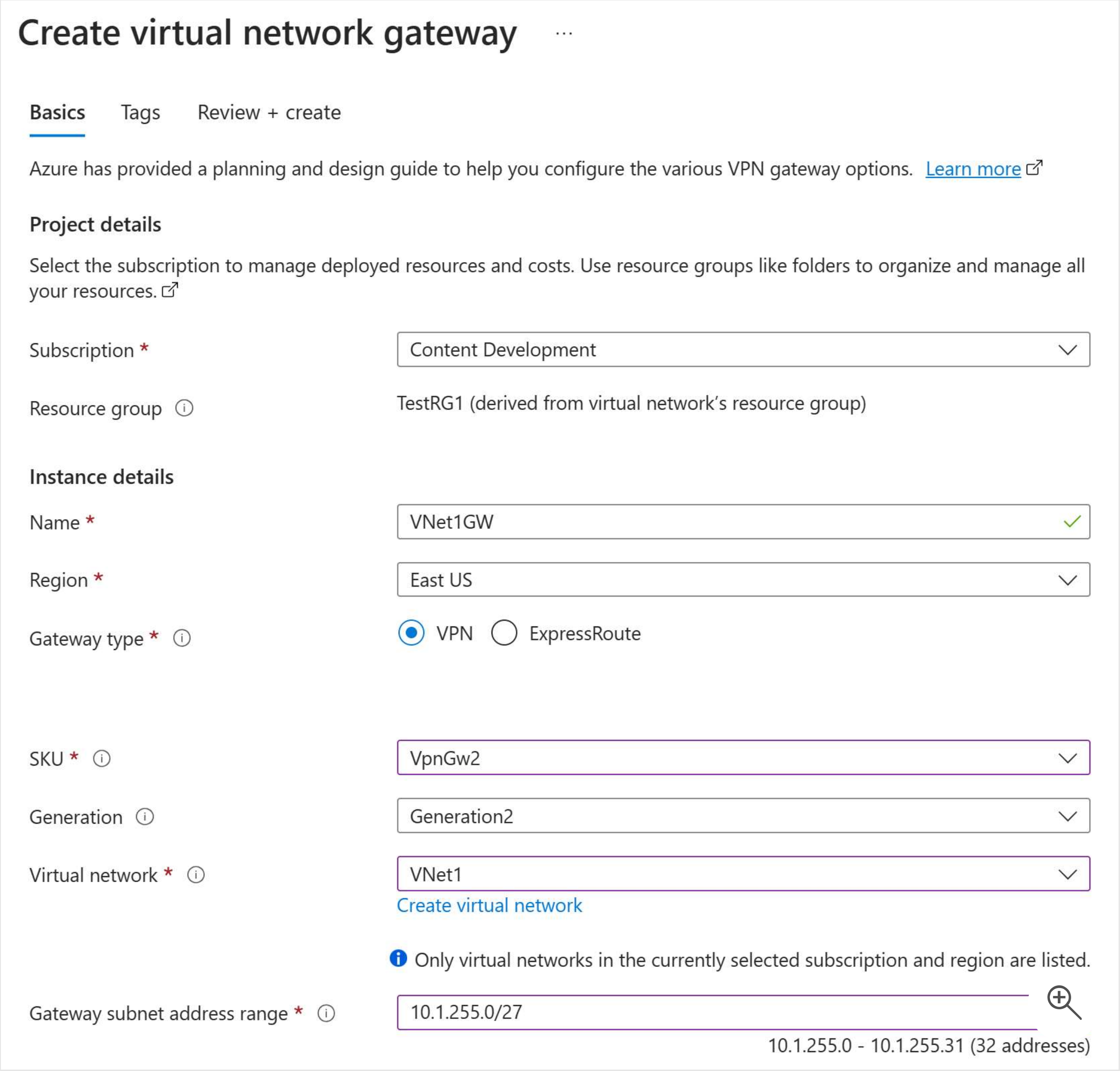
- **Name:** VNet1GW
- **Region:** East US
- **Gateway type:** VPN
- **SKU:** VpnGw2
- **Generation:** Generation 2
- **Virtual network:** VNet1
- **Gateway subnet address range:** 10.1.255.0/27
- **Public IP address:** Create new
- **Public IP address name:** VNet1GWpip
- **Enable active-active mode:** Disabled
- **Configure BGP:** Disabled

1. In **Search resources, services, and docs (G+/)** type **virtual network gateway**. Locate **Virtual network gateway** in the Marketplace search results and select it to open the **Create virtual network gateway** page.



virtual network gateway

2. On the **Basics** tab, fill in the values for **Project details** and **Instance details**.



Create virtual network gateway ...

Basics Tags Review + create

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 * : Content Development

Resource group : TestRG1 (derived from virtual network's resource group)

Instance details

Name * : VNet1GW

Region * : East US

Gateway type * : ● VPN ○ ExpressRoute

SKU * : VpnGw2

Generation : Generation2

Virtual network * : VNet1

Create virtual network

Only virtual networks in the currently selected subscription and region are listed.

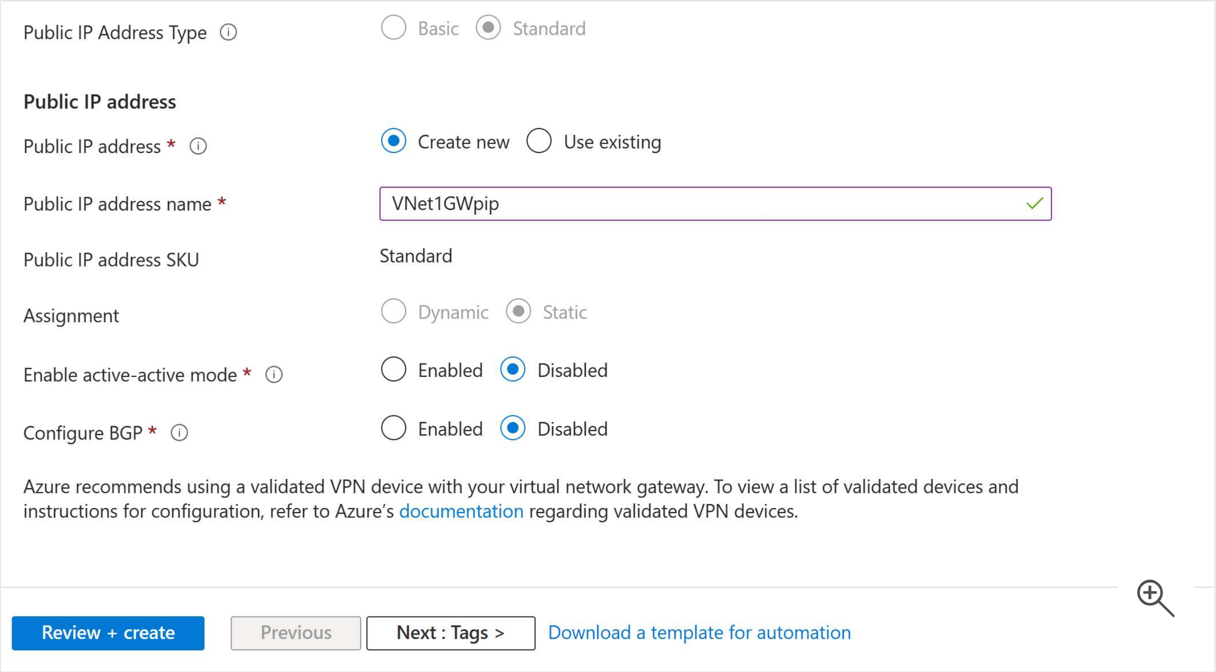
Gateway subnet address range * : 10.1.255.0/27

10.1.255.0 - 10.1.255.31 (32 addresses)

- **Subscription**: Select the subscription you want to use from the dropdown.
- **Resource Group**: This setting is autofilled when you select your virtual network on this page.
- **Name**: Name your gateway. Naming your gateway not the same as naming a gateway subnet. It's the name of the gateway object you're creating.
- **Region**: Select the region in which you want to create this resource. The region for the gateway must be the same as the virtual network.
- **Gateway type**: Select **VPN**. VPN gateways use the virtual network gateway type **VPN**.
- **SKU**: Select the gateway SKU that supports the features you want to use from the dropdown. See Gateway SKUs. In the portal, the SKUs available in the dropdown depend on the `VPN type` you select. The Basic SKU can only be configured using Azure CLI or PowerShell. You can't configure the Basic SKU in the Azure portal.

- **Generation**: Select the generation you want to use. We recommend using a Generation2 SKU. For more information, see Gateway SKUs.
- **Virtual network**: From the dropdown, select the virtual network to which you want to add this gateway. If you can't see the VNet for which you want to create a gateway, make sure you selected the correct subscription and region in the previous settings.
- **Gateway subnet address range**: This field only appears if your VNet doesn't have a gateway subnet. It's best to specify /27 or larger (/26,/25 etc.). This allows enough IP addresses for future changes, such as adding an ExpressRoute gateway. If you already have a gateway subnet, you can view GatewaySubnet details by navigating to your virtual network. Select **Subnets** to view the range. If you want to change the range, you can delete and recreate the GatewaySubnet.

3. Specify in the values for **Public IP address**. These settings specify the public IP address object that gets associated to the VPN gateway. The public IP address is assigned to this object when the VPN gateway is created. The only time the primary public IP address changes is when the gateway is deleted and re-created. It doesn't change across resizing, resetting, or other internal maintenance/upgrades of your VPN gateway.



Public IP Address Type ⓘ	○ Basic ● Standard
Public IP address	
Public IP address * ⓘ	● Create new ○ Use existing
Public IP address name *	VNet1GWpip ✓
Public IP address SKU	Standard
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.

- **Public IP address type**: For this exercise, if you have the option to choose the address type, select **Standard**.
- **Public IP address**: Leave **Create new** selected.
- **Public IP address name**: In the text box, type a name for your public IP address instance.

- **Public IP address SKU**: Setting is autoselected.
- **Assignment**: The assignment is typically autoselected and can be either Dynamic or Static.
- **Enable active-active mode**: Select **Disabled**. Only enable this setting if you're creating an active-active gateway configuration.
- **Configure BGP**: Select **Disabled**, unless your configuration specifically requires this setting. If you do require this setting, the default ASN is 65515, although this value can be changed.

4. Select **Review + create** to run validation.

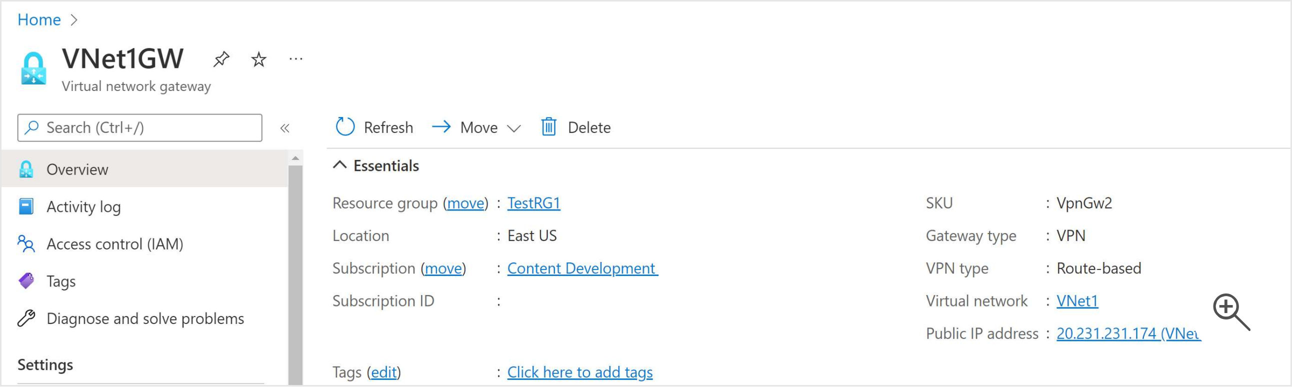
5. Once validation passes, select **Create** to deploy the VPN gateway.

You can see the deployment status on the Overview page for your gateway. A gateway can take up to 45 minutes to fully create and deploy. After the gateway is created, you can view the IP address that has been assigned to it by looking at the virtual network in the portal. The gateway appears as a connected device.

> ⓘ **Important**
>
> When working with gateway subnets, avoid associating a network security group (NSG) to the gateway subnet. Associating a network security group to this subnet may cause your virtual network gateway (VPN and Express Route gateways) to stop functioning as expected. For more information about network security groups, see **What is a network security group?**.

View the public IP address

You can view the gateway public IP address on the **Overview** page for your gateway.



Resource group (move) : TestRG1
Location : East US
Subscription (move) : Content Development
Subscription ID :
Tags (edit) : Click here to add tags
SKU : VpnGw2
Gateway type : VPN
VPN type : Route-based
Virtual network : VNet1
Public IP address : 20.231.231.174 (VNe

To see additional information about the public IP address object, select the name/IP address link next to **Public IP address**.

Create a local network gateway

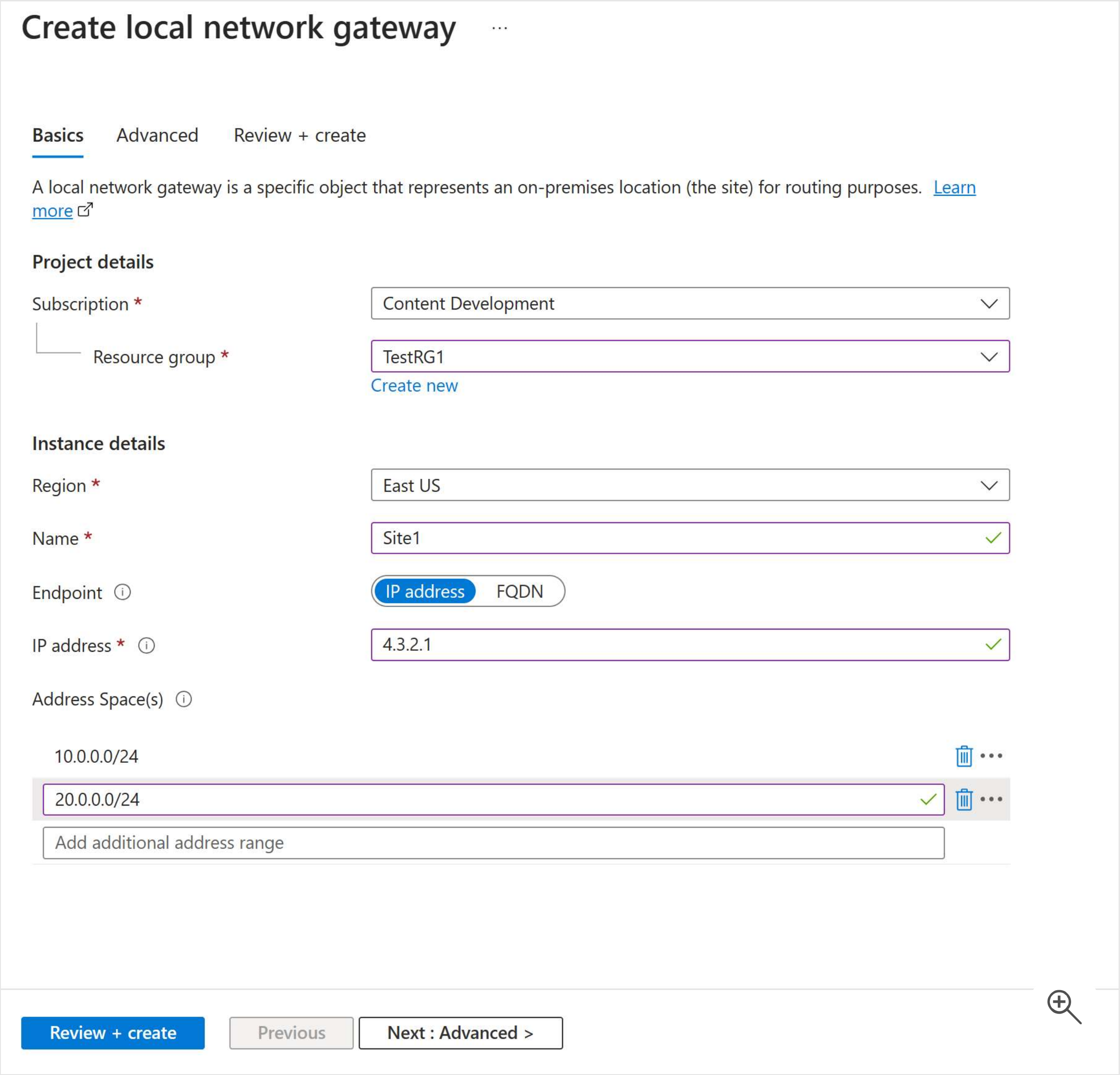
The local network gateway is a specific object that represents your on-premises location (the site) for routing purposes. You give the site a name by which Azure can refer to it, then specify the IP address of the on-premises VPN device to which you'll create a connection. You also specify the IP address prefixes that will be routed through the VPN gateway to the VPN device. The address prefixes you specify are the prefixes located on your on-premises network. If your on-premises network changes or you need to change the public IP address for the VPN device, you can easily update the values later.

Create a local network gateway using the following values:

- **Name:** Site1
- **Resource Group:** TestRG1
- **Location:** East US

1. From the Azure portal, in **Search resources, services, and docs (G+/)** type **local network gateway**. Locate **local network gateway** under **Marketplace** in the search results and select it. This opens the **Create local network gateway** page.

2. On the **Create local network gateway page**, on the **Basics** tab, specifiy the values for your local network gateway.



Create local network gateway ...

Basics | Advanced | Review + create

A local network gateway is a specific object that represents an on-premises location (the site) for routing purposes. Learn more

Project details

Subscription *	Content Development
Resource group *	TestRG1 Create new

Instance details

Region *	East US
Name *	Site1 ✓
Endpoint ⓘ	● IP address ○ FQDN
IP address * ⓘ	4.3.2.1 ✓

Address Space(s) ⓘ

10.0.0.0/24

20.0.0.0/24 ✓

Add additional address range

- **Subscription:** Verify that the correct subscription is showing.
- **Resource Group:** Select the resource group that you want to use. You can either create a new resource group, or select one that you've already created.
- **Region:** Select the region that this object will be created in. You may want to select the same location that your VNet resides in, but you aren't required to do so.
- **Name:** Specify a name for your local network gateway object.
- **Endpoint:** Select the endpoint type for the on-premises VPN device - **IP address** or **FQDN (Fully Qualified Domain Name)**.
    - **IP address**: If you have a static public IP address allocated from your Internet service provider for your VPN device, select the IP address option and fill in the IP address as shown in the example. This is the public IP address of the VPN device that you want Azure VPN gateway to connect to. If you don't have the IP address right now, you can use the values shown in the example,

    but you'll need to go back and replace your placeholder IP address with the public IP address of your VPN device. Otherwise, Azure won't be able to connect.
  - **FQDN**: If you have a dynamic public IP address that could change after certain period of time, often determined by your Internet service provider, you can use a constant DNS name with a Dynamic DNS service to point to your current public IP address of your VPN device. Your Azure VPN gateway resolves the FQDN to determine the public IP address to connect to.
- **Address Space** refers to the address ranges for the network that this local network represents. You can add multiple address space ranges. Make sure that the ranges you specify here don't overlap with ranges of other networks that you want to connect to. Azure routes the address range that you specify to the on-premises VPN device IP address. *Use your own values here if you want to connect to your on-premises site, not the values shown in the example*.

> ⓘ **Note**
>
> - Azure VPN supports only one IPv4 address for each FQDN. If the domain name resolves to multiple IP addresses, Azure VPN Gateway will use the first IP address returned by the DNS servers. To eliminate the uncertainty, we recommend that your FQDN always resolve to a single IPv4 address. IPv6 is not supported.
> - Azure VPN Gateway maintains a DNS cache refreshed every 5 minutes. The gateway tries to resolve the FQDNs for disconnected tunnels only. Resetting the gateway will also trigger FQDN resolution.

3. On the **Advanced** tab, you can configure BGP settings if needed.

4. When you have finished specifying the values, select **Review + create** at the bottom of the page to validate the page.

5. Select **Create** to create the local network gateway object.

Configure your VPN device

Site-to-site connections to an on-premises network require a VPN device. In this step, you configure your VPN device. When configuring your VPN device, you need the following values:

- A shared key. This is the same shared key that you specify when creating your site-to-site VPN connection. In our examples, we use a basic shared key. We recommend that you generate a more complex key to use.
- The public IP address of your virtual network gateway. You can view the public IP address by using the Azure portal, PowerShell, or CLI. To find the public IP address of your VPN gateway using the Azure portal, go to **Virtual network gateways**, then select the name of your gateway.

To download VPN device configuration scripts:

Depending on the VPN device that you have, you may be able to download a VPN device configuration script. For more information, see Download VPN device configuration scripts.

See the following links for additional configuration information:

- For information about compatible VPN devices, see VPN Devices.

- Before configuring your VPN device, check for any Known device compatibility issues for the VPN device that you want to use.

- For links to device configuration settings, see Validated VPN Devices. The device configuration links are provided on a best-effort basis. It's always best to check with your device manufacturer for the latest configuration information. The list shows the versions we've tested. If your OS isn't on that list, it's still possible that the version is compatible. Check with your device manufacturer to verify that OS version for your VPN device is compatible.

- For an overview of VPN device configuration, see Overview of 3rd party VPN device configurations.

- For information about editing device configuration samples, see Editing samples.

- For cryptographic requirements, see About cryptographic requirements and Azure VPN gateways.

- For information about IPsec/IKE parameters, see About VPN devices and IPsec/IKE parameters for site-to-site VPN gateway connections. This link shows information about IKE version, Diffie-Hellman Group, Authentication method, encryption and hashing algorithms, SA lifetime, PFS, and DPD, in addition to other parameter information that you need to complete your configuration.

- For IPsec/IKE policy configuration steps, see Configure IPsec/IKE policy for S2S VPN or VNet-to-VNet connections.
- To connect multiple policy-based VPN devices, see Connect Azure VPN gateways to multiple on-premises policy-based VPN devices using PowerShell.

Create VPN connections

Create a site-to-site VPN connection between your virtual network gateway and your on-premises VPN device.

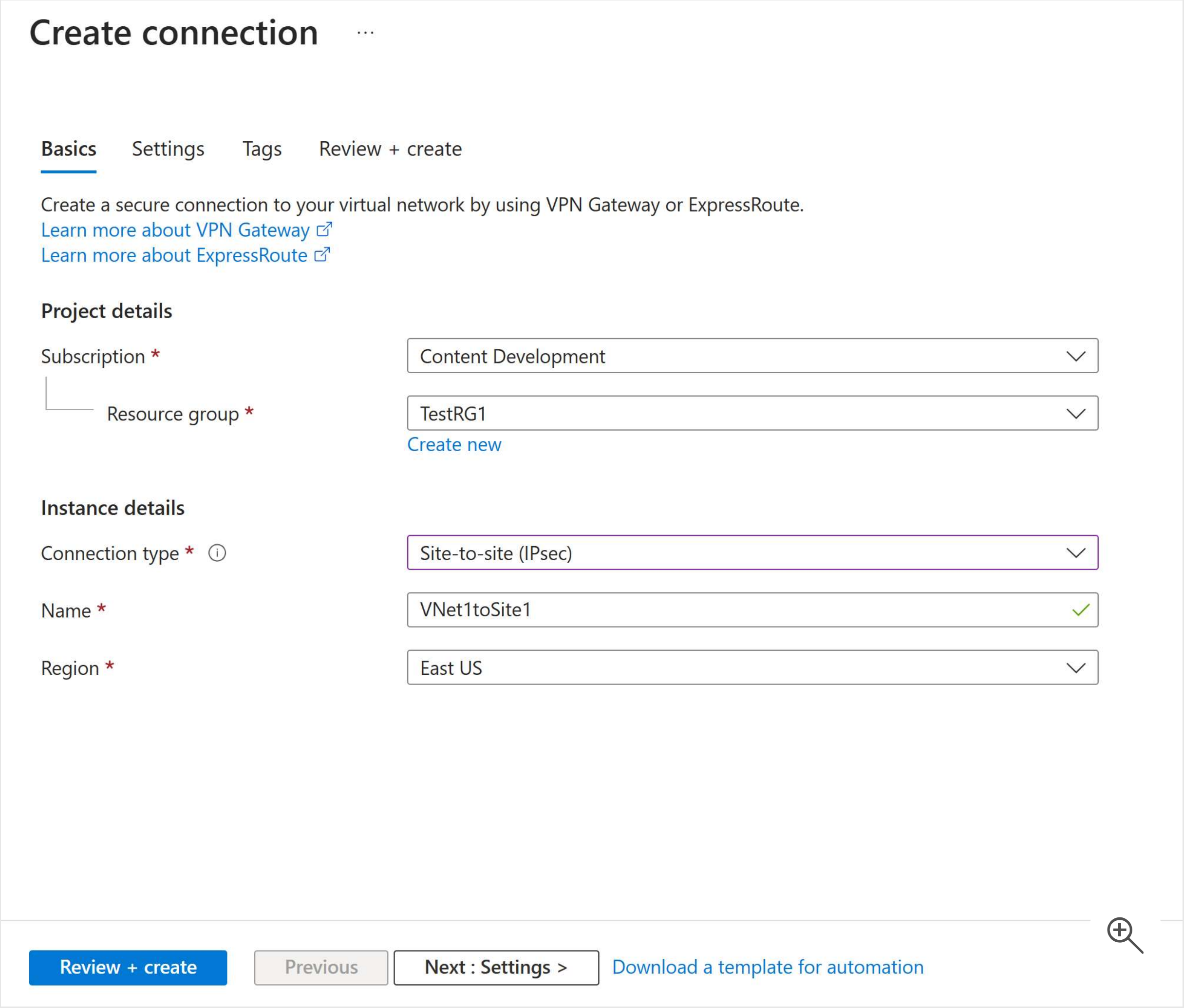
Create a connection using the following values:

- **Local network gateway name:** Site1
- **Connection name:** VNet1toSite1
- **Shared key:** For this example, we use abc123. But, you can use whatever is compatible with your VPN hardware. The important thing is that the values match on both sides of the connection.

1. Go to your virtual network. On your VNet page, select **Connected devices** on the left. Locate your VPN gateway and click to open it.

2. On the page for the gateway, select **Connections**.

3. At the top of the Connections page, select **+Add** to open the **Create connection** page.



Create connection ···

Create a secure connection to your virtual network by using VPN Gateway or ExpressRoute.
Learn more about VPN Gateway
Learn more about ExpressRoute

Project details

Subscription * : Content Development

Resource group * : TestRG1

Create new

Instance details

Connection type * : Site-to-site (IPsec)

Name * : VNet1toSite1

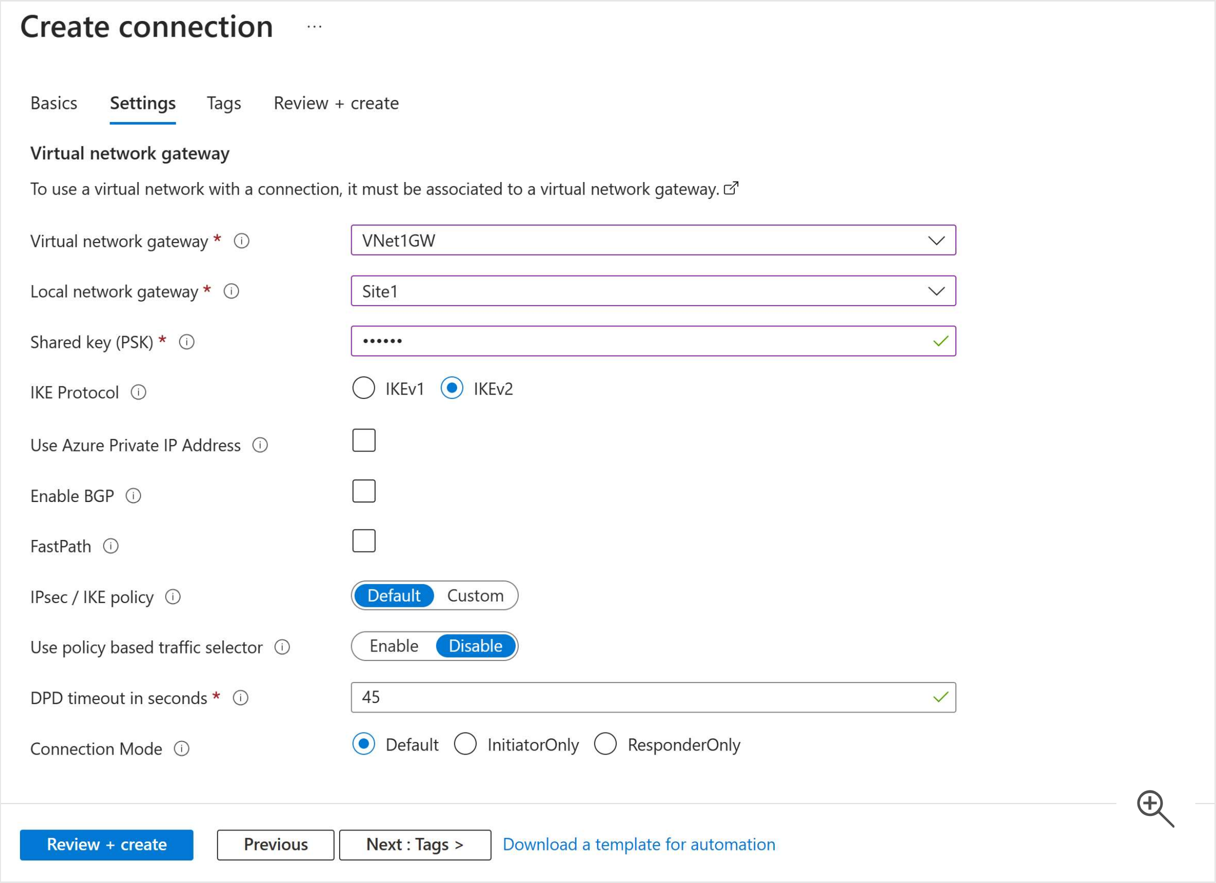
Region * : East US

4. On the Create connection **Basics** page, configure the values for your connection.

   - For **Project details**, select the subscription and the Resource group where your resources are located.

   - For **Instance details**, configure the following settings:
     - **Connection type:** Select **Site-to-site (IPSec)**.
     - **Name:** Name your connection.
     - **Region:** Select the region for this connection.

5. Select **Settings** to navigate to the settings page.



Create connection ···

Basics | Settings | Tags | Review + create

Virtual network gateway

To use a virtual network with a connection, it must be associated to a virtual network gateway.

Virtual network gateway *	VNet1GW
Local network gateway *	Site1
Shared key (PSK) *	•••••• ✓
IKE Protocol	○ IKEv1 ● IKEv2
Use Azure Private IP Address	□
Enable BGP	□
FastPath	□
IPsec / IKE policy	[✓ Default] Custom
Use policy based traffic selector	Enable [✓ Disable]
DPD timeout in seconds *	45 ✓
Connection Mode	● Default ○ InitiatorOnly ○ ResponderOnly

- **Virtual network gateway:** Select the virtual network gateway from the dropdown.
- **Local network gateway:** Select the local network gateway from the dropdown.
- **Shared Key:** the value here must match the value that you're using for your local on-premises VPN device.
- Select **IKEv2**.
- Leave **Use Azure Private IP Address** deselected.
- Leave **Enable BGP** deselected.
- Leave **FastPath** deselected.
- **IPse/IKE policy:** Default.
- **Use policy based traffic selector:** Disable.
- **DPD timeout in seconds:** 45
- **Connection Mode:** leave as Default. This setting is used to specify which gateway can initiate the connection. For more information, see VPN Gateway settings - connection modes.

6. For **NAT Rules Associations**, leave both Ingress and Egress as **0 selected**.

7. Select **Review + create** to validate your connection settings.

8. Select **Create** to create the connection.

9. Once the deployment is complete, you can view the connection in the **Connections** page of the virtual network gateway. The Status goes from *Unknown* to *Connecting*, and then to *Succeeded*.

To configure additional connection settings (optional)

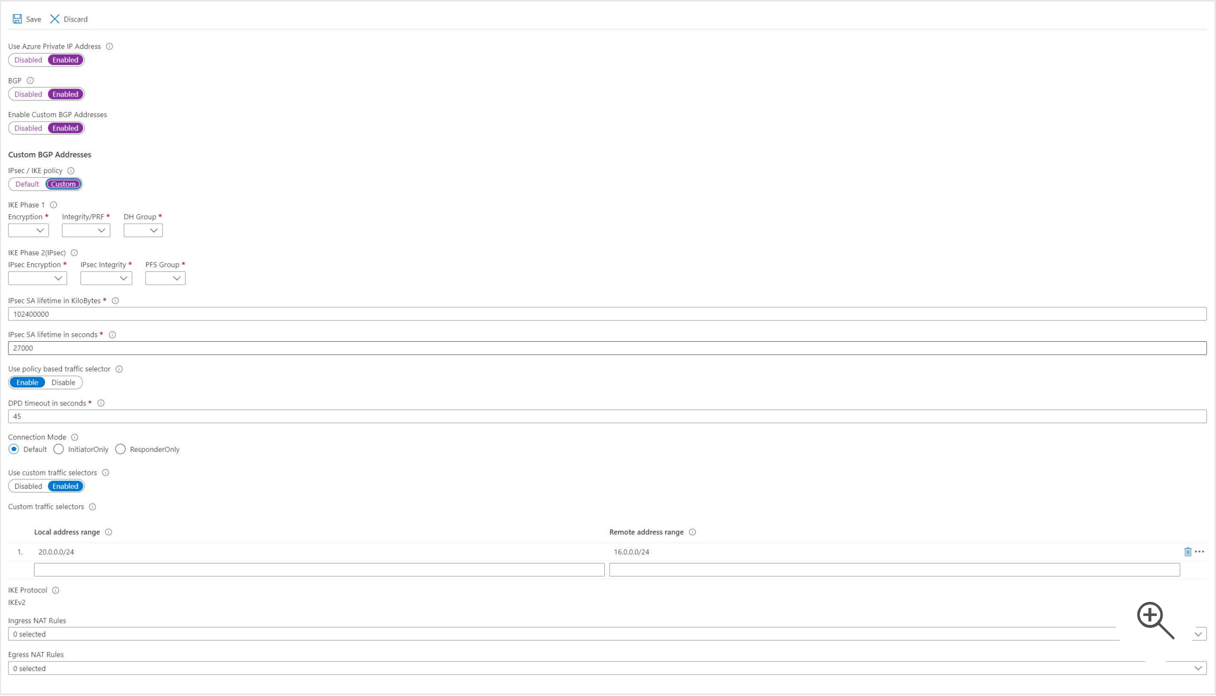
You can configure additional settings for your connection, if necessary. Otherwise, skip this section and leave the defaults in place. For more information, see Configure custom IPsec/IKE connection policies.

1. Go to your virtual network gateway and select **Connections** to open the Connections page.

2. Select the name of the connection you want to configure to open the **Connection** page.

3. On the Connection page left side, select **Configuration** to open the Configuration page. Make any necessary changes, then **Save**.

   In the following screenshot, we've enabled all the settings to show you the configuration settings available in the portal. Click the screenshot to see the expanded view. When you configure your connections, only configure the settings that you require. Otherwise, leave the default settings in place.



Use Azure Private IP Address: Disabled [✓ Enabled]

BGP: Disabled [✓ Enabled]

Enable Custom BGP Addresses: Disabled [✓ Enabled]

Custom BGP Addresses

IPsec / IKE policy: Default [✓ Custom]

IKE Phase 1
Encryption * | Integrity/PRF * | DH Group *

IKE Phase 2(IPsec)
IPsec Encryption * | IPsec Integrity * | PFS Group *

IPsec SA lifetime in KiloBytes *: 102400000

IPsec SA lifetime in seconds *: 27000

Use policy based traffic selector: [✓ Enable] Disable

DPD timeout in seconds *: 45

Connection Mode: ● Default ○ InitiatorOnly ○ ResponderOnly

Use custom traffic selectors: Disabled [✓ Enabled]

Custom traffic selectors

	Local address range	Remote address range
1.	20.0.0.0/24	16.0.0.0/24

IKE Protocol: IKEv2

Ingress NAT Rules: 0 selected

Egress NAT Rules: 0 selected

Verify the VPN connection

In the Azure portal, you can view the connection status of a VPN gateway by navigating to the connection. The following steps show one way to navigate to your connection and verify.

1. In the Azure portal menu, select **All resources** or search for and select **All resources** from any page.
2. Select to your virtual network gateway.
3. On the blade for your virtual network gateway, click **Connections**. You can see the status of each connection.
4. Click the name of the connection that you want to verify to open **Essentials**. In Essentials, you can view more information about your connection. The **Status** is 'Succeeded' and 'Connected' when you have made a successful connection.

Connect to a virtual machine

You can connect to a VM that's deployed to your VNet by creating a Remote Desktop Connection to your VM. The best way to initially verify that you can connect to your VM is to connect by using its private IP address, rather than computer name. That way, you're testing to see if you can connect, not whether name resolution is configured properly.

1. Locate the private IP address. You can find the private IP address of a VM by either looking at the properties for the VM in the Azure portal, or by using PowerShell.

   - Azure portal - Locate your virtual machine in the Azure portal. View the properties for the VM. The private IP address is listed.

   - PowerShell - Use the example to view a list of VMs and private IP addresses from your resource groups. You don't need to modify this example before using it.

     Azure PowerShell

     ```
     $VMs = Get-AzVM
     $Nics = Get-AzNetworkInterface | Where-Object VirtualMachine -ne
     $null

     foreach ($Nic in $Nics) {
     $VM = $VMs | Where-Object -Property Id -eq $Nic.VirtualMachine.Id
     $Prv = $Nic.IpConfigurations | Select-Object -ExpandProperty
     PrivateIpAddress
     $Alloc = $Nic.IpConfigurations | Select-Object -ExpandProperty
     ```

```
PrivateIpAllocationMethod
Write-Output "$($VM.Name): $Prv,$Alloc"
}
```

2. Verify that you're connected to your VNet.

3. Open **Remote Desktop Connection** by typing "RDP" or "Remote Desktop Connection" in the search box on the taskbar, then select Remote Desktop Connection. You can also open Remote Desktop Connection using the 'mstsc' command in PowerShell.

4. In Remote Desktop Connection, enter the private IP address of the VM. You can select "Show Options" to adjust additional settings, then connect.

Troubleshoot a connection

If you're having trouble connecting to a virtual machine over your VPN connection, check the following:

- Verify that your VPN connection is successful.

- Verify that you're connecting to the private IP address for the VM.

- If you can connect to the VM using the private IP address, but not the computer name, verify that you have configured DNS properly. For more information about how name resolution works for VMs, see Name Resolution for VMs.

- For more information about RDP connections, see Troubleshoot Remote Desktop connections to a VM.

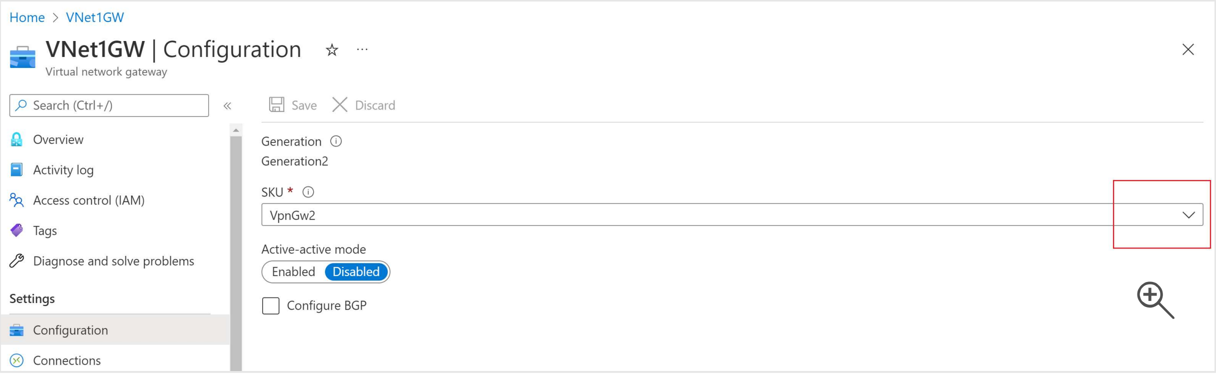
Optional steps

Resize a gateway SKU

There are specific rules regarding resizing vs. changing a gateway SKU. In this section, we'll resize the SKU. For more information, see Gateway settings - resizing and changing SKUs.

1. Go to the **Configuration** page for your virtual network gateway.

2. On the right side of the page, click the dropdown arrow to show the available SKUs list.



Generation
Generation2

SKU *
VpnGw2

Active-active mode
Enabled [✓ Disabled]

□ Configure BGP

3. Select the SKU from the dropdown. The list only includes SKUs you can resize your SKU to. If you don't see the SKU you want to use, instead of resizing, you have to change a SKU.

Reset a gateway

Resetting an Azure VPN gateway is helpful if you lose cross-premises VPN connectivity on one or more site-to-site VPN tunnels. In this situation, your on-premises VPN devices are all working correctly, but aren't able to establish IPsec tunnels with the Azure VPN gateways.

1. In the portal, go to the virtual network gateway that you want to reset.
2. On the **Virtual network gateway** page, in the left pane, scroll down to **Reset**.
3. On the **Reset** page, click **Reset**. Once the command is issued, the current active instance of the Azure VPN gateway is rebooted immediately. Resetting the gateway will cause a gap in VPN connectivity, and may limit future root cause analysis of the issue.

Add another connection

You can create a connection to multiple on-premises sites from the same VPN gateway. If you want to configure multiple connections, the address spaces can’t overlap between any of the connections.

1. To add an additional connection, go to the VPN gateway, then select **Connections** to open the Connections page.
2. Select **+Add** to add your connection. Adjust the connection type to reflect either VNet-to-VNet (if connecting to another VNet gateway), or Site-to-site.
3. If you're connecting using Site-to-site and you haven't already created a local network gateway for the site you want to connect to, you can create a new one.

4. Specify the shared key that you want to use, then select **OK** to create the connection.

Additional configuration considerations

S2S configurations can be customized in a variety of ways. For more information, see the following articles:

- For information about BGP, see the BGP Overview and How to configure BGP.
- For information about forced tunneling, see About forced tunneling.
- For information about Highly Available Active-Active connections, see Highly Available cross-premises and VNet-to-VNet connectivity.
- For information about how to limit network traffic to resources in a virtual network, see Network Security.
- For information about how Azure routes traffic between Azure, on-premises, and Internet resources, see Virtual network traffic routing.

Clean up resources

If you're not going to continue to use this application or go to the next tutorial, delete these resources using the following steps:

1. Enter the name of your resource group in the **Search** box at the top of the portal and select it from the search results.
2. Select **Delete resource group**.
3. Enter your resource group for **TYPE THE RESOURCE GROUP NAME** and select **Delete**.

Next steps

Once you've configured a S2S connection, you can add a P2S connection to the same gateway.

Point-to-Site VPN connections