😊 Azure Site-to-Site VPN

Azure Site-to-Site (S2S) VPN is a networking solution that enables you to connect your on-premises network to an Azure Virtual Network (VNet) over the internet securely. Here's an overview of how Azure S2S VPN works and how to set it up:

How Azure S2S VPN Works

1. **Gateway Deployment:** You deploy a VPN gateway in Azure and configure it as the endpoint for the VPN connection.
2. **On-Premises VPN Device Configuration:** You configure your on-premises VPN device (e.g., router, firewall) to establish a VPN connection with the Azure VPN gateway.
3. **IPsec Tunnel Establishment:** The VPN devices negotiate an IPsec tunnel, creating a secure encrypted connection between your on-premises network and the Azure VNet.
4. **Routing Configuration:** You configure routing to enable traffic flow between your on-premises network and Azure resources.

Features of Azure S2S VPN

1. **Secure Communication:** Uses IPsec protocols for encrypted communication.
2. **Scalability:** Supports high-throughput connections to accommodate various workload demands.
3. **Compatibility:** Works with a wide range of VPN devices from various vendors.
4. **Redundancy:** Provides high availability and redundancy options for resilient connections.
5. **Monitoring and Logging:** Offers visibility into VPN connection health and traffic flow.

The end goal is to establish a secure Site-to-Site VPN connection between an on-premises network and an Azure Virtual Network. This enables secure and seamless communication between resources hosted in Azure and the on-premises network, facilitating scenarios like hybrid cloud setups, remote office connectivity, and secure data transfers.

😄 To begin with the Lab:

1. First, we will create a Virtual Machine that will be part of our previous resource group.
2. Follow the below snapshots to create your VM.

Project details

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

Subscription * ⓘ — Azure Pass - Sponsorship

Resource group * ⓘ — new-grp

Create new

Instance details

Virtual machine name * ⓘ — CompanyVM

Region * ⓘ — (Europe) North Europe

Availability options ⓘ — No infrastructure redundancy required

Security type ⓘ — Trusted launch virtual machines

Configure security features

Image * ⓘ — Windows Server 2022 Datacenter - x64 Gen2

See all images | Configure VM generation

Size * ⓘ — Standard_D2s_v3 - 2 vcpus, 8 GiB memory (₹12,085.69/month)

See all sizes

Enable Hibernation ⓘ

Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernate to enable this feature. Learn more

Administrator account

Username * ⓘ — company

Password * — ••••••••••••

Confirm password * — ••••••••••••

3. Then in the networking you need to create a new Virtual network.

Basics | Disks | **Networking** | Management | Monitoring | Advanced | Tags | Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ — (new) Company-VN

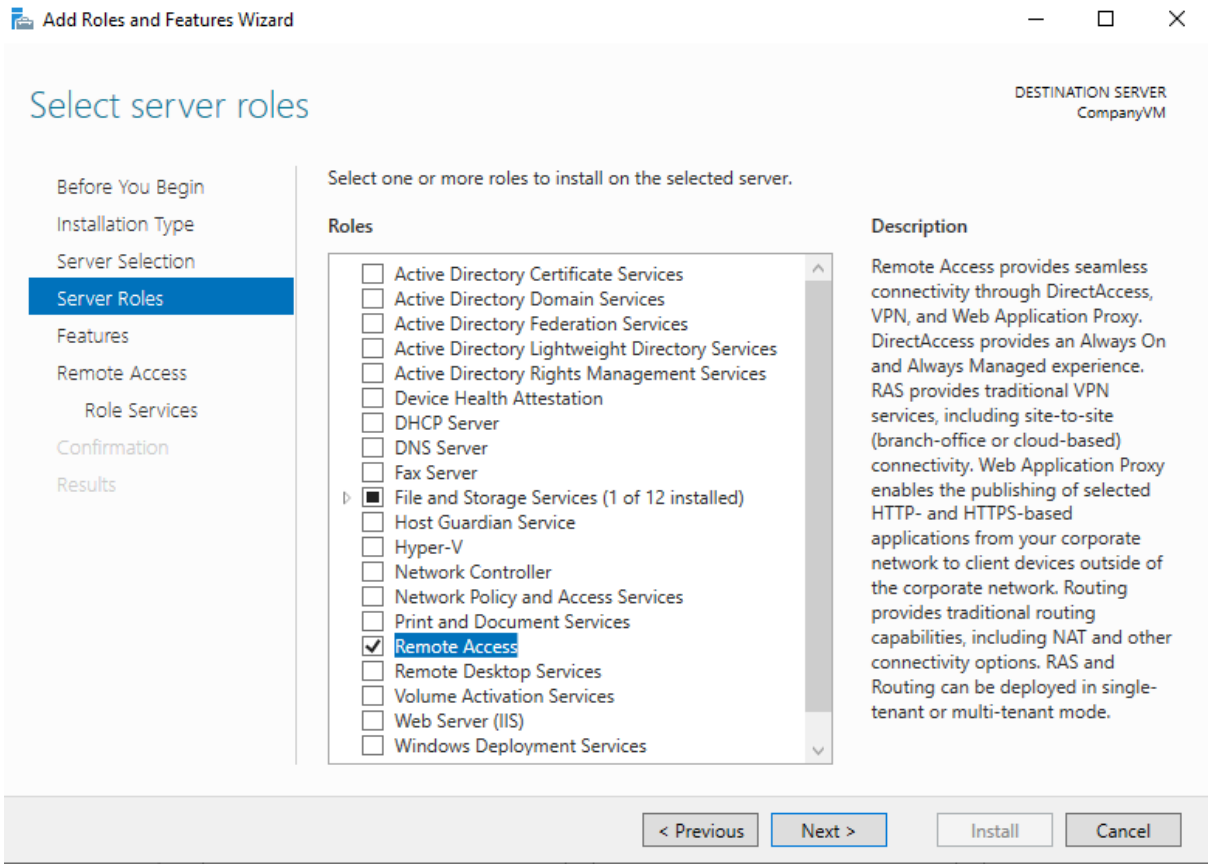
Create new

Subnet * ⓘ — (new) default (10.2.0.0/24)

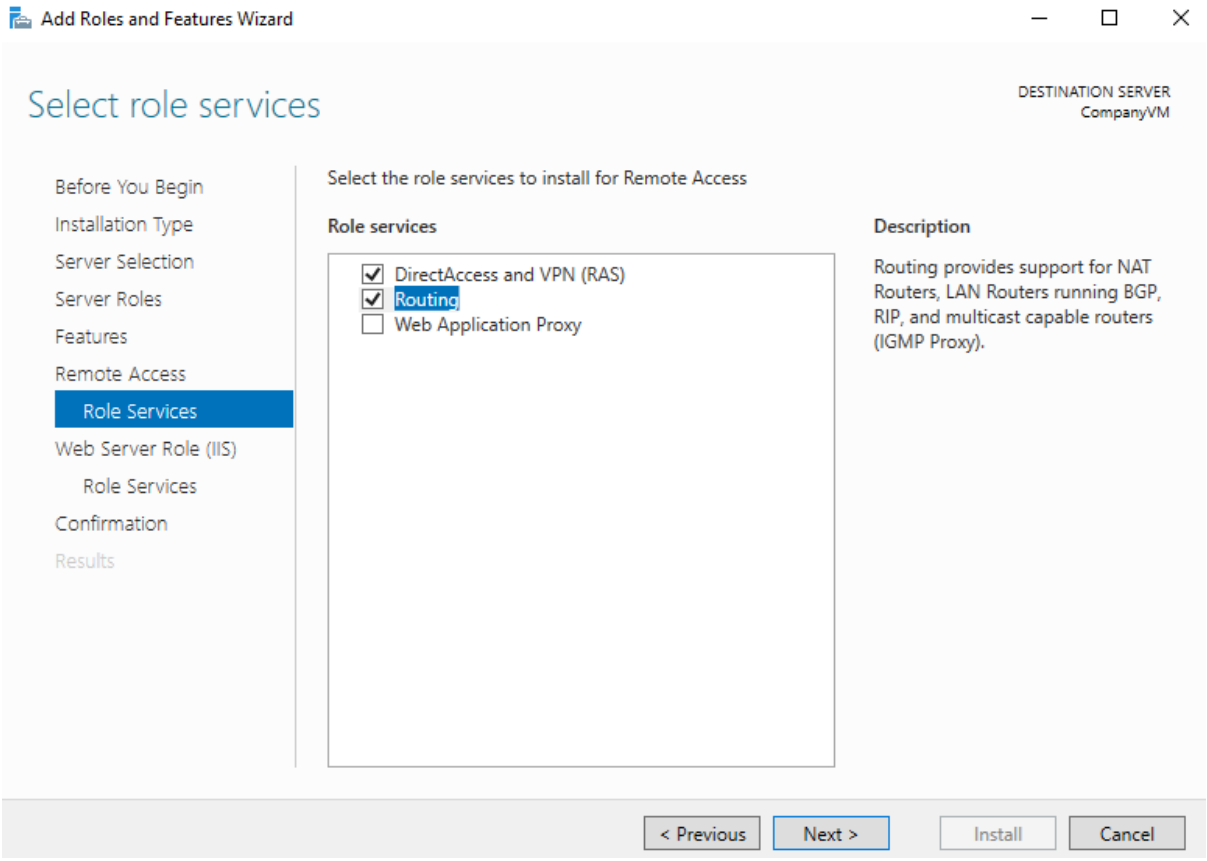
Public IP ⓘ — (new) CompanyVM-ip

Create new

4. Then jump directly to the review page and create your VM. Once your VM is deployed, then login to it.
5. Now inside your VM you have to install remote access instead of the web server this time.



6. After that in role services you have to choose both of the services shown below.
7. Also we are installing these roles so that our VM will behave as a software router.



8. So, for this to work we also need to create a local gateway. For that in your Portal from the marketplace search for the local network gateway.

9. Then you need to choose your resource group, after that give it a name and in the IP address you have to put the Public IP address of your company VM and then in the address space put the address space of the company VM. You can get the address space of the company VM from its virtual network.

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 * Azure Pass - Sponsorship

Resource group * new-grp

Create new

Instance details

Region * North Europe

Name * localgateway

Endpoint IP address FQDN

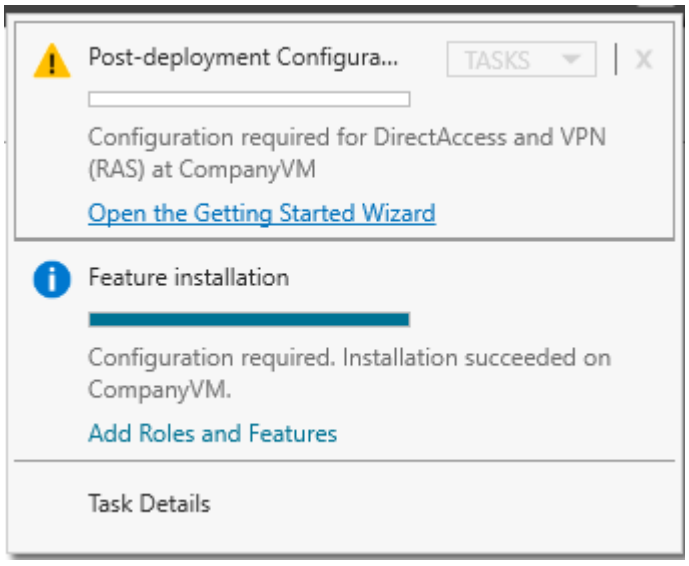
IP address * 52.164.187.68

Address Space(s)

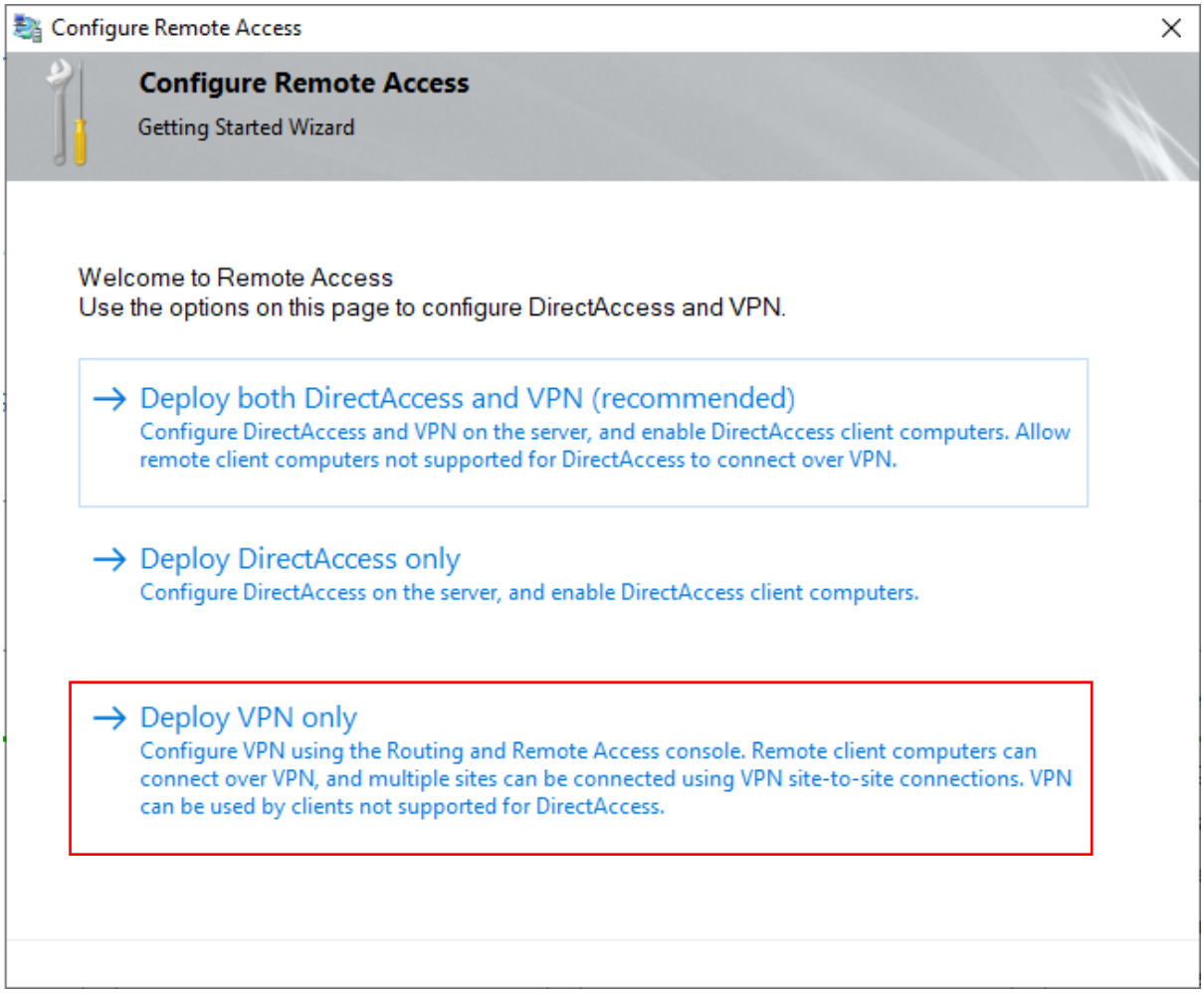
10.2.0.0/16

Add additional address range

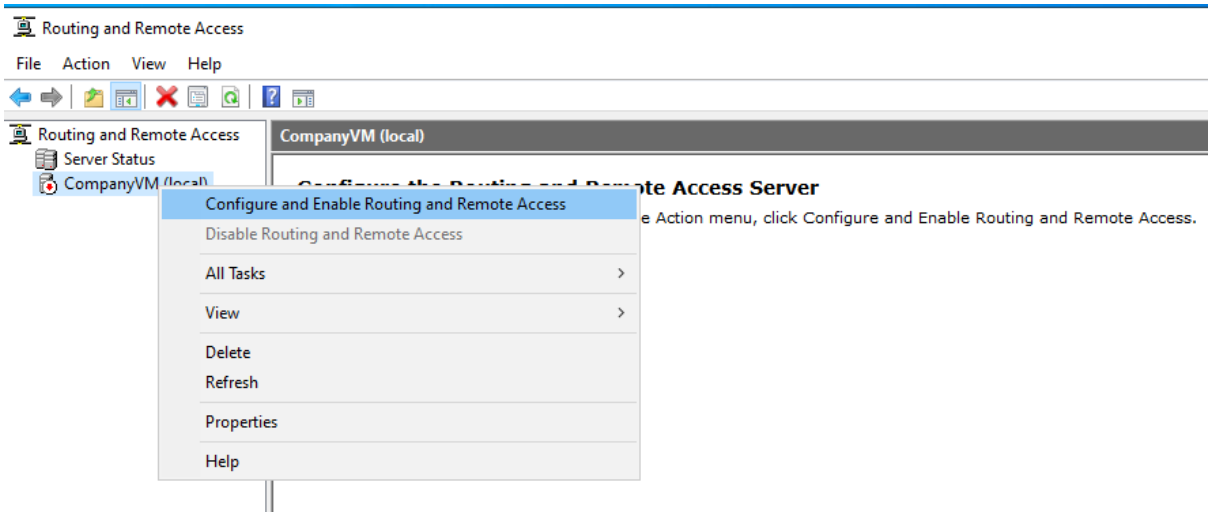
10. Once it is deployed, then you need to go back to your VM and you will see that the installation is also complete. You need to configure it now.



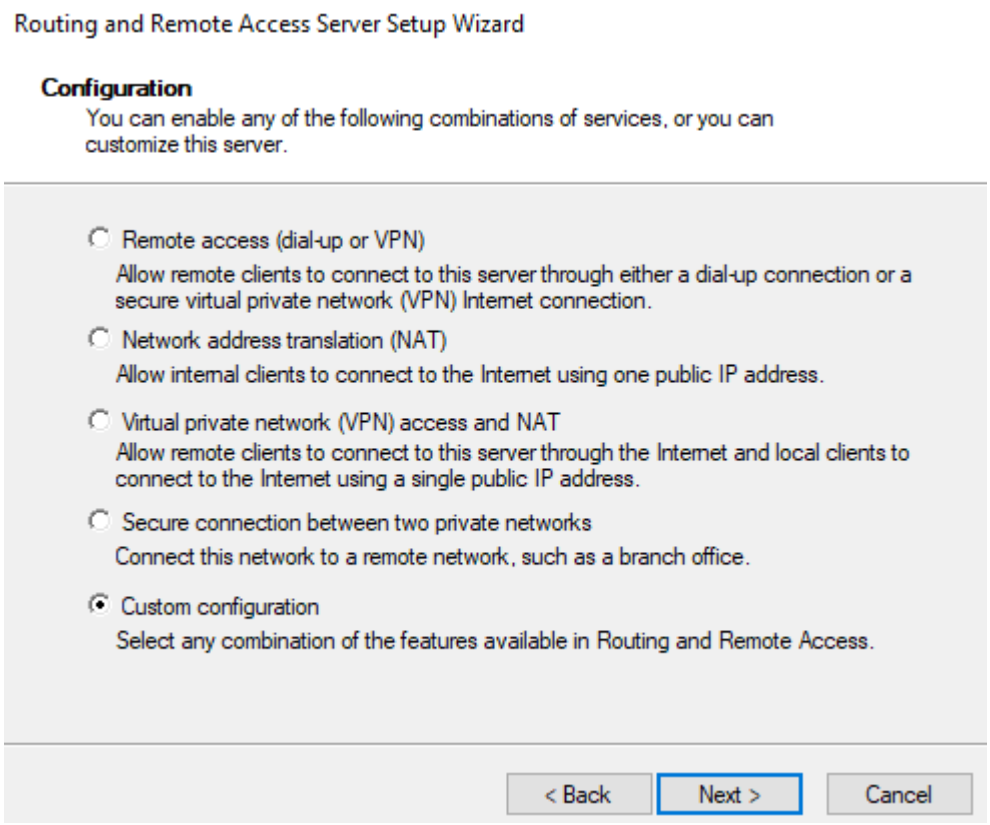
11. Then you have to choose deploy VPN only.



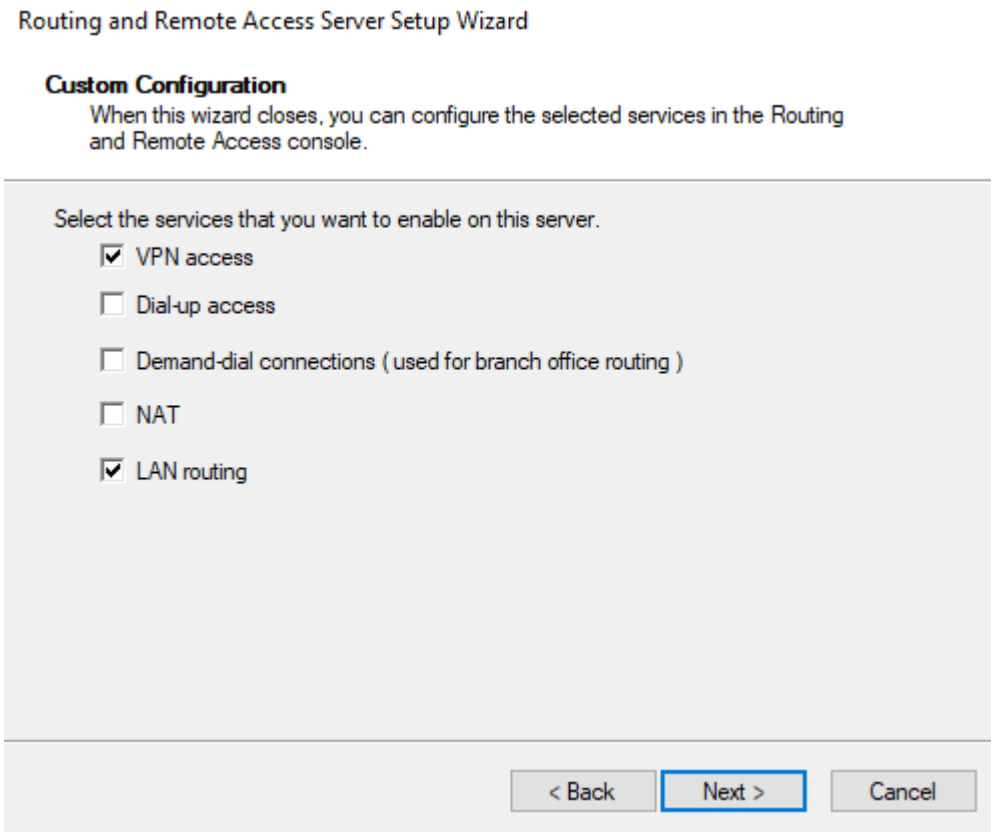
12. Now it will open up the wizard for routing and remote access, then choose company VM and right click on it then choose configure and enable.



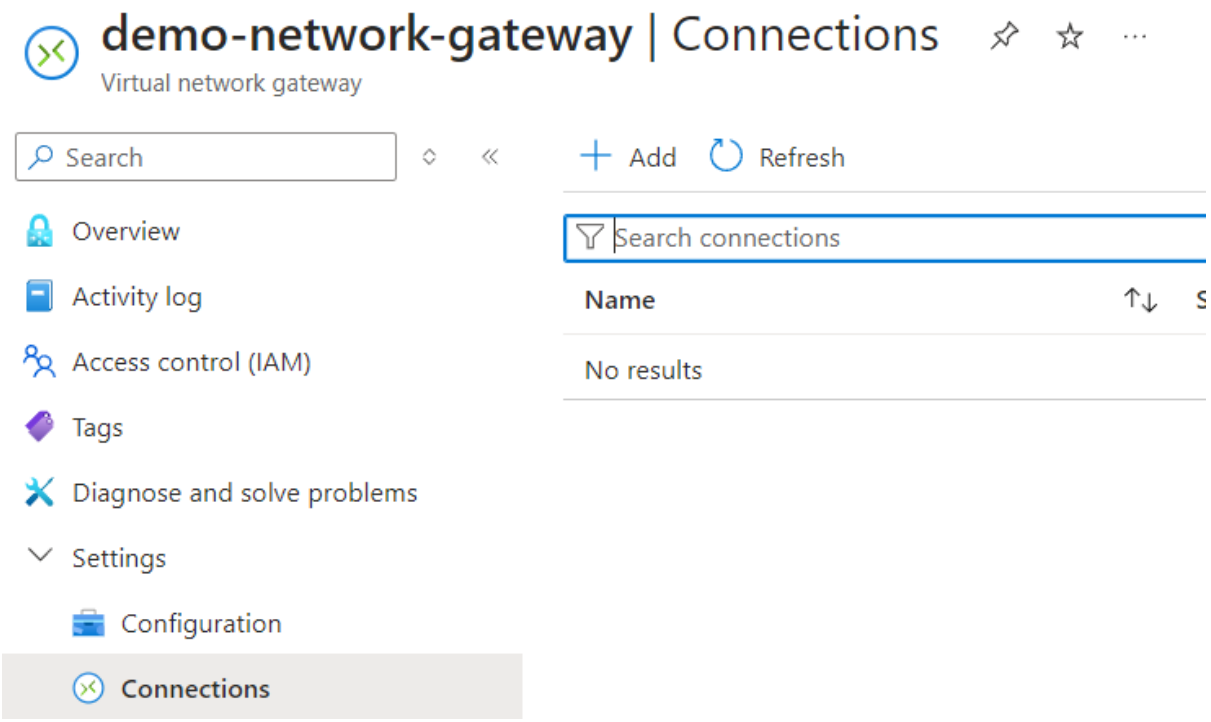
13. Then you have to choose custom configuration and click on next.



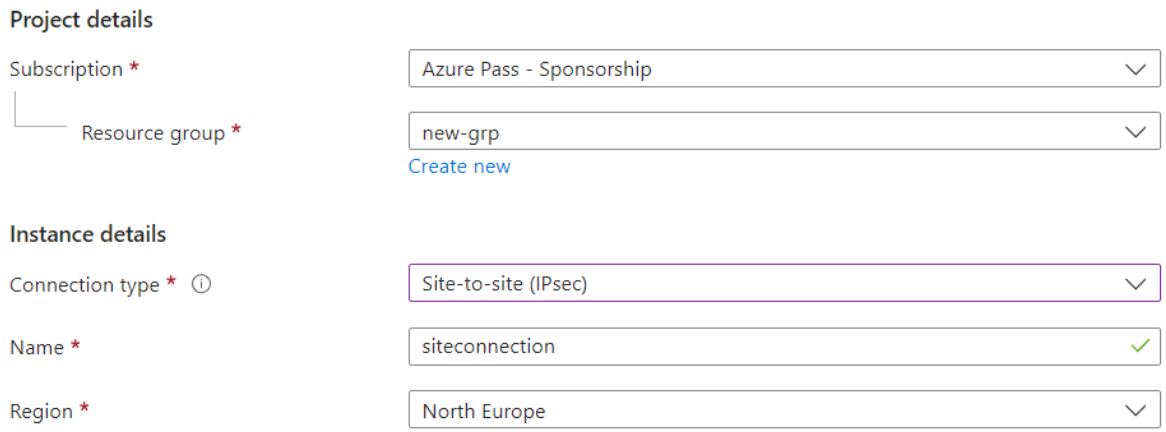
14. After that you have to choose VPN access and LAN routing. Then just finish up the process then you will get the pop up to start the service click on it.



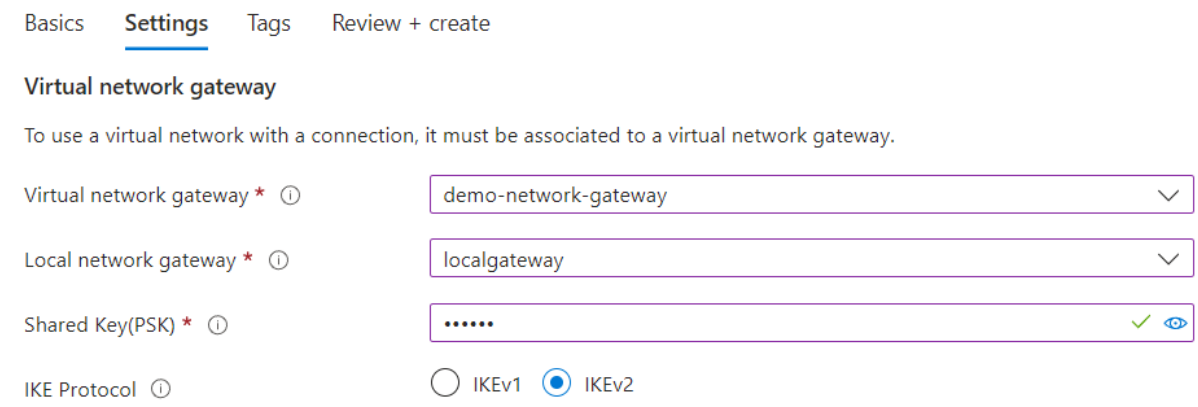
15. After that you need to go to Virtual network gateway and go to connection then click on add.



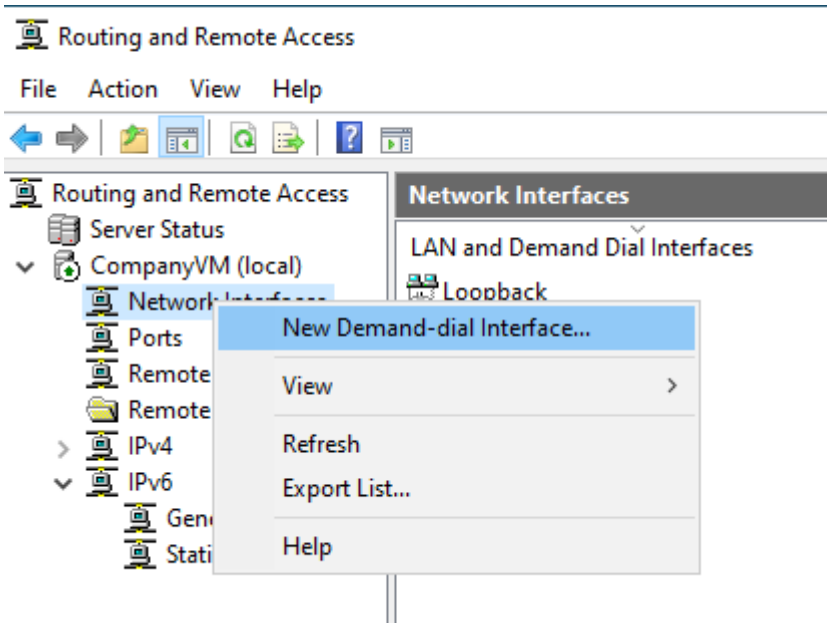
16. Then you need to choose your resource group and choose the connection type as shown below.



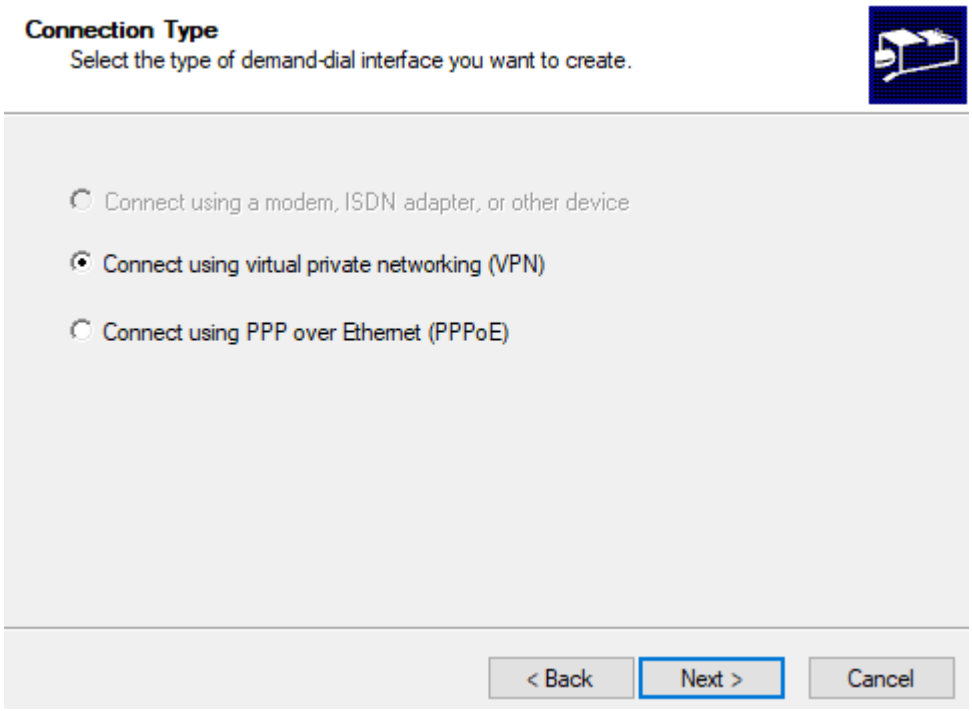
17. Now you need to choose your virtual network gateway and local network gateway. After that, you have to give the shared key, think of it like a password, and write down anything like abc123.

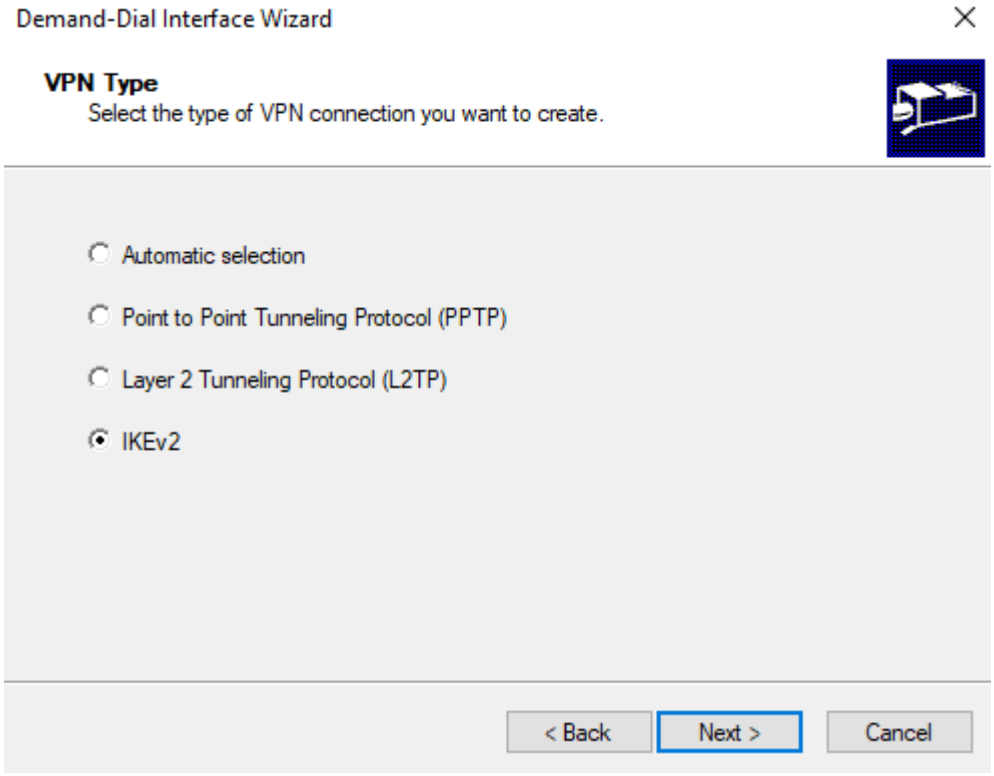


18. After that just move to the review page and create it.
19. Now on our company VM we need to tell how to connect to our virtual network gateway.
20. Then go to the network interface right-click on it and choose the new demand-dial interface.

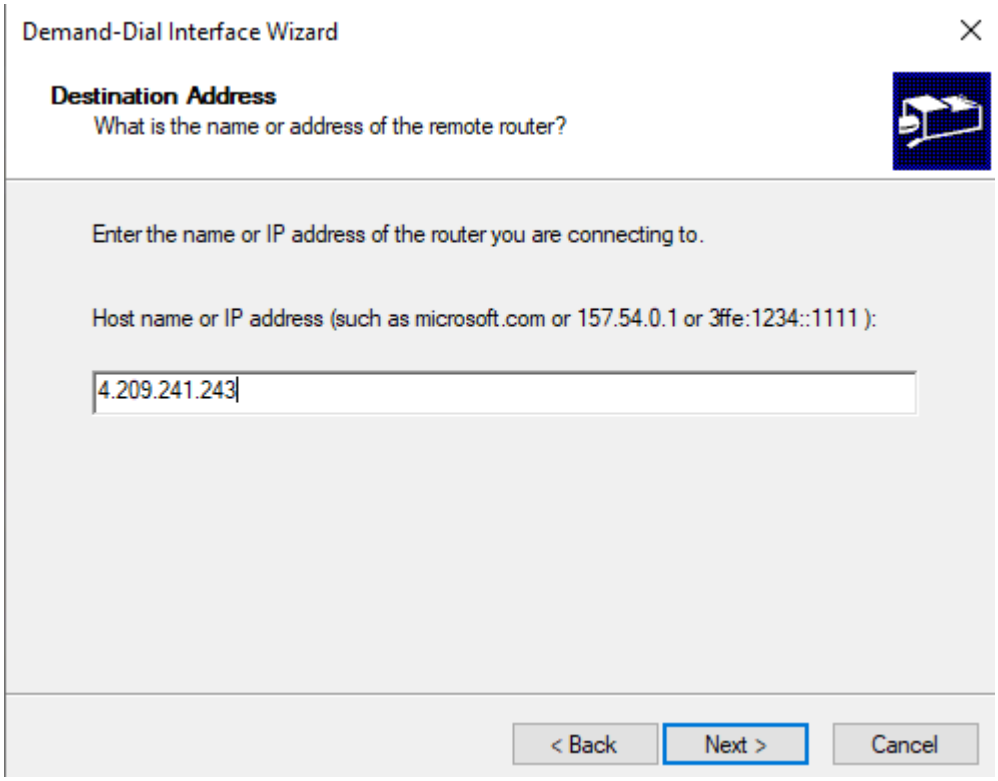


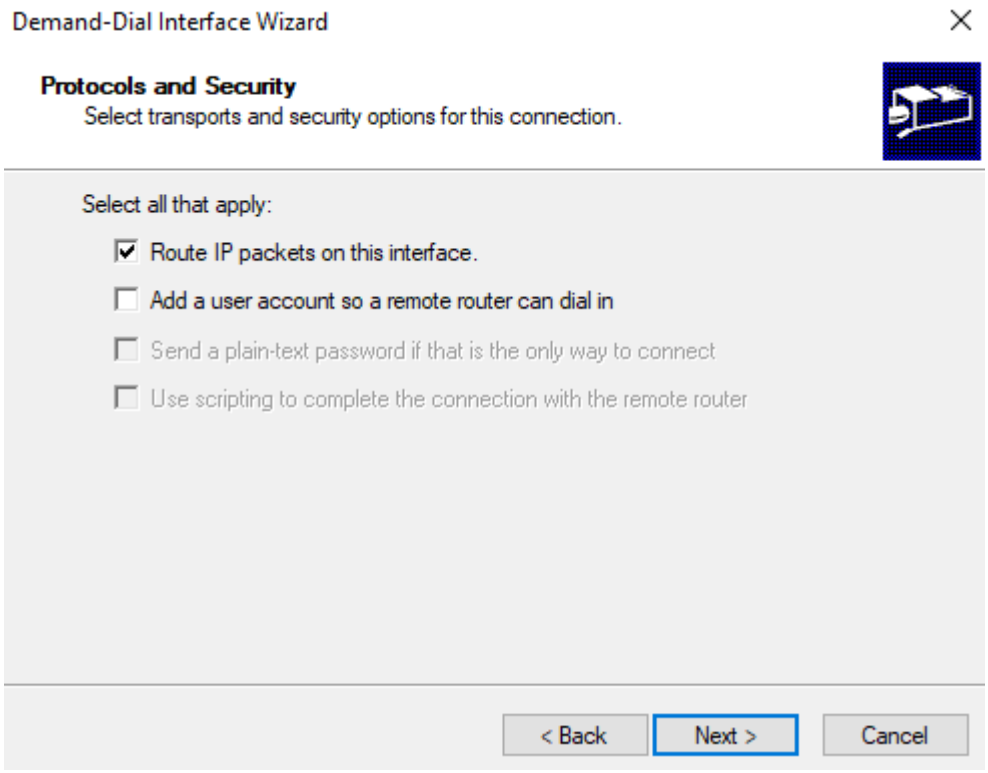
21. Now follow the snapshots to fill out the properties.



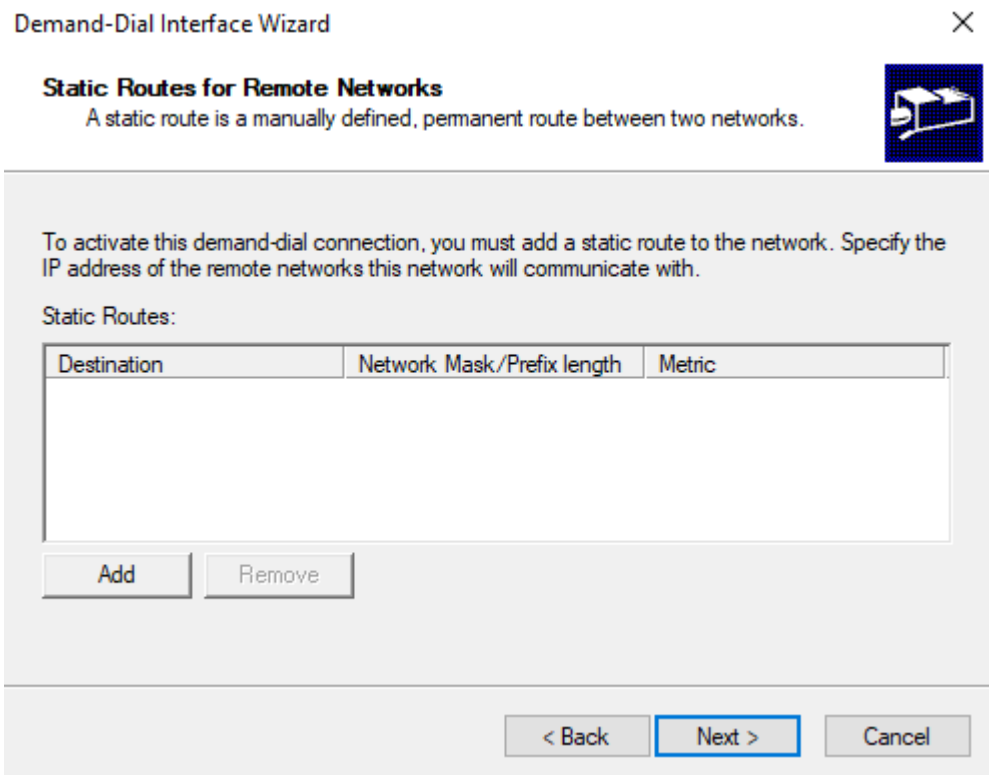


22. Here you need to write the IP address of your virtual network gateway.

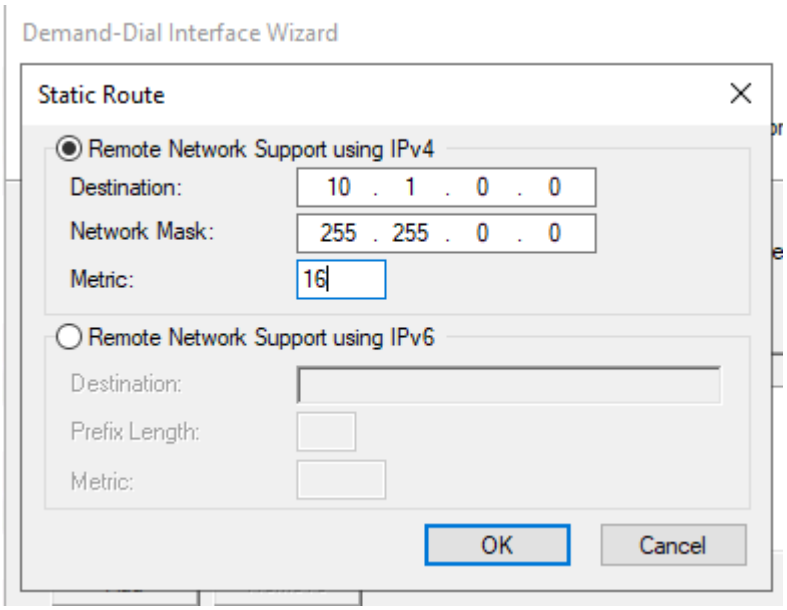




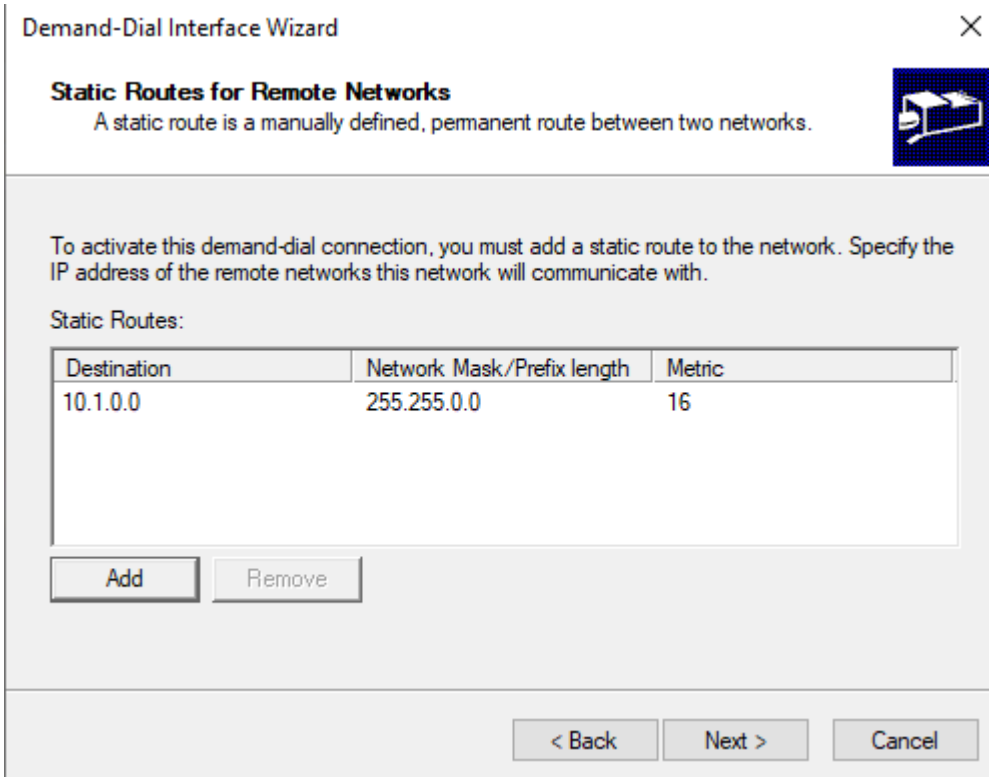
23. Now you need to click on add and the static route.



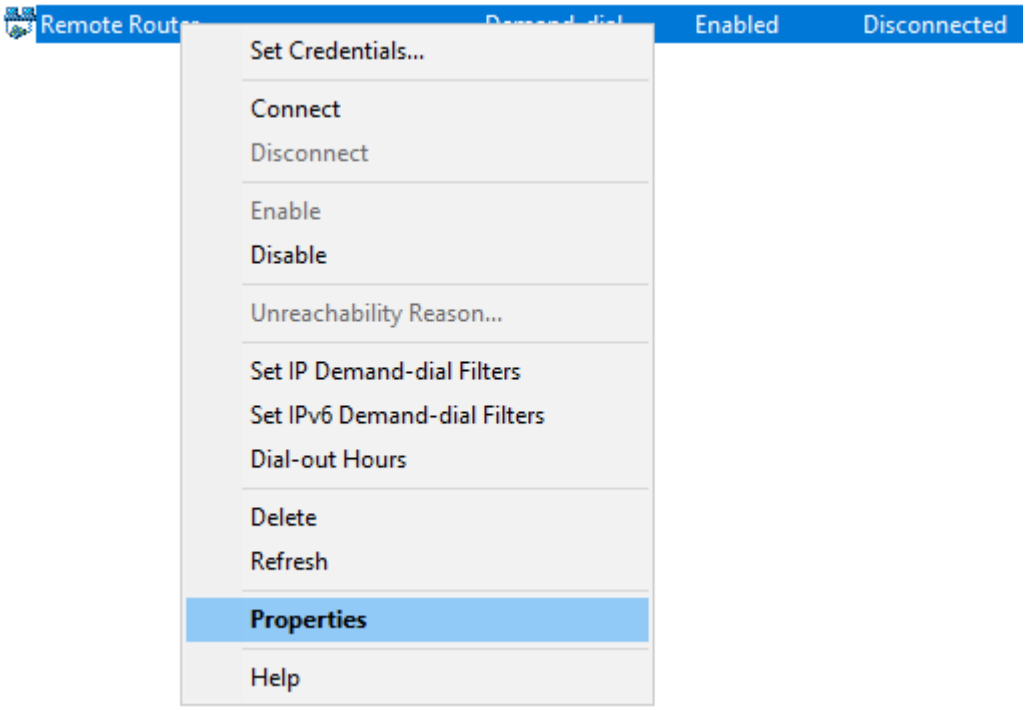
24. To add the static route, you need to go and see the address space of your demo VM because we want our traffic to route there. Then fill out the destination with a private IP address and the network is based /16.



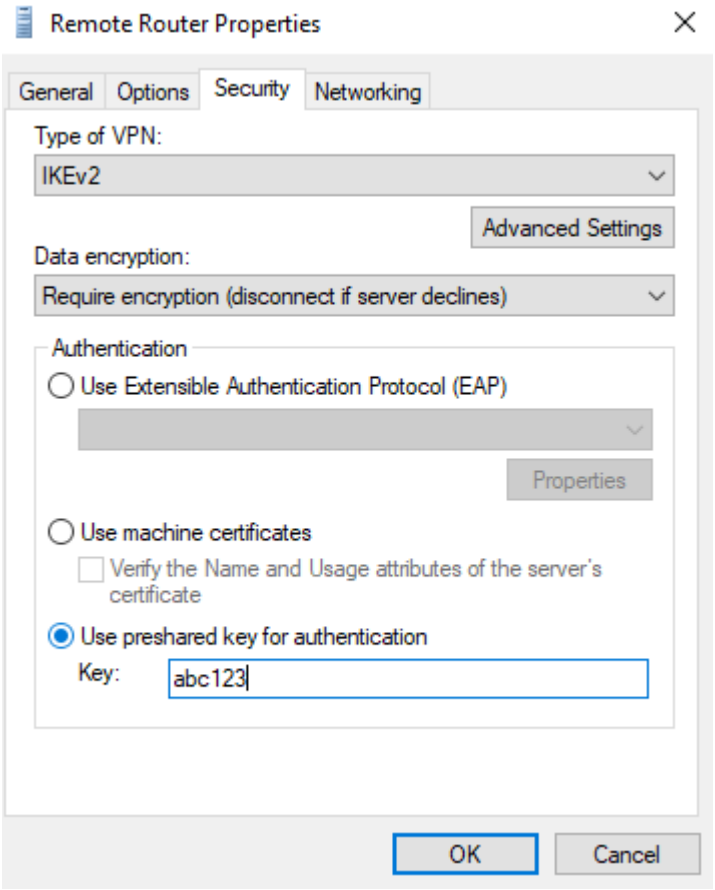
25. Below you can see that the static route has been added. After that just finish up the things.



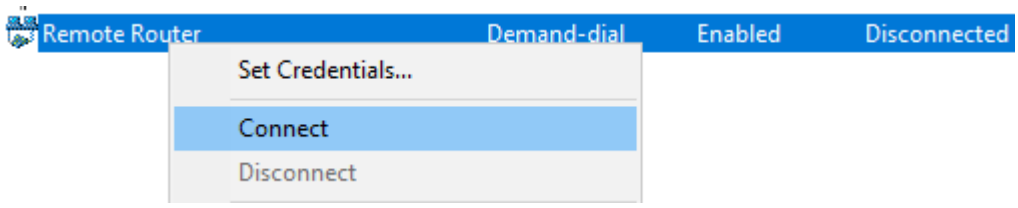
26. Then you need to right click on the demand-dial interface and choose properties.



27. Now you need to go to security and enter that pre-shared key for authentication, which we had entered when creating the site-to-site connection for a virtual network gateway.



28. Now again right click on the remote router and click on connect.



29. Now you need to open the Edge browser and paste the Private IP address of your Demo VM and you will see the web page as expected from your company VM.