Step-by-Step Setup: Configuring a Point-to-Site (P2S) VPN Connection from Your PC to Azure

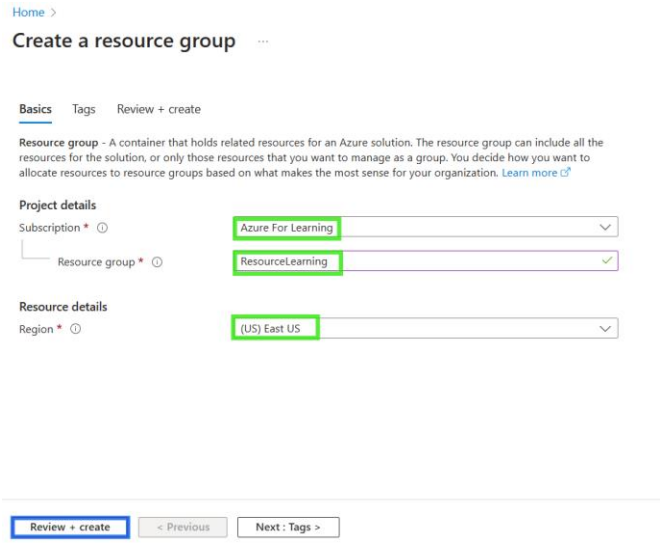
A **Point-to-Site** (P2S) **Virtual Private Network** (VPN) is a secure connection that allows an individual device (like a laptop or PC) to connect to a remote cloud network, such as an Azure Virtual Network (VNet), over the internet. Unlike a Site-to-Site (S2S) VPN, which connects entire networks, a P2S VPN connects individual devices to the network. This makes it ideal for remote workers or anyone needing secure access to resources in a cloud environment like Azure. It offers key features like **secure remote access**, **cost efficiency**, **scalability**, and **enhanced security** for connecting individual devices to cloud resources.

Step 1: Create a Subscription

1.1 Log in to Azure portal (portal.azure.com)
1.2 Navigate to *Subscription*
1.3 Click on *Create* to create a new subscription and provide the name of the subscription
1.4 Follow on-screen instructions to set up the subscription

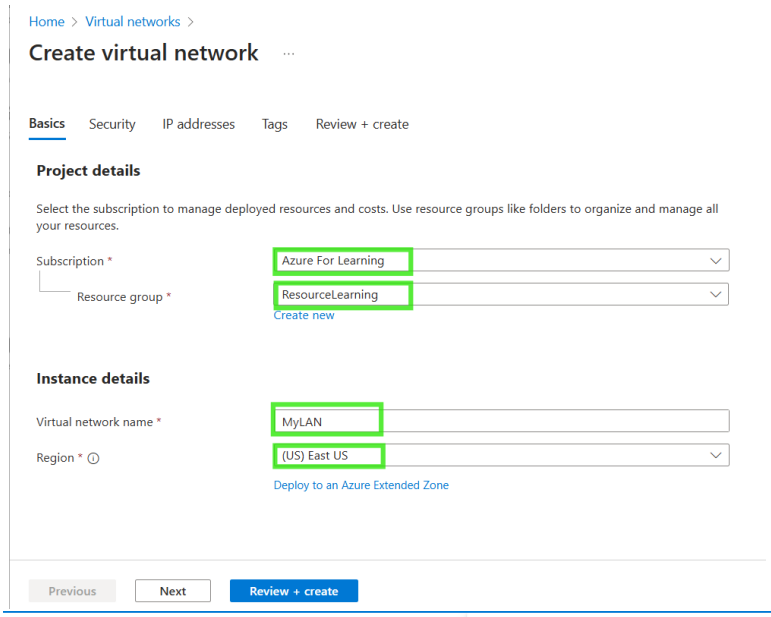
Step 2: Create a Resource group

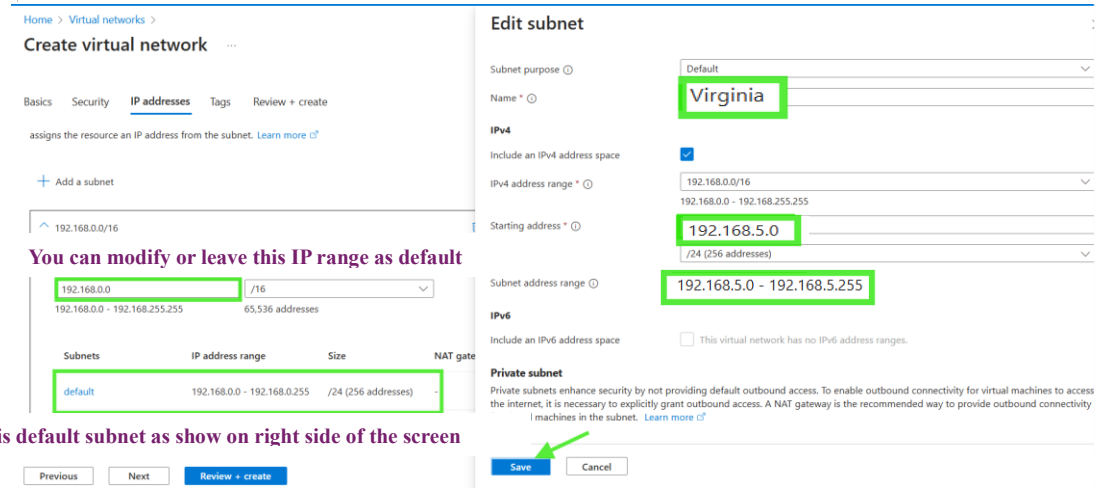
2.1 Navigate to *Resource group*
2.2 Click on *Create* and provide the name of the resource group
2.3 Select the subscription you have created earlier
2.4 Select the region for the resource group
2.5 Click on *Review + create* and then *Create* for the completion



Step 3: Create a Virtual Network

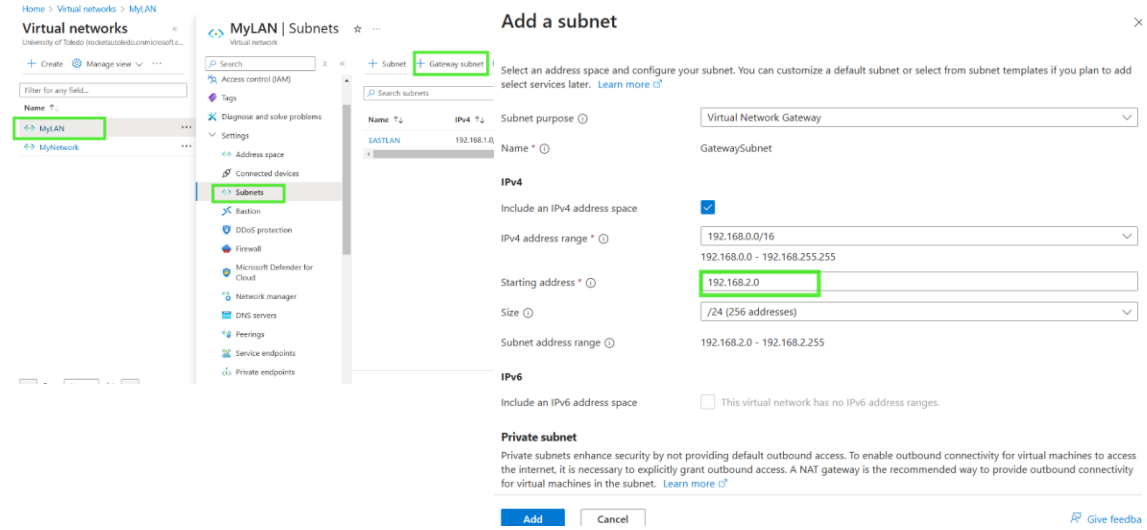
3.1 Navigate to *Virtual network* in azure portal
3.2 Click *Create* to create a new virtual network
3.3 Select the subscription
3.4 Select resource group and location for virtual network
3.4 Provide a name for the virtual
3.5 Define the IP address space for the virtual network
3.6 Edit the default subnet, modify its IP range, name the subnet and save
3.7 Click *Review + create* and then *Create* to create the virtual network

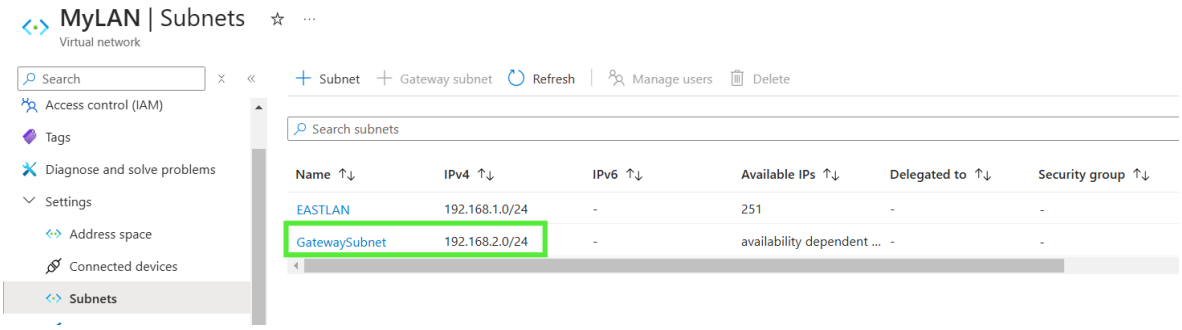




Step 4: Create the gateway subnet

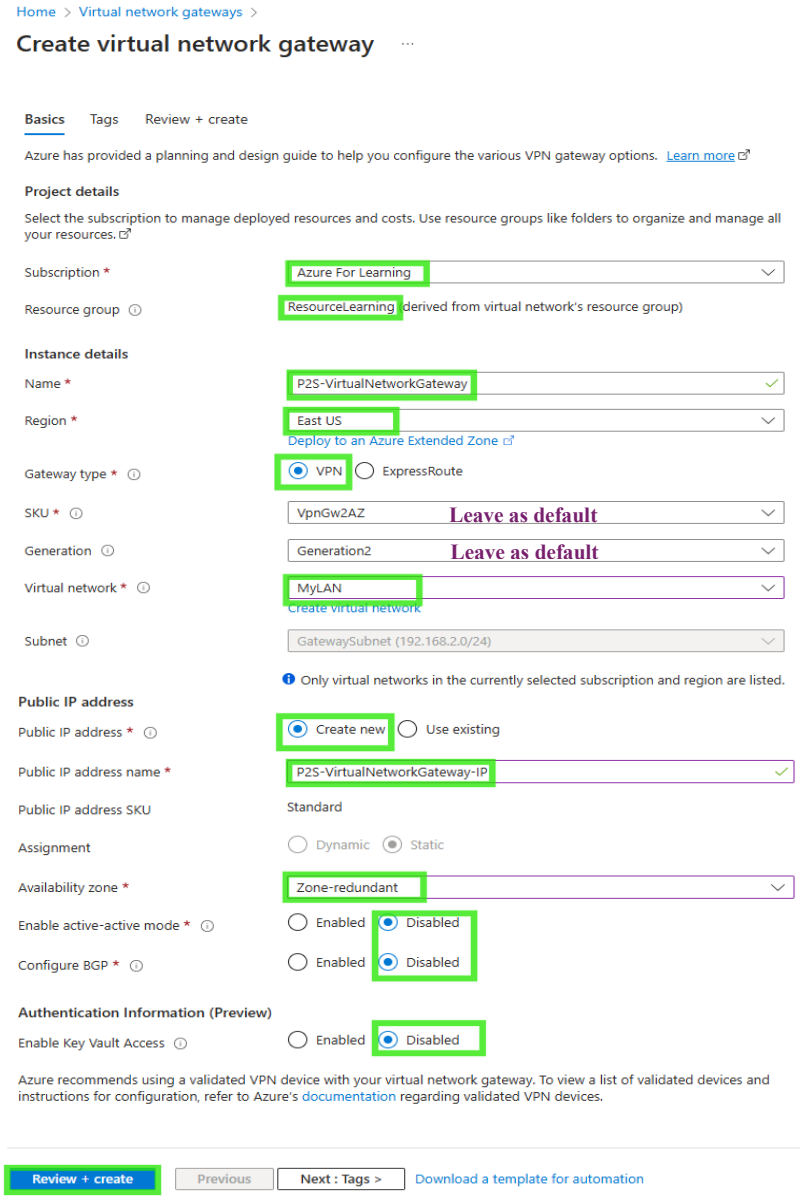
4.1 Navigate to the setting of Virtual network (e.g., MyLAN)
4.2 Click on + *Gateway subnet*
4.3 You can name it or leave as default (e.g., GatewaySubnet)
4.4 Define the IP range within the IP range of Virtual Network
4.5 Click on *Add* to save the gateway subnet





Step 5: Create a Virtual Network Gateway

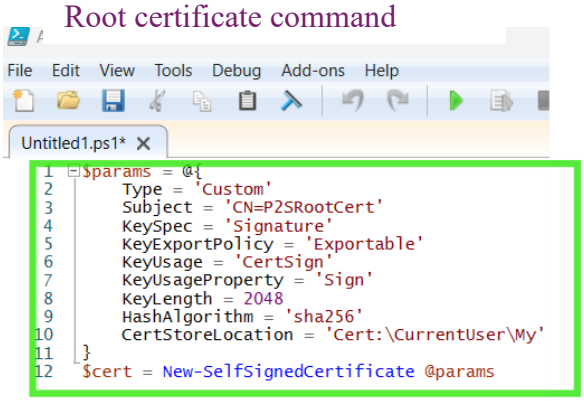
5.1 Navigate *Virtual network gateway* in Azure portal
5.2 Click *Create* to add a new virtual network gateway
5.3 Provide necessary details such as subscription, resource group, etc.
5.4 Select VPN type, SKU, and virtual network as shown below
5.5 Select the same resource group as created earlier
5.6 Click *Review + create* and wait for the deployment to be completed



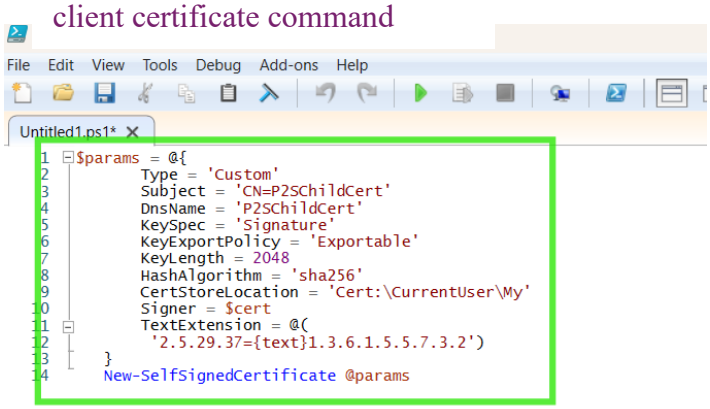
Step 6: Create a self-signed root certificate

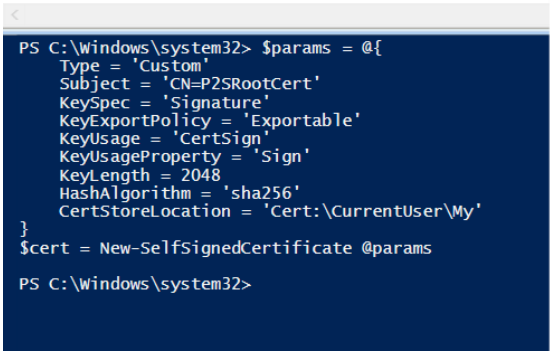
6.1 Click on this link for all details: https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site
6.2 Open PowerShell in your PC or laptop
6.3 Copy the commands from the link above and run for root and client certificates
6.4 Run the command *certmgr* in PowerShell to open the Mange user certificates window
6.5 Export the root certificate to download folder in your PC follow the screenshots shown below

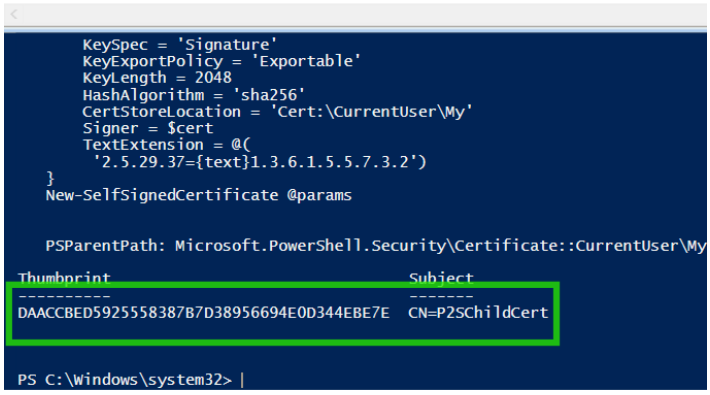
Root certificate command

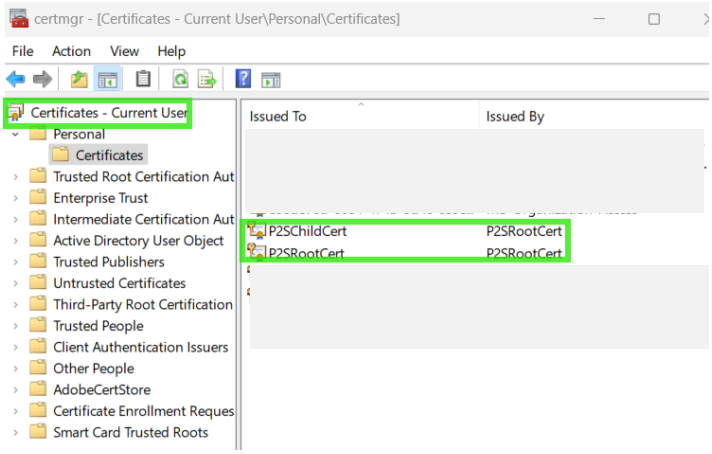


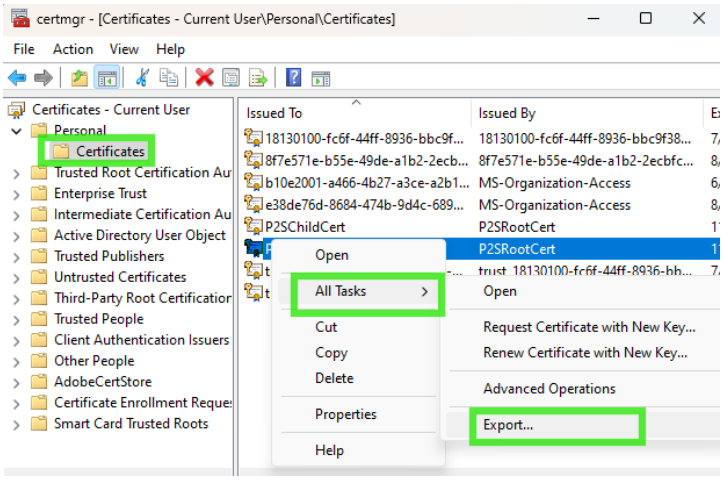
client certificate command

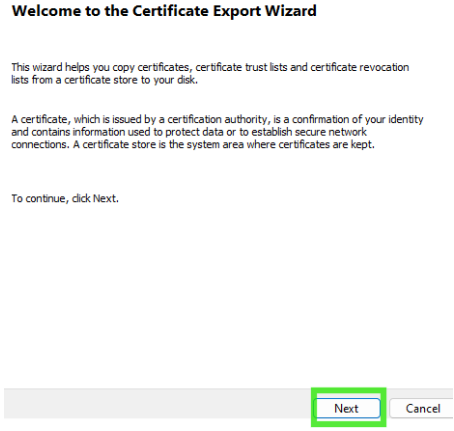


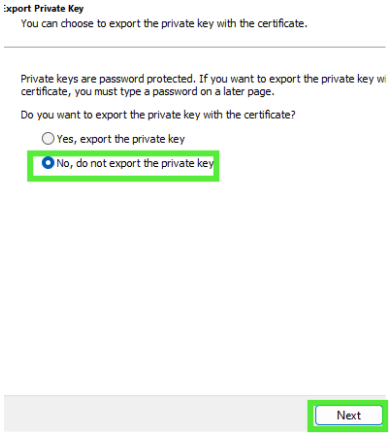


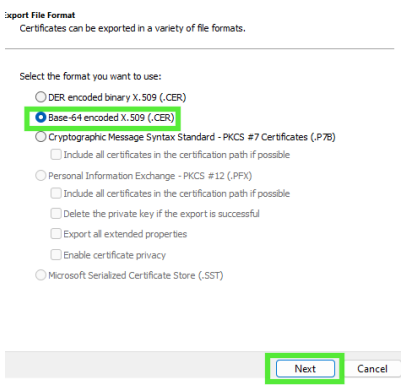


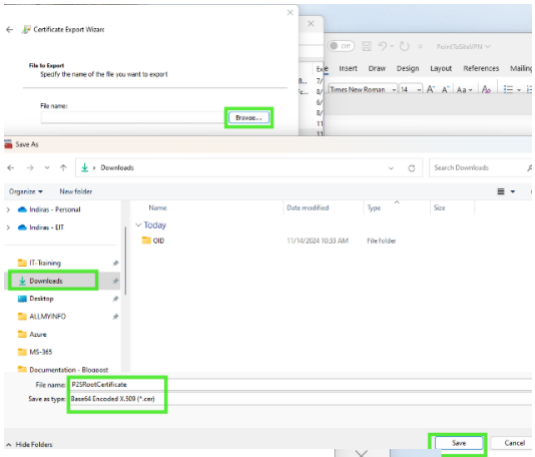


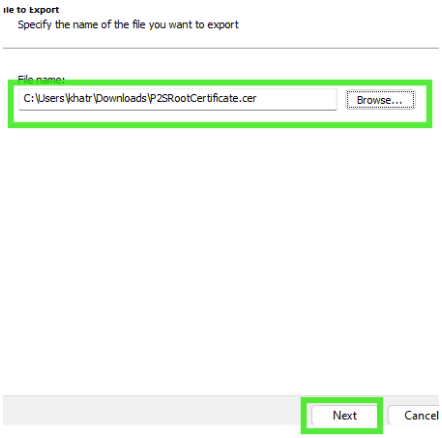

certmgr - [Certificates - Current User\Personal\Certificates]
File Action View Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
Other People
AdobeCertStore
Certificate Enrollment Reque
Smart Card Trusted Roots
Issued To
Issued By
18130100-fc6f-44ff-8936-bbc9f...
8f7e571e-b55e-49de-a1b2-2ecb...
b10e2001-a466-4b27-a3ce-a2b1...
e38de76d-8684-474b-9d4c-689...
P2SChildCert
P2SRootCert
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Advanced Operations
Export...

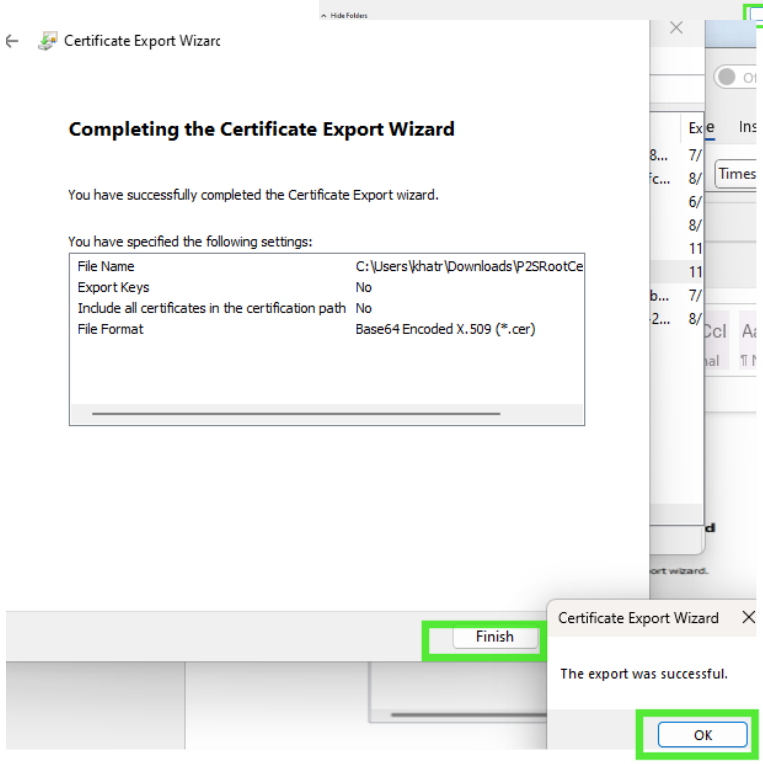

Welcome to the Certificate Export Wizard
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
Next
Cancel


Export Private Key
You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key wi certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
Yes, export the private key
No, do not export the private key
Next

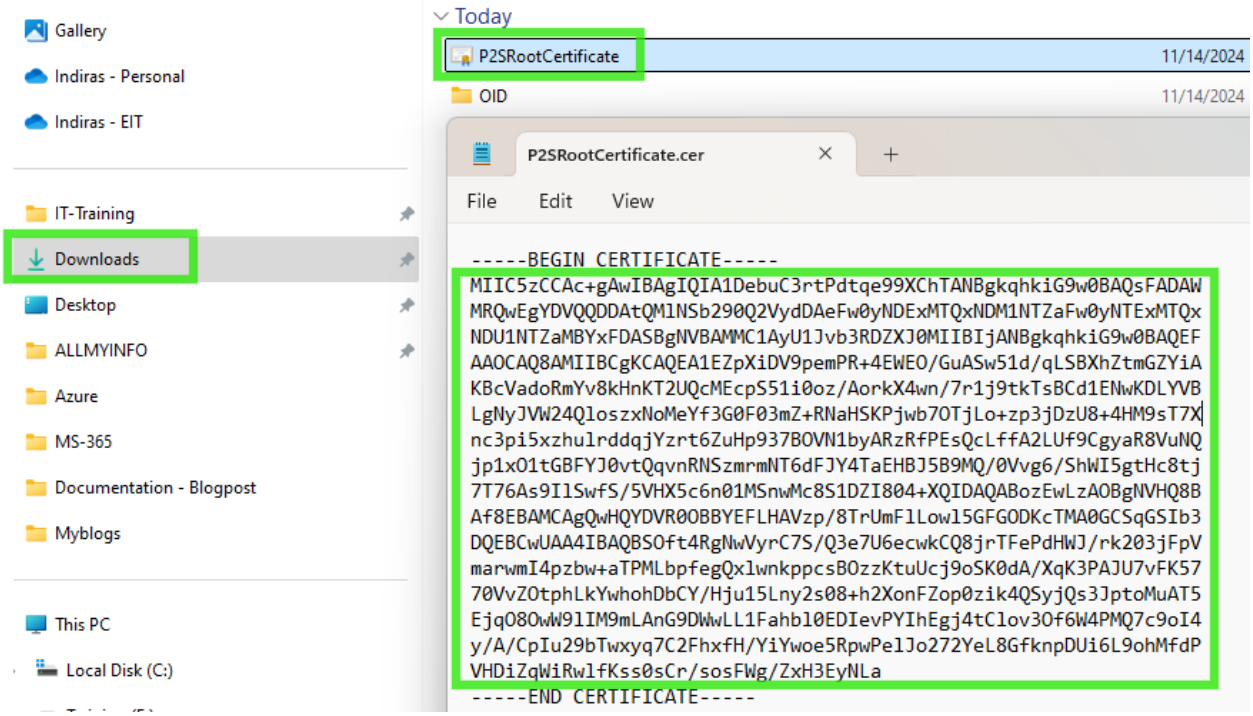

Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Delete the private key if the export is successful
Export all extended properties
Enable certificate privacy
Microsoft Serialized Certificate Store (.SST)
Next
Cancel


Certificate Export Wizard
Save As
Downloads
Today
IT-Training
Downloads
Desktop
Azure
MS-365
File name: P2SRootCertificate
Save as type: Base64 Encoded X.509 (*.cer)
Hide Folders
Save
Cancel


File to Export
Specify the name of the file you want to export
File name:
C:\Users\khatr\Downloads\P2SRootCertificate.cer
Browse...
Next
Cancel

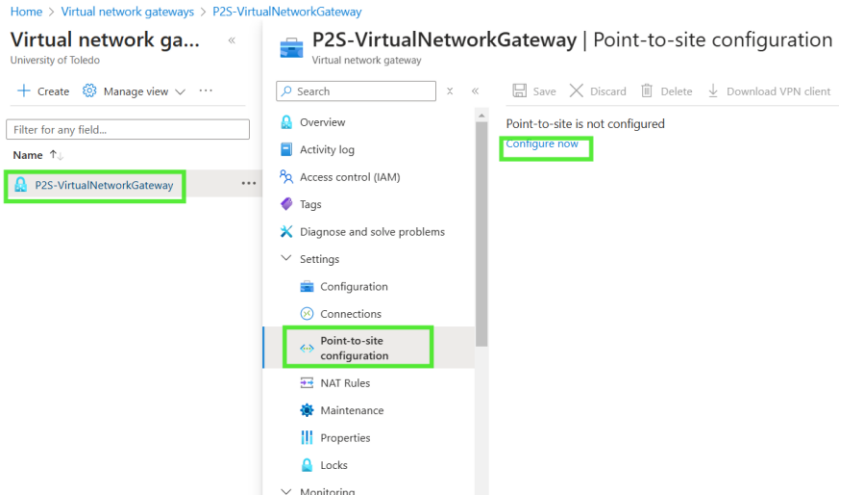

Certificate Export Wizard
Completing the Certificate Export Wizard
You have successfully completed the Certificate Export wizard.
You have specified the following settings:
File Name C:\Users\khatr\Downloads\P2SRootCe
Export Keys No
Include all certificates in the certification path No
File Format Base64 Encoded X.509 (*.cer)
Finish
Certificate Export Wizard
The export was successful.
OK

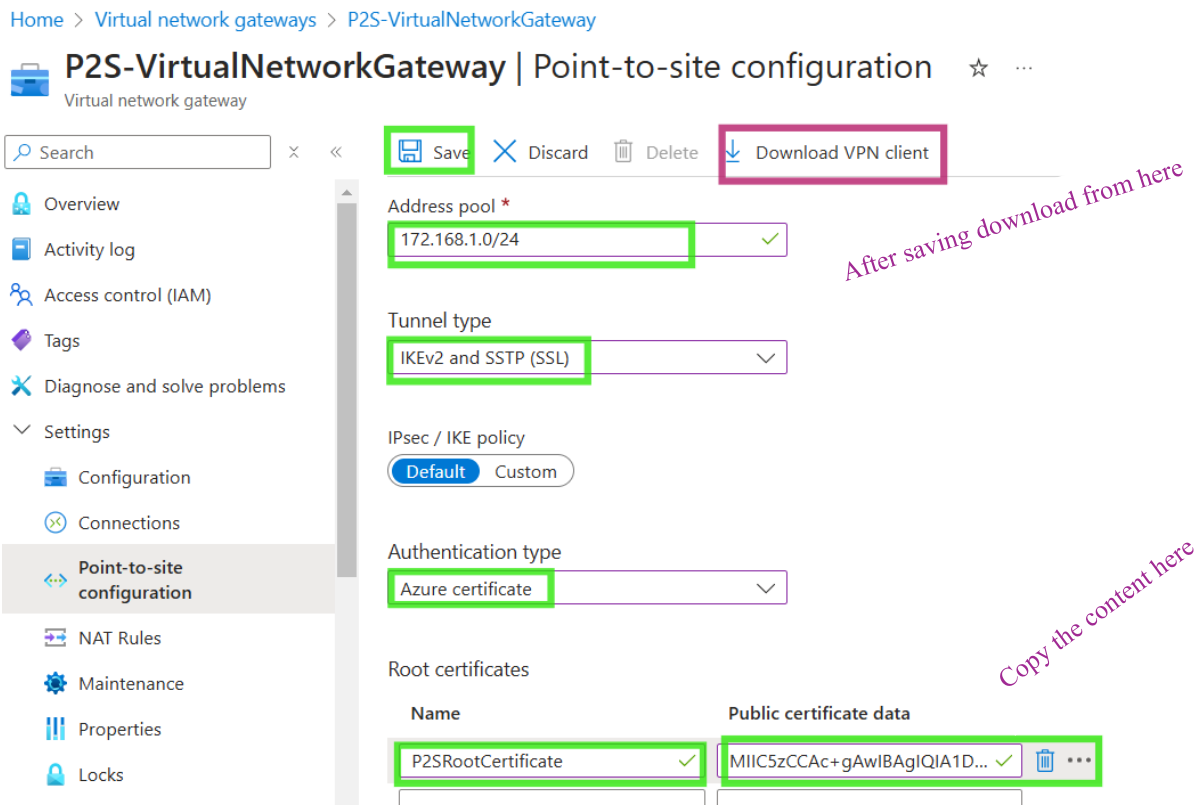
6.6 Open the file P2SRootCertificate from downloads folder and copy it



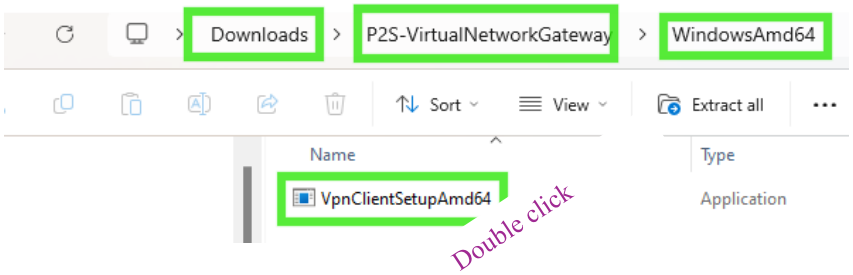
Step 7: Configuration of Virtual Network Gateway

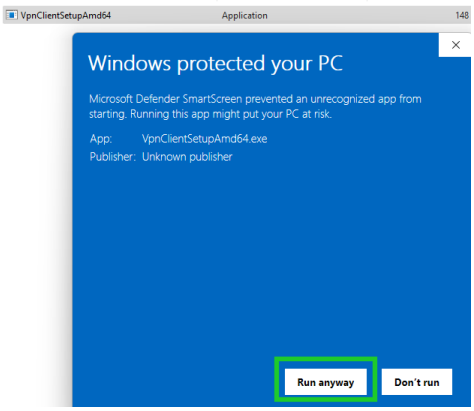
7.1 After the deployment completion go to the virtual network gateway configuration page
7.2 Click on previously created virtual network gateway (e.g., P2S-VirtualNetworkGateway)
7.3 In setting click on Point-to-site configuration and then click on *Configure now*
7.4 Assign non-overlapping address pool with virtual network IP (client will get IP from this)
7.5 Select all requirements such as tunnel, Authentication type, etc.
7.6 Copy the content of root certificate (shown in step 6) to public certificate data and save
7.7 After saving the configuration, download from *Download VPN client*

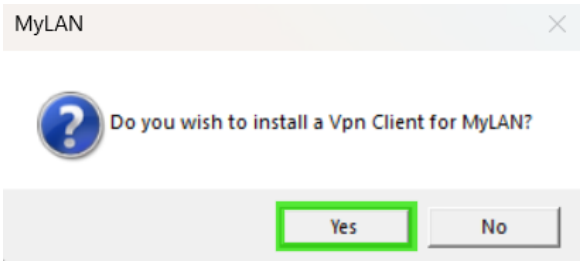




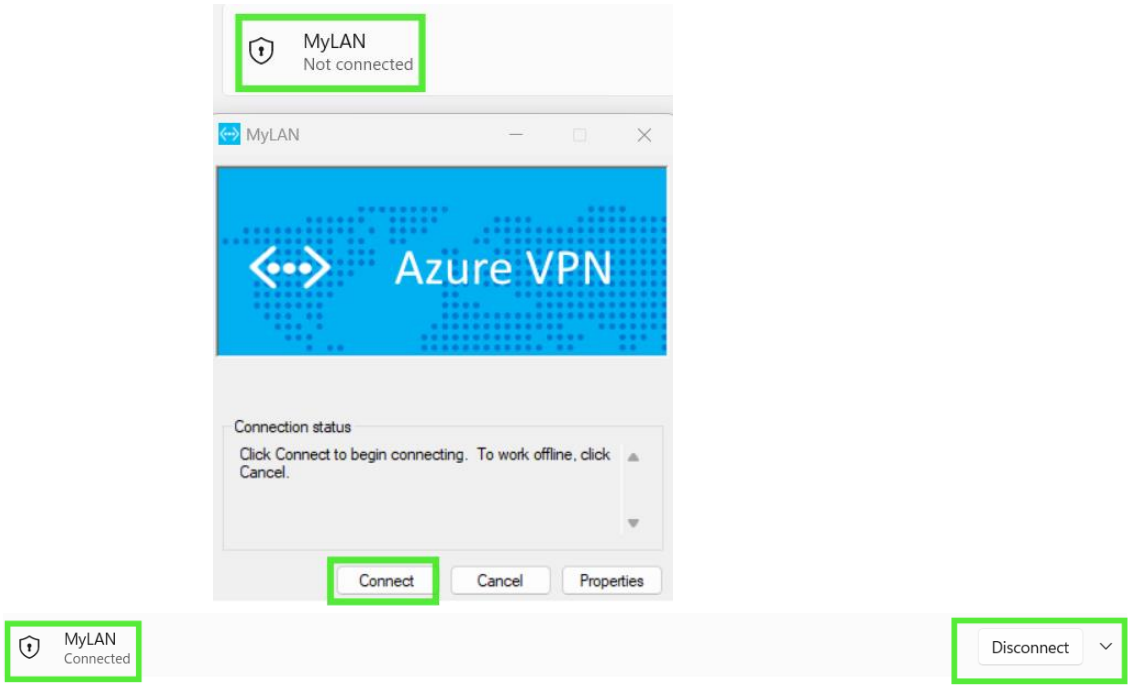
7.8 Run the file *VpnClientSetupAmd64* from the downloaded folder and install it





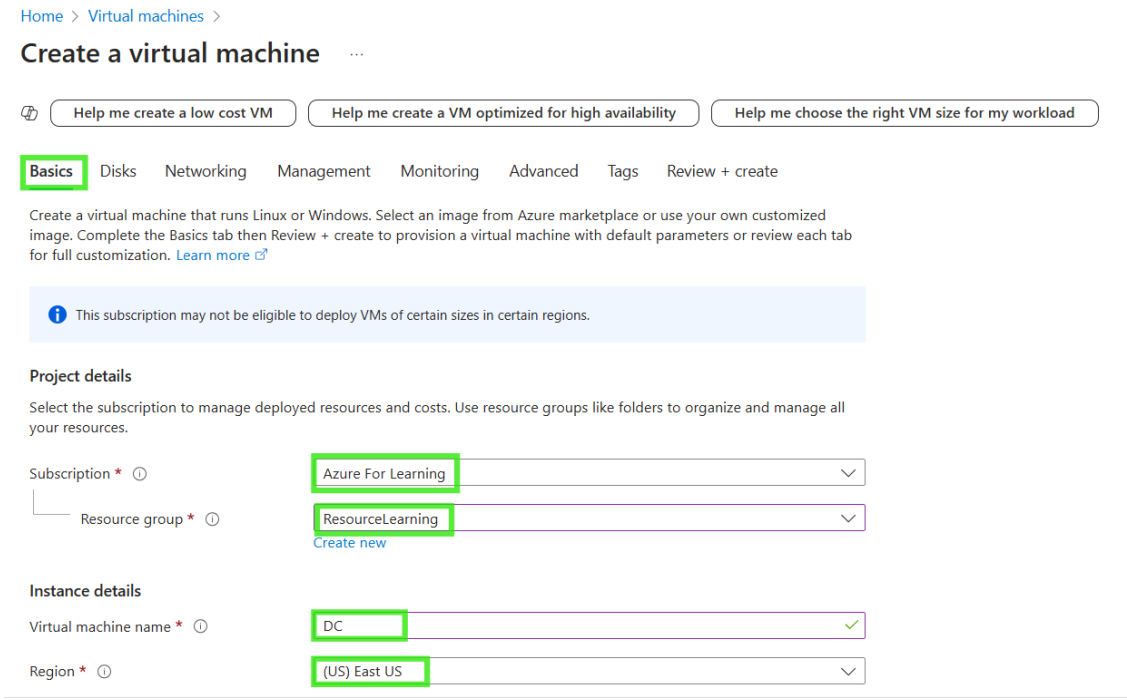


7.9 After the installation connect to the VPN (e.g., MyLAN)



Step 8: Create a Virtual Machine

8.1 Navigate to *Virtual machines* and click on *Create* to add a virtual machine
8.2 Fill out all the required details (e.g., Window Server 2022, etc.)
8.3 Click *Review + create* to create a new virtual machine



Availability options: No infrastructure redundancy required

Security type: Trusted launch virtual machines

Configure security features

Image *: Windows Server 2022 Datacenter: Azure Edition Hotpatch - x64 Gen2 (free

See all images | Configure VM generation

VM architecture: Arm64 / x64

Arm64 is not supported with the selected image.

Run with Azure Spot discount

You are in the free trial period. Costs associated with this VM can be covered by any remaining credits on your subscription.
Learn more

Size *: Standard_DC1s_v3 - 1 vcpu, 8 GiB memory ($103.66/month)

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 *: ikhatri

Password *: ••••••••••••••

Confirm password *: ••••••••••••••

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports *: None / Allow selected ports

Select inbound ports *: RDP (3389)

All traffic from the internet will be blocked by default. You will be able to

< Previous | Next : Disks > | Review + create

OS disk

OS disk size: Image default (127 GiB)

OS disk type *: Premium SSD (locally-redundant storage)

Delete with VM: ☑

Key management: Platform-managed key

Enable Ultra Disk compatibility: ☐

Ultra disk is supported in Availability Zone(s) 2 for the selected VM size Standard_DC1s_v3.

Data disks for DC

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM

Create and attach a new disk Attach an existing disk

Advanced

< Previous Next : Networking > Review + create

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

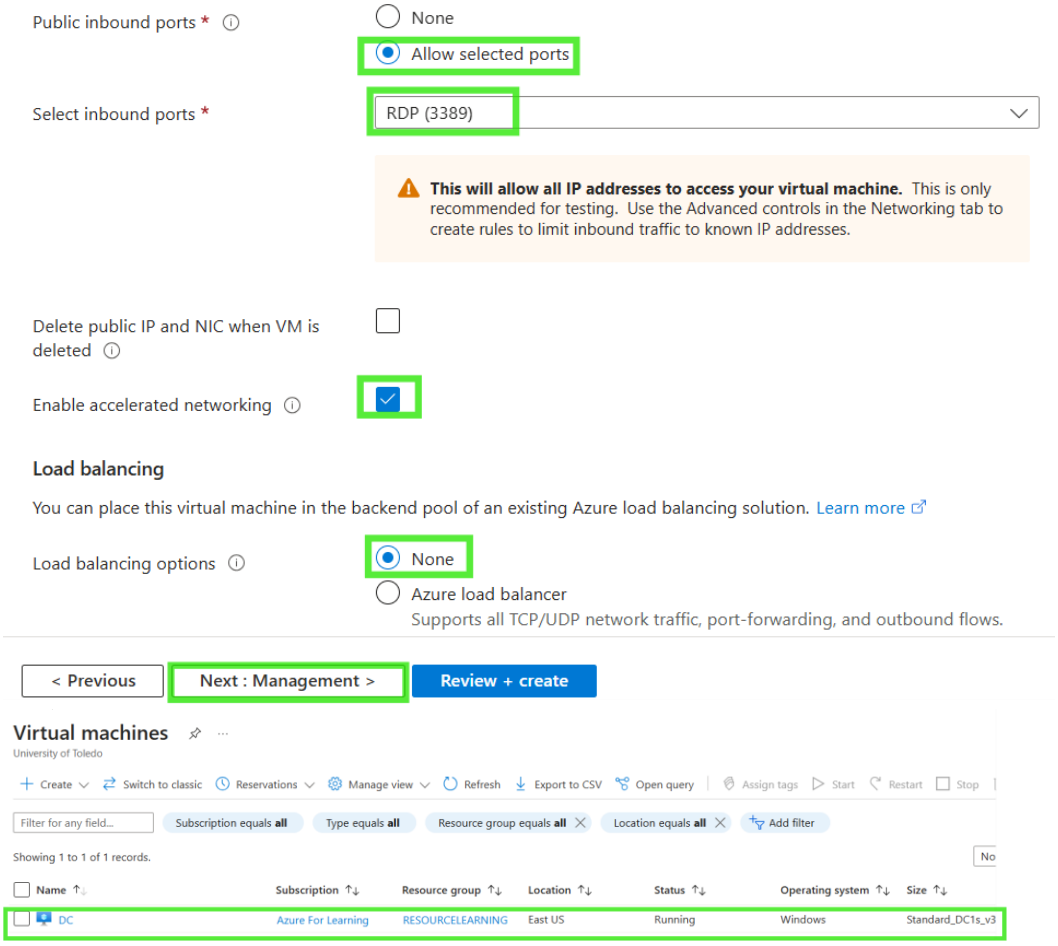
When creating a virtual machine, a network interface will be created for you.

Virtual network *: MyLAN
Create new

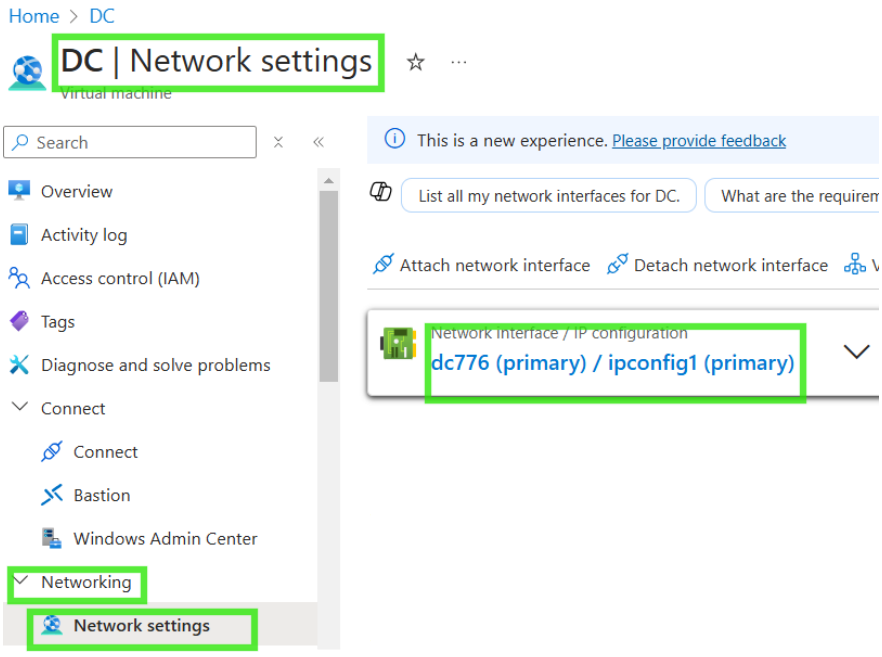
Subnet *: Virginia (192.168.5.0/24)
Manage subnet configuration

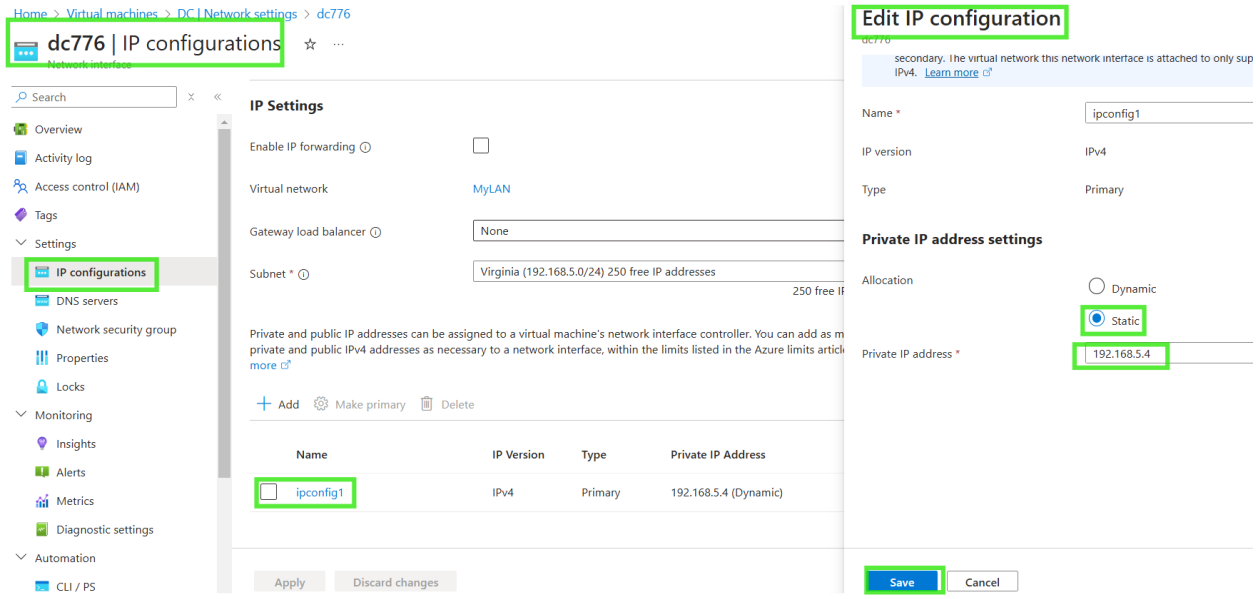
Public IP: (new) DC-ip
Create new

NIC network security group:
- ○ None
- ◉ Basic
- ○ Advanced



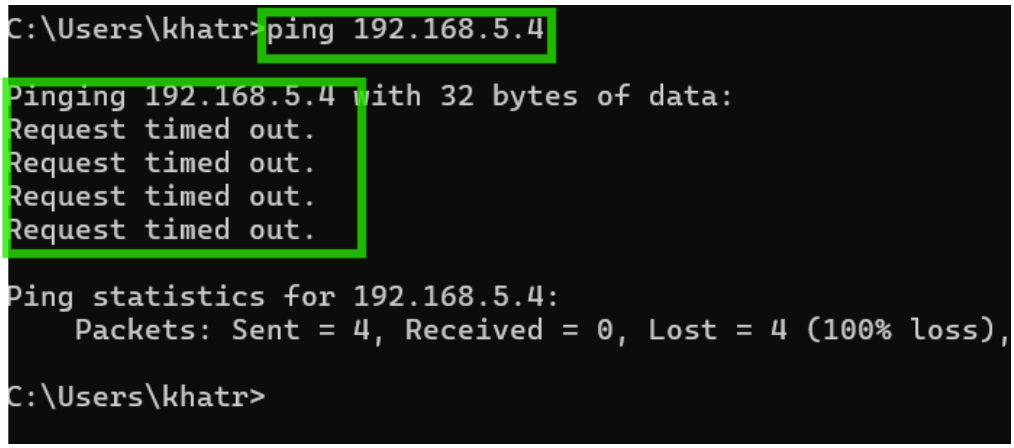
8.4 Change the private IP address from dynamic to static by clicking *ipconfig 1*



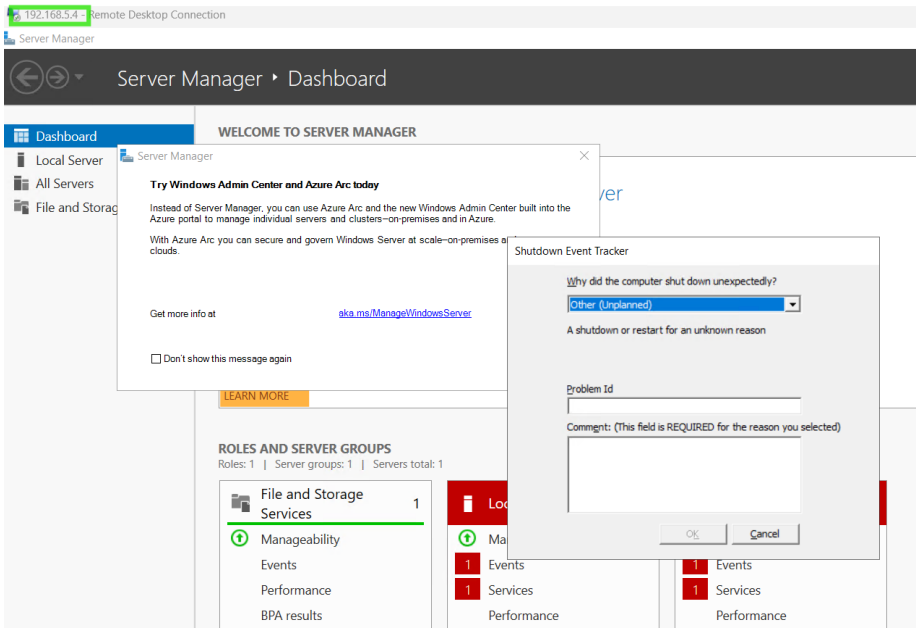


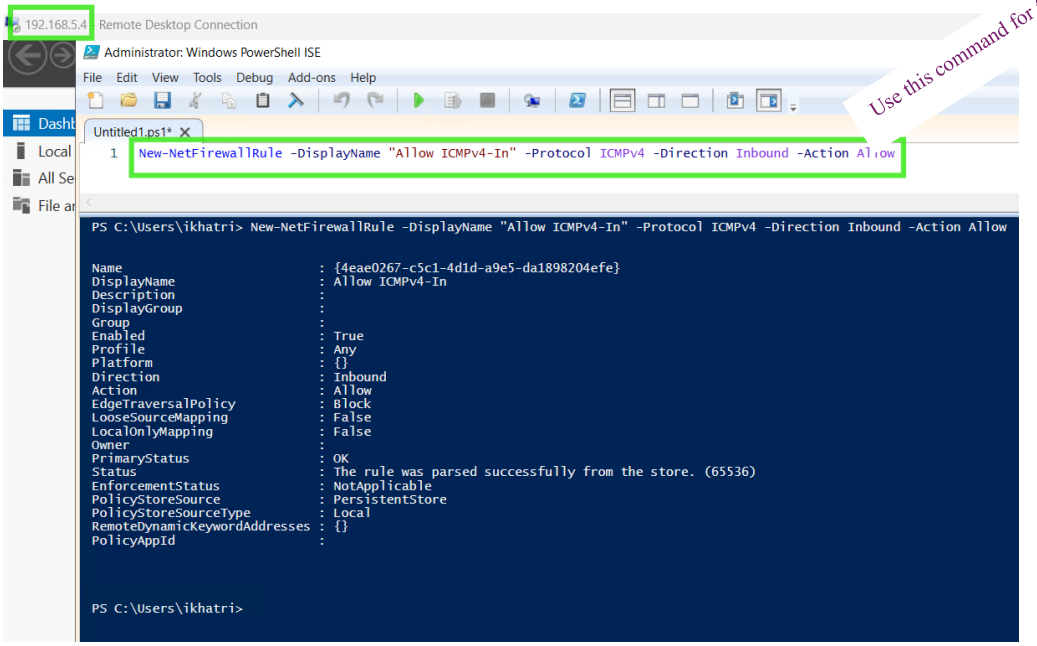
Step 9: Testing the connection

9.1 Open the command prompt in your PC and ping to private IP address of VM

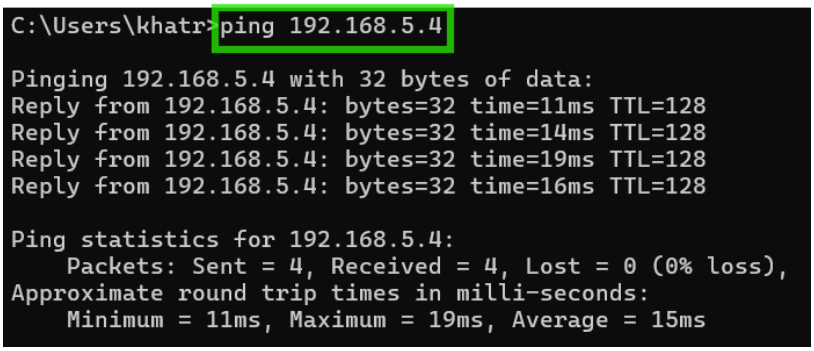


9.2 Create the inbound firewall rule in VM using following steps and command
9.3 Establish a Remote Desktop Connection from your PC to the VM
9.4 Execute the following command in PowerShell on the VM to create firewall rule
9.5 Open the command prompt on your PC again and ping the private IP address of VM





Use this command for firewall inbound rule



Conclusions

A Point-to-Site VPN connection to Azure provides secure, remote access for individual devices to an Azure Virtual Network, enabling users to connect to cloud resources as if they were on a local network. It's a simple, cost-effective solution for remote workers or small teams needing secure access to Azure resources.

Note

1. For optimal results, it's usually best to keep your VM and VPN gateway in the same region, reducing latency and avoiding cross-region data transfer fees.
2. Proper configuration of address spaces, security rules, and firewall settings will ensure a seamless and secure remote connection to your Azure environment.

Thank you for reading. I hope it was useful

Author: Indiras Khatri

****