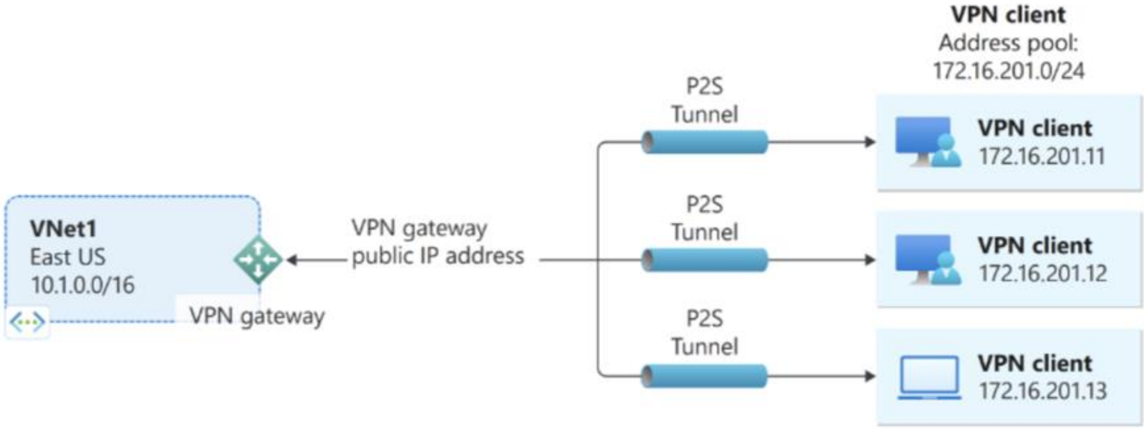
Point-to-Site

Overview:

A Point-to-Site (P2S) connection in the Azure portal is a secure virtual private network (VPN) connection that allows individual client devices to connect to an Azure Virtual Network (VNet). This enables remote access to resources hosted within the VNet, providing a secure way for users or devices to connect to the cloud-based network over the internet.

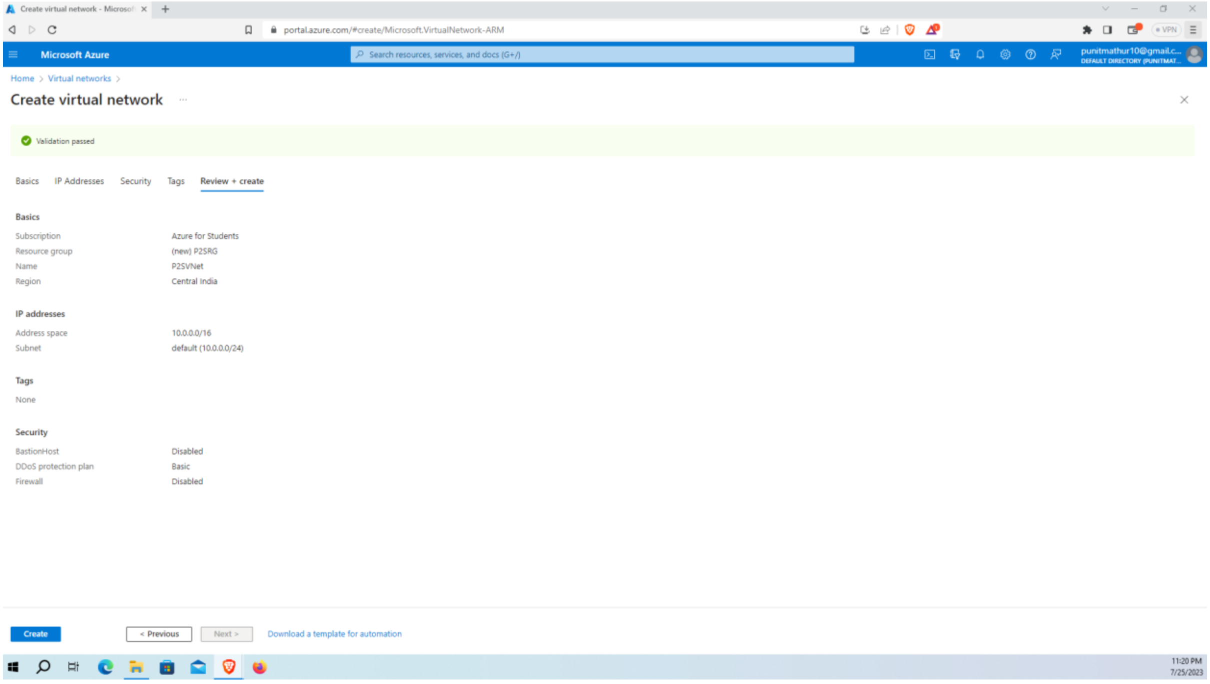
P2S Architecture :-



Now we will follow a process which will help us to create a point-to-site connection on azure with azure AD authentication :

Step 1 - Create a Virtual Network :

Create a virtual network named as **P2SVNet** and in the resource group named as **P2SRG** in the region **Central india** with address space as **10.0.0.0/16** and subnet as **default (10.0.0.0/24)**


Create virtual network - Microsoft
portal.azure.com/#create/Microsoft.VirtualNetwork-ARM
Microsoft Azure
Search resources, services, and docs (G+/)
punitmathur10@gmail.c...
DEFAULT DIRECTORY (PUNITMAT...
Home > Virtual networks >
Create virtual network
Basics
IP Addresses
Security
Tags
Review + create
Create
< Previous
Next >
Download a template for automation
11:20 PM
7/25/2023

Validation passed

Basics

Subscription	Azure for Students
Resource group	(new) P2SRG
Name	P2SVNet
Region	Central India

IP addresses

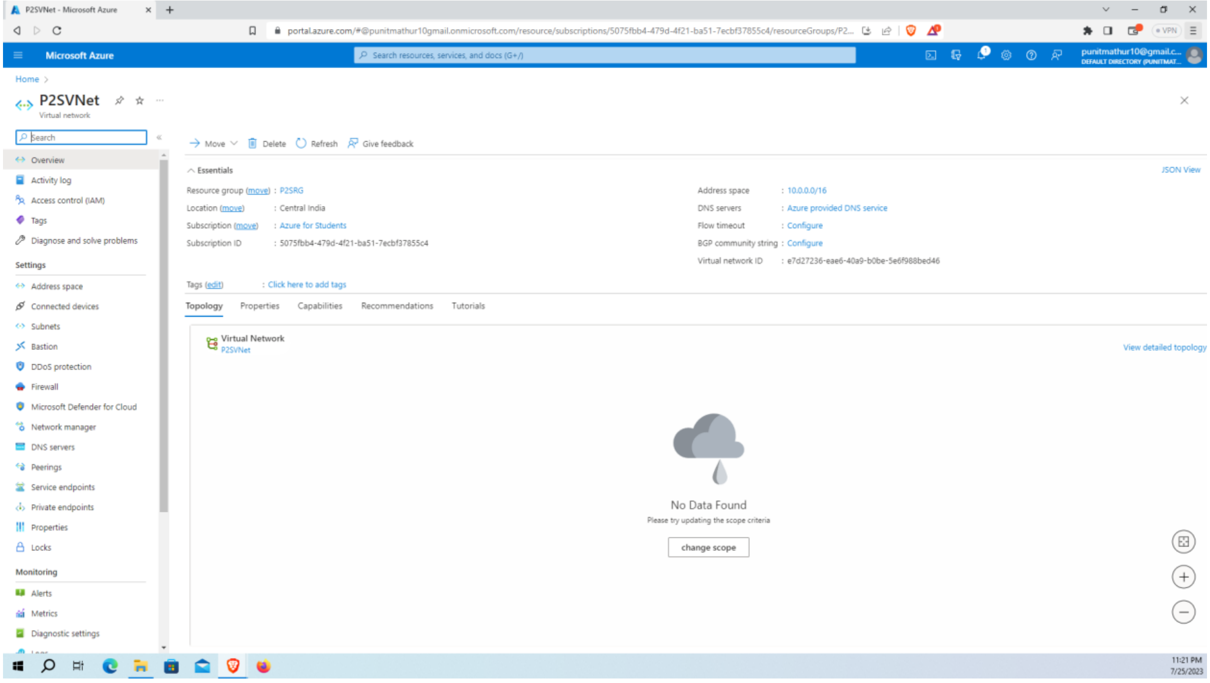
Address space	10.0.0.0/16
Subnet	default (10.0.0.0/24)

Tags

None

Security

BastionHost	Disabled
DDoS protection plan	Basic
Firewall	Disabled

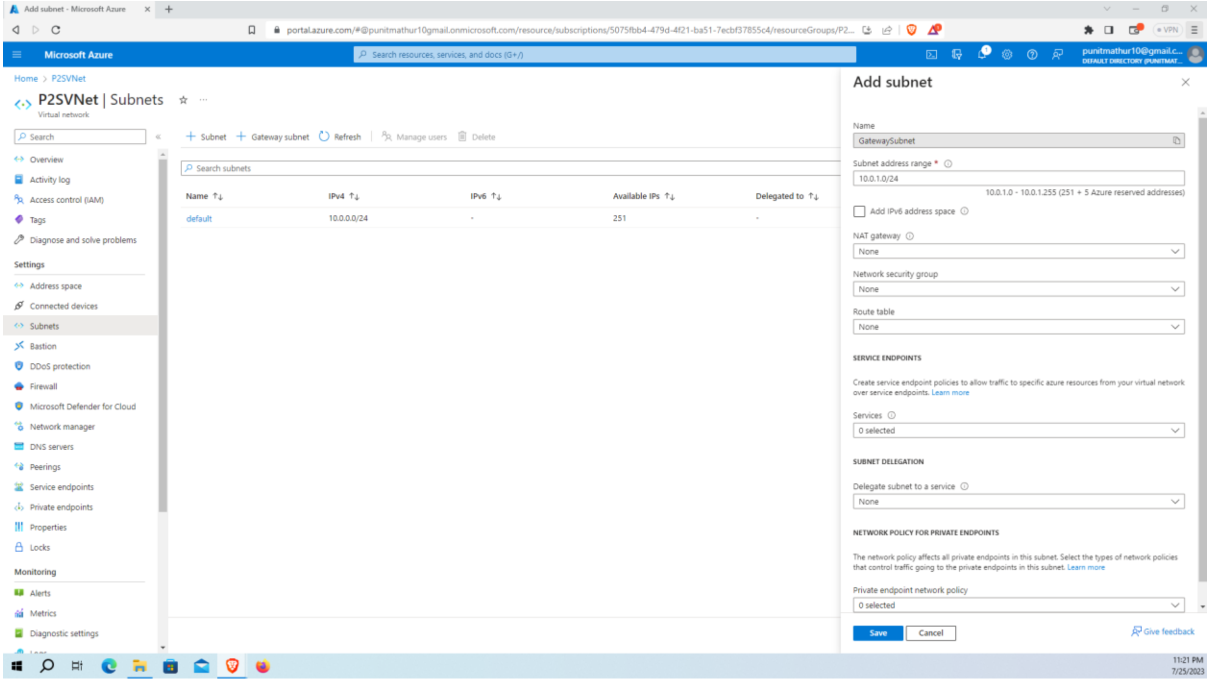


Resource group (move) : P2SRG
Location (move) : Central India
Subscription (move) : Azure for Students
Subscription ID : 5075fbb4-479d-4f21-ba51-7ecbf37855c4
Tags (edit) : Click here to add tags

Address space : 10.0.0.0/16
DNS servers : Azure provided DNS service
Flow timeout : Configure
BGP community string : Configure
Virtual network ID : e7d27236-eae6-40a9-b0be-5e6f988bed46

No Data Found
Please try updating the scope criteria

Now in this virtual network we will add a gateway subnet by going into the subnet section of this Vnet. Then clicking on gateway subnet and leaving everything at default and save.



Name	IPv4	IPv6	Available IPs	Delegated to
default	10.0.0.0/24	-	251	-

Add subnet

Name: GatewaySubnet

Subnet address range *: 10.0.1.0/24

10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

☐ Add IPv6 address space

NAT gateway: None

Network security group: None

Route table: None

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more

Services: 0 selected

SUBNET DELEGATION

Delegate subnet to a service: None

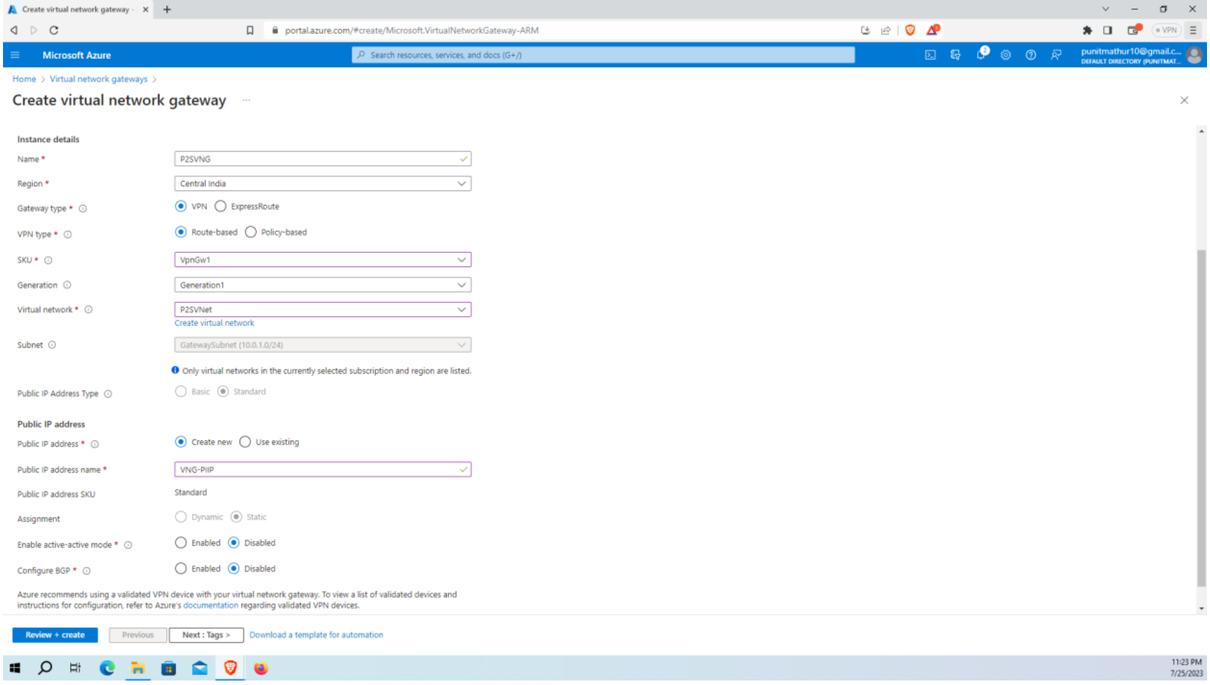
NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. Select the types of network policies that control traffic going to the private endpoints in this subnet. Learn more

Private endpoint network policy: 0 selected

Step 2 - Now we will create a virtual network gateway.

Now we will create a virtual network gateway with the name of **P2SVNG** Region of central india, Gateway type : VPN, VPN type : Route based, SKU: VpnGw1, Generation : 1, Virtual network : **P2SVNet** and public ip address name as **VNG-PIP.**



Create virtual network gateway
portal.azure.com/#create/Microsoft.VirtualNetworkGateway-ARM
Microsoft Azure
Search resources, services, and docs (G+/)
punitmathur10@gmail.c...
DEFAULT DIRECTORY (PUNITMAT...
Home > Virtual network gateways >

Create virtual network gateway

Instance details

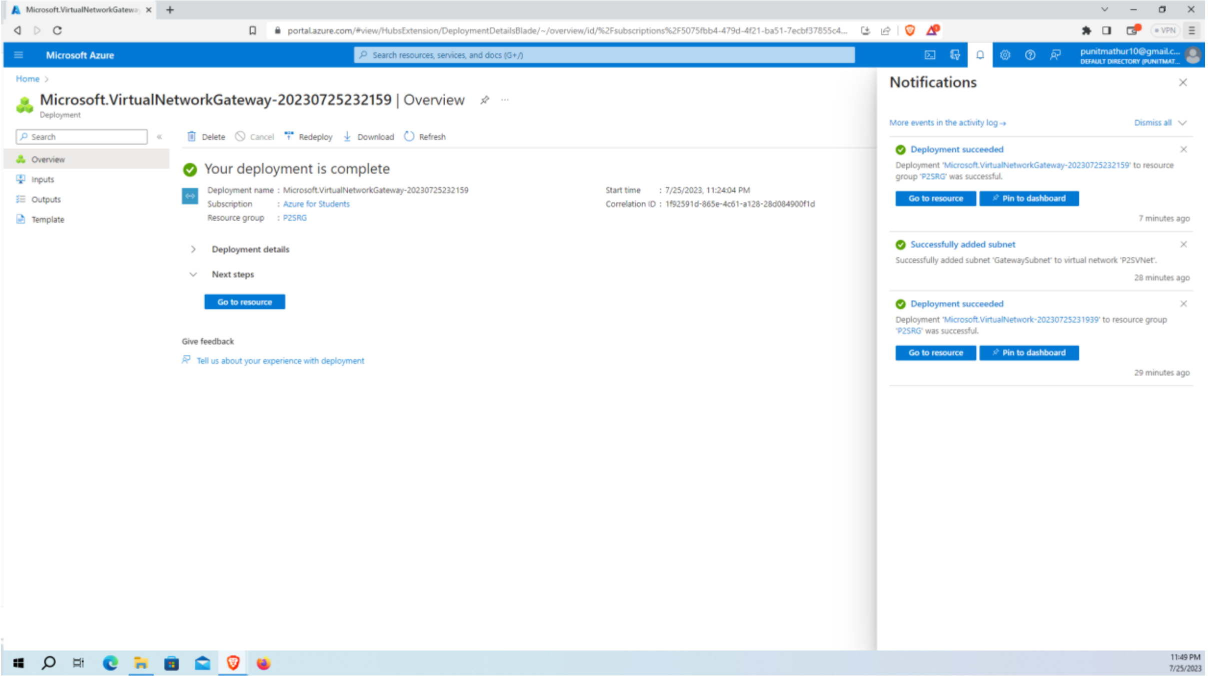
Name *	P2SVNG
Region *	Central India
Gateway type *	● VPN ○ ExpressRoute
VPN type *	● Route-based ○ Policy-based
SKU *	VpnGw1
Generation	Generation1
Virtual network *	P2SVNet Create virtual network
Subnet	GatewaySubnet (10.0.1.0/24)
	Only virtual networks in the currently selected subscription and region are listed.
Public IP Address Type	○ Basic ● Standard

Public IP address

Public IP address *	● Create new ○ Use existing
Public IP address name *	VNG-PIIP
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.

This will roughly take 35-40 minutes to get deployed.



Microsoft.VirtualNetworkGatewa
portal.azure.com/#view/HubsExtension/DeploymentDetailsBlade/~/overview/id/%2Fsubscriptions%2F5075fbb4-479d-4f21-ba51-7ecbf37855c4...
Microsoft Azure
Search resources, services, and docs (G+/)
punitmathur10@gmail.c...
DEFAULT DIRECTORY (PUNITMAT...
Home >
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh

Microsoft.VirtualNetworkGateway-20230725232159 | Overview
Deployment

Your deployment is complete

Deployment name	: Microsoft.VirtualNetworkGateway-20230725232159
Subscription	: Azure for Students
Resource group	: P2SRG
Start time	: 7/25/2023, 11:24:04 PM
Correlation ID	: 1f92591d-865e-4c61-a128-28d084900f1d

Deployment details
Next steps
Go to resource
Give feedback
Tell us about your experience with deployment

Notifications

More events in the activity log →
Dismiss all

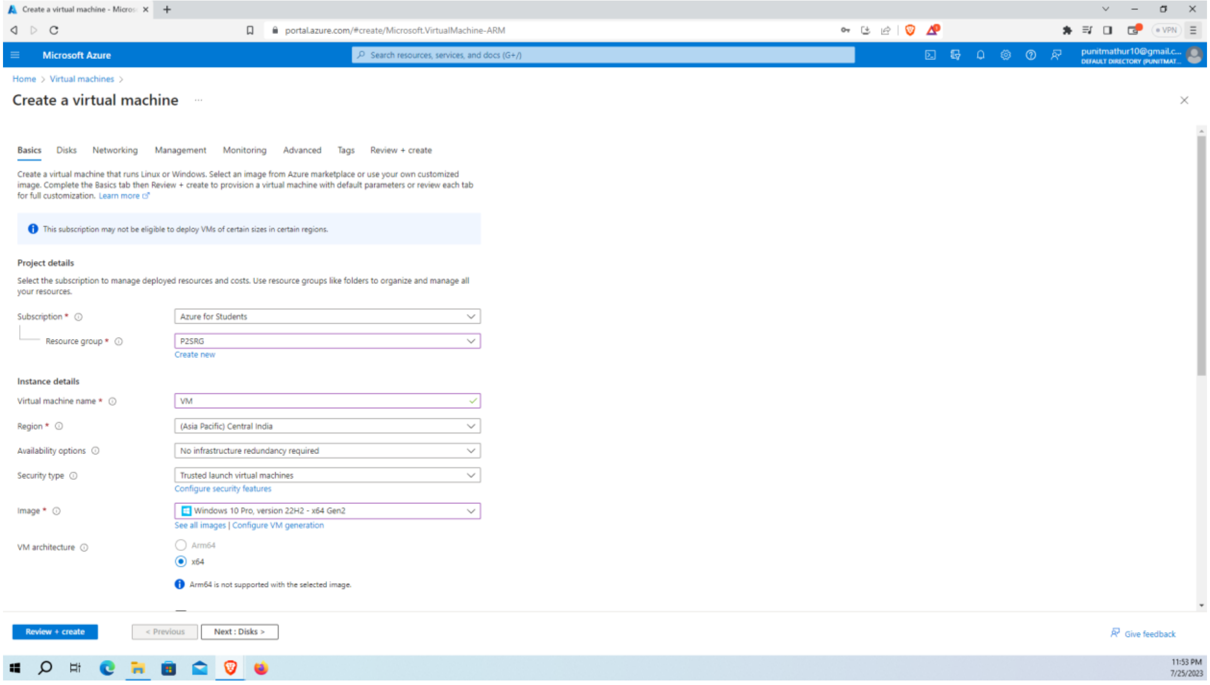
Deployment succeeded
Deployment 'Microsoft.VirtualNetworkGateway-20230725232159' to resource group 'P2SRG' was successful.
7 minutes ago

Successfully added subnet
Successfully added subnet 'GatewaySubnet' to virtual network 'P2SVNet'.
28 minutes ago

Deployment succeeded
Deployment 'Microsoft.VirtualNetwork-20230725231939' to resource group 'P2SRG' was successful.
29 minutes ago

Step 3 : Creating a virtual machine

Now we will create a virtual machine named as **VM** on the same resource group we created earlier while creating our virtual network. Our image will be **Windows 10 pro.** Now in the networking section we will select the virtual network as **P2SVNet** with default subnetting settings.



portal.azure.com/#create/Microsoft.VirtualMachine-ARM

Home > Virtual machines >

Create a virtual machine

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

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

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 for Students

Resource group * : P2SRG

Instance details

Virtual machine name * : VM

Region * : (Asia Pacific) Central India

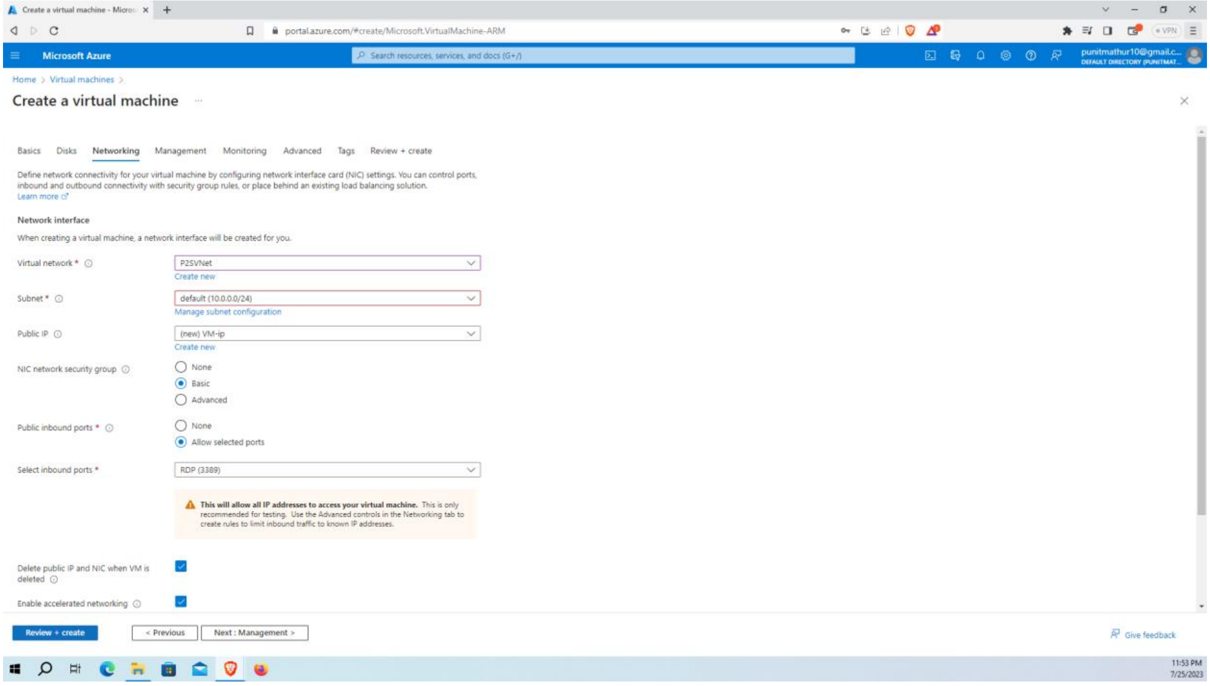
Availability options : No infrastructure redundancy required

Security type : Trusted launch virtual machines

Image * : Windows 10 Pro, version 22H2 - x64 Gen2

VM architecture : ○ Arm64 ● x64

Arm64 is not supported with the selected image.



portal.azure.com/#create/Microsoft.VirtualMachine-ARM

Home > Virtual machines >

Create a virtual machine

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 * : P2SVNet

Subnet * : default (10.0.0.0/24)

Public IP : (new) VM-ip

NIC network security group : ○ None ● Basic ○ Advanced

Public inbound ports * : ○ None ● Allow selected ports

Select inbound ports * : RDP (3389)

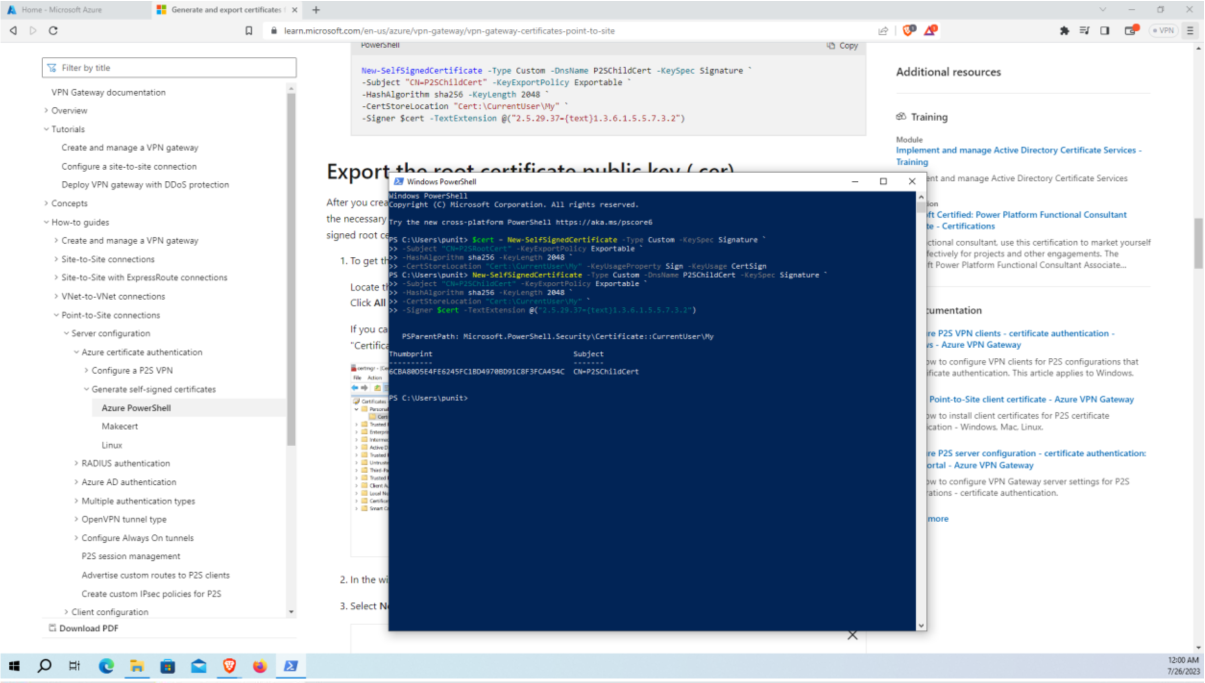
This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Delete public IP and NIC when VM is deleted : ☑

Enable accelerated networking : ☑

Step 4 - : Creation of Root and Client Certificate.

Now we will google microsoft azure root and client certificate and google will take us to a microsoft's web page from where we will just copy and paste the content in our powershell to generate root and client certificate. We will also type **certmgr.msc** in powershell to view our certificate generated by running the code on powershell.

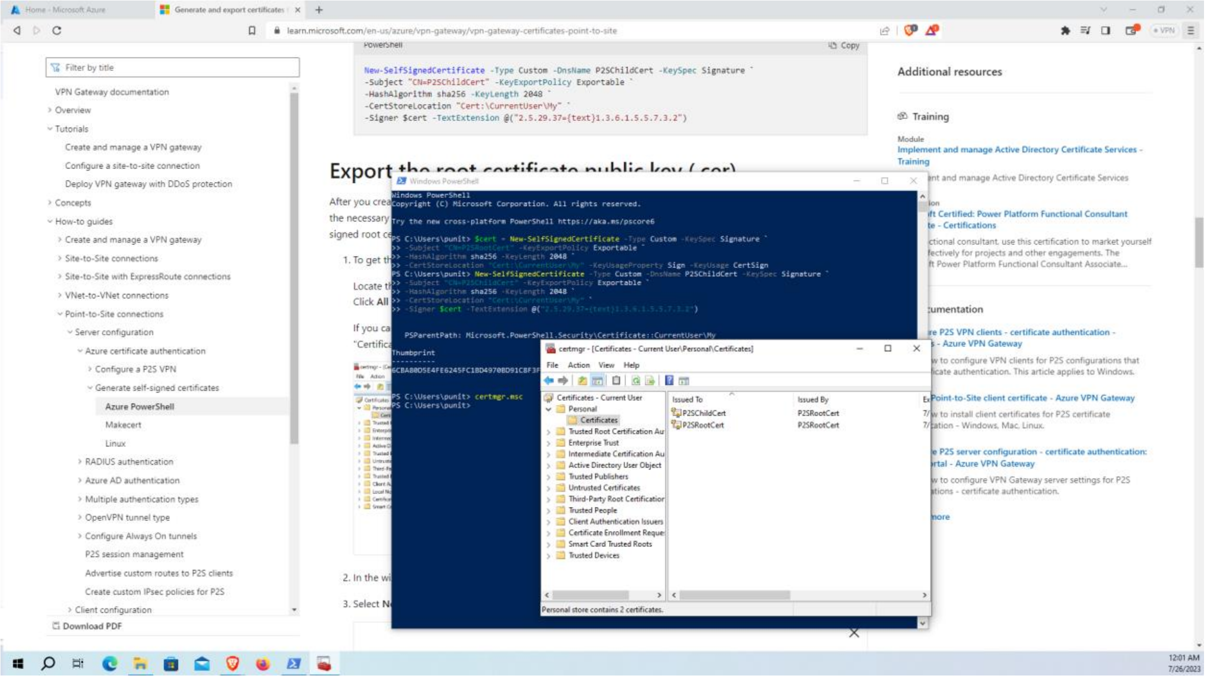


learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site

```
New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
-Subject "CN=P2SChildCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\punit> $cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
>> -Subject "CN=P2SRootCert" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign
PS C:\Users\punit> New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
>> -Subject "CN=P2SChildCert" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUser\My" `
>> -Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")


   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My

Thumbprint                                Subject
----------                                -------
6CBA80D5E4FE6245FC1BD4970BD91C8F3FCA454C  CN=P2SChildCert


PS C:\Users\punit>
```

Export the root certificate public key (.cer)
Additional resources
Training
VPN Gateway documentation
Azure PowerShell
Download PDF
12:00 AM
7/26/2023



```
PS C:\Users\punit> certmgr.msc
PS C:\Users\punit>
```

certmgr - [Certificates - Current User\Personal\Certificates]

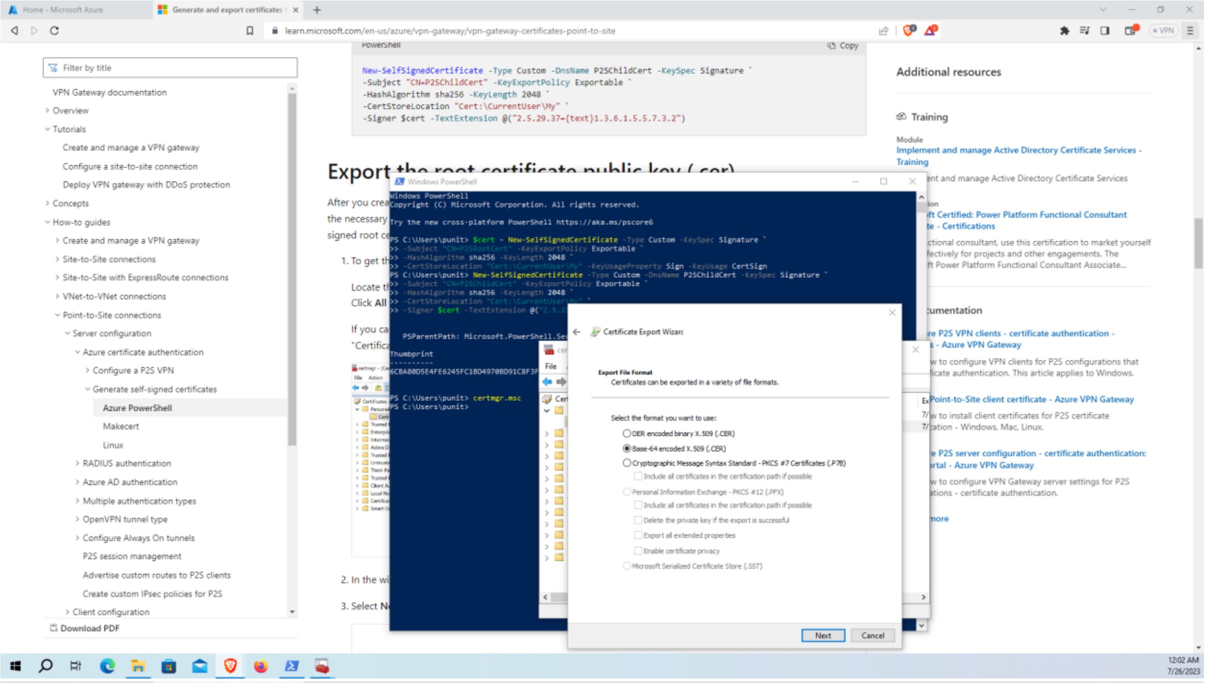
Issued To	Issued By
P2SChildCert	P2SRootCert
P2SRootCert	P2SRootCert

Personal store contains 2 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
Certificate Enrollment Reque
Smart Card Trusted Roots
Trusted Devices
12:01 AM
7/26/2023

Step 5 - Export of certificate

Now we will export our root and client certificate. While in root certificate we won't use a private key to export but in client certificate we will do the same by using passwords.



learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site

```
New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
-Subject "CN=P2SChildCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
```

Export the root certificate public key (.cer)

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\punit> $cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
>> -Subject "CN=P2SRootCert" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign
PS C:\Users\punit> New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
>> -Subject "CN=P2SChildCert" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUser\My" `
>> -Signer $cert -TextExtension @("2.5.2

   PSParentPath: Microsoft.PowerShell.Se

Thumbprint
----------
6CBA80D5E4FE6245FC1BD4970BD91CBF3F

PS C:\Users\punit> certmgr.msc
PS C:\Users\punit>
```

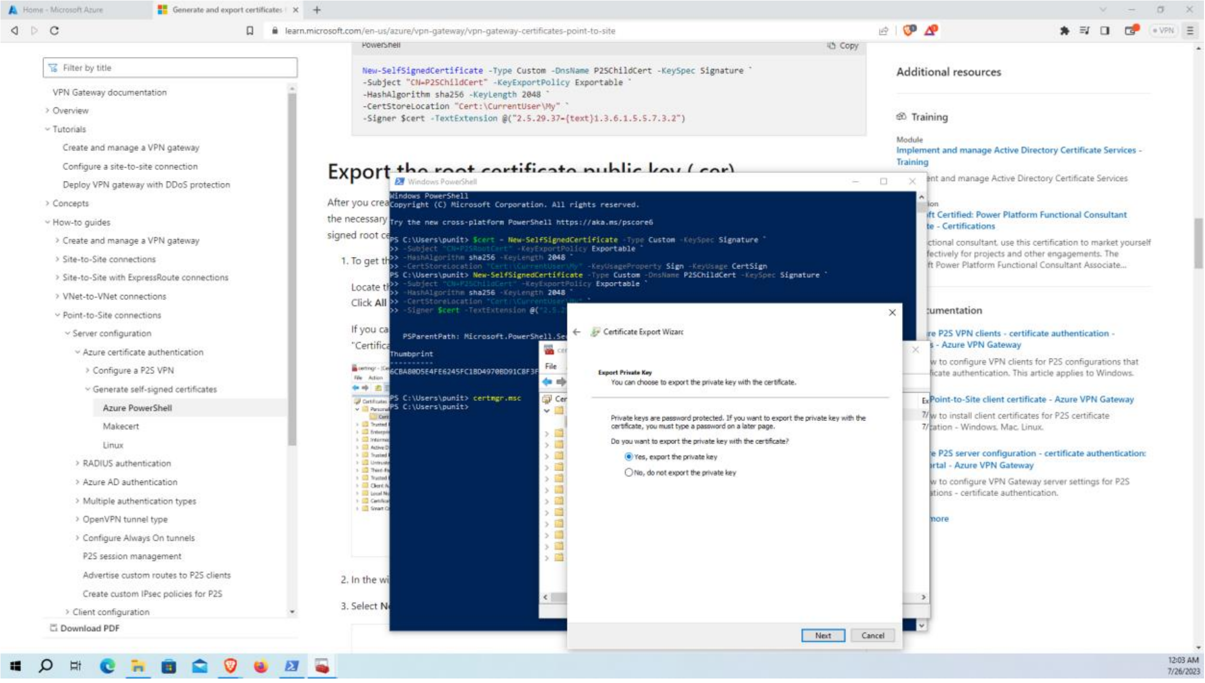
Certificate Export Wizard

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



learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site

```
New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
-Subject "CN=P2SChildCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
```

Certificate Export Wizard

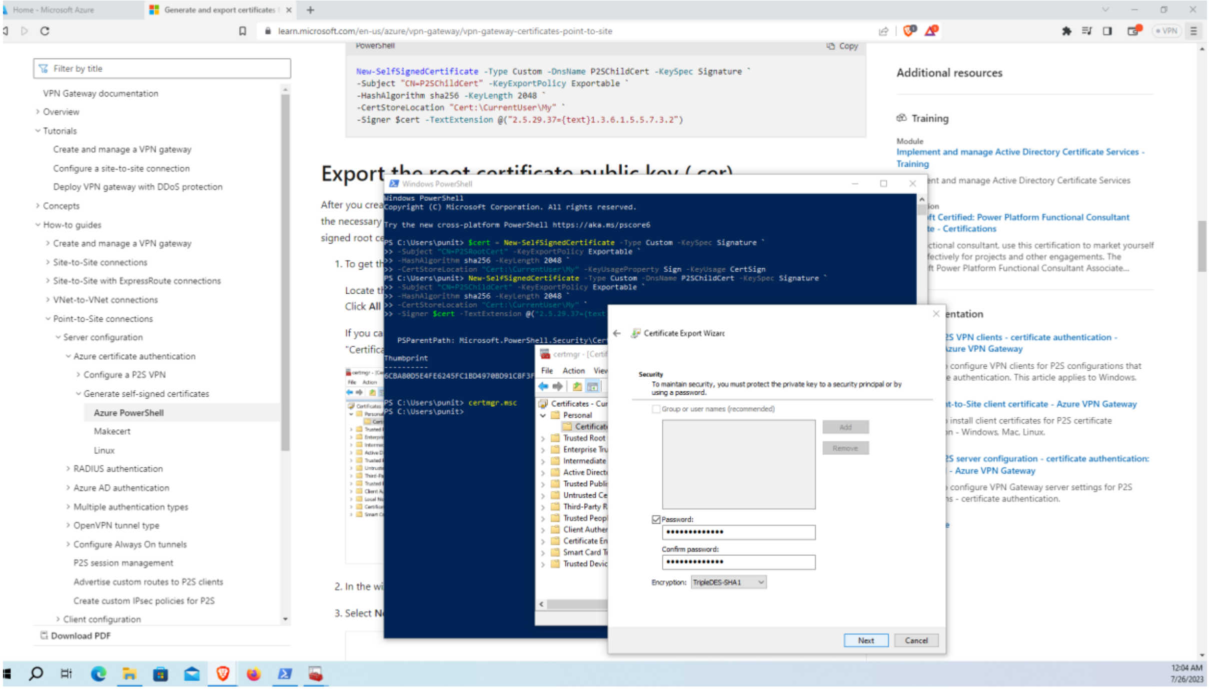
Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the 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 Cancel



learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site

```
New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
-Subject "CN=P2SChildCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
```

Export the root certificate public key (.cer)

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\punit> $cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
>> -Subject "CN=P2SRootCert" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign
PS C:\Users\punit> New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
>> -Subject "CN=P2SChildCert" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUser\My" `
>> -Signer $cert -TextExtension @("2.5.29.37={text


   PSParentPath: Microsoft.PowerShell.Security\Cer

Thumbprint
----------
6CBA80D5E4FE6245FC1BD49708D91C8F3F

PS C:\Users\punit> certmgr.msc
PS C:\Users\punit>
```

Certificate Export Wizard

Security

To maintain security, you must protect the private key to a security principal or by using a password.

□ Group or user names (recommended)

☑ Password: ••••••••••••••

Confirm password: ••••••••••••••

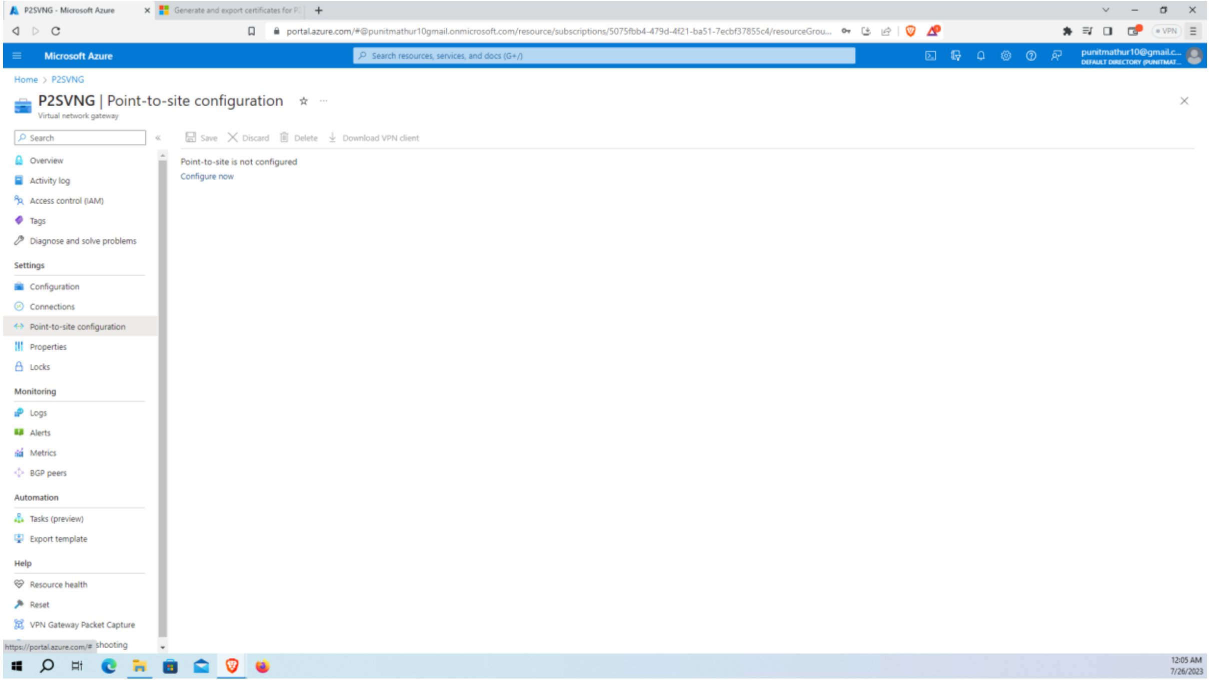
Encryption: TripleDES-SHA1

Home - Microsoft Azure
Generate and export certificates
Filter by title
VPN Gateway documentation
Overview
Tutorials
Create and manage a VPN gateway
Configure a site-to-site connection
Deploy VPN gateway with DDoS protection
Concepts
How-to guides
Create and manage a VPN gateway
Site-to-Site connections
Site-to-Site with ExpressRoute connections
VNet-to-VNet connections
Point-to-Site connections
Server configuration
Azure certificate authentication
Configure a P2S VPN
Generate self-signed certificates
Azure PowerShell
Makecert
Linux
RADIUS authentication
Azure AD authentication
Multiple authentication types
OpenVPN tunnel type
Configure Always On tunnels
P2S session management
Advertise custom routes to P2S clients
Create custom IPsec policies for P2S
Client configuration
Download PDF
Additional resources
Training
Module
Implement and manage Active Directory Certificate Services - Training
Copy
Add
Remove
Next
Cancel
certmgr
File
Action
View
Personal
Trusted Root
Intermediate
Client Authen
12:04 AM
7/26/2023

While we were doing this procedure, our Virtual Network Gateway was deployed.

Step 6 : Point-to-Site Configuration

Now we will go to VNG then go to **Point-to-Site Configuration** and then to **configure now.**



P2SVNG - Microsoft Azure
Generate and export certificates for P
portal.azure.com/#@punitmathur10gmail.onmicrosoft.com/resource/subscriptions/5075fbb4-479d-4f21-ba51-7ecbf37855c4/resourceGrou...
Microsoft Azure
Search resources, services, and docs (G+/)
punitmathur10@gmail.c...
DEFAULT DIRECTORY (PUNITMAT...
Home > P2SVNG
P2SVNG | Point-to-site configuration
Virtual network gateway
Search
Save
Discard
Delete
Download VPN client
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Connections
Point-to-site configuration
Properties
Locks
Monitoring
Logs
Alerts
Metrics
BGP peers
Automation
Tasks (preview)
Export template
Help
Resource health
Reset
VPN Gateway Packet Capture
https://portal.azure.com/# shooting
12:05 AM
7/26/2023

Point-to-site is not configured

Configure now

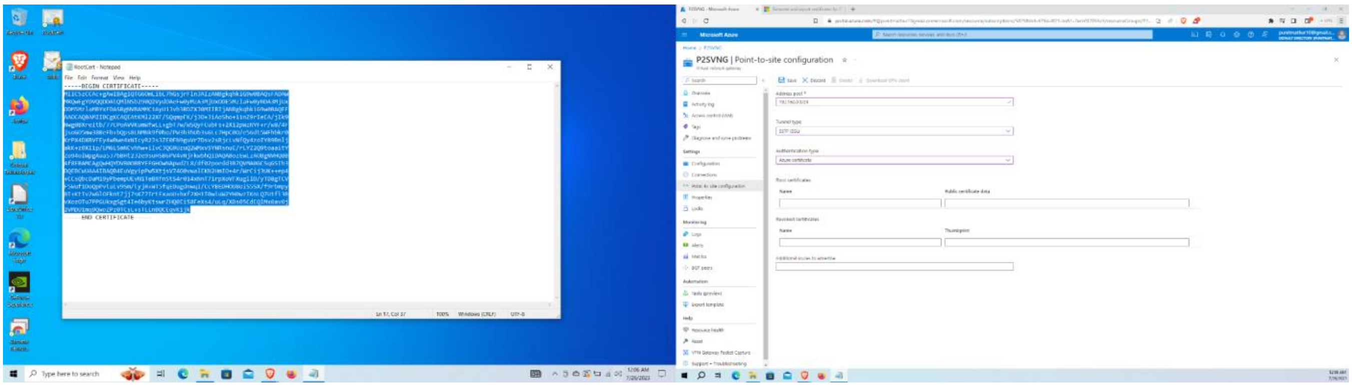
Now in configure now :-

Address Pool : 192.168.0.0/24.

Tunnel type : SSTP(SSL).

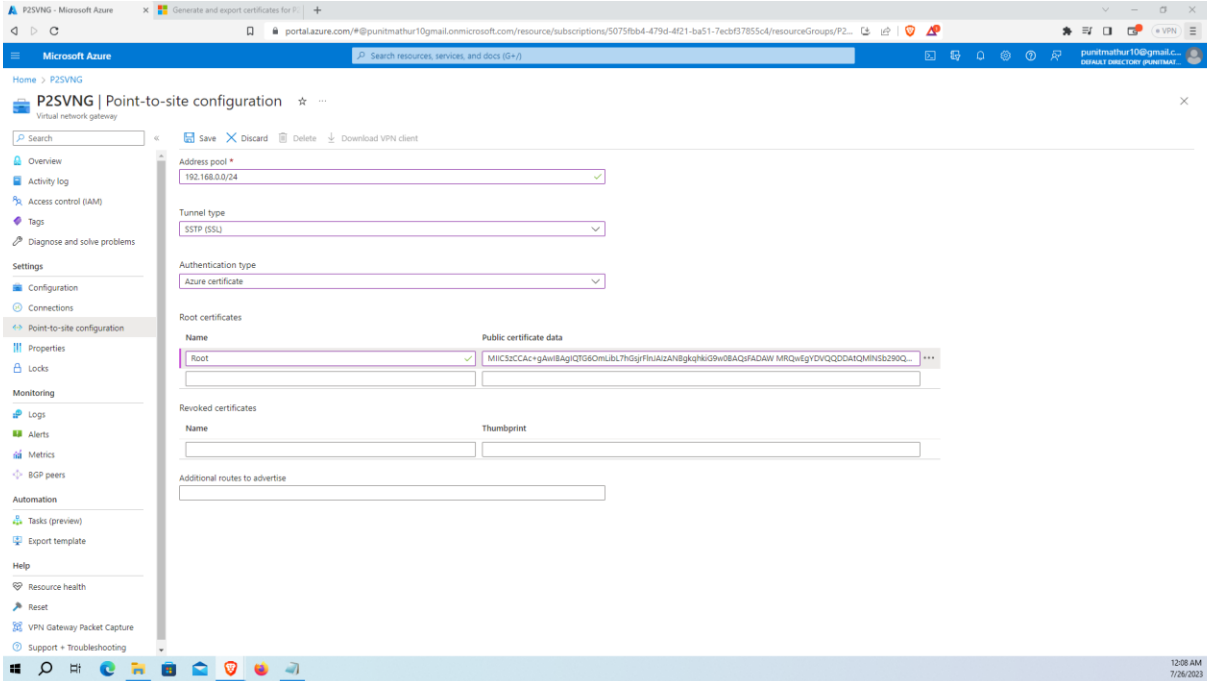
Authentication type : Azure Certificate

Now we will go to the root certificate and open it in the notepad and copy the content in it and paste that content into the Public **certificate data** section.



RootCert - Notepad

```
-----BEGIN CERTIFICATE-----
[illegible]
-----END CERTIFICATE-----
```



P2SVNG - Microsoft Azure
Generate and export certificates for P
portal.azure.com/#@punitmathur10gmail.onmicrosoft.com/resource/subscriptions/5075fbb4-479d-4f21-ba51-7ecbf37855c4/resourceGroups/P2...
Microsoft Azure
Search resources, services, and docs (G+/)
punitmathur10@gmail.c...
DEFAULT DIRECTORY (PUNITMAT...
Home > P2SVNG
Virtual network gateway
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Connections
Point-to-site configuration
Properties
Locks
Monitoring
Logs
Alerts
Metrics
BGP peers
Automation
Tasks (preview)
Export template
Help
Resource health
Reset
VPN Gateway Packet Capture
Support + Troubleshooting
Save
Discard
Delete
Download VPN client
12:08 AM
7/26/2023

P2SVNG | Point-to-site configuration

Address pool *: 192.168.0.0/24

Tunnel type: SSTP (SSL)

Authentication type: Azure certificate

Root certificates

Name	Public certificate data
Root	MIIC5zCCAc+gAwIBAgIQTG6OmLibL7hGsjrFlnJAIzANBgkqhkiG9w0BAQsFADAW MRQwEgYDVQQDDAtQMlNSb290Q...

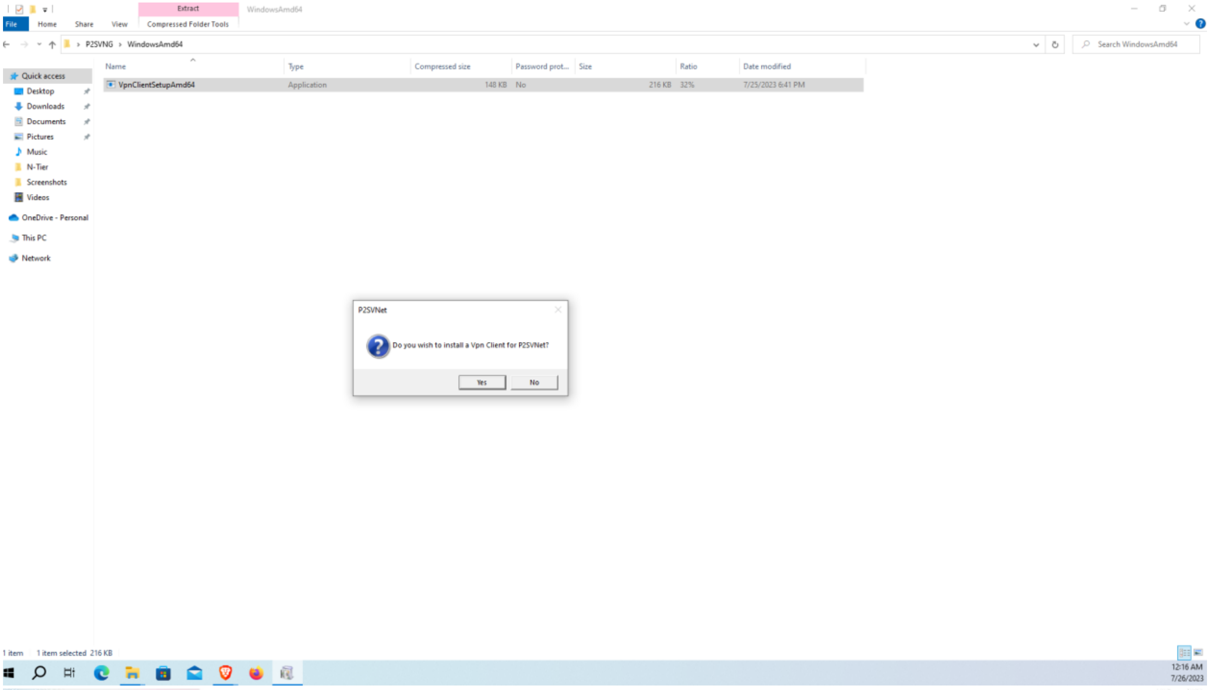
Revoked certificates

Name	Thumbprint

Additional routes to advertise

Step 7 - Download the VPN

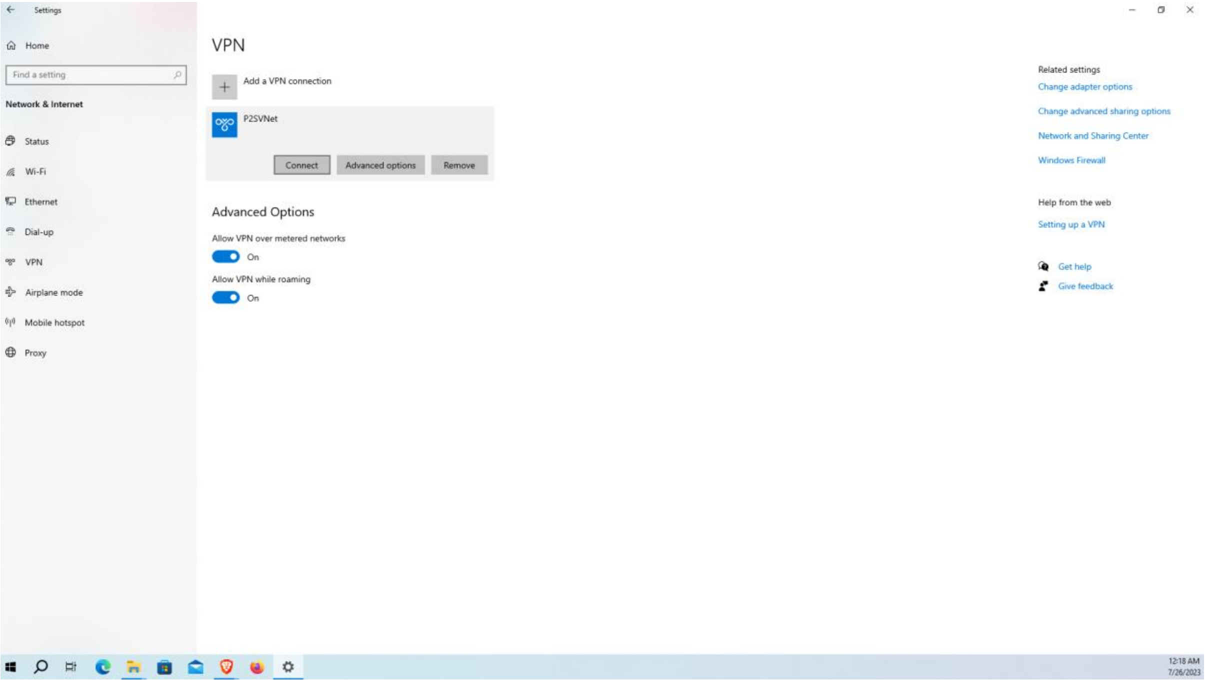
Now after doing this click on **download VPN client** and this will download a folder named as P2SVNG in your local machine now extract it and install the right VPN according to your local machine.



Name	Type	Compressed size	Password prot...	Size	Ratio	Date modified
VpnClientSetupAmd64	Application	148 KB	No	216 KB	32%	7/25/2023 6:41 PM

P2SVNet

Do you wish to install a Vpn Client for P2SVNet?



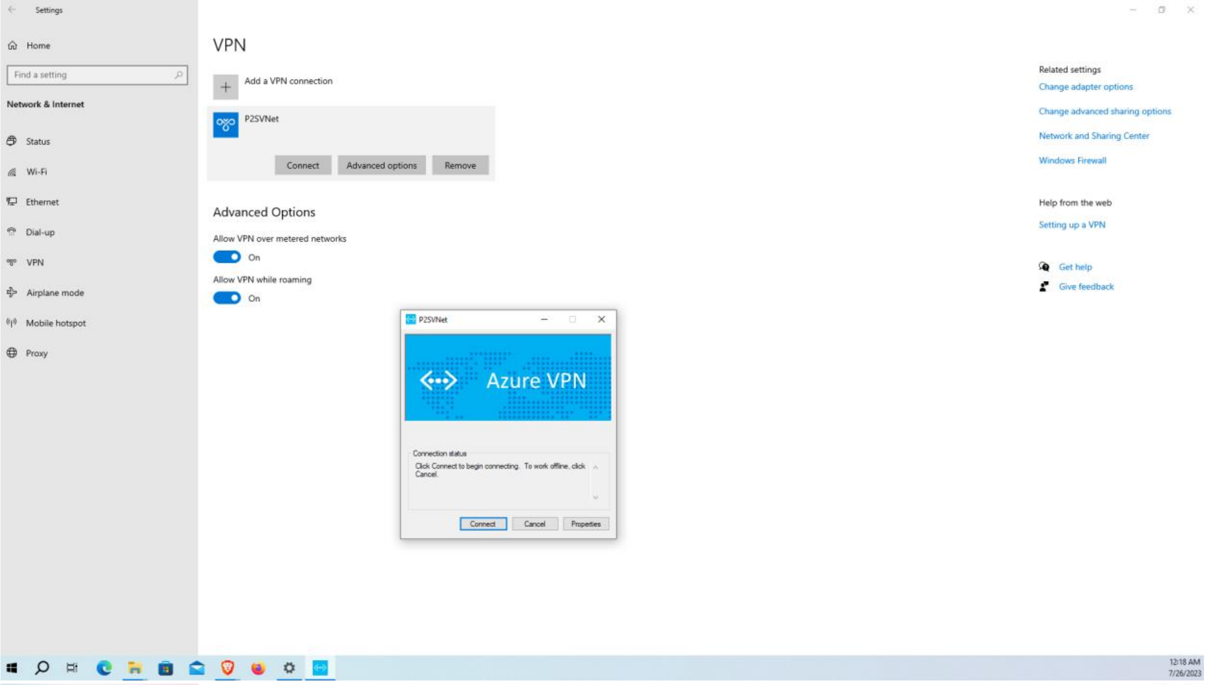
Advanced Options

Allow VPN over metered networks: On

Allow VPN while roaming: On

Step 8 - Connection with VPN

Now go to the setting of your local machine and go to VPN setting in that, we can see that our P2SVNet named vpn is already there. Now click connect on that.



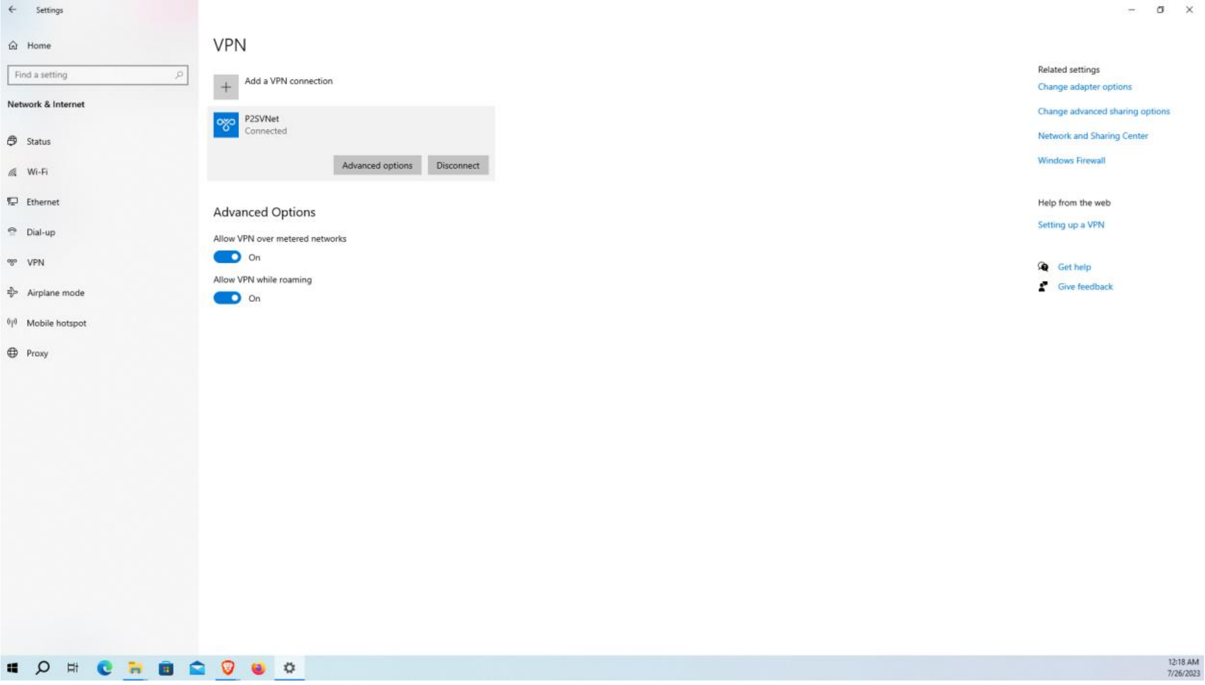
Advanced Options

Allow VPN over metered networks: On

Allow VPN while roaming: On

Connection status

Click Connect to begin connecting. To work offline, click Cancel.



P2SVNet
Connected

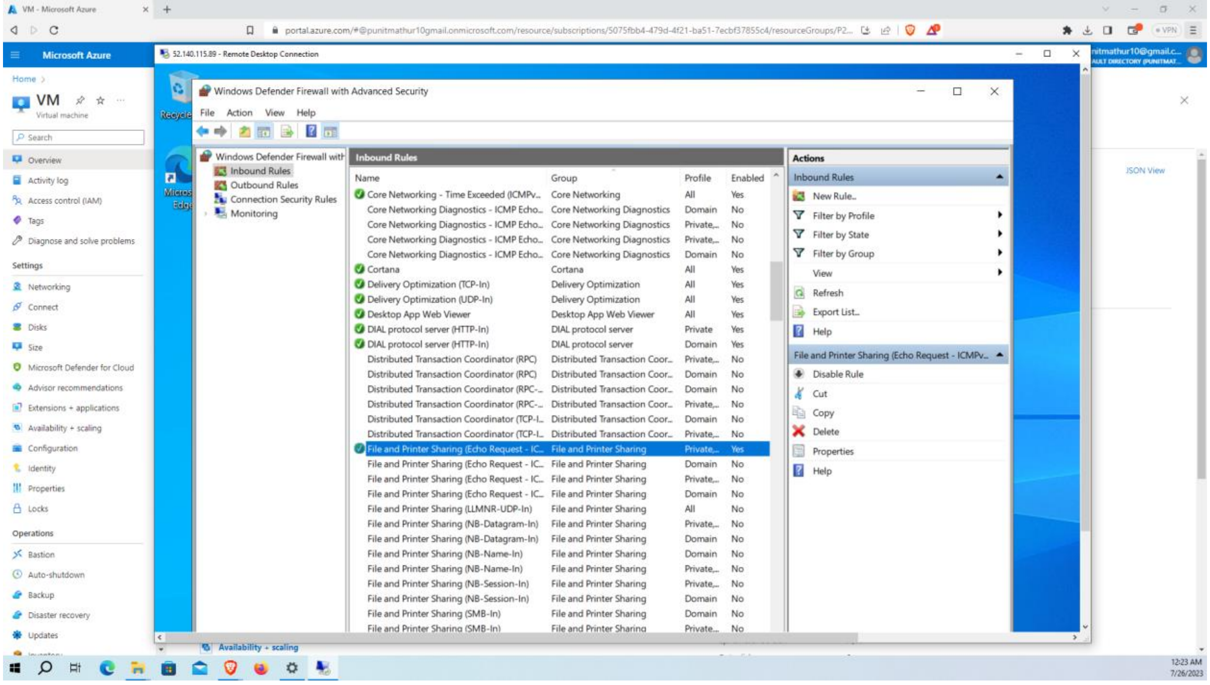
Advanced Options

Allow VPN over metered networks: On

Allow VPN while roaming: On

Step 9 - Enabling ICMP port in your Virtual machine.

Now connect to your virtual machine machine using RDP and then go to the advance firewall options in it and in there in inbound rules there is a ICMP rule, Enable it. We enable ICMP rule to make the smooth Point-to-Site Connection.



Inbound Rules

Name	Group	Profile	Enabled
✓ Core Networking - Time Exceeded (ICMPv...	Core Networking	All	Yes
Core Networking Diagnostics - ICMP Echo...	Core Networking Diagnostics	Domain	No
Core Networking Diagnostics - ICMP Echo...	Core Networking Diagnostics	Private,...	No
Core Networking Diagnostics - ICMP Echo...	Core Networking Diagnostics	Private,...	No
Core Networking Diagnostics - ICMP Echo...	Core Networking Diagnostics	Domain	No
✓ Cortana	Cortana	All	Yes
✓ Delivery Optimization (TCP-In)	Delivery Optimization	All	Yes
✓ Delivery Optimization (UDP-In)	Delivery Optimization	All	Yes
✓ Desktop App Web Viewer	Desktop App Web Viewer	All	Yes
✓ DIAL protocol server (HTTP-In)	DIAL protocol server	Private	Yes
✓ DIAL protocol server (HTTP-In)	DIAL protocol server	Domain	Yes
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coor...	Private,...	No
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coor...	Domain	No
Distributed Transaction Coordinator (RPC-...	Distributed Transaction Coor...	Domain	No
Distributed Transaction Coordinator (RPC-...	Distributed Transaction Coor...	Private,...	No
Distributed Transaction Coordinator (TCP-I...	Distributed Transaction Coor...	Domain	No
Distributed Transaction Coordinator (TCP-I...	Distributed Transaction Coor...	Private,...	No
✓ File and Printer Sharing (Echo Request - IC...	File and Printer Sharing	Private,...	Yes
File and Printer Sharing (Echo Request - IC...	File and Printer Sharing	Domain	No
File and Printer Sharing (Echo Request - IC...	File and Printer Sharing	Private,...	No
File and Printer Sharing (Echo Request - IC...	File and Printer Sharing	Domain	No
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	No
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Private,...	No
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Private,...	No
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Private,...	No
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	Private,...	No

Step 10 - Point-to-site connection established.