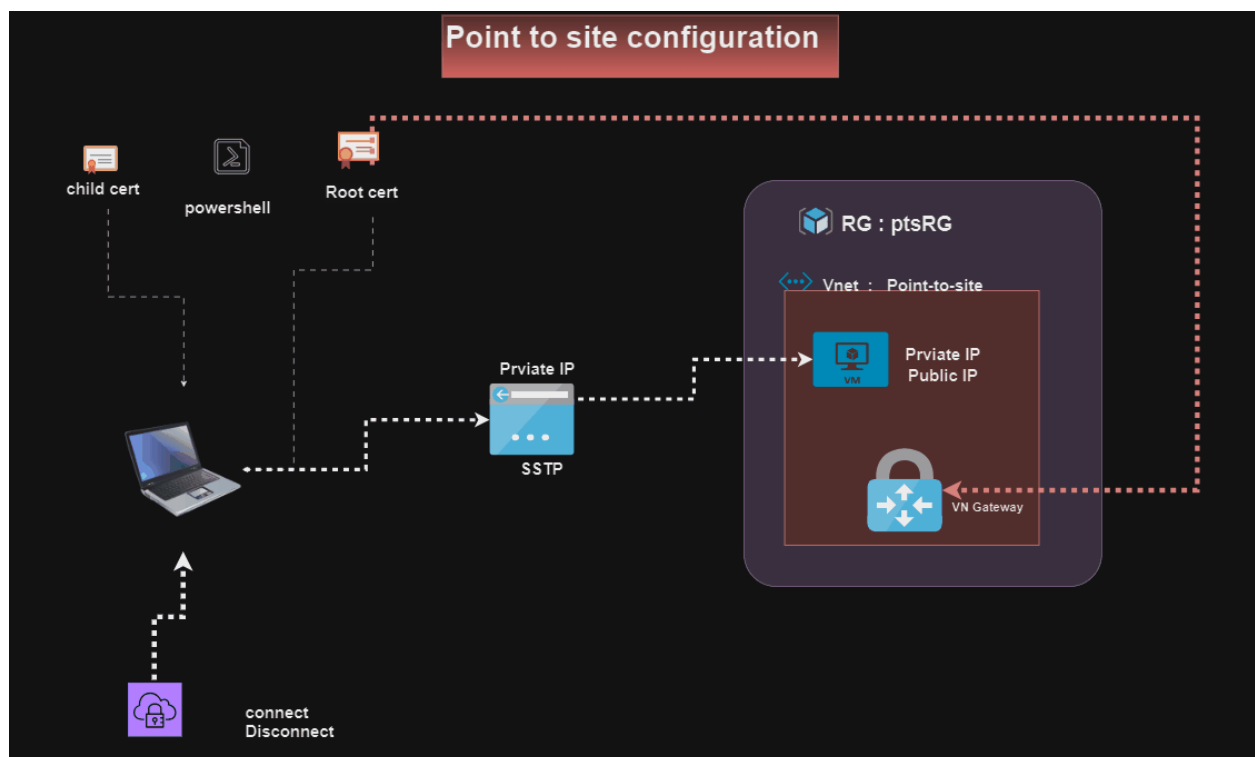




Stories 20: Azure point to site connection using azure Gateway

Point-to-Site (P2S) :

In Microsoft Azure, a Point-to-Site (P2S) connection is a type of VPN (Virtual Private Network) connection that enables secure communication between individual devices (such as laptops, desktops, or mobile devices) and an Azure Virtual Network. This type of connection is useful when users need to access resources within an Azure virtual network remotely, providing a secure and encrypted connection over the internet.



Azure Point-to-Site connections include:

1. **User Authentication:** Point-to-Site VPN connections use authentication protocols to verify the identity of the user connecting to the Azure Virtual Network. Azure supports multiple authentication methods, including Azure Active Directory (Azure AD), **certificates**, or a combination of both.
2. **Secure Communication:** The communication between the user's device and the Azure Virtual Network is **encrypted**, ensuring the confidentiality and integrity of data transmitted over the connection. This helps secure sensitive information, especially when accessing corporate resources in the cloud.
3. **VPN Client Software:** To establish a Point-to-Site connection, users need to install a VPN client on their devices. Azure provides a VPN client that can be downloaded and configured to connect to the Azure Virtual Network. The VPN client handles the establishment of the secure connection.
4. **Resource Access:** Once the Point-to-Site connection is established, users can access resources within the Azure Virtual Network as if they were directly connected to the network. This can include accessing virtual machines, web applications, databases, and other services hosted in Azure.
5. **Scalability:** Point-to-Site connections are scalable, allowing multiple users to connect simultaneously. This makes it suitable for scenarios where remote workers or traveling employees need secure access to Azure resources.

To set up a Point-to-Site connection in Azure, the following general steps are typically involved:

- **Create a Virtual Network:** Define and configure a Virtual Network in Azure where the resources are hosted.
- **Configure VPN Gateway:** Set up a VPN Gateway within the Virtual Network to handle Point-to-Site connections.
- **Define Address Pool:** Specify the address pool from which IP addresses are assigned to the connected devices.

- **Configure Authentication:** Choose the authentication method, such as Azure AD, certificates, or both.
- **Install VPN Client:** Users install the Azure VPN client on their devices and configure it with the necessary authentication details.

SSTP (**Secure Socket Tunneling Protocol**) VPN connection in Azure, you'll follow similar steps to setting up a Point-to-Site (P2S) VPN, with a few differences specific to SSTP. Here's a guide:

Prerequisites:

1. **Azure Subscription:** You need access to an Azure subscription.
2. **Azure Virtual Network:** Create a virtual network if you haven't already.
3. **Gateway Subnet:** Ensure that you have a subnet reserved for the VPN gateway.
4. **Public IP Address:** You need a public IP address for the VPN gateway.
5. **Client Certificates:** Generate or obtain client certificates for authentication.
6. **VPN Client:** Ensure your client machines have the VPN client software installed (SSTP VPN client or native VPN clients for supported OS).

root certificate

A **root certificate**, also known as a root CA (Certificate Authority) certificate, is a digital certificate that serves as the foundation of a public key infrastructure (PKI). It is a critical component in the trust model of SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols, used to secure communication over the Internet.

Create a self-signed root certificate

Use the `New-SelfSignedCertificate` cmdlet to create a self-signed root certificate. For additional parameter information, see [New-SelfSignedCertificate](#).

1. From a computer running Windows 10 or later, or Windows Server 2016, open a Windows PowerShell console with elevated privileges.
2. Create a self-signed root certificate. The following example creates a self-signed root certificate named 'P2SRootCert' that's automatically installed in 'Certificates-Current User\Personal\Certificates'. You can view the certificate by opening *certmgr.msc*, or *Manage User Certificates*.

Make any needed modifications before using this sample. The 'NotAfter' parameter is optional. By default, without this parameter, the certificate expires in 1 year.

```
$params = @{
    Type = 'Custom'
    Subject = 'CN=P2SRootCert'
    KeySpec = 'Signature'
    KeyExportPolicy = 'Exportable'
    KeyUsage = 'CertSign'
    KeyUsageProperty = 'Sign'
    KeyLength = 2048
    HashAlgorithm = 'sha256'
    NotAfter = (Get-Date).AddMonths(24)
    CertStoreLocation = 'Cert:\CurrentUser\My'
}
$cert = New-SelfSignedCertificate @params
```

client-side certificate

A client-side certificate, also known as a client certificate or user certificate, is a digital certificate that is used to authenticate and identify a user or client device in a secure communication context, such as SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols. Unlike server certificates (such as SSL certificates for websites), which are presented by servers to prove their identity to

clients, client-side certificates are presented by clients to authenticate themselves to servers.

Generate a client certificate

Each client computer that connects to a VNet using point-to-site must have a client certificate installed. You generate a client certificate from the self-signed root certificate, and then export and install the client certificate. If the client certificate isn't installed, authentication fails.

The following steps walk you through generating a client certificate from a self-signed root certificate. You may generate multiple client certificates from the same root certificate. When you generate client certificates using the steps below, the client certificate is automatically installed on the computer that you used to generate the certificate. If you want to install a client certificate on another client computer, export the certificate.

The examples use the [New-SelfSignedCertificate](#) cmdlet to generate a client certificate.

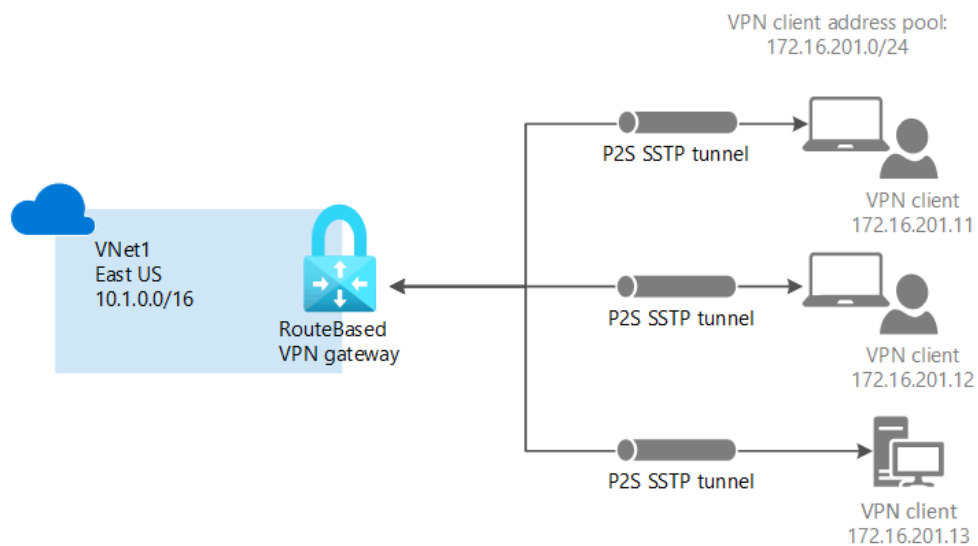
Example 1 - PowerShell console session still open

Use this example if you haven't closed your PowerShell console after creating the self-signed root certificate. This example continues from the previous section and uses the declared '\$cert' variable. If you closed the PowerShell console after creating the self-signed root certificate, or are creating additional client certificates in a new PowerShell console session, use the steps in [Example 2](#).

Modify and run the example to generate a client certificate. If you run the following example without modifying it, the result is a client certificate named 'P2SChildCert'. If you want to name the child certificate something else, modify the CN value. Don't change the TextExtension when running this example. The client certificate that you generate is automatically installed in 'Certificates - Current User\Personal\Certificates' on your computer.

```
$params = @{
    Type = 'Custom'
    Subject = 'CN=P2SChildCert'
    DnsName = 'P2SChildCert'
    KeySpec = 'Signature'
    KeyExportPolicy = 'Exportable'
    KeyLength = 2048
    HashAlgorithm = 'sha256'
    NotAfter = (Get-Date).AddMonths(18)
    CertStoreLocation = 'Cert:\CurrentUser\My'
    Signer = $cert
    TextExtension = @(
        '2.5.29.37={text}1.3.6.1.5.5.7.3.2')
}
New-SelfSignedCertificate @params
```

Lab: To configure Azure point to site connection using azure virtual network gateway



Solution :

Estimated Time Required : 55 min

Quick Glance

1. **Create A Resource Group pointositeRG**
2. ***Create a VNet name it as pointositeVnet***
3. ***Create a virtual Gateway (Search VPN to get this)***
4. ***Create a VM in pointositeVnet***
5. ***Create a Root certificate by running the script in powershell from azure documentation***
6. ***Export the root certificate***
7. ***Create Client side certificate***
8. ***Export the client side certificate***
9. ***Configure the point to site by adding root certificate.***
10. **Save configuration**
11. ***Download the VPN(allowed from popup blocker)***

Reference Microsoft documentation link below

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal>

Step 1:

Create a vnet as shown in the figure below

Virtual networks

mubeen507

+ Create Manage view Refresh Export to CSV Open query Assign tags

Filter for any field...

Subscription equals all

Resource group equals all

Location equals all

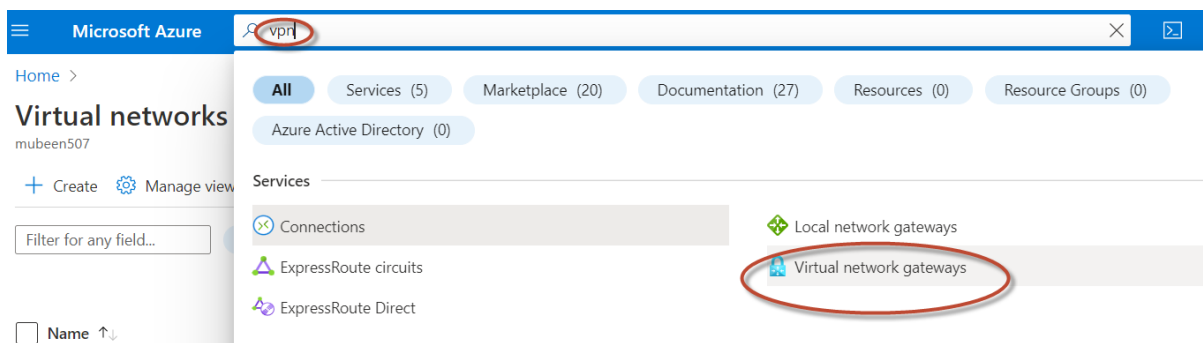
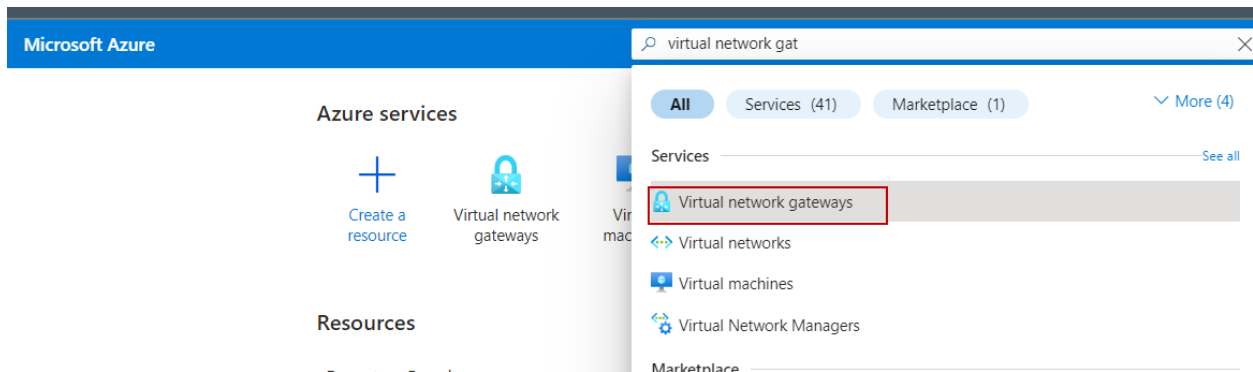
+ Add filter

No grouping

Name ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓
<input type="checkbox"/> <=> mubeenRG-vnet	mubeenRG	Central India	Azure for Students
<input type="checkbox"/> <=> mubeenRGvnet314	mubeenRG	South India	Azure for Students
<input checked="" type="checkbox"/> <=> point-to-site	mubeenRG	South India	Azure for Students

Step 2 :

Now create a virtual private network



Microsoft Azure

Home > Virtual network gateways >

Create virtual network gateway

your resources.

Subscription * Azure for Students

Resource group ① Select a virtual network to get resource group

Instance details

Name * site2 ✓

Region * South India

Gateway type * ① ☒ VPN ☐ ExpressRoute

VPN type * ① ☒ Route-based ☐ Policy-based

SKU * ① VpnGw2

Generation ① Generation2

Virtual network * ①

Public IP Address Type * ①

Public IP address

Public IP address * ① ☒ Create new ☐ Use existing

Public IP address name * myvpnlp ✓

Public IP address SKU Standard

Assignment ☐ Dynamic ☒ Static

Enable active-active mode * ① ☐ Enabled ☒ Disabled

Configure BGP * ① ☐ Enabled ☒ Disabled

Filter virtual networks

Can be associated to virtual network gateway

mubeenRGvnet314

point-to-site2

⚠️ We recommend using a validated VPN device with your virtual network gateway. To view a list of validated devices and

Review + create Previous Next : Tags > Download a template for automation

Click on create wait until its deployed

Home >

Microsoft.VirtualNetworkGateway-20220719155049 | Overview ⚙️ ...

Deployment

Search (Ctrl+F) << Delete Cancel Redeploy Refresh

Overview

Inputs

Outputs

Template

We'd love your feedback! →

... Deployment is in progress

Deployment name: Microsoft.VirtualNetworkGateway-2022071915... Start time: 7/19/2022, 3:56:47 PM
Subscription: Azure for Students Correlation ID: a4ceb44f-23be-4903-8470-05fd31e19fb4
Resource group: mubeenRG

Deployment details (Download)

Resource	Type	Status	Operator
point-to-site2/GatewaySubnet	Microsoft.Network/virtualNetworks/subnets	OK	Operator

Step 3:

Create Virtual machine

[Home](#) > [Virtual machines](#) >

Create a virtual machine ...

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](#)

i 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 * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Virtual machine name * ⓘ

Region * ⓘ

Availability options ⓘ

Security type ⓘ

Image * ⓘ [See all images](#) | [Configure VM generation](#)

Run with Azure Spot discount ⓘ ☐

Size * ⓘ [See all sizes](#)

Administrator account

Username * ⓘ

Password * ⓘ

Confirm password * ⓘ

[Review + create](#)

< Previous

Next : Disks >

[Basics](#) [Disks](#) [Networking](#) [Management](#) [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 * ⓘ [Create new](#)

Subnet * ⓘ [Manage subnet configuration](#)

Public IP ⓘ [Create new](#)

NIC network security group ⓘ ☐ None ☒ Basic ☐ Advanced

Public inbound ports * ⓘ ☐ None

[Review + create](#)

< Previous

Next : Management >

Note Don't forget to create in the same Resource group

Step 4 :

Now create Root Certificate :

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site>

2. Use the following example to create the self-signed root certificate. The following example creates a self-signed root certificate named 'P2SRootCert' that is automatically installed in 'Certificates-Current User\Personal\Certificates'. You can view the certificate by opening *certmgr.msc*, or *Manage User Certificates*.

Run the following example with any necessary modifications.

```
PowerShell Copy

$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
-Subject "CN=P2SRootCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign
```

3. Leave the PowerShell console open and proceed with the next steps to generate a client certificate.

Step 5:

Copy and paste the root certificate script in power shell

```
Administrator: Windows PowerShell

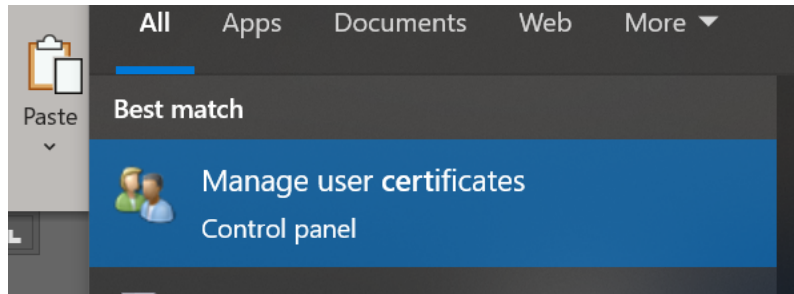
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

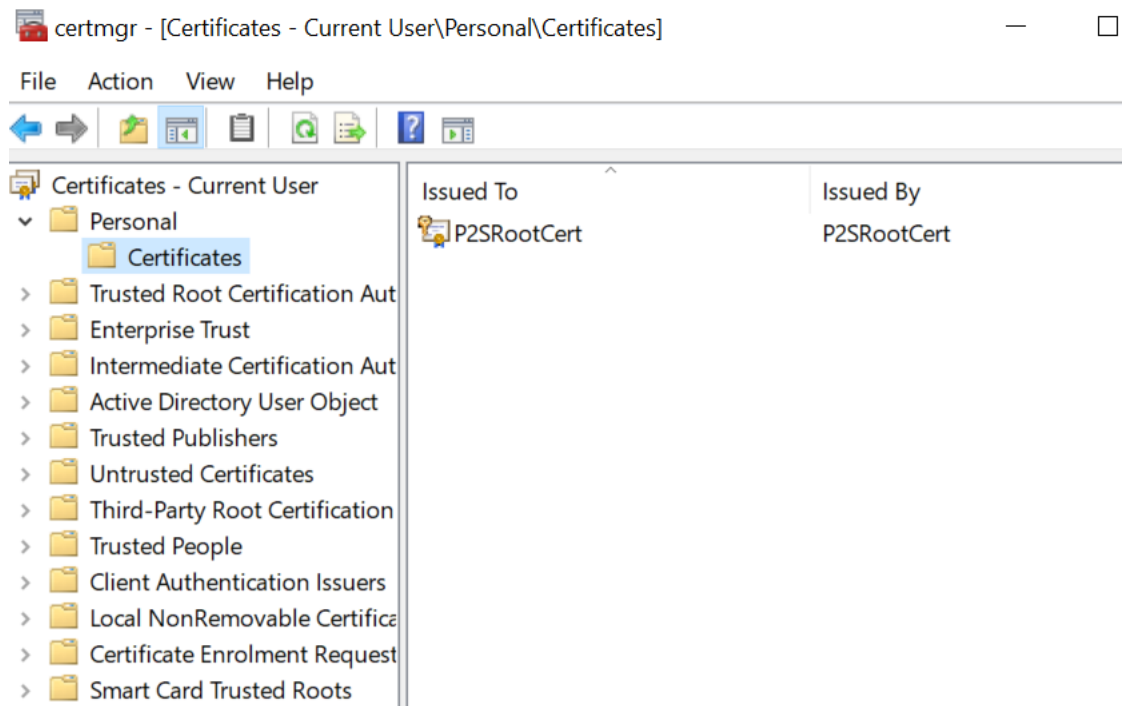
PS C:\Windows\system32> $cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
>> -Subject "CN=P2SRootCert" -KeyExportPolicy Exportable `
>> -HashAlgorithm sha256 -KeyLength 2048 `
>> -CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign
PS C:\Windows\system32>
```

After Running the script a root certificate will be generated in windows machine

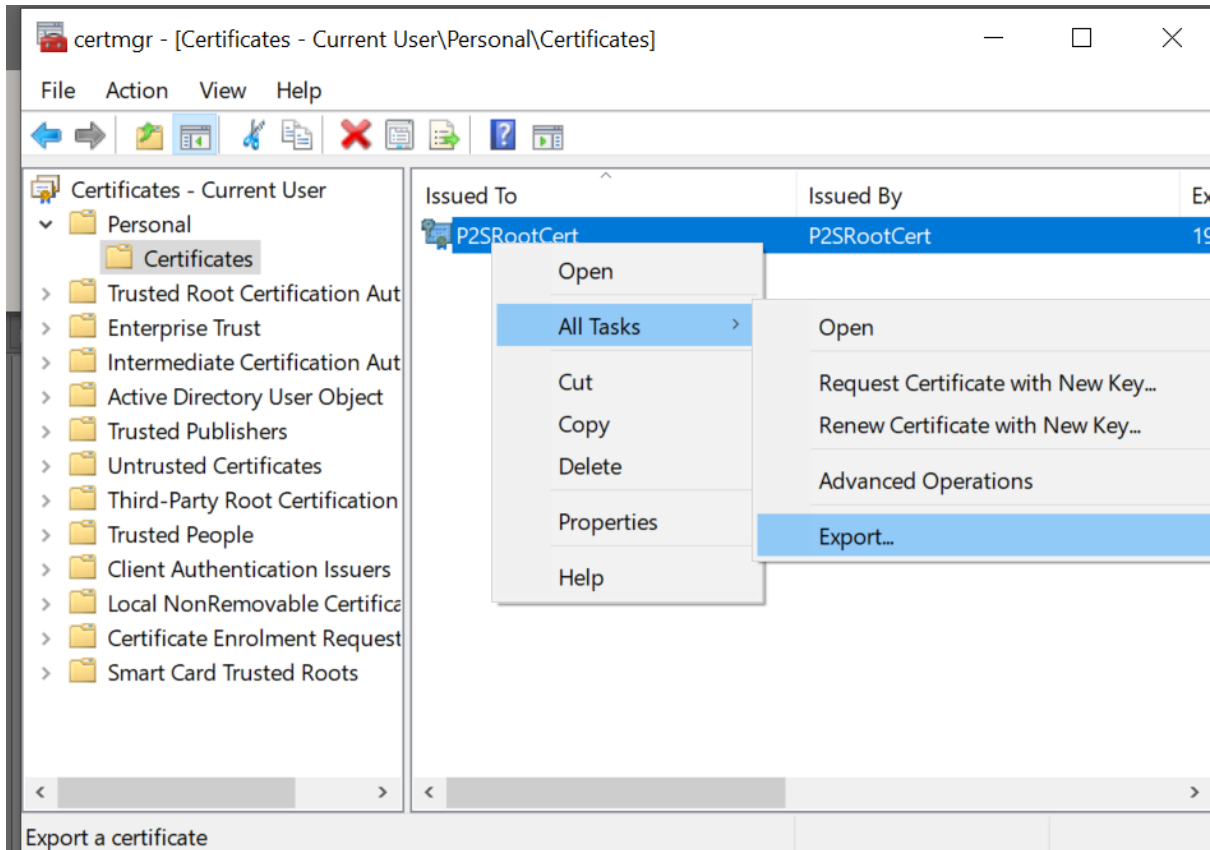
Now go to



Open and to go below location to export the certificate



Export the certificate and save it



Export >No,I don't want to save private key > base 64 >give location >SAVE

Step 6:

Now in the same way generate the client side certificate

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

Filter by title

- 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

4. Modify and run the example to generate a client certificate. If you run the following example without modifying it, the result is a client certificate named 'P2SChildCert'. If you want to name the child certificate something else, modify the CN value. Don't change the TextExtension when running this example. The client certificate that you generate is automatically installed in 'Certificates - Current User\Personal\Certificates' on your computer.

```

PowerShell
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)"

```

Copy the script and paste it in the powershell to generate the client side certificate

```
Administrator: Windows PowerShell

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

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

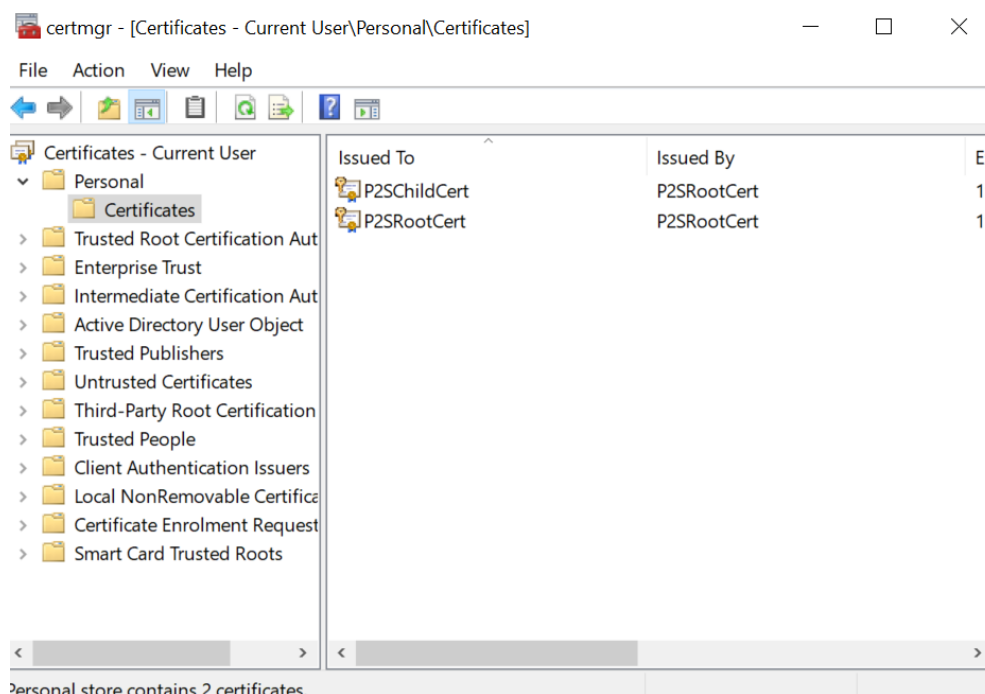
PS C:\Windows\system32> $cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
> -Subject "CN=P2SRootCert" -KeyExportPolicy Exportable `
> -HashAlgorithm sha256 -KeyLength 2048 `
> -CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign
PS C:\Windows\system32> 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
-----
53 [redacted] CN=P2SChild [redacted]

PS C:\Windows\system32>
```

Goto manage user certificate and export the client side certificate and save it



- All task > Export > yes,I want to save private key> next> next >

← Certificate Export Wizard

Security

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

☐ Group or usernames (recommended)

Add

Remove

☒ Password:

••••••••

Confirm password:

••••••••

Encryption: TripleDES-SHA1

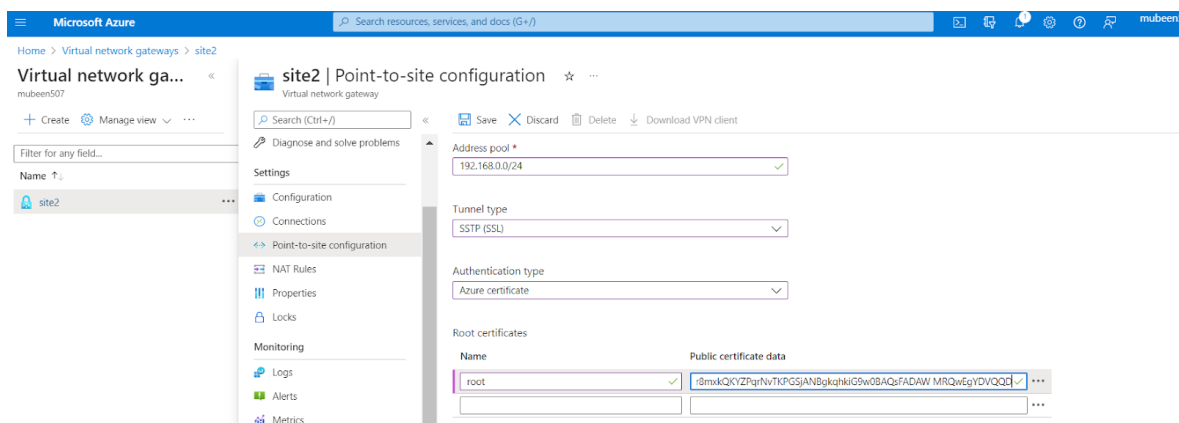
Next

Cancel

STEP 7 :

Now goto virtual network Gateway to configure point to site

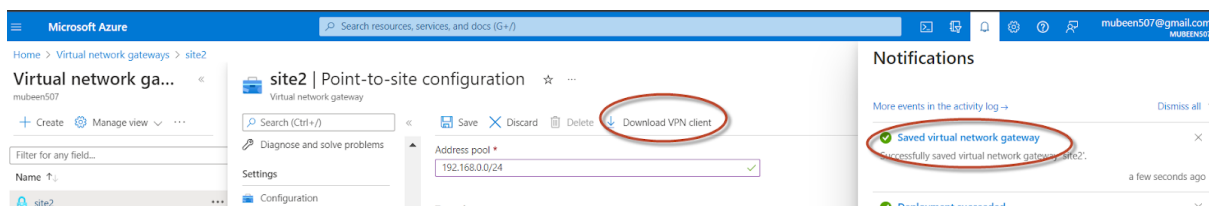
Note : Virtual netowrk connection creation time will be around 40 mins



Note : Root certificate should be paste in Virtual network Gateway

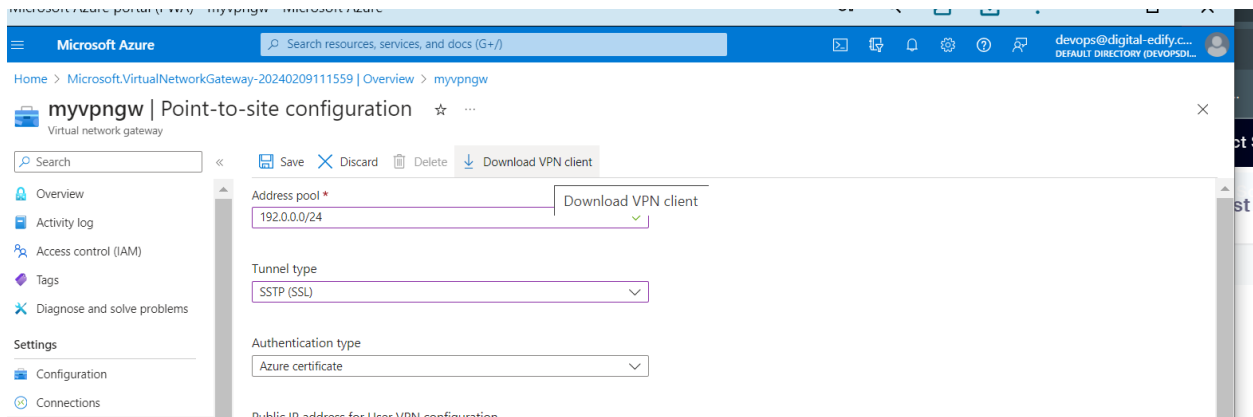


and client certificate should be added to manage user certificate in client pc

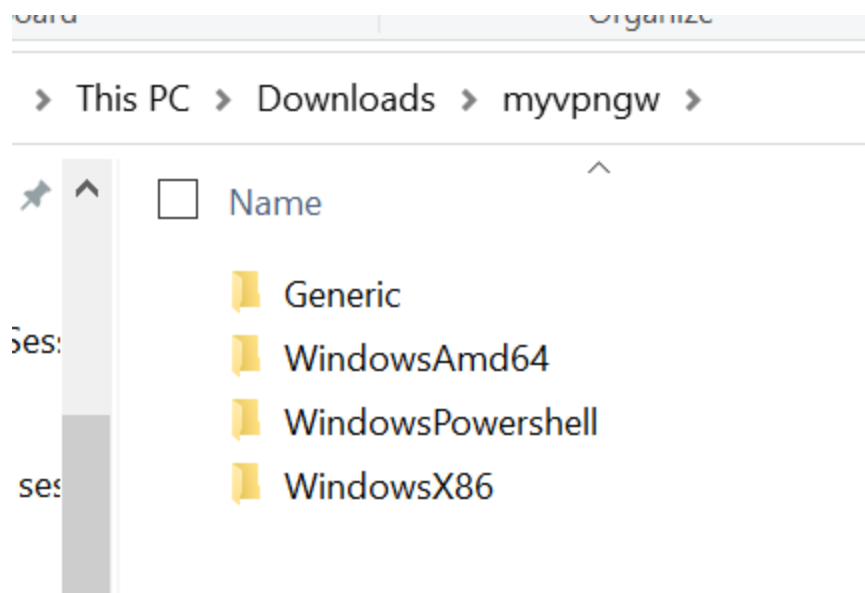


After successfully configure you can download the vpn client software as shown above

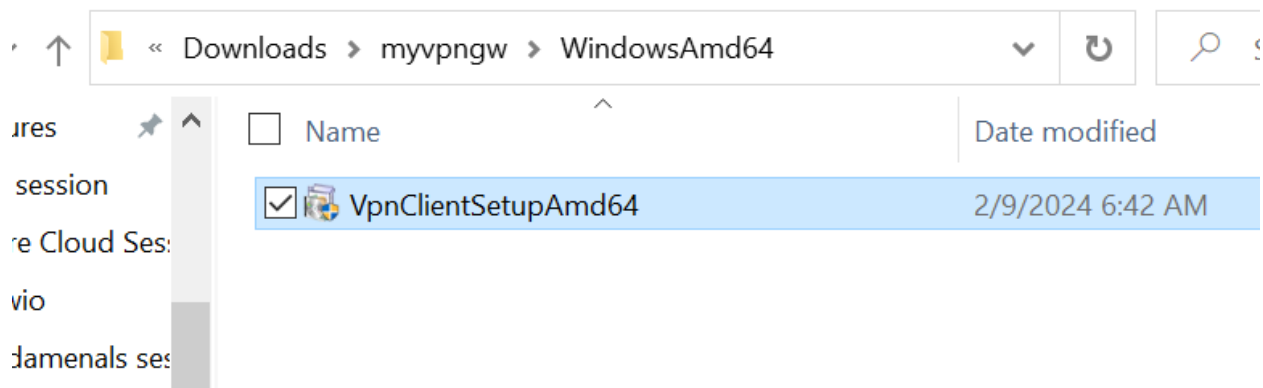
Step 8 : install the vpn client



Note : Click on Allow if not downloaded



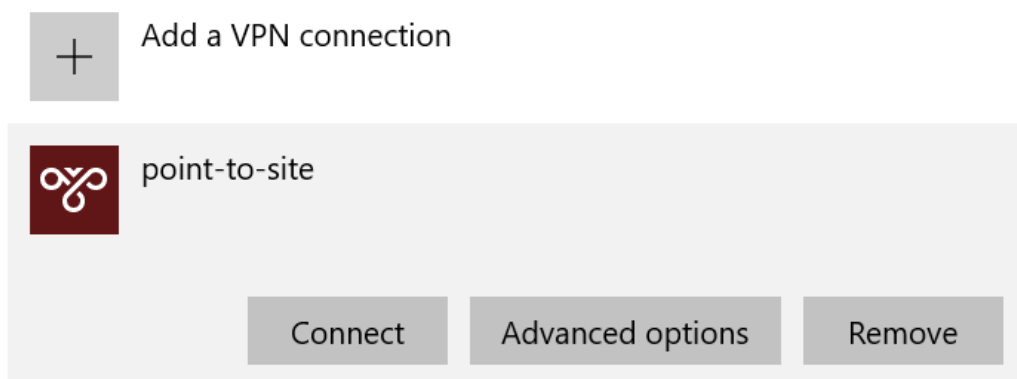
Download and extract

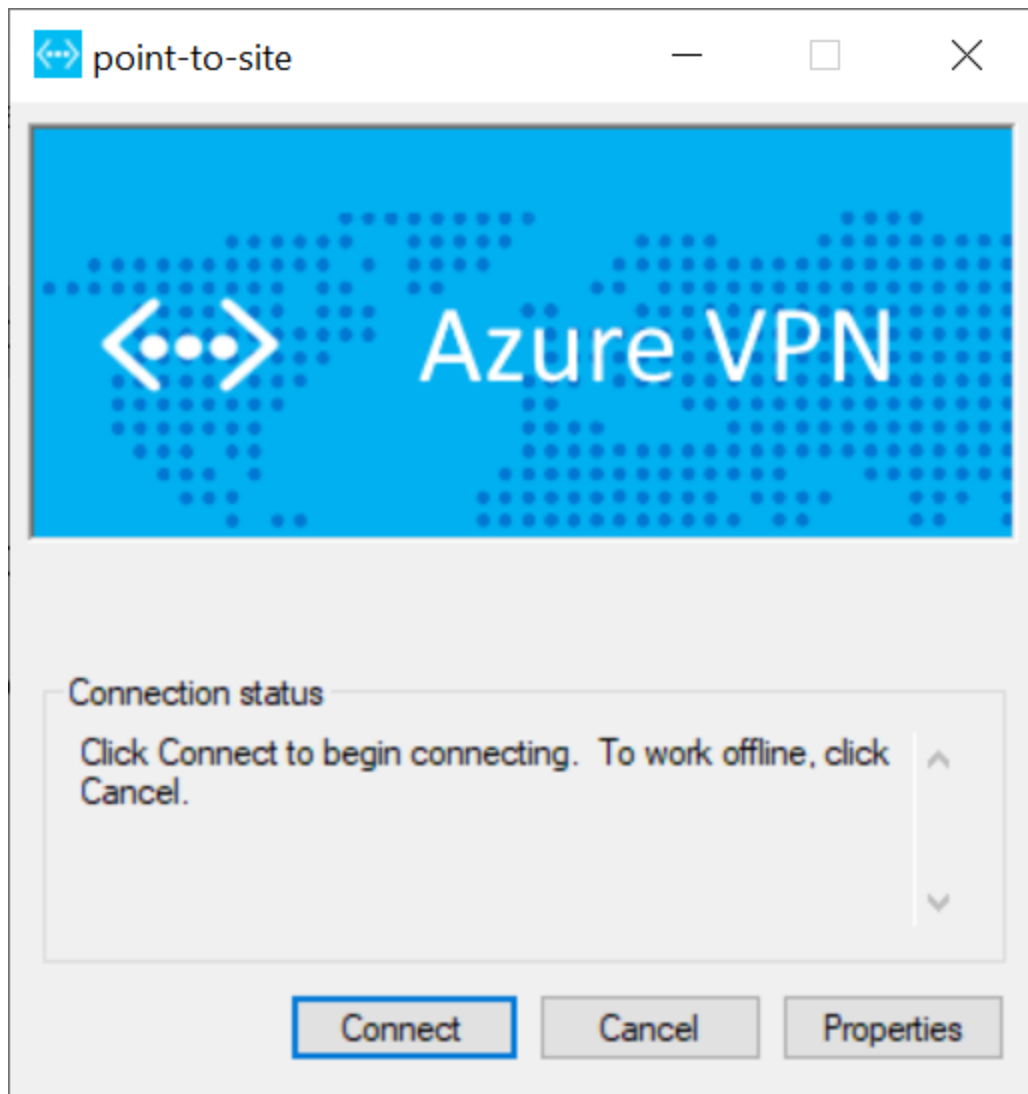


Click on wifi

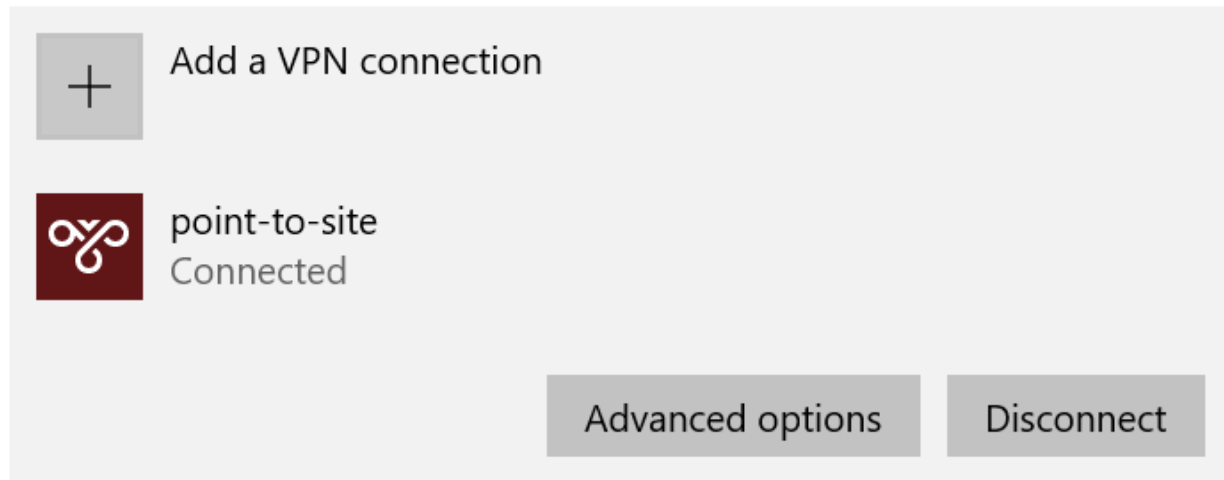
click on connect

VPN



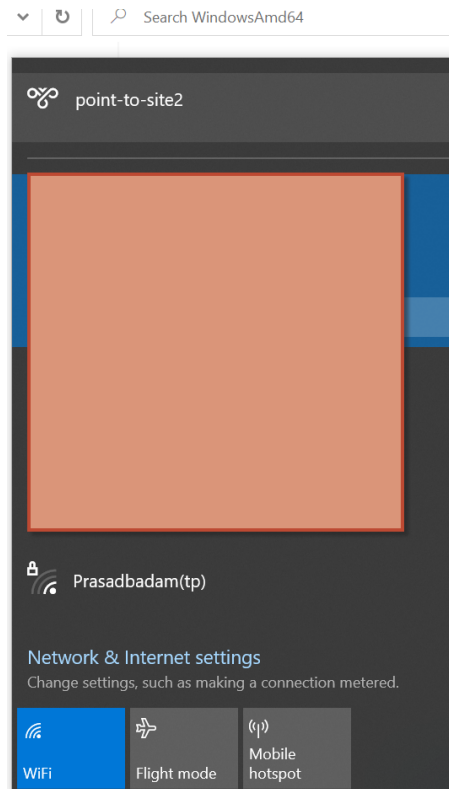


VPN

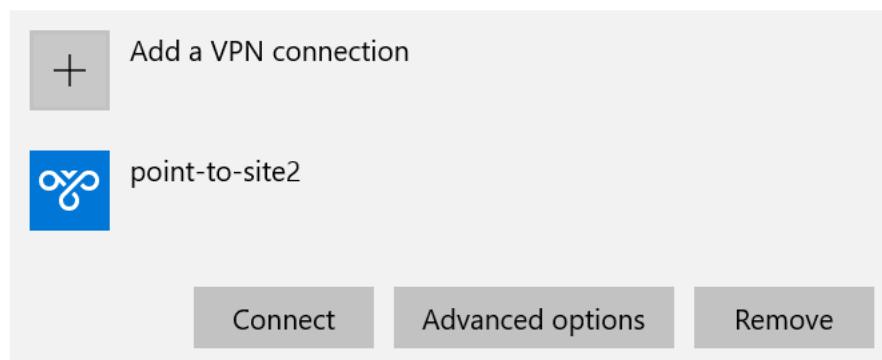


Step 9 :

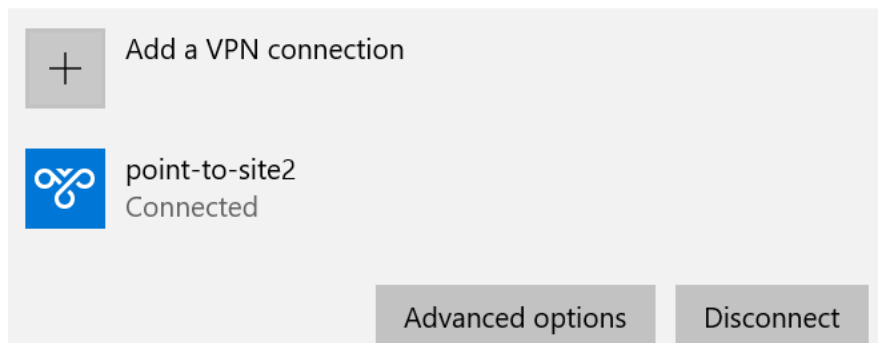
After installing you can connect to vpn



VPN

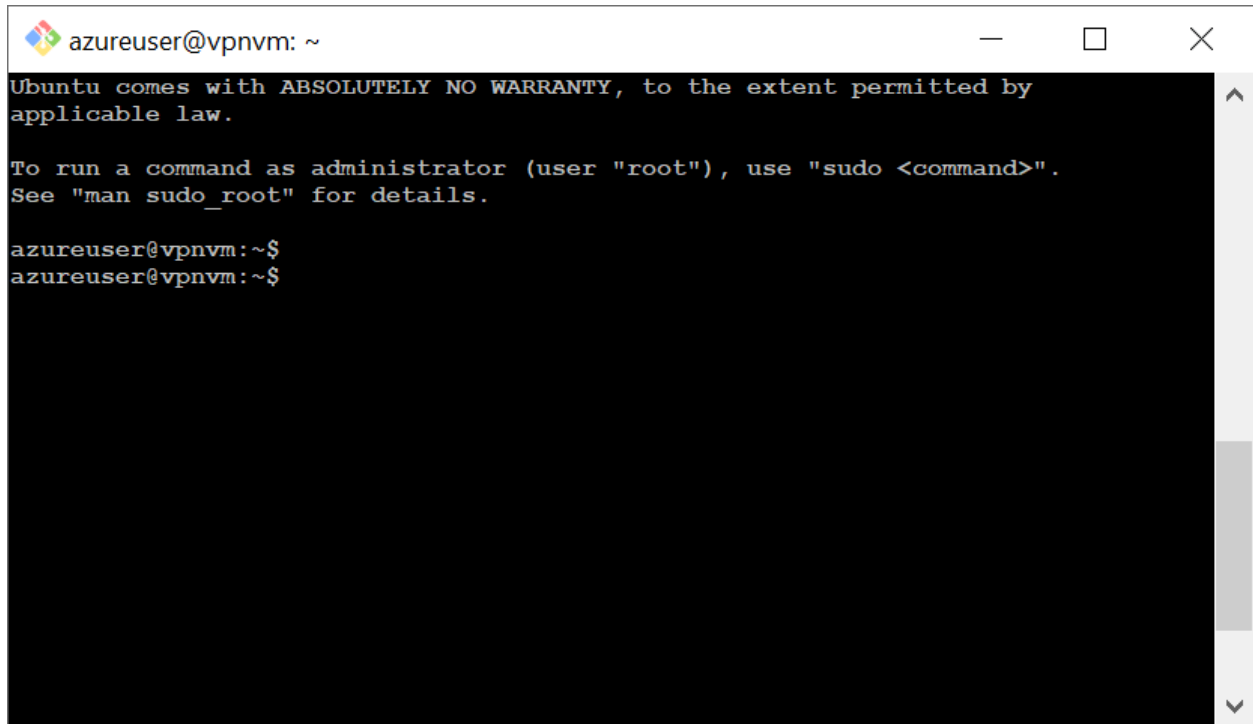


VPN



Now connect to azure vm with local IP

```
azureuser@vpnm: ~  
s  
AbdulMubeen@DESKTOP-MNV4JE1 MINGW64 /  
$ ssh azureuser@  
10.3.0.4  
  
[1]+  Stopped                  ssh azureuser@  
bash: 10.3.0.4: command not found  
  
AbdulMubeen@DESKTOP-MNV4JE1 MINGW64 /  
$ ssh azureuser@10.3.0.4  
The authenticity of host '10.3.0.4 (10.3.0.4)' can't be established.  
ED25519 key fingerprint is SHA256:YIQnVzPmEDEncv13TPv1r/hwss8jqLGkjPx5RL0W5Xo.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.3.0.4' (ED25519) to the list of known hosts.  
azureuser@10.3.0.4's password:  
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1054-azure x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/pro  
  
System information as of Fri Feb  9 06:50:27 UTC 2024
```



```
azureuser@vpnvm: ~  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
azureuser@vpnvm:~$  
azureuser@vpnvm:~$
```