😊 Point to site VPN Set Up

Azure Point-to-Site (P2S) VPN is a secure and flexible way for individual clients to connect to an Azure Virtual Network (VNet) from remote locations. It’s particularly useful for users who need to connect from different locations and devices, and it can be set up without the need for a dedicated on-premises VPN gateway. Here's an overview of how Azure P2S VPN works and how to set it up:

How Azure P2S VPN Works

1. Client Initiation: The VPN client on the user’s device initiates a connection to the Azure VPN gateway.
2. Authentication: The client uses certificates or Azure Active Directory (Azure AD) to authenticate.
3. VPN Tunnel: Once authenticated, a secure VPN tunnel is established between the client and the Azure VPN gateway.
4. Network Access: Through this tunnel, the client can securely access resources within the Azure VNet.

Features of Azure P2S VPN

1. Secure Communication: Uses SSL/TLS protocols for secure communication.
2. Authentication Options: Supports native Azure AD, RADIUS, or certificate-based authentication.
3. Device Compatibility: Works with Windows, macOS, Linux, iOS, and Android.
4. Scalability: Easily scales to support multiple connections without requiring extensive hardware investments.

Setting Up Azure P2S VPN

Prerequisites

1. An Azure subscription.
2. A configured Azure VNet.
3. A VPN gateway created for the VNet.
4. Steps to Configure Azure P2S VPN

Create a Virtual Network Gateway:

1. In the Azure portal, go to "Create a resource".
2. Search for "Virtual Network Gateway" and click "Create".
3. Configure the settings, such as gateway type (VPN), VPN type (Route-based), and SKU (based on performance requirements).

Configure Point-to-Site VPN:

1. Once the gateway is created, navigate to it in the Azure portal.
2. Under "Settings", select "Point-to-site configuration".

3. Configure the address pool (the range of IP addresses that will be assigned to clients), tunnel type (IKEv2, SSTP, or OpenVPN), and authentication type (Azure AD, RADIUS, or certificates).

Generate VPN Client Configuration Files:

1. After configuring the Point-to-Site settings, generate the VPN client configuration package.
2. This package contains the necessary information for clients to establish a VPN connection.

Distribute VPN Client Configuration:

1. Download the configuration package and distribute it to your users.
2. Users install the VPN client and configuration on their devices.

Connect to the VPN:

- Users open the VPN client and establish a connection to the Azure VPN gateway using their credentials (depending on the authentication method chosen).

Authentication Methods

1. Azure Certificate Authentication: Requires generating and uploading a root certificate to Azure. Users are provided with a client certificate derived from the root certificate for authentication.
2. Azure Active Directory Authentication: Users authenticate using their Azure AD credentials. This method simplifies management, especially for organizations using Azure AD.
3. RADIUS Authentication: Integrates with existing on-premises RADIUS server for authentication. Suitable for organizations that want to leverage their existing RADIUS infrastructure.

Benefits of Azure P2S VPN

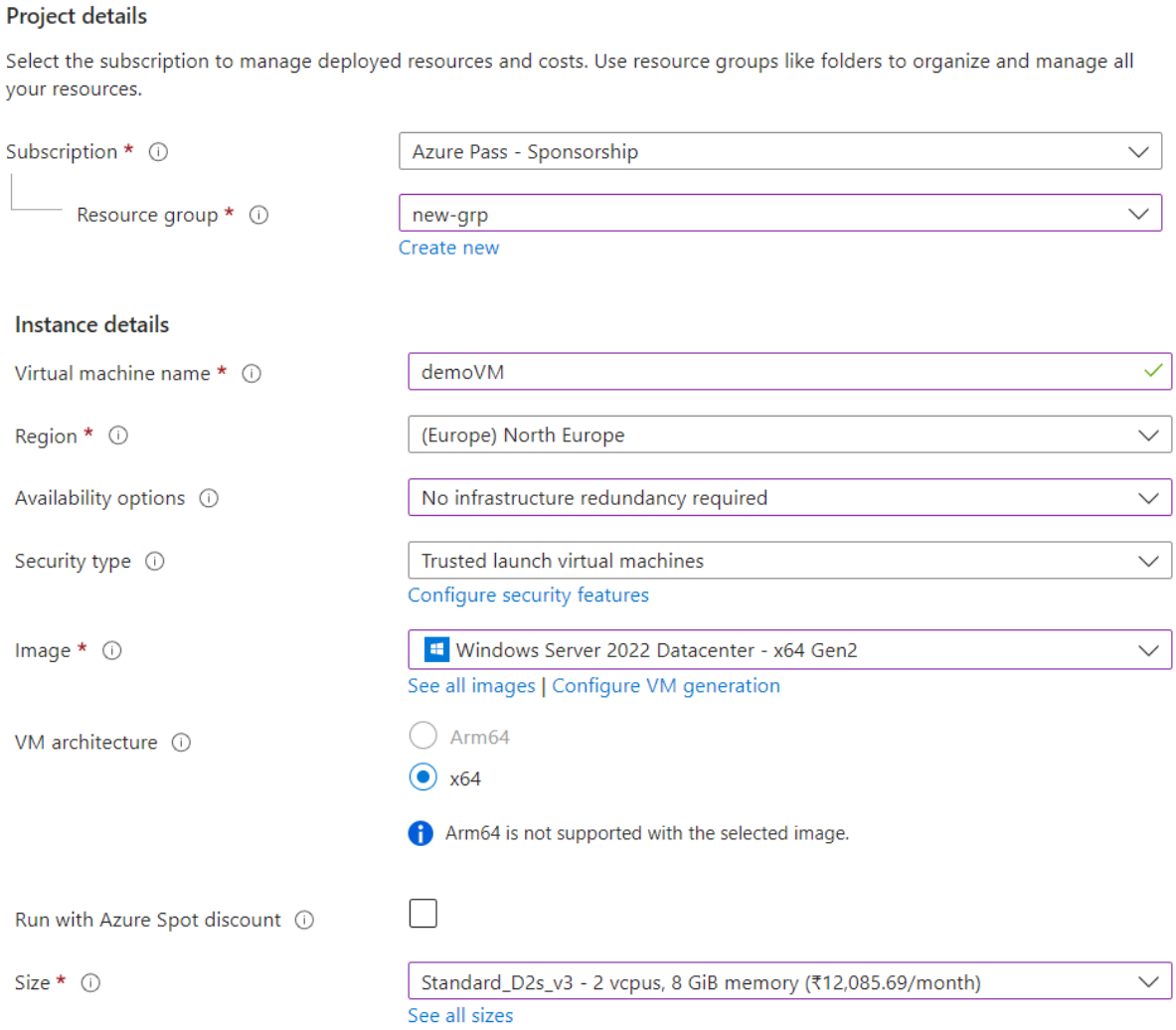
1. **Flexibility:** Users can connect from any location with internet access.
2. **Security:** Securely connects remote users to Azure resources.
3. **Scalability:** Easily scales to accommodate more users.
4. **Integration:** Seamless integration with Azure AD and existing infrastructure.
5. Troubleshooting Tips
6. **Connection Issues:** Ensure the VPN client is correctly configured and the address pool is not exhausted.
7. **Authentication Failures:** Verify that certificates are correctly installed and valid, or that Azure AD credentials are correct.
8. **Network Access Problems:** Check network security group (NSG) rules and routing configurations within the VNet.

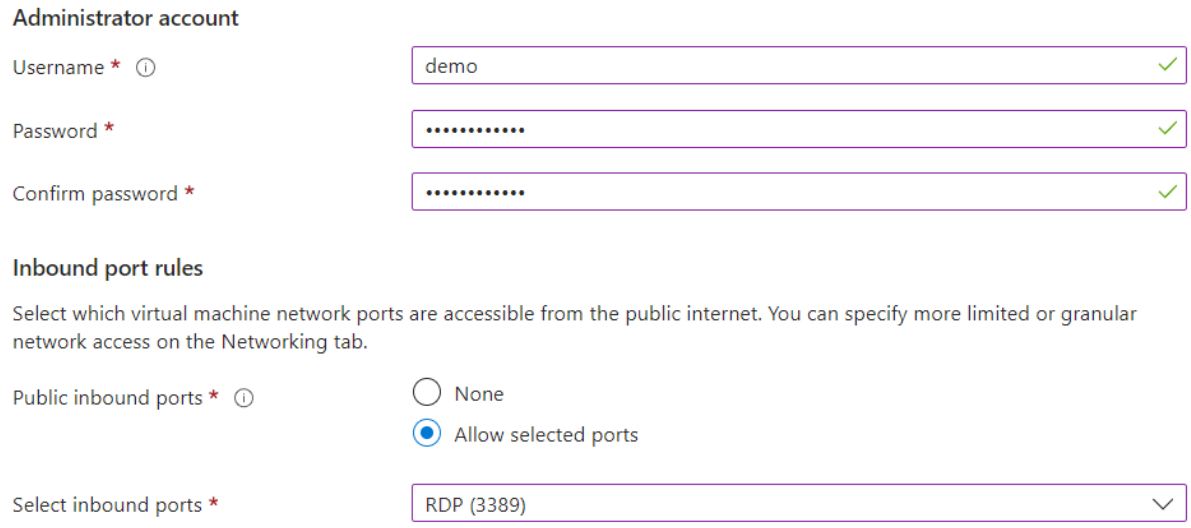
Azure Point-to-Site VPN is a powerful solution for providing secure remote access to Azure VNets. By following the configuration steps and understanding the features and benefits, organizations can effectively manage remote connectivity for their users.

The end goal is to securely connect a remote client to an Azure Virtual Network using a Point-to-Site VPN, allowing access to resources within the VNet, such as the web server on the VM. This setup demonstrates secure remote connectivity and resource access without needing a public IP address.

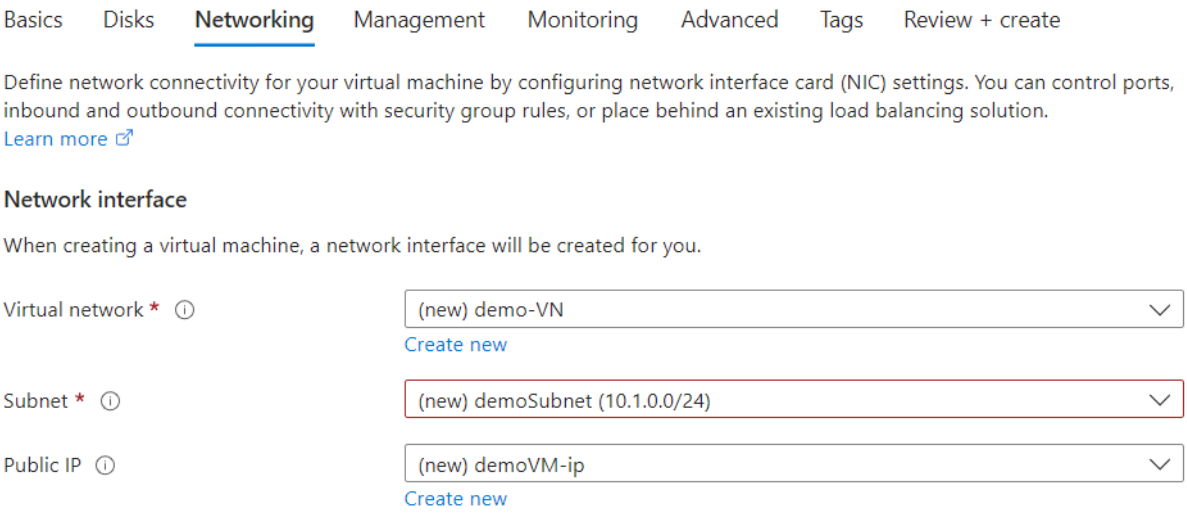
😄 To begin with the Lab:

1. First, we are going to launch a virtual machine based on Windows Server 2022 and install a Web Server (IIS) on it. With that, we also want to create a HTML page so that we can identify the VM for ourselves.

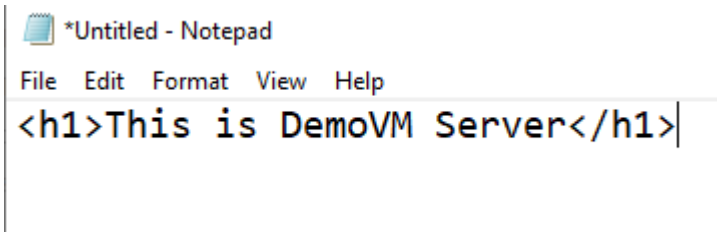


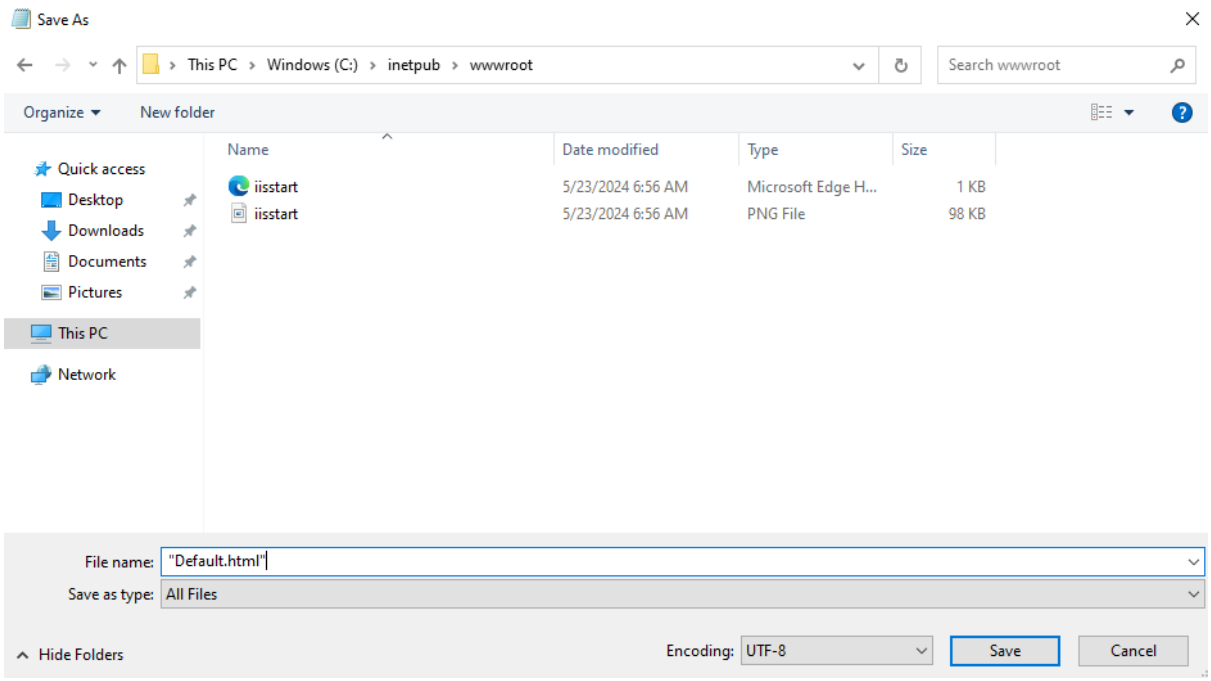


2. Now in the Networking create a new Virtual Network and choose to public IP so that we can configure our VM by logging in to it.

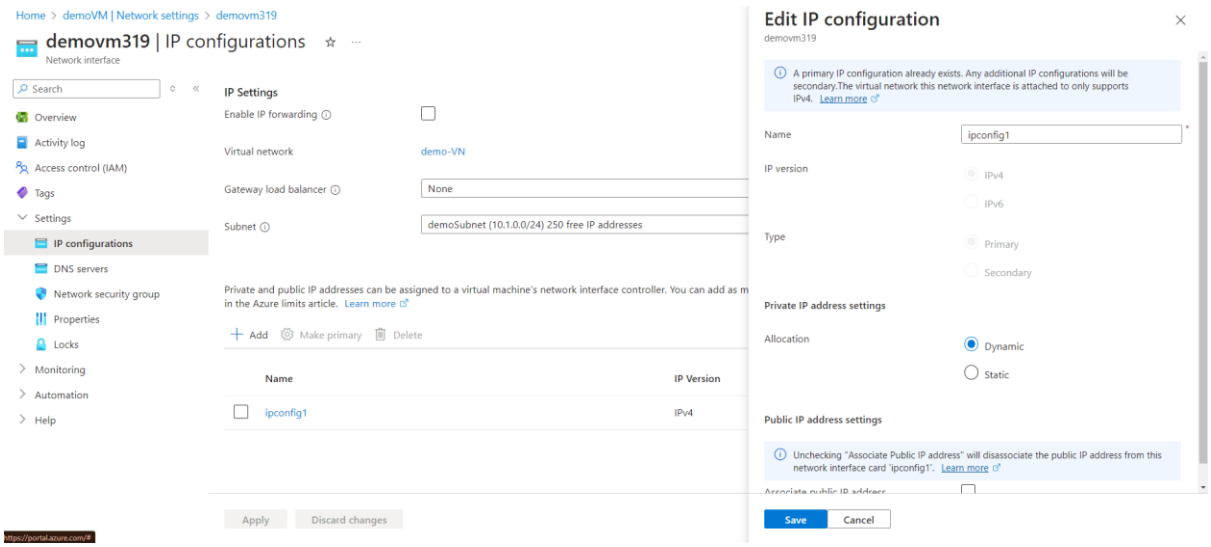


3. After that move to the Review page and Create your Virtual Machine.
4. Once the deployment is complete then you need to login to your VM and install Web Server on it.
5. Once the web server is installed then you need to create a default.html page at this location shown below.



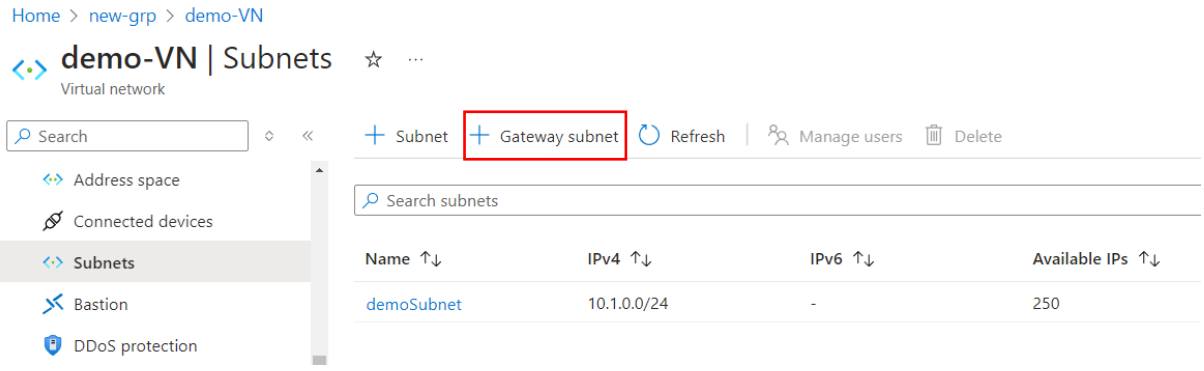


6. Once you have done this now you are going to remove the Public IP address from this demo VM and delete the Public IP address from your resources.
7. For that go to Network Interface of Demo VM and then go to IP configuration and disassociate the Public IP address. After that go to resources and delete the Public IP.

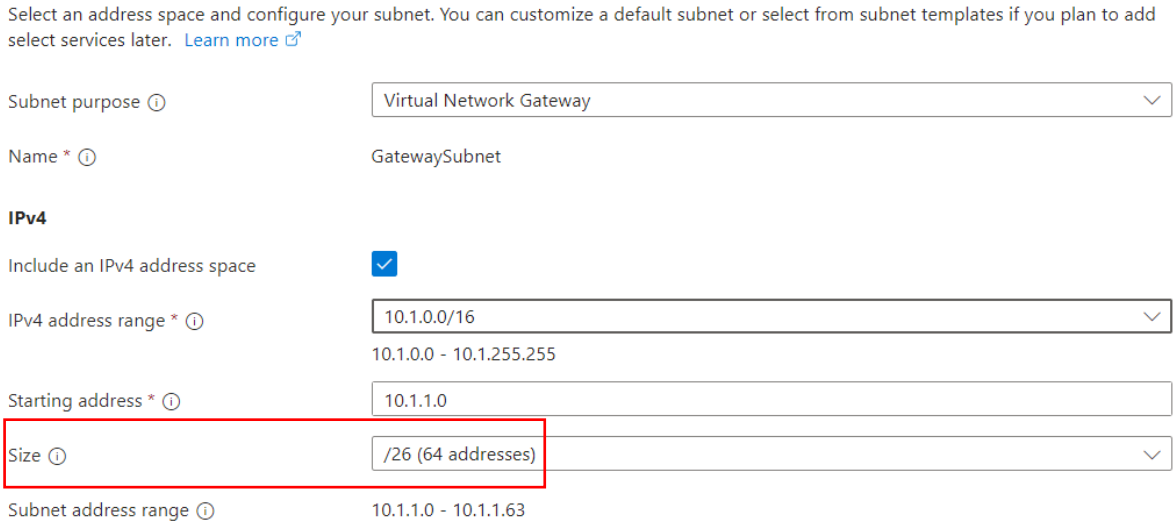


😊 Setting Up the Gateway

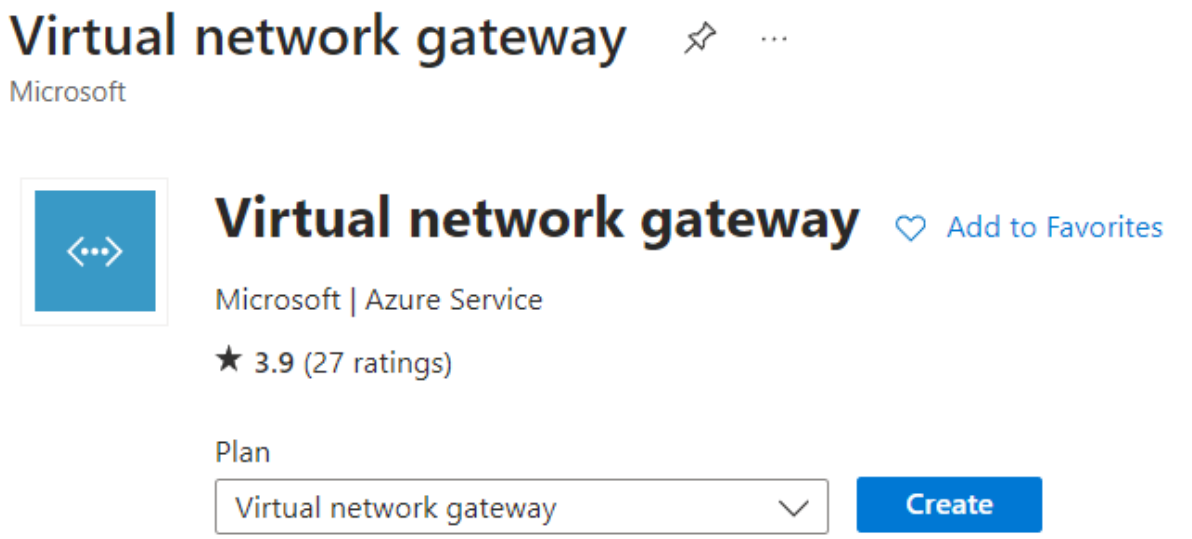
1. In this lab, we are going to deploy our VPN gateway. This will be the entry point for the clients onto the virtual network.
2. To have the VPN gateway in place we need to have an empty subnet. This is known as the gateway subnet.
3. Go to the virtual network and then go to subnets, there is a direct option to create Gateway subnet. Click on it.



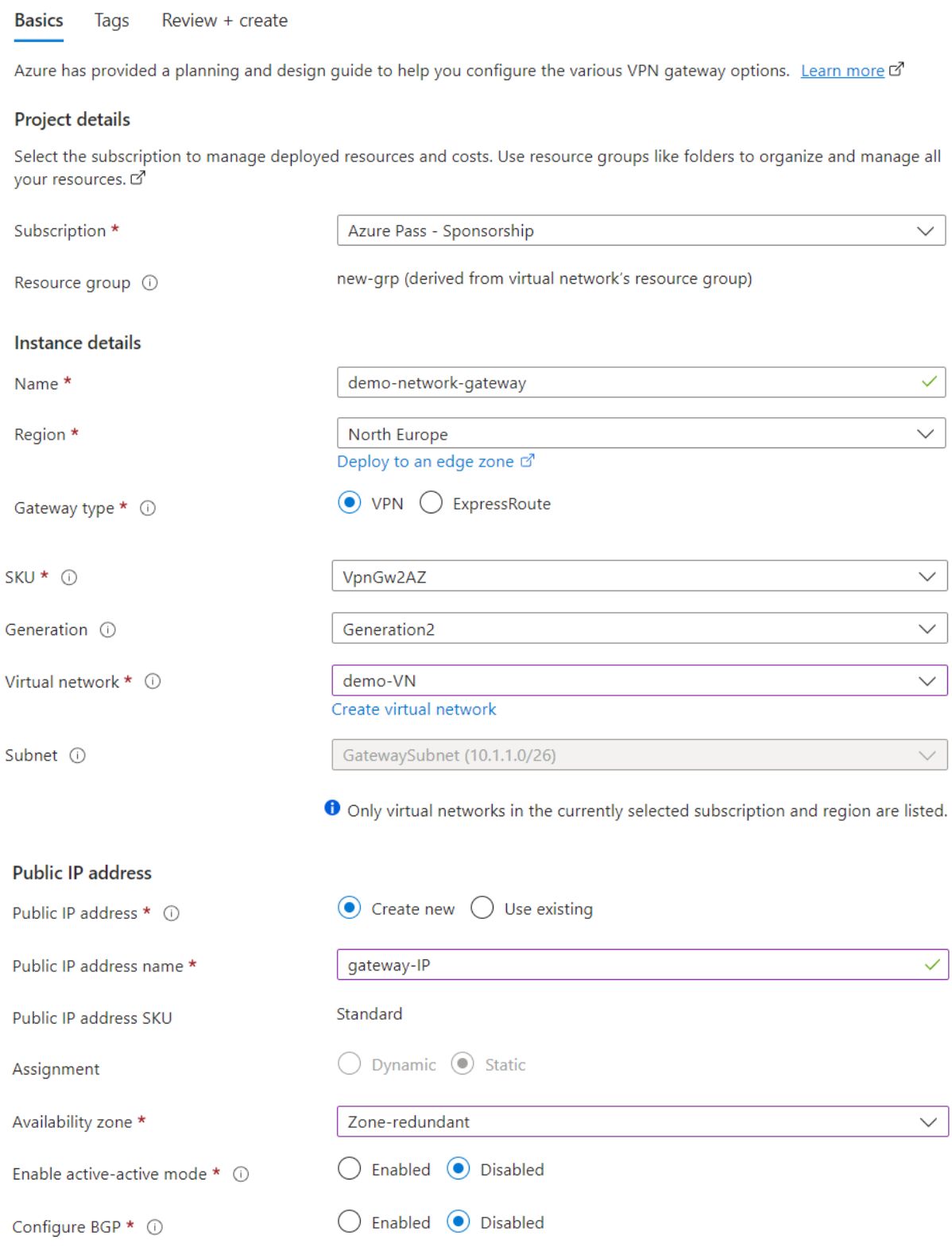
4. Then while creating it you need to change the size to /26.



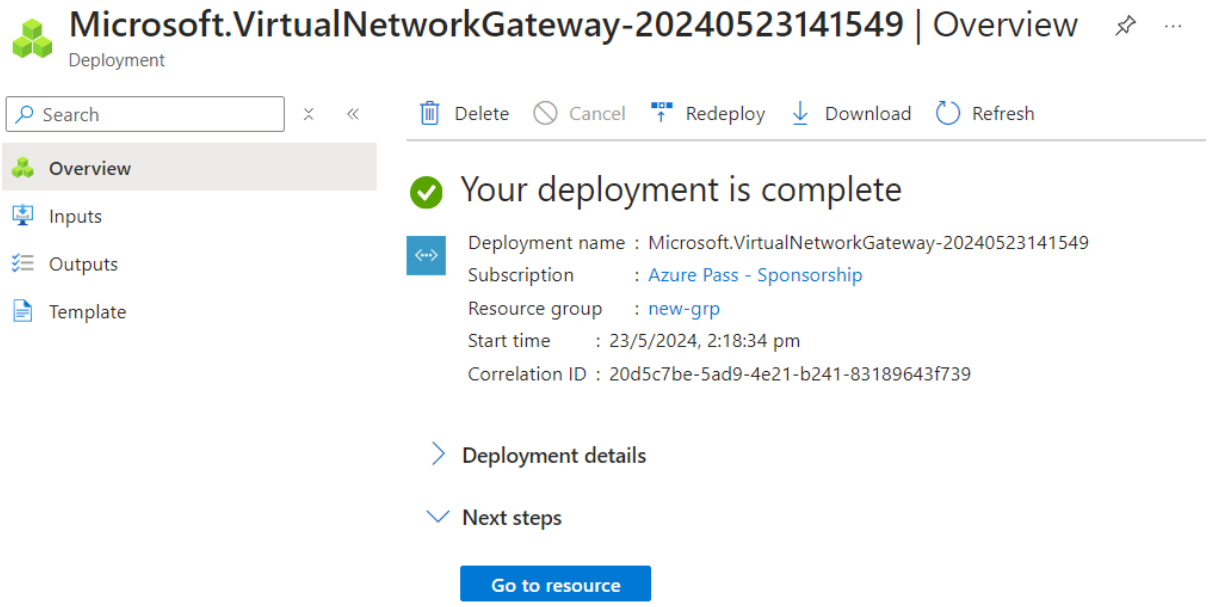
5. After that you have to go to the marketplace and search for virtual network gateway and choose this service accordingly.



6. Then you must follow the snapshots below to create your gateway.

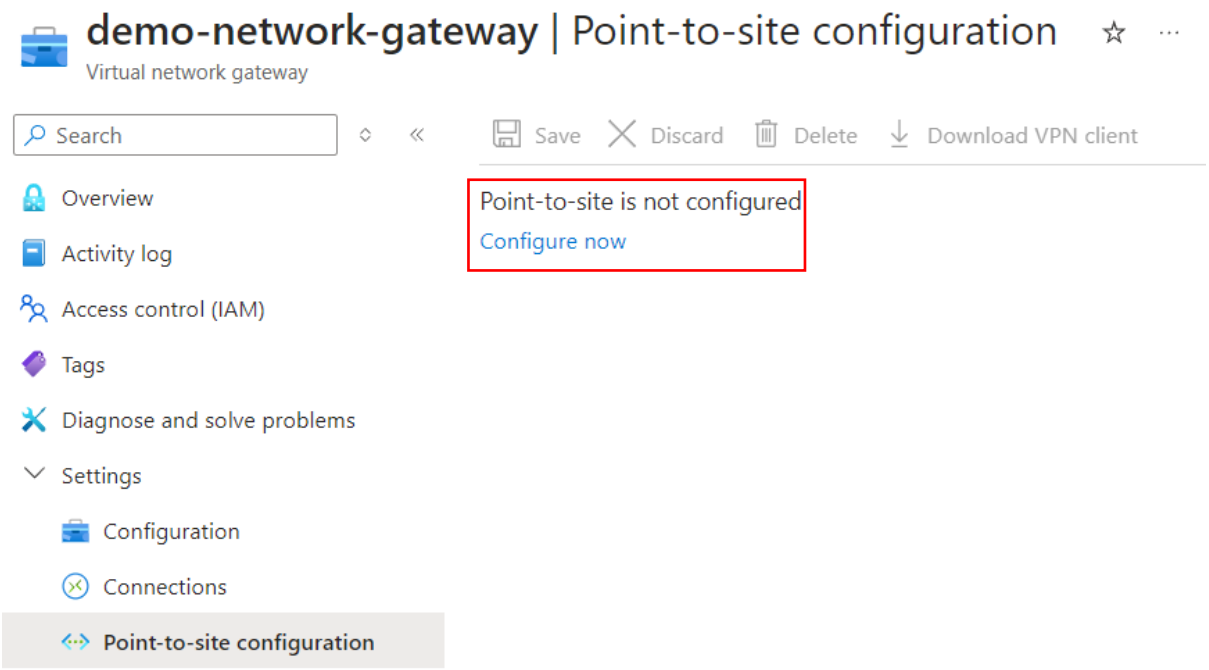


7. After that move to the review page and create your gateway. Now this will take time at least 30-40 minutes.
8. Below you can see that the deployment is completed.

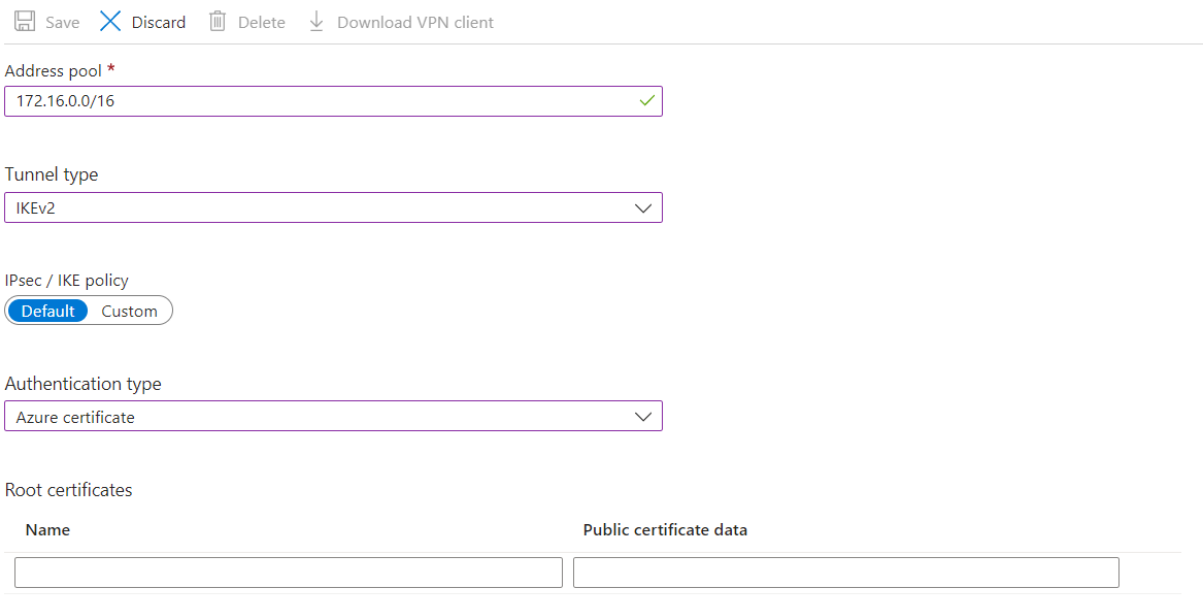


😊 Certificate for Authentication

1. Now you need to go to Virtual Network Gateway and then go to Point to site configuration then click on configure now.



2. Now here you have to write a private address pool as shown below and choose the tunnel type as IKEv2, then you have to choose the authentication type as Azure certificate.

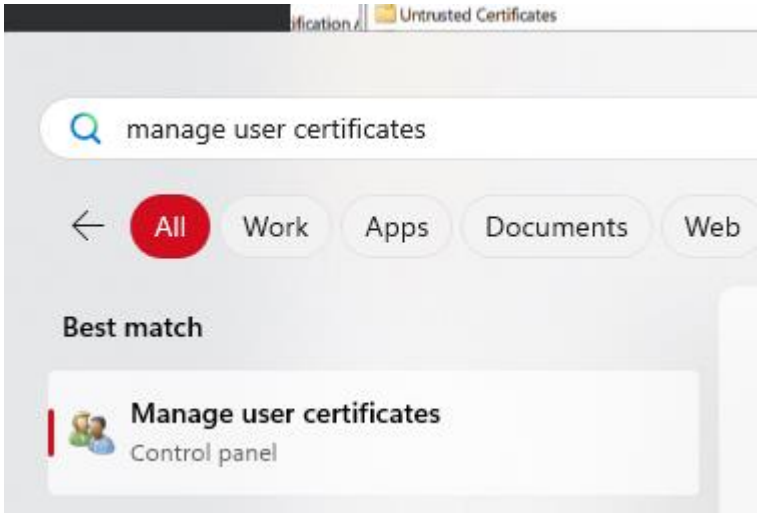


3. Now we need to create a certificate on our local machine or say our laptop. For that, you need to visit the site mentioned below, copy the script, and paste it into your PowerShell.

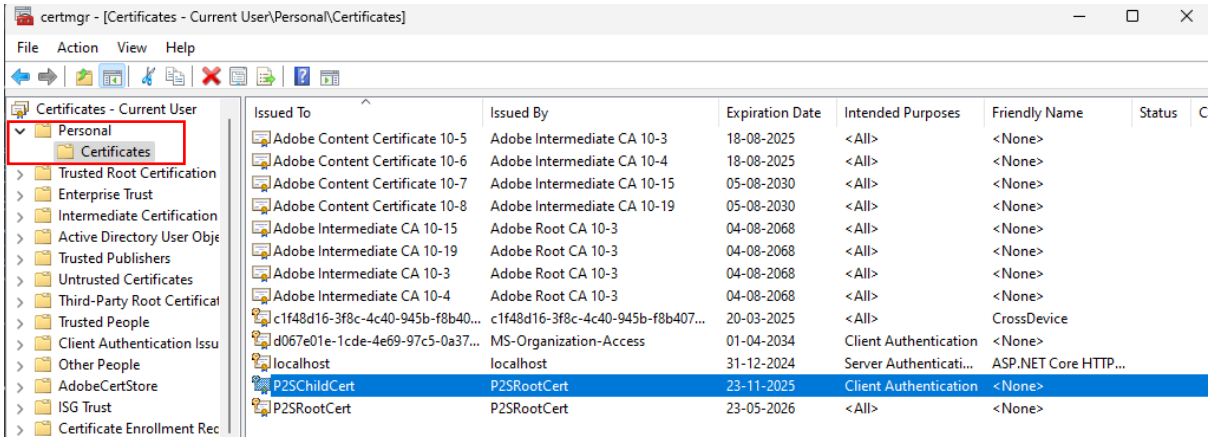
   https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site
4. First, from this website you are going to copy the certificate for root and then the certificate for the child.
5. Below you can see the snapshot of how it will look when you will paste the script.

```
Windows PowerShell
PS C:\Users\PULKIT> $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'
>> }
PS C:\Users\PULKIT> $cert = New-SelfSignedCertificate @params
PS C:\Users\PULKIT> $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')
>>     }
PS C:\Users\PULKIT>     New-SelfSignedCertificate @params


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

Thumbprint                                Subject
----------                                -------
CCFB694159E08B8B28696A42A0F463848F0A0A98  CN=P2SChildCert
```

6. If you want to see these certificates then you need to search for manage user certificates on your local machine and open it.



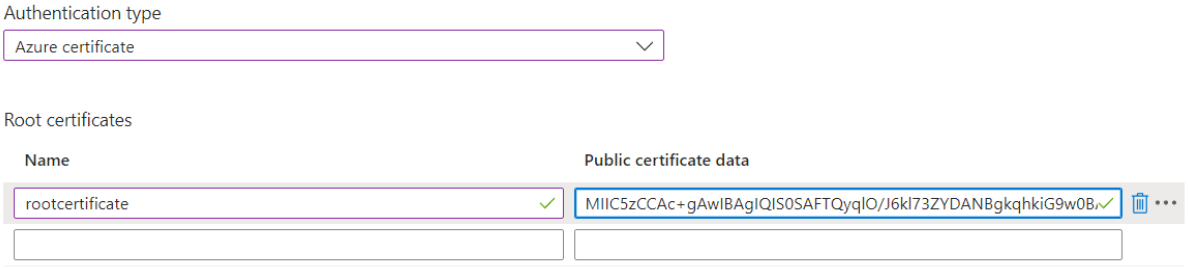
7. There you need to expand personal and then click on certificates. You will see your certificates.



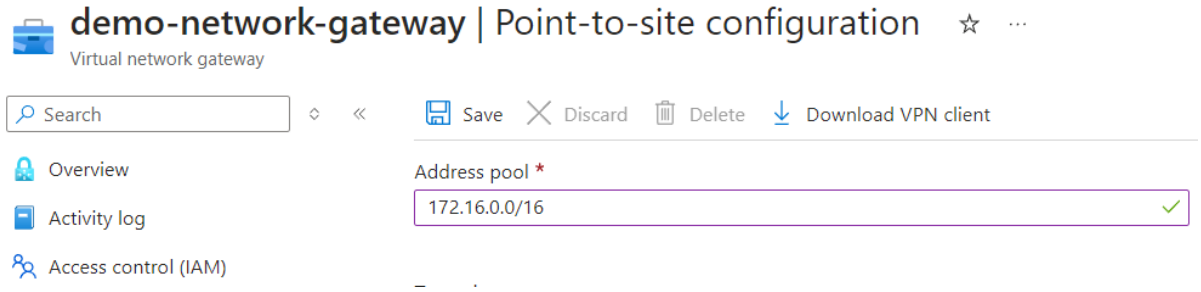
8. We now need to export this root certificate so that we can paste its contents onto our point-to-site VPN connection. I will right-click on the root certificate, choose all tasks, and choose the export option.
9. Follow the below steps to export the root certificate.
10. **I will right-click on the root certificate, choose all tasks, and choose the export option. In the Wizard I'll click on next. I'll say not to export the private key. Click on next. I'll choose Base64 encoded. Click on Next. I'll just browse, so I'll just save this.**
11. Now we need to copy the data from our root certificate and paste it in Point to site configuration. For that right click on your certificate and choose to open it in notepad.
12. Then you just need to copy the highlighted text as shown below and paste it in point to site configuration.

```
-----BEGIN CERTIFICATE-----
MIIC5zCCAc+gAwIBAgIQIS0SAFTQyqlO/J6kl73ZYDANBgkqhkiG9w0BAQsFADAW
MRQwEgYDVQQDDAtQMlNSb290Q2VydDAeFw0yNDA1MjMwOTIwNDlaFw0yNjA1MjMw
OTMwNDdaMBYxFDASBgNVBAMMC1AyU1Jvb3RDZXJ0MIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAraYOWG2INpwwXlzuQPfdqTk4ZKnKdN5rBnbuHYfBu5uW
3sZFoAT5CkjltGVcNkANYARXd8vHNaqNXXOkHyzQ8nuCoroSpN8iYUa6TjJ3XvI8
YDAZ/1k4t4K8WB8apRiJkiuZmuUtBpVzlGJKL/QVkKH3l1SK3Zms4effwf58oogo
pFCRABRsKC2yOXzr4Lodp6Zugj2yEdnPXxbjOW/z5zSVmgZ5fH14RNRr6b/R6sLv
COSCKD9tqSuQ2O4+xcQzjHIwT8XEJeBuVmRZ3NHUG40bCJgslTxDtT3uVssJxsPc
AOppS/rh0MV5OQTXXLa2JzDs1xMGsIHydGAE2MJAAQIDAQABozEwLzAOBgNVHQ8B
Af8EBAMCAgQwHQYDVR0OBBYEFEheZJiar0I+oYJiV7PmhFU8Q+SJMA0GCSqGSIb3
DQEBCwUAA4IBAQAGID1evsZ22QXkgqiN4YnMw4/0MTMxSl0l0ko0W90r8oZq+C2U
ZC042JKmJX19X/OOJe5NGia1Wgo3e1DrL+Vph31Tw3SFqvCStqf4uvN+5HiS4PVX
6gpfxjNGajwSpKgmmjrS3SExyYxtu/FTgYLZkEOelPH44DA+cqZ8psbLkjie0WZr
e/kA5w8WIISTYQEZzJ7xZDxuLRd1SWSKcacqNT9vic+rDCiBQDA0bhDbGboXCL+A
CtYjLZ/1hbFYwAjR87uV6qkwL30WZUtJi44epEVwccbS8hI2zgUsTRVMAROuRo4o
CH9rjex2cRCxKLnvmfybS0lYUgOudBNbrzX/
-----END CERTIFICATE-----
```

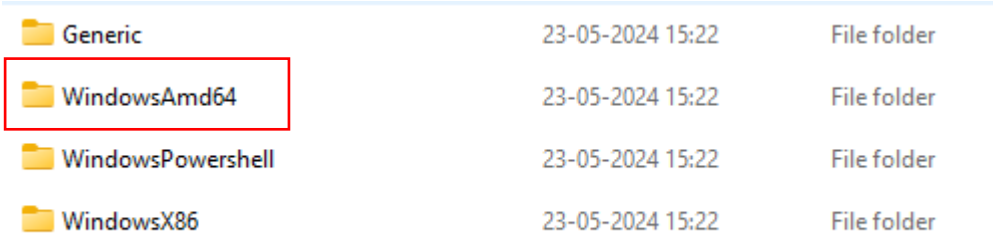
13. after that just click on save.



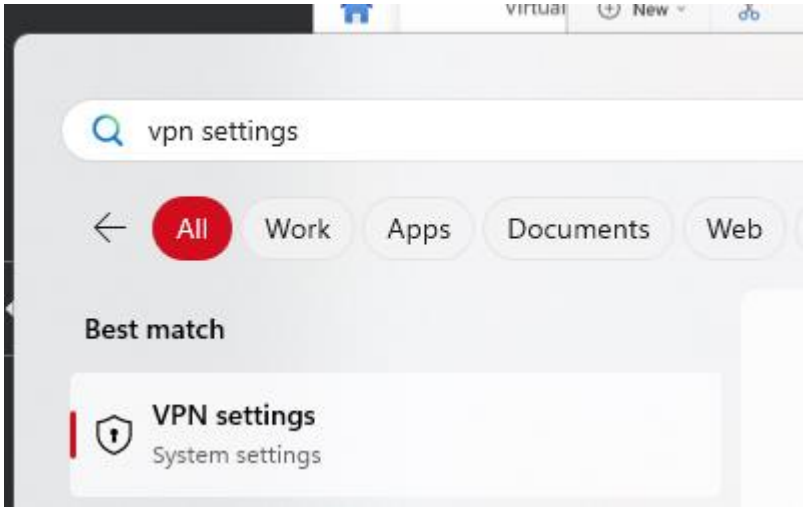
14. Once your connection is saved you will get the option to download the VPN client. You will see that a zip file has been downloaded and you have to extract it.



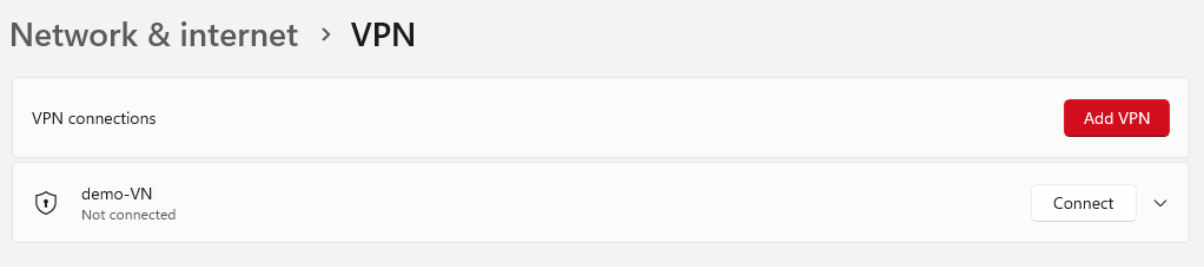
15. You will see that there are different installers in place here we have to choose Windows AMD 64.



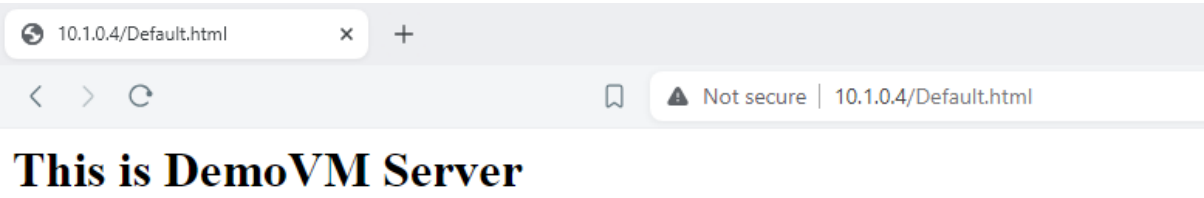
16. Then you have to install it. After that you have to search for VPN settings.



17. Here you will see that you have the option to connect with it. Click on connect.



18. Then you have to go to your VM and copy the Private IP address because we don't have the public IP.
19. You will see that your Web Server is running as expected.



20. You are connecting via the private IP address of the machine, and this is all being done. The traffic is all being routed via the virtual network Gateway.
21. Once you are done with this lab do not delete the resources.