Step-By-Step: Creating an Azure Point-to-Site VPN

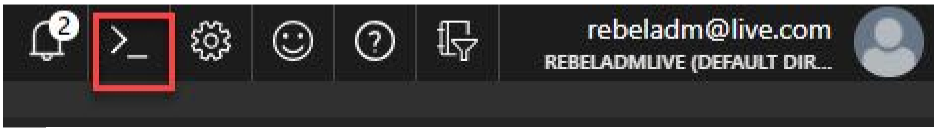
Site-to-Site VPN is the most common method organizations use to connect on-premises network to Azure vNet. This VPN connection is initiated in your edge firewall or router level. But what if you connecting from remote location such as home? We can use point-to-site method to do that. In this method it will use certificates to do the authentication between end point and azure virtual network.

So,
let's go ahead and see how we can do that,

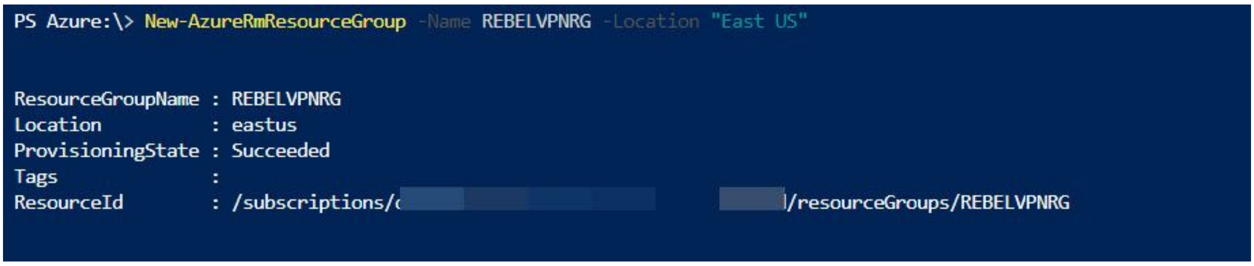
<u>Create Resource Group</u>

In this exercise, I like to use separate resource group for virtual network and other components.

1. Log in to **Azure portal** as global administrator
2. Launch Cloud Shell



1. Then run **New-AzureRmResourceGroup -Name REBELVPNRG -Location "East US".** In here **REBELVPNRG** is resource group name and **East US** is the location.



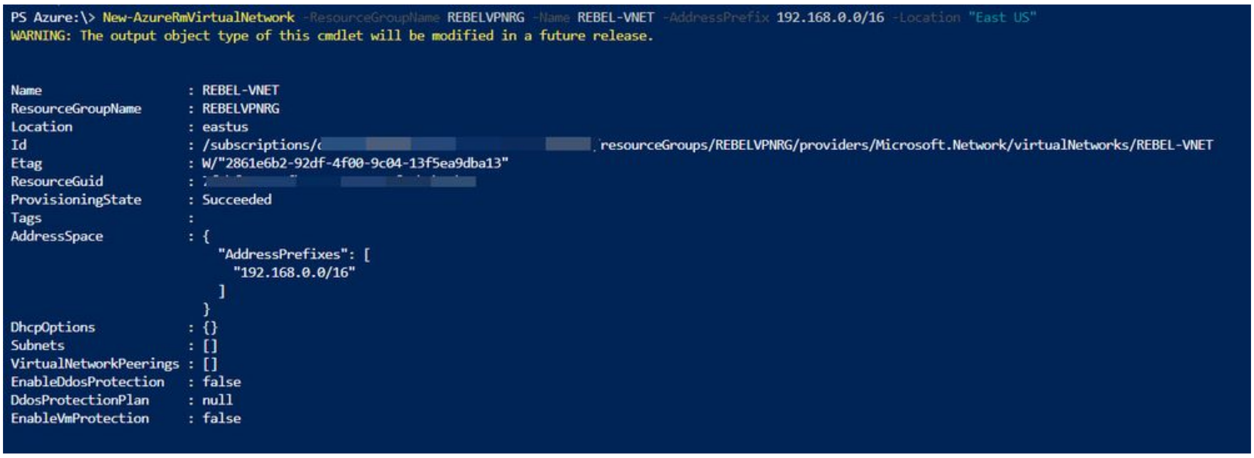
```
PS Azure:\> New-AzureRmResourceGroup -Name REBELVPNRG -Location "East US"


ResourceGroupName : REBELVPNRG
Location          : eastus
ProvisioningState : Succeeded
Tags              :
ResourceId        : /subscriptions/[redacted]/resourceGroups/REBELVPNRG
```

<u>Create Virtual Network</u>

Now we need to create new virtual network. We can create virtual network using,

New-AzureRmVirtualNetwork -ResourceGroupName REBELVPNRG -Name REBEL-VNET -AddressPrefix 192.168.0.0/16 -Location "East US"

In above, **REBEL-VNET** is the virtual network name. it uses **192.168.0.0/16** IP address range.



```
PS Azure:\> New-AzureRmVirtualNetwork -ResourceGroupName REBELVPNRG -Name REBEL-VNET -AddressPrefix 192.168.0.0/16 -Location "East US"
WARNING: The output object type of this cmdlet will be modified in a future release.


Name                   : REBEL-VNET
ResourceGroupName      : REBELVPNRG
Location               : eastus
Id                     : /subscriptions/[redacted]resourceGroups/REBELVPNRG/providers/Microsoft.Network/virtualNetworks/REBEL-VNET
Etag                   : W/"2861e6b2-92df-4f00-9c04-13f5ea9dba13"
ResourceGuid           : [redacted]
ProvisioningState      : Succeeded
Tags                   :
AddressSpace           : {
                           "AddressPrefixes": [
                             "192.168.0.0/16"
                           ]
                         }
DhcpOptions            : {}
Subnets                : []
VirtualNetworkPeerings : []
EnableDdosProtection   : false
DdosProtectionPlan     : null
EnableVmProtection     : false
```

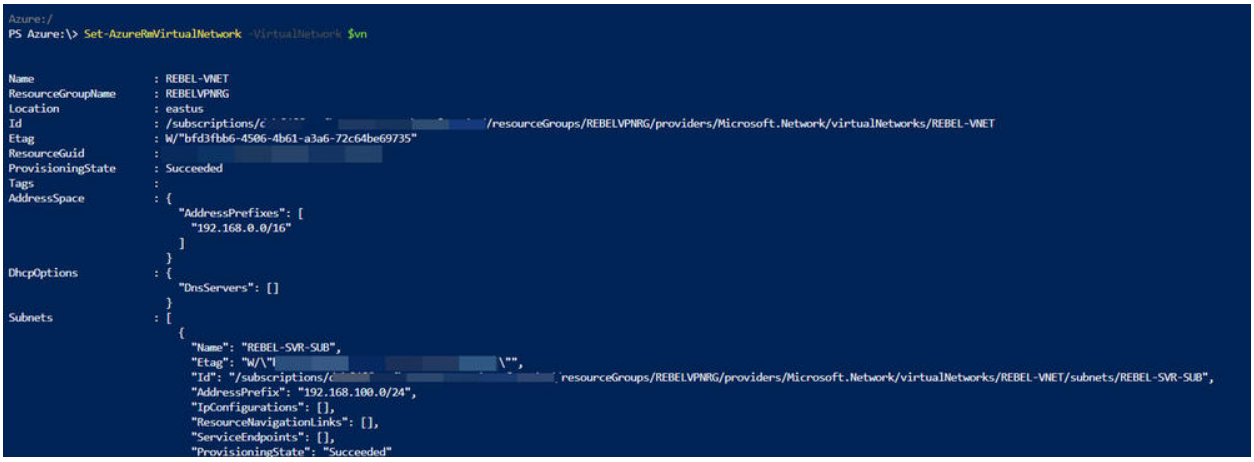
Create Subnets

Under the virtual network I am going to create a subnet for my servers. To create subnet use,

$vn = Get-AzureRmVirtualNetwork -ResourceGroupName REBELVPNRG -Name REBEL-VNET

Add-AzureRmVirtualNetworkSubnetConfig -Name REBEL-SVR-SUB -VirtualNetwork $vn -AddressPrefix 192.168.100.0/24

Set-AzureRmVirtualNetwork -VirtualNetwork $vn



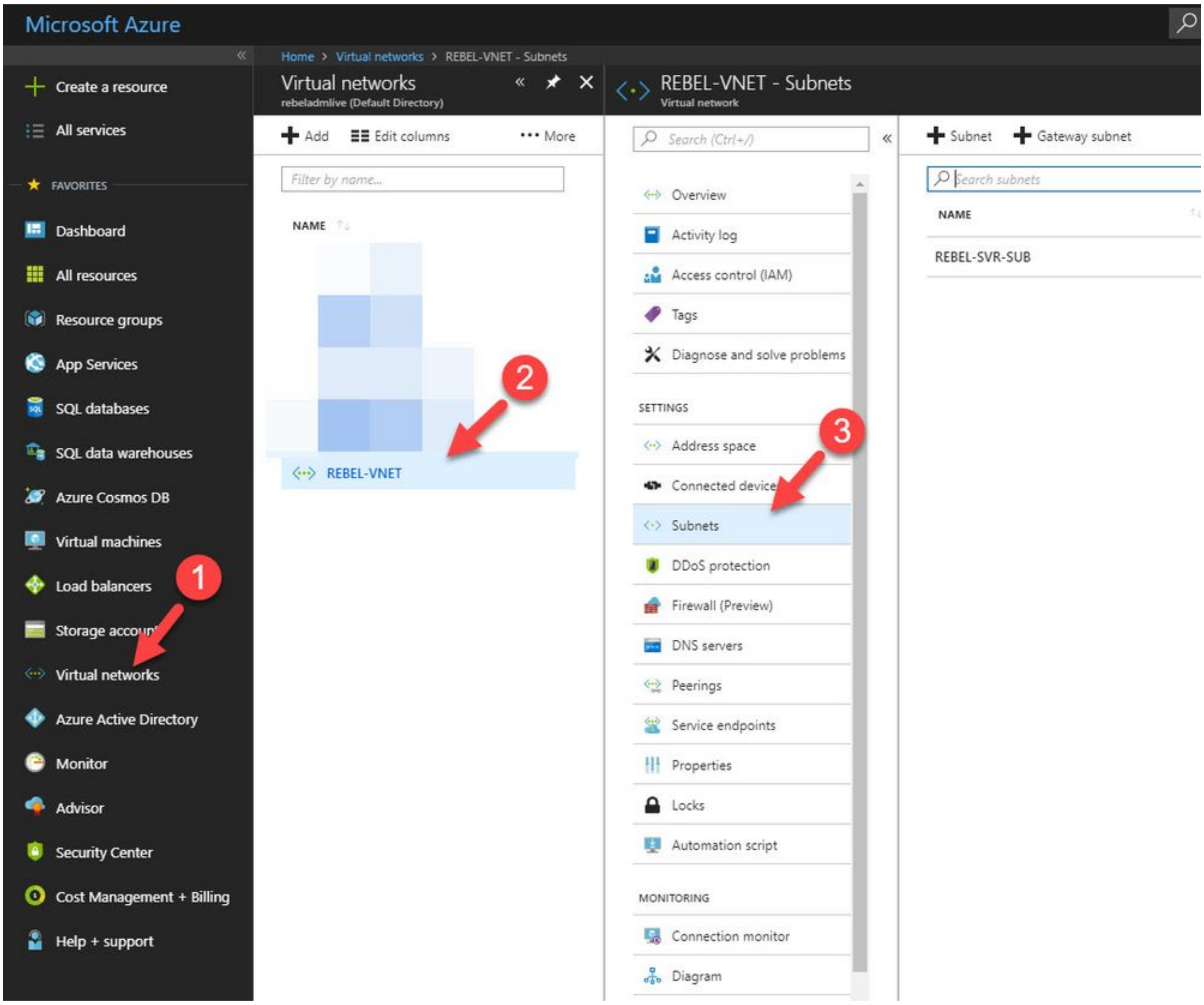
```
Azure:/
PS Azure:\> Set-AzureRmVirtualNetwork -VirtualNetwork $vn


Name                   : REBEL-VNET
ResourceGroupName      : REBELVPNRG
Location               : eastus
Id                     : /subscriptions/[redacted]/resourceGroups/REBELVPNRG/providers/Microsoft.Network/virtualNetworks/REBEL-VNET
Etag                   : W/"bfd3fbb6-4506-4b61-a3a6-72c64be69735"
ResourceGuid           : [redacted]
ProvisioningState      : Succeeded
Tags                   :
AddressSpace           : {
                           "AddressPrefixes": [
                             "192.168.0.0/16"
                           ]
                         }
DhcpOptions            : {
                           "DnsServers": []
                         }
Subnets                : [
                           {
                             "Name": "REBEL-SVR-SUB",
                             "Etag": "W/\"[redacted]\"",
                             "Id": "/subscriptions/[redacted]resourceGroups/REBELVPNRG/providers/Microsoft.Network/virtualNetworks/REBEL-VNET/subnets/REBEL-SVR-SUB",
                             "AddressPrefix": "192.168.100.0/24",
                             "IpConfigurations": [],
                             "ResourceNavigationLinks": [],
                             "ServiceEndpoints": [],
                             "ProvisioningState": "Succeeded"
```

Create Gateway Subnet

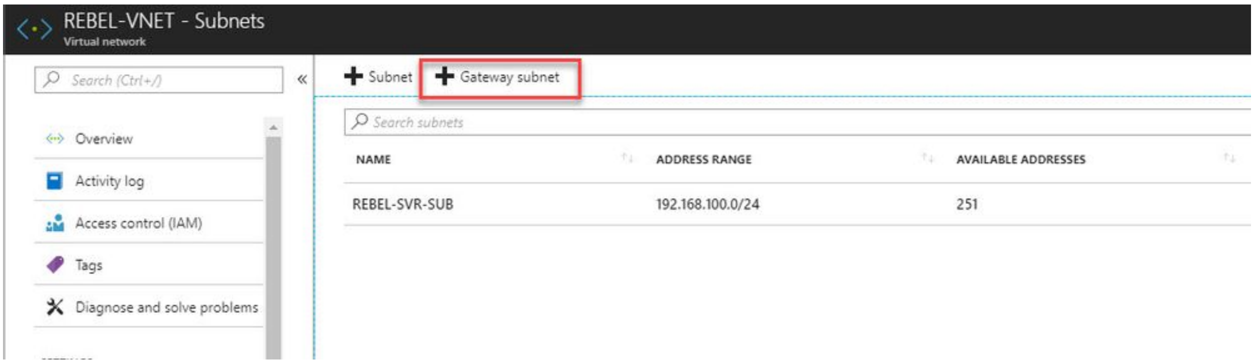
Before we create VN gateway, we need to create gateway subnet for it. so gateway will use ip addresses assigned in this subnet.

To do that,

- Log in to Azure portal as global administrator
- Go to **Virtual Networks | REBEL-VNET** (VNet created on previous steps) **| Subnets**

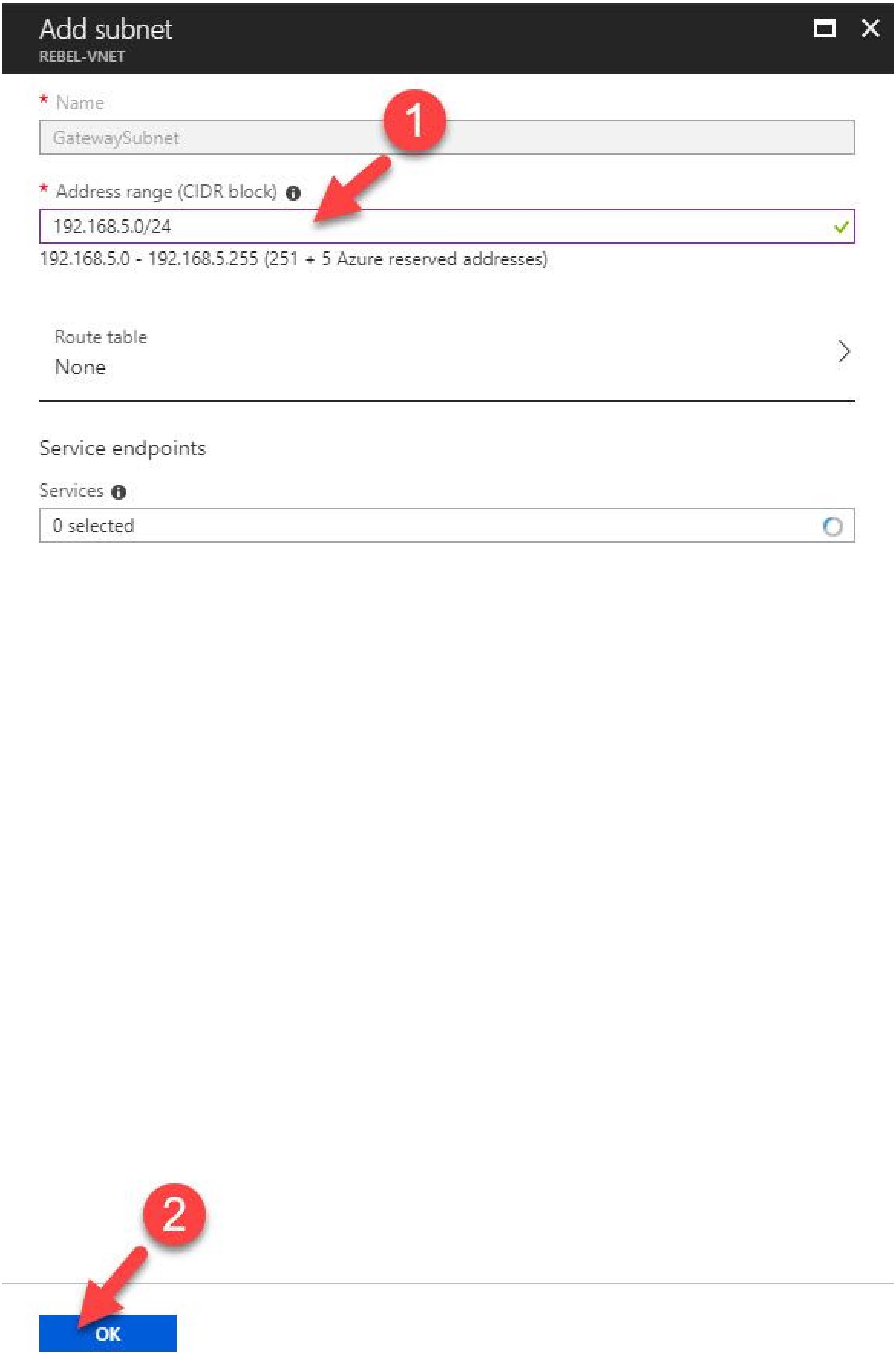


- Click on **Gateway Subnet**



NAME	ADDRESS RANGE	AVAILABLE ADDRESSES
REBEL-SVR-SUB	192.168.100.0/24	251

- In new window, define the ip range for gateway subnet and click **Ok**



Add subnet

REBEL-VNET

* Name

GatewaySubnet

* Address range (CIDR block)

192.168.5.0/24

192.168.5.0 - 192.168.5.255 (251 + 5 Azure reserved addresses)

Route table

None

Service endpoints

Services

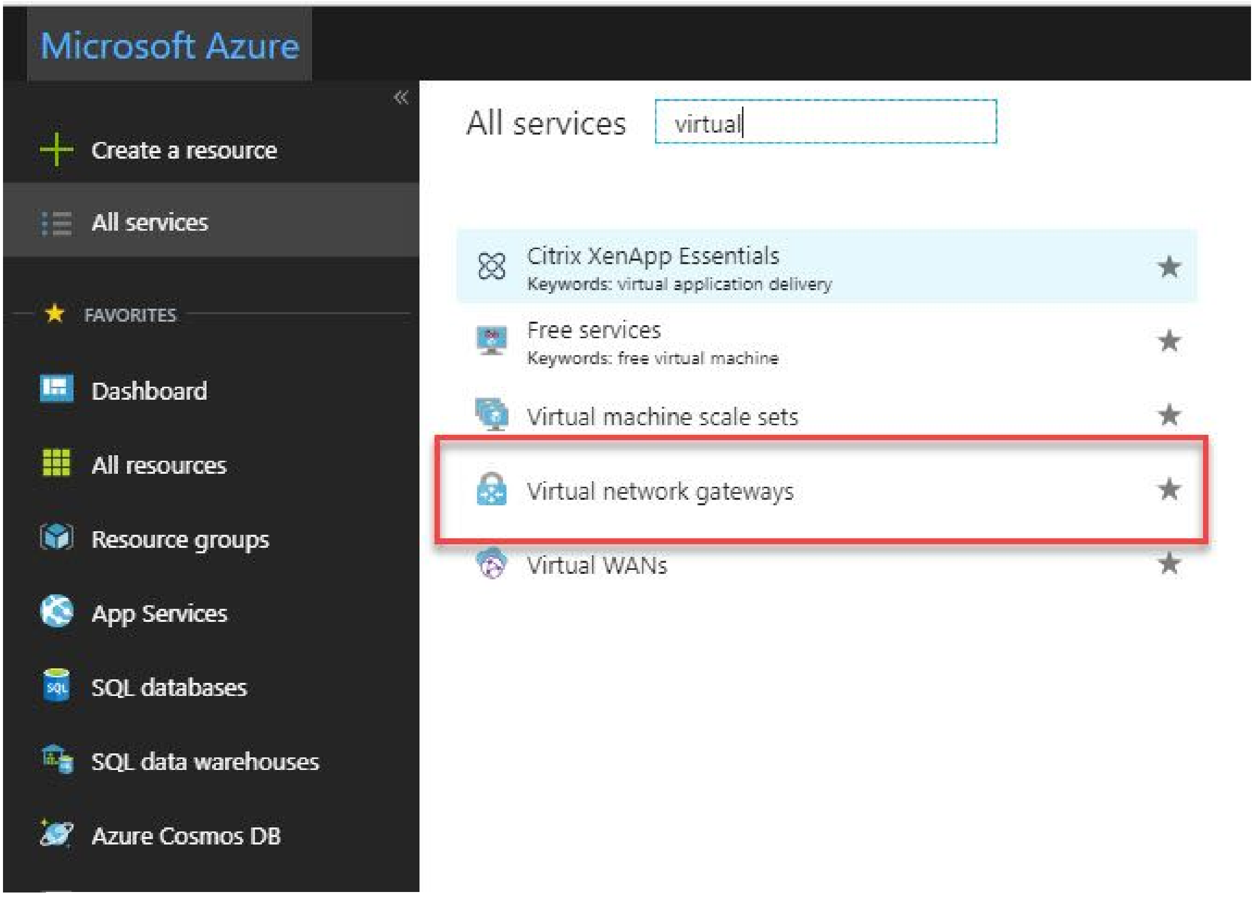
0 selected

Create Virtual Network Gateway

Now we have all the things needed to create new VN gateway. To do that,

- Log in to Azure portal as global administrator

- Go to **All Services** and search for virtual network gateway. Once it is in list, click on it.

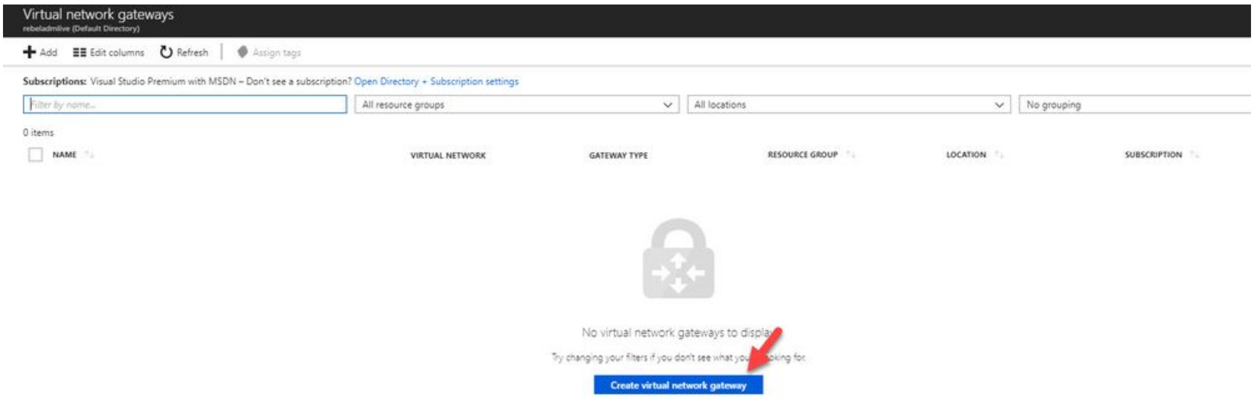


All services: virtual

Citrix XenApp Essentials — Keywords: virtual application delivery

Free services — Keywords: free virtual machine

- Then click on **Create virtual network gateway**



Subscriptions: Visual Studio Premium with MSDN – Don't see a subscription? Open Directory + Subscription settings

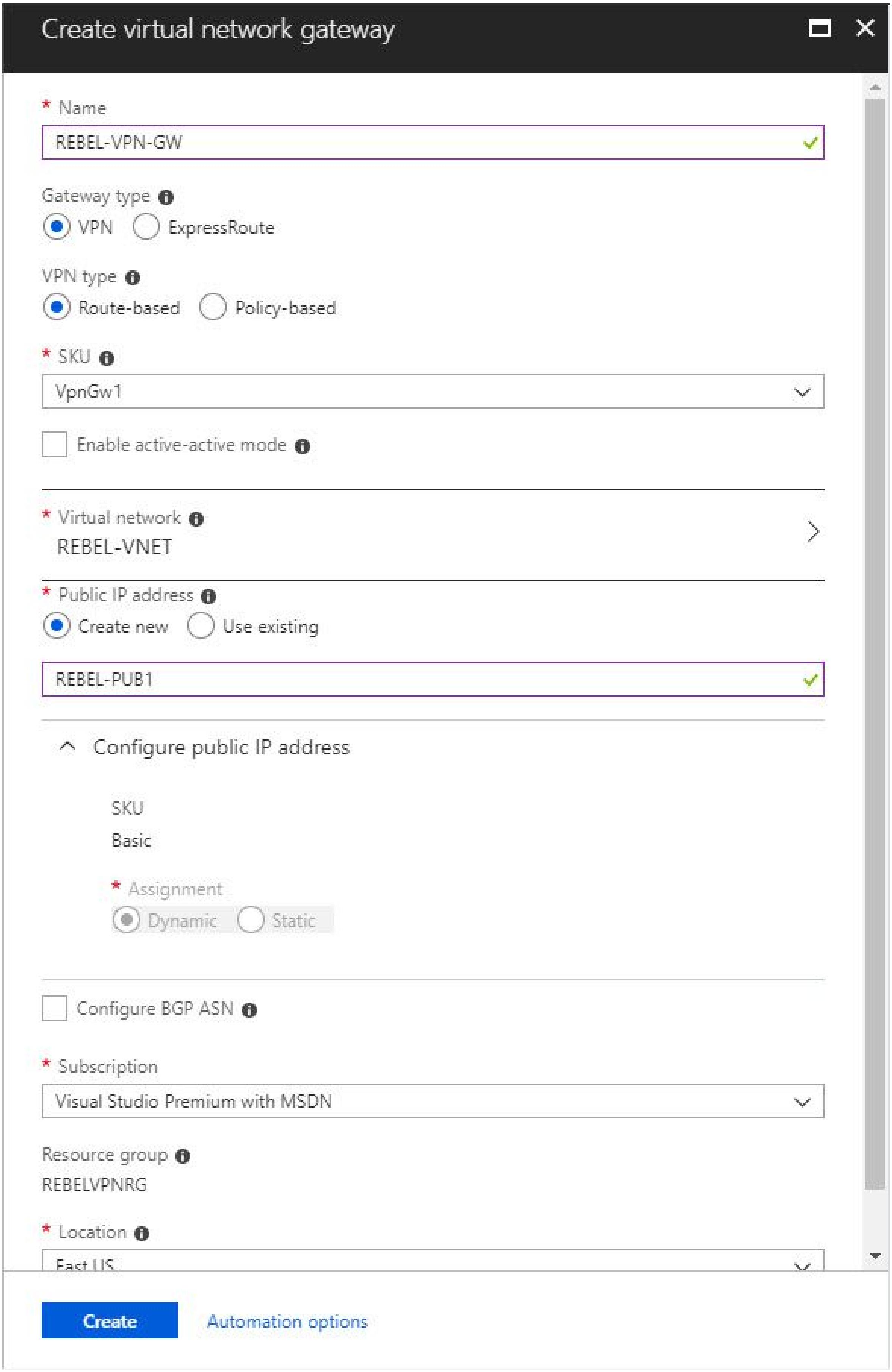
0 items

No virtual network gateways to display

Try changing your filters if you don't see what you're looking for.

- In new window fill relevant info and click on **Create**

In here, **REBEL-VPN-GW** is the gateway name. I have selected **REBEL-VNET** as the virtual network. I am also creating public ip called **REBEL-PUB1**. This is only supported with dynamic mode. This doesn't mean it is going to change randomly. It will only happen when gateway is deleted or read.



Create virtual network gateway

* Name

REBEL-VPN-GW ✓

Gateway type

● VPN ○ ExpressRoute

VPN type

● Route-based ○ Policy-based

* SKU

VpnGw1

□ Enable active-active mode

* Virtual network

REBEL-VNET

* Public IP address

● Create new ○ Use existing

REBEL-PUB1 ✓

Configure public IP address

SKU

Basic

* Assignment

● Dynamic ○ Static

□ Configure BGP ASN

* Subscription

Visual Studio Premium with MSDN

Resource group

REBELVPNRG

* Location

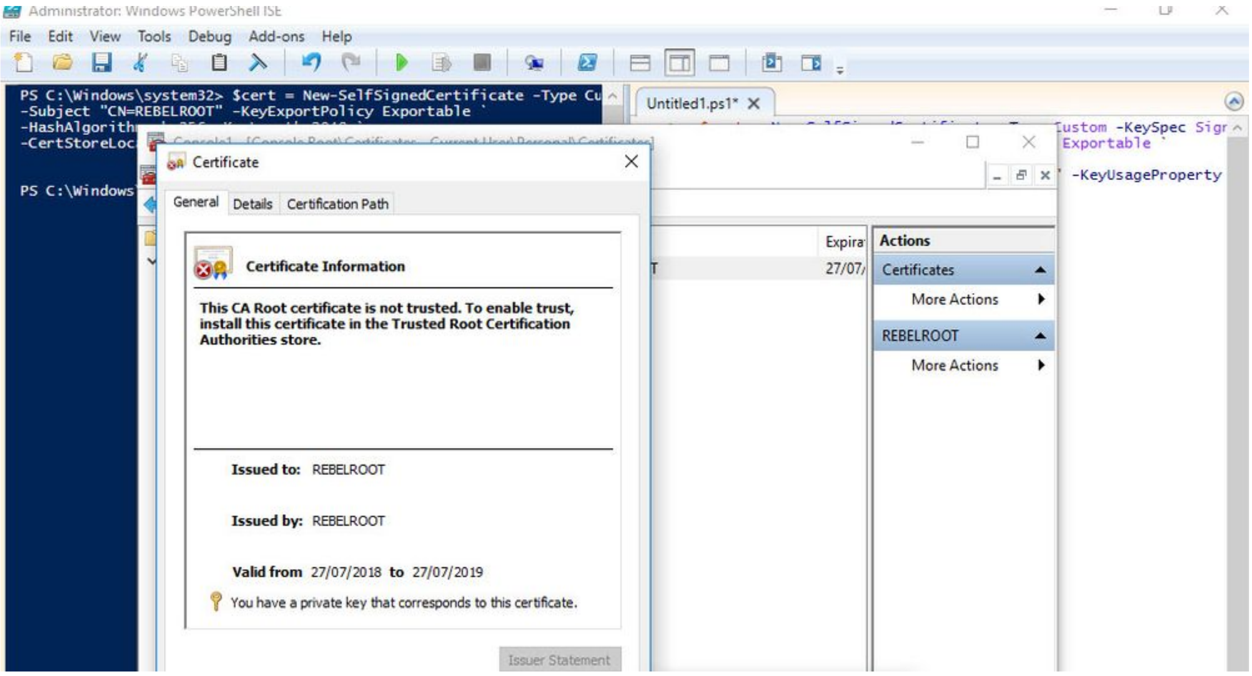
East US

Create Self-sign root & client certificate

If your organization using internal CA, you always can use it to generate relevant certificates for this exercise. If you do not have internal CA, we still can use self-sign certs to do the job.
As first step I am going to create root certificate. In Windows 10 machine I can run this to create root cert first.

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

This will create root cert and install it under current user cert store.



```
PS C:\Windows\system32> $cert = New-SelfSignedCertificate -Type Cu
-Subject "CN=REBELROOT" -KeyExportPolicy Exportable `
-HashAlgorith
-CertStoreLoc

PS C:\Windows
```

```
ustom -KeySpec Sigr
Exportable `
` -KeyUsageProperty
```

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: REBELROOT

Issued by: REBELROOT

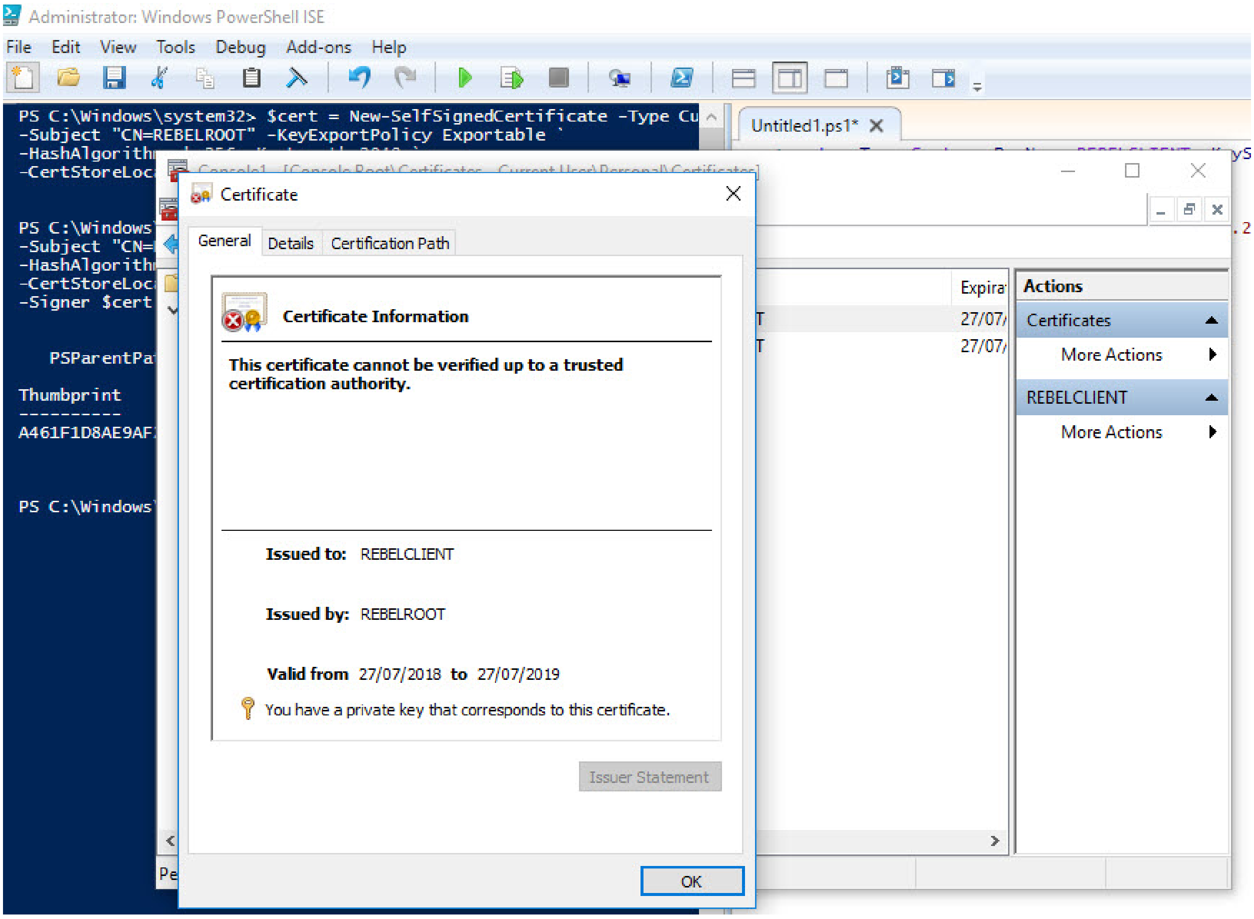
Valid from 27/07/2018 **to** 27/07/2019

You have a private key that corresponds to this certificate.

Then we need to create client certificate. We can do this using

```
New-SelfSignedCertificate -Type Custom -DnsName REBELCLIENT -KeySpec Signature `
-Subject "CN=REBELCLIENT" -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")
```

This will create cert called **REBELCLIENT** and install in same store location.



```
PS C:\Windows\system32> $cert = New-SelfSignedCertificate -Type Cu
-Subject "CN=REBELROOT" -KeyExportPolicy Exportable `
-HashAlgorith
-CertStoreLoc


PS C:\Windows
-Subject "CN=
-HashAlgorith
-CertStoreLoc
-Signer $cert


   PSParentPa

Thumbprint
----------
A461F1D8AE9AF


PS C:\Windows
```

Certificate

General | Details | Certification Path

Certificate Information

This certificate cannot be verified up to a trusted certification authority.

Issued to: REBELCLIENT

Issued by: REBELROOT

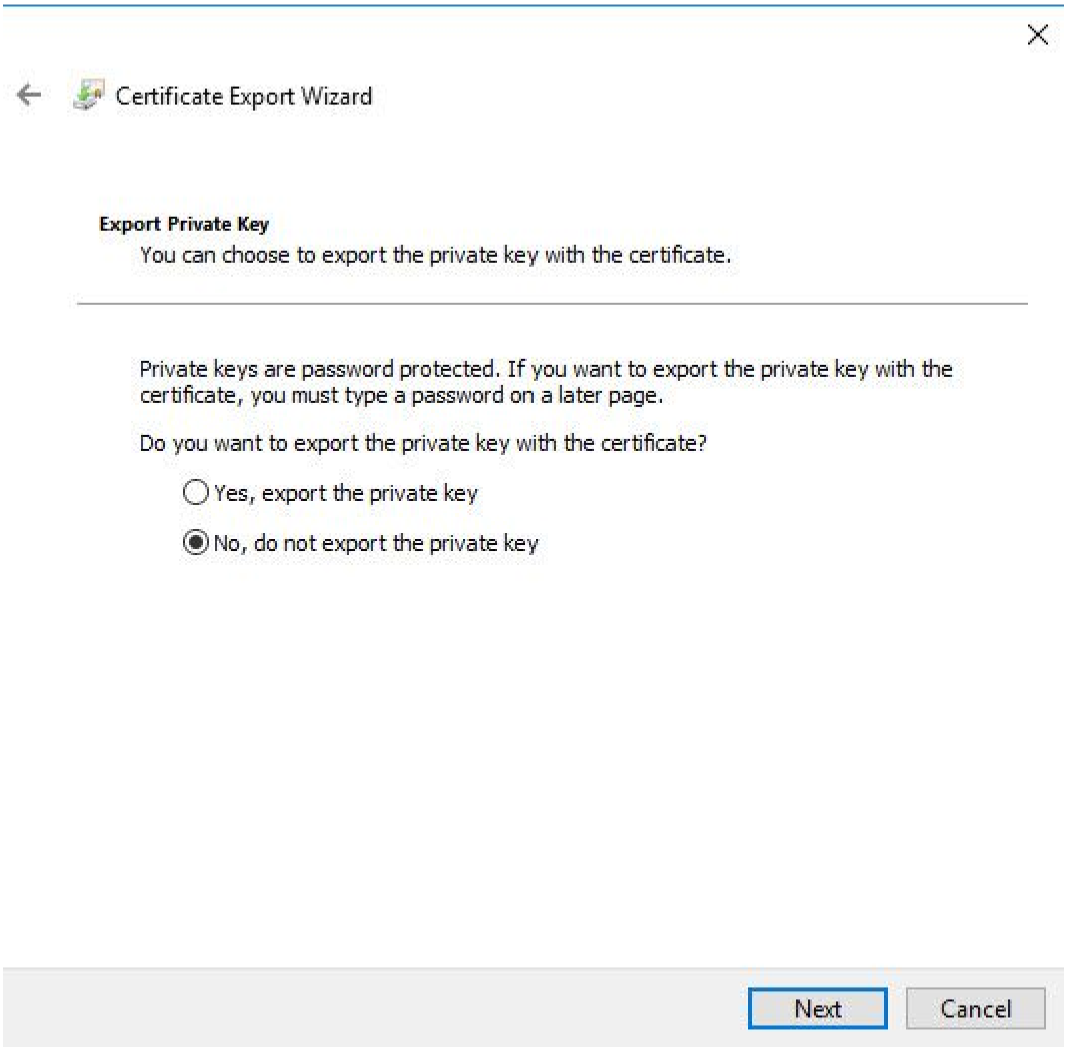
Valid from 27/07/2018 **to** 27/07/2019

You have a private key that corresponds to this certificate.

Now we have certs in place. But we need to export these so we can upload it to Azure.

To export root certificate,

- Right click on root cert inside certificate mmc.
- Click on **Export**
- In private key page, select not to export private key



Export Private Key

You can choose to export the private key with the certificate.

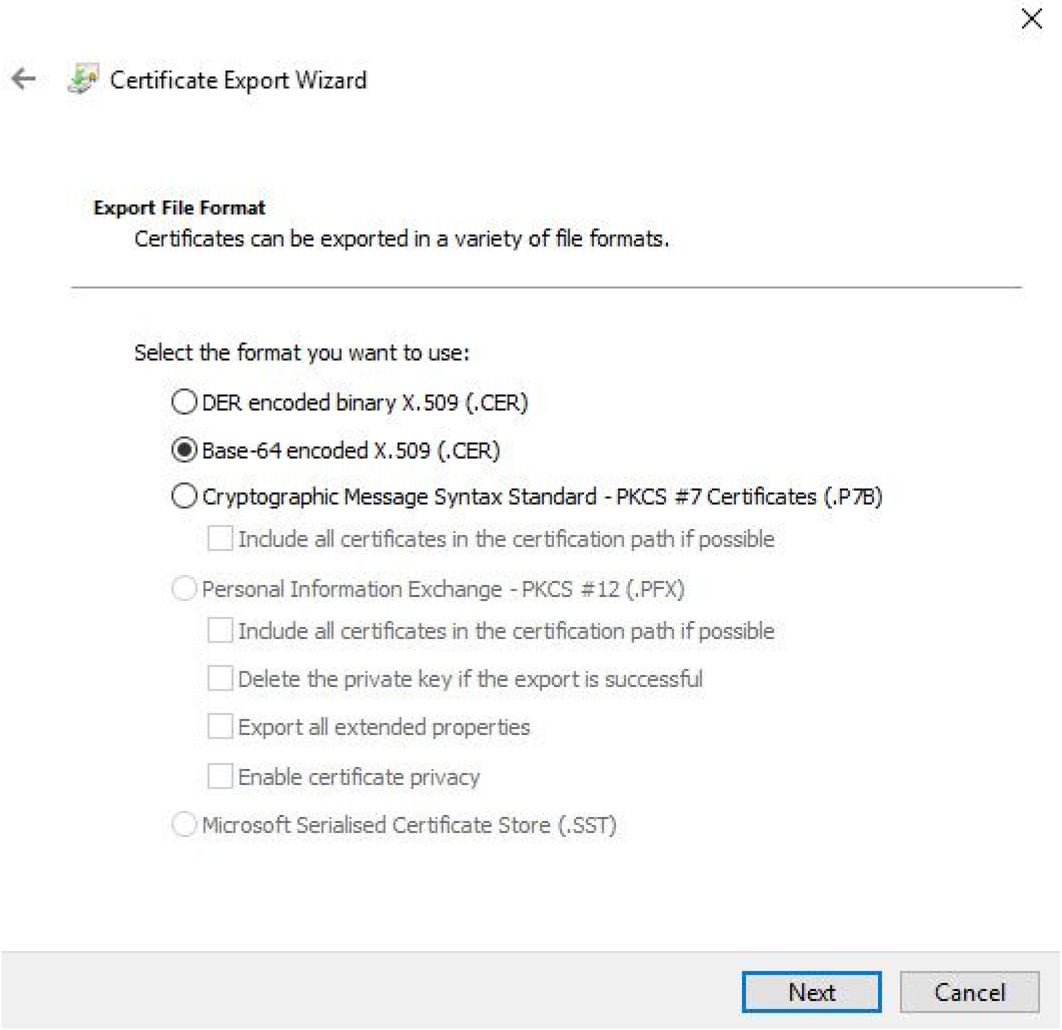
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

- Select Base-64 encoded X.509 as export file format.



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

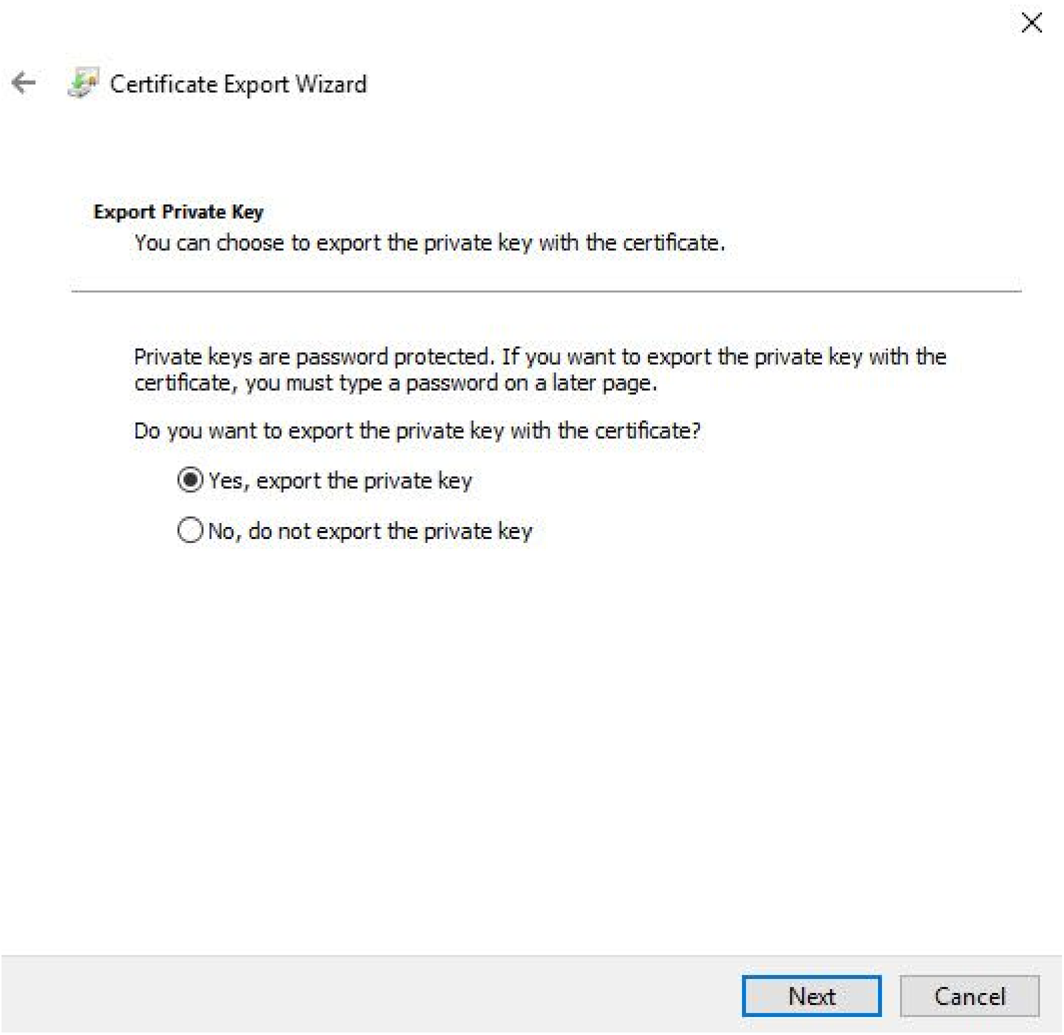
□ Enable certificate privacy

○ Microsoft Serialised Certificate Store (.SST)

- Complete the wizard and save the cert in pc.

To export client certificate,

- Use same method to export as root cert, but this time under private key page, select option to export private key.



Export Private Key

You can choose to export the private key with the certificate.

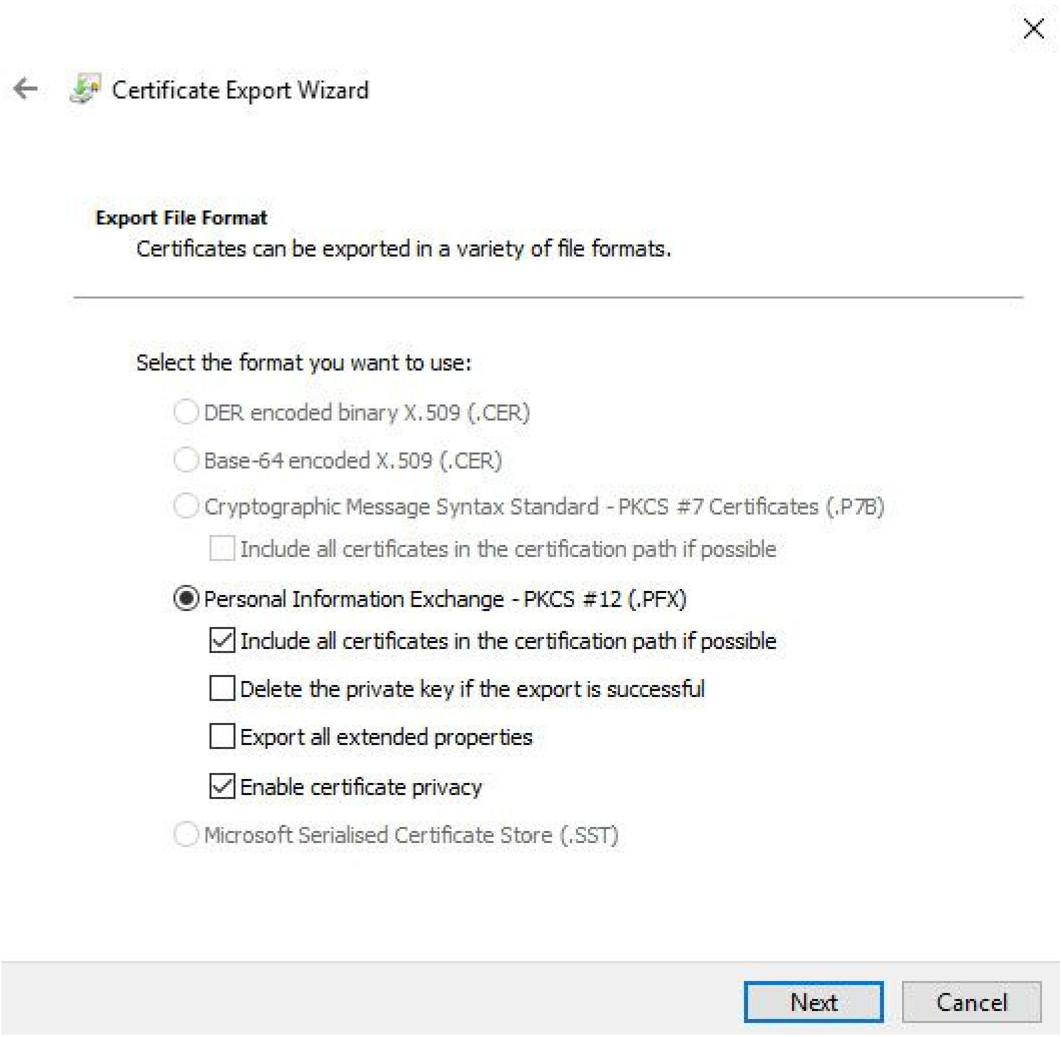
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

- In file format page, leave the default as following and click **Next**



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 Serialised Certificate Store (.SST)

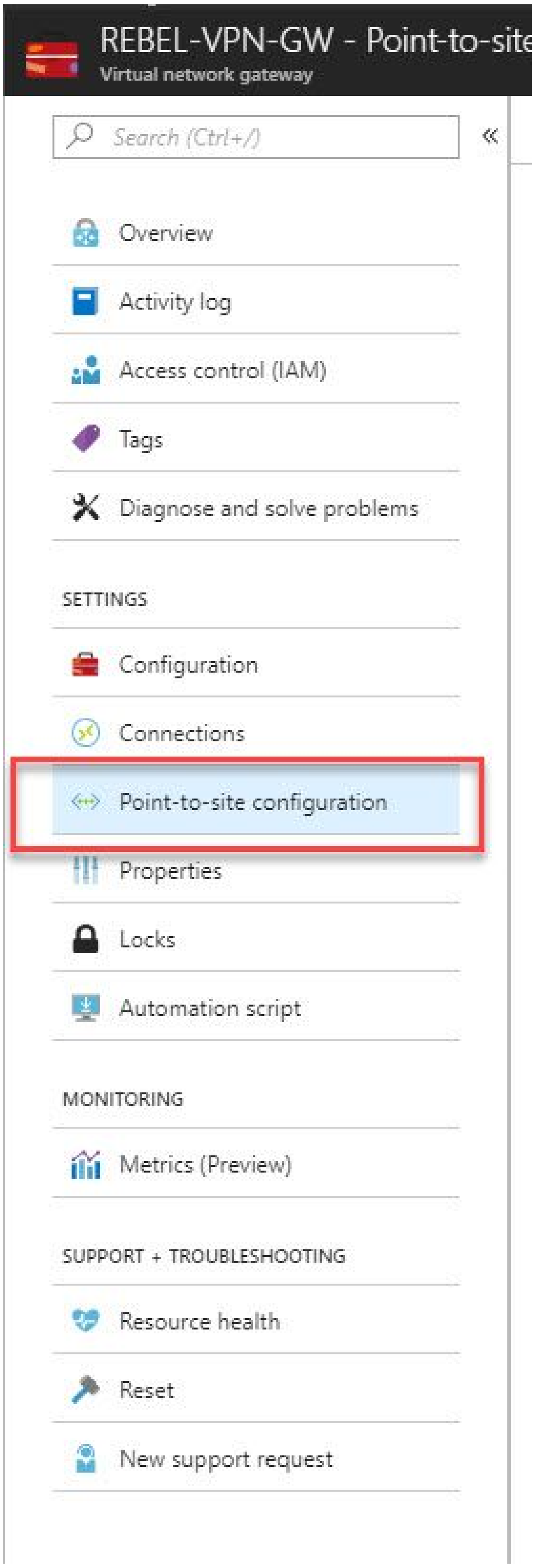
- Define password for the pfx file and complete the wizard.

Note – Only root cert will use in Azure VPN, client certificate can install on other computers which need P2S connections.

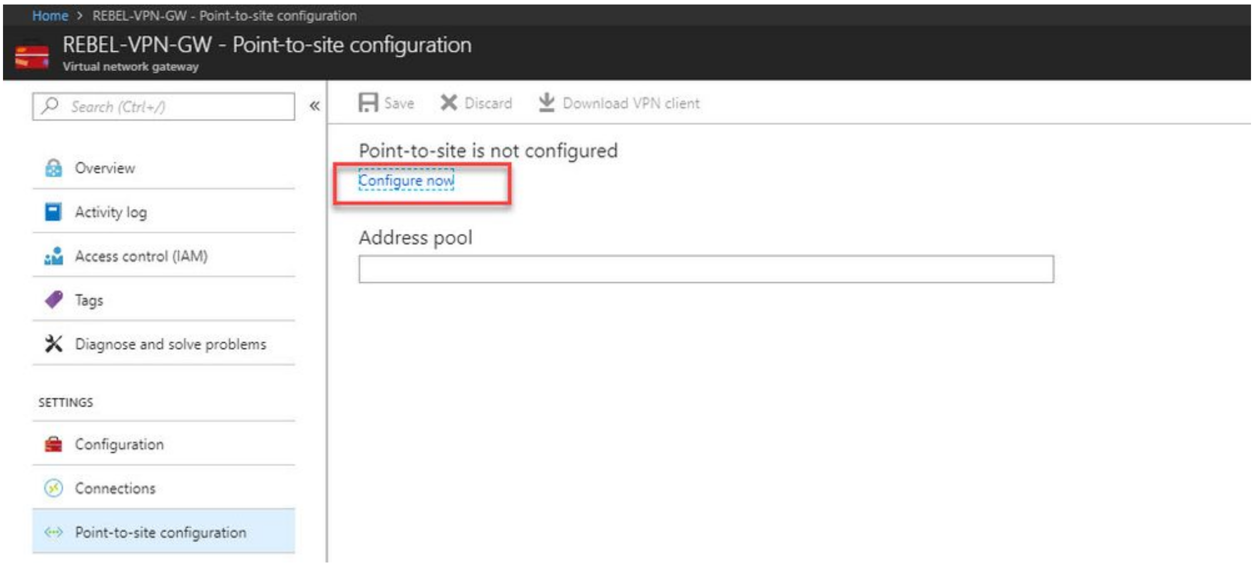
Configure Point-to-Site Connection

Next step of this configuration is to configure the point-to-site connection. In here we will define client ip address pool as well. It is for VPN clients.

- Click on newly created VPN gateway connection.
- Then in new window click on **Point-to-site configuration**



- After that, click on **Configure Now**

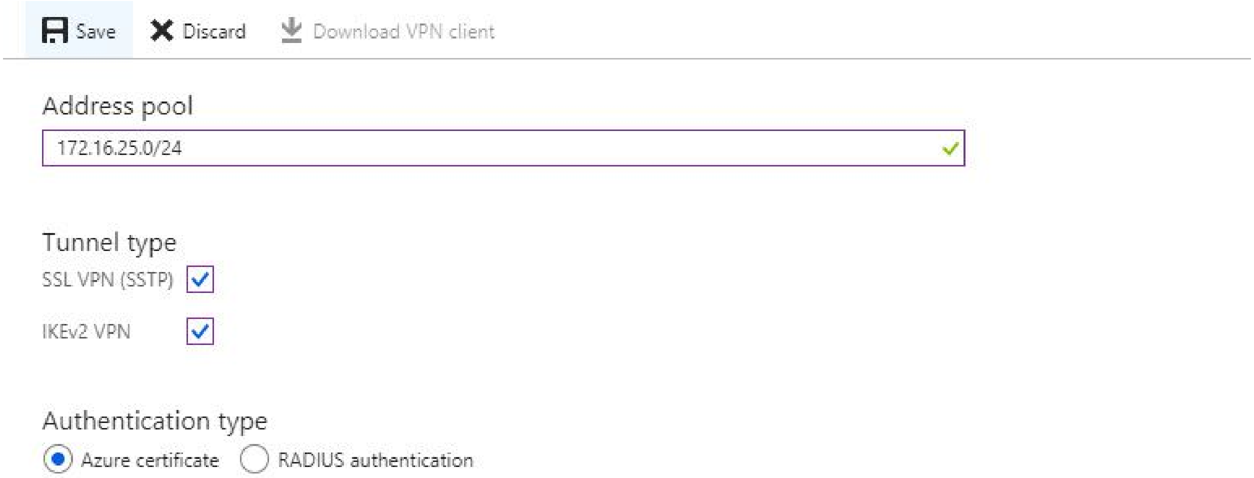

Home > REBEL-VPN-GW - Point-to-site configuration
REBEL-VPN-GW - Point-to-site configuration
Virtual network gateway
Search (Ctrl+/)
«
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
SETTINGS
Configuration
Connections
Point-to-site configuration
Save
Discard
Download VPN client

Point-to-site is not configured

Configure now

Address pool

- In new window type IP address range for VPN address pool. In this demo I will be using **172.16.25.0/24**. For tunnel type use both **SSTP & IKEv2**. Linux and other mobile clients by default use **IKEv2** to connect. Windows also use **IKEv2** first and then try **SSTP**. For authentication type use **Azure Certificates**.



Address pool

172.16.25.0/24

Tunnel type

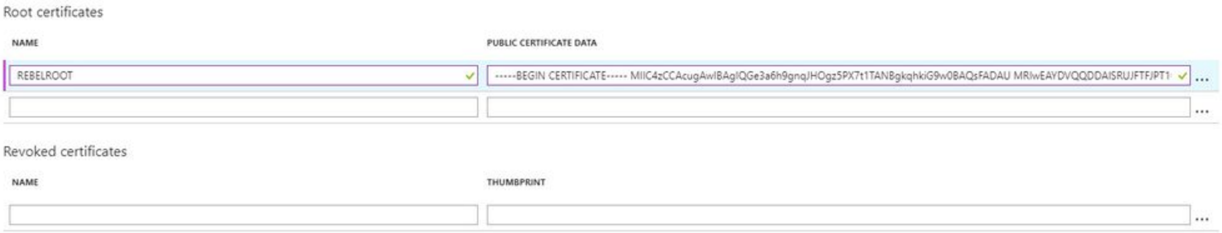
SSL VPN (SSTP) ☑

IKEv2 VPN ☑

Authentication type

● Azure certificate ○ RADIUS authentication

- In same window there is place to define root certificate. Under root certificate name type the cert name and under public certificate data, paste the root certificate data (you can open cert in notepad to get data).

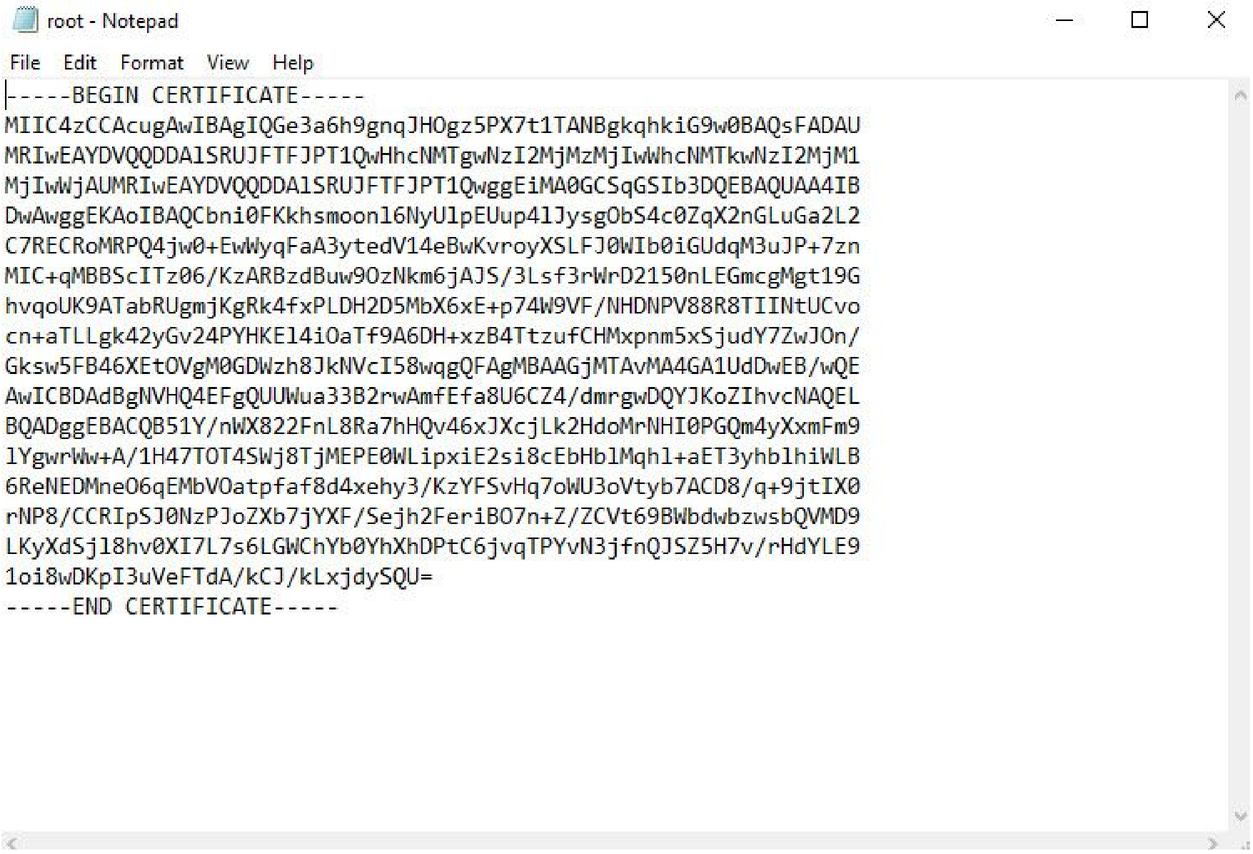


Root certificates

NAME	PUBLIC CERTIFICATE DATA
REBELROOT	-----BEGIN CERTIFICATE----- MIIC4zCCAcugAwIBAgIQGe3a6h9gnqJHOgz5PX7t1TANBgkqhkiG9w0BAQsFADAU MRIwEAYDVQQDDAlSRUJFTFJPT1

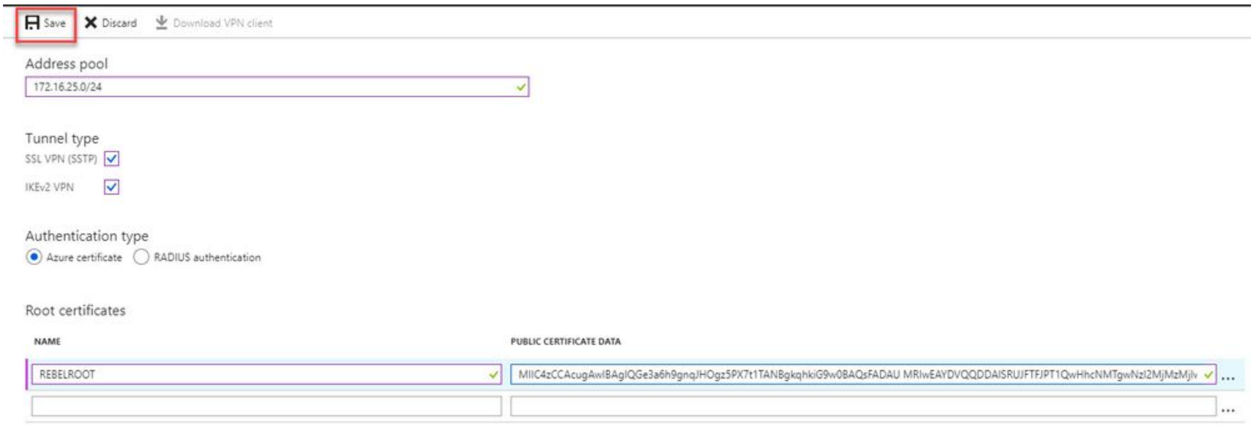
Revoked certificates

NAME	THUMBPRINT



```
-----BEGIN CERTIFICATE-----
MIIC4zCCAcugAwIBAgIQGe3a6h9gnqJHOgz5PX7t1TANBgkqhkiG9w0BAQsFADAU
MRIwEAYDVQQDDAlSRUJFTFJPT1QwHhcNMTgwNzI2MjMzMjIwWhcNMTkwNzI2MjM1
MjIwWjAUMRIwEAYDVQQDDAlSRUJFTFJPT1QwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCbni0FKkhsmoonl6NyUlpEUup4lJysgObS4c0ZqX2nGLuGa2L2
C7RECRoMRPQ4jw0+EwWyqFaA3ytedV14eBwKvroyXSLFJ0WIb0iGUdqM3uJP+7zn
MIC+qMBBScITz06/KzARBzdBuw9OzNkm6jAJS/3Lsf3rWrD2150nLEGmcgMgt19G
hvqoUK9ATabRUgmjKgRk4fxPLDH2D5MbX6xE+p74W9VF/NHDNPV88R8TIINtUCvo
cn+aTLLgk42yGv24PYHKEl4iOaTf9A6DH+xzB4TtzufCHMxpnm5xSjudY7ZwJOn/
Gksw5FB46XEtOVgM0GDWzh8JkNVcI58wqgQFAgMBAAGjMTAvMA4GA1UdDwEB/wQE
AwICBDAdBgNVHQ4EFgQUUWua33B2rwAmfEfa8U6CZ4/dmrgwDQYJKoZIhvcNAQEL
BQADggEBACQB51Y/nWX822FnL8Ra7hHQv46xJXcjLk2HdoMrNHI0PGQm4yXxmFm9
lYgwrWw+A/1H47TOT4SWj8TjMEPE0WLipxiE2si8cEbHblMqhl+aET3yhblhiWLB
6ReNEDMneO6qEMbVOatpfaf8d4xehy3/KzYFSvHq7oWU3oVtyb7ACD8/q+9jtIX0
rNP8/CCRIpSJ0NzPJoZXb7jYXF/Sejh2FeriBO7n+Z/ZCVt69BWbdwbzwsbQVMD9
LKyXdSjl8hv0XI7L7s6LGWChYb0YhXhDPtC6jvqTPYvN3jfnQJSZ5H7v/rHdYLE9
1oi8wDKpI3uVeFTdA/kCJ/kLxjdySQU=
-----END CERTIFICATE-----
```

- Then click on **Save** to complete the process.



Address pool

172.16.25.0/24

Tunnel type

SSL VPN (SSTP) ☑

IKEv2 VPN ☑

Authentication type

● Azure certificate ○ RADIUS authentication

Root certificates

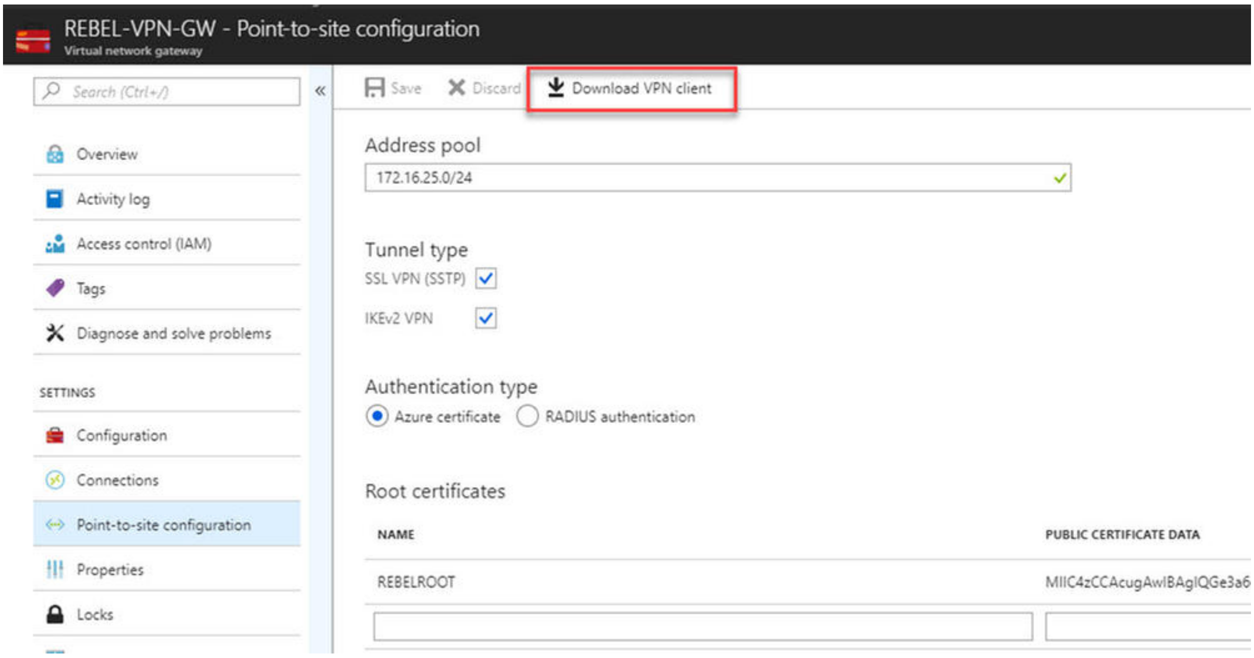
NAME	PUBLIC CERTIFICATE DATA
REBELROOT	MIIC4zCCAcugAwIBAgIQGe3a6h9gnqJHOgz5PX7t1TANBgkqhkiG9w0BAQsFADAU MRIwEAYDVQQDDAlSRUJFTFJPT1QwHhcNMTgwNzI2MjMzMjIv

Note : when you paste certificate data, do not copy -----BEGIN CERTIFICATE----- & -----END CERTIFICATE----- text.

Testing VPN connection

Now we have finished with configuration. As next step, we need to test the connection. To do that log in to the same pc where we generate certificates. If you going to use different PC, first you need to import root cert & client certificate we exported.

- Log in to Azure portal from machine and go to VPN gateway config page.
- In that page, click on **Point-to-site configuration**
- After that, click on **Download VPN client**



REBEL-VPN-GW - Point-to-site configuration

Address pool
172.16.25.0/24 ✓

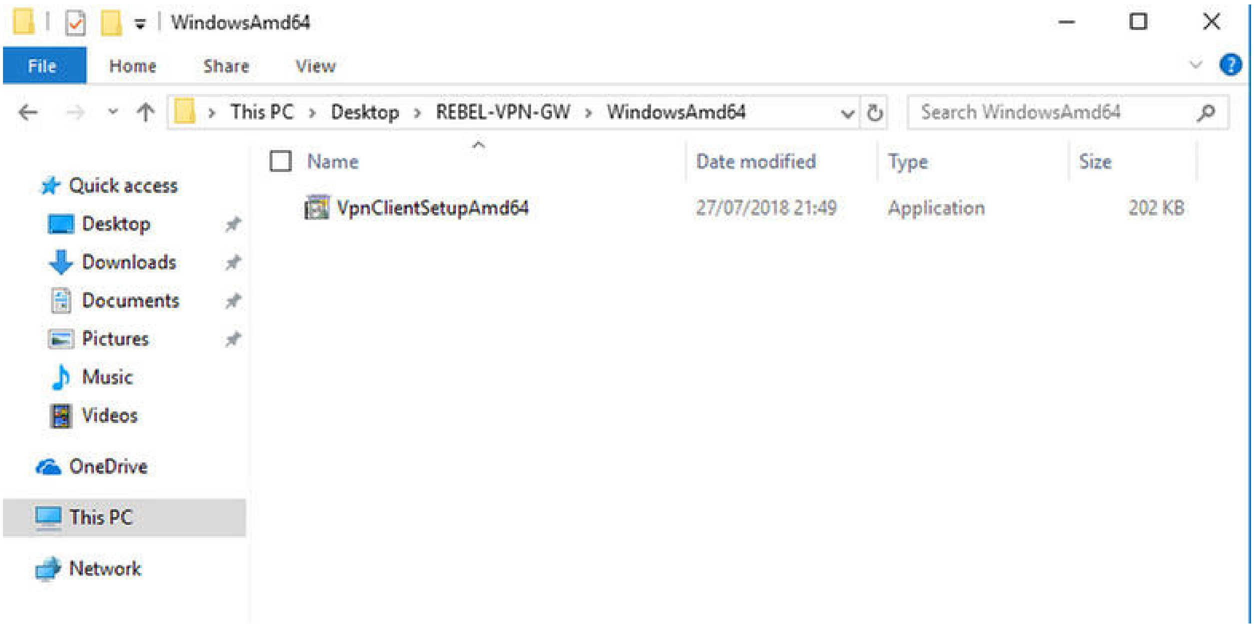
Tunnel type
SSL VPN (SSTP) ☑
IKEv2 VPN ☑

Authentication type
● Azure certificate ○ RADIUS authentication

Root certificates

NAME	PUBLIC CERTIFICATE DATA
REBELROOT	MIIC4zCCAcugAwIBAgIQGe3a6

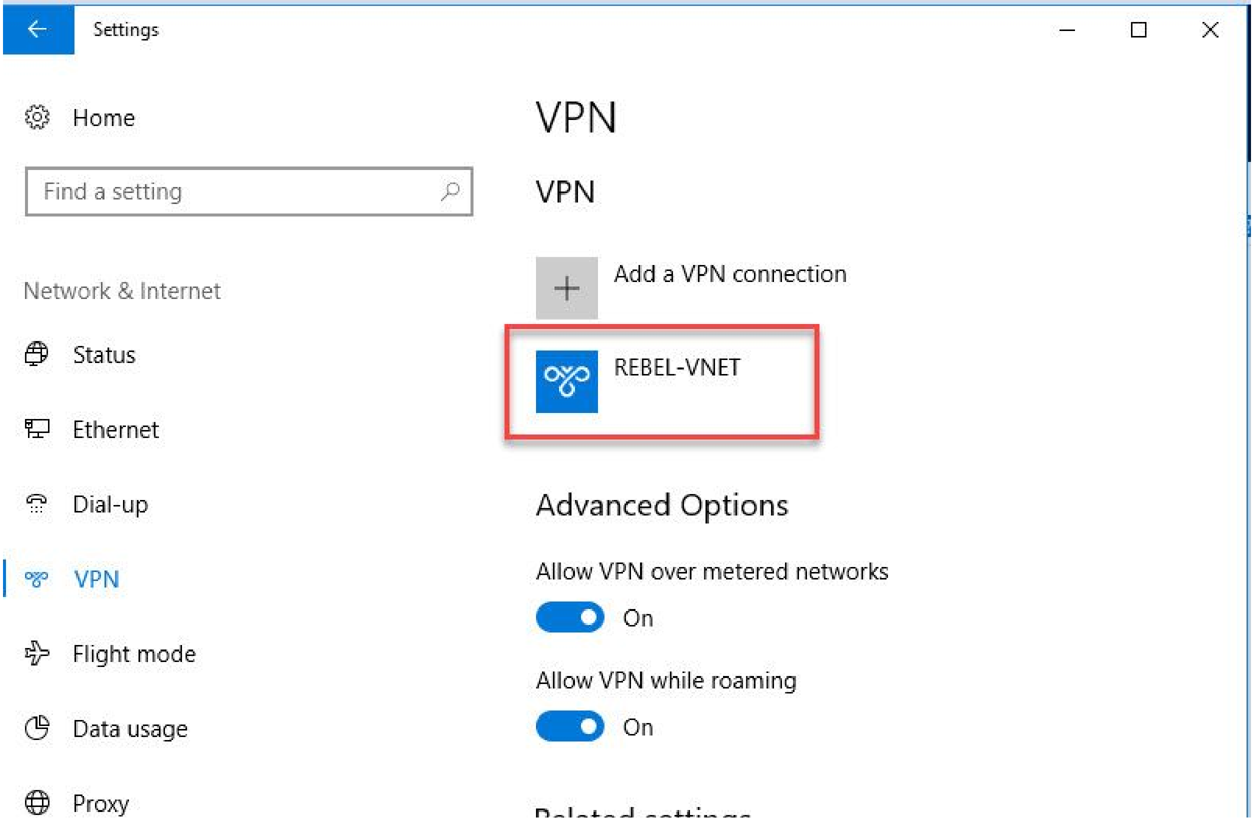
- Then double click on the VPN client setup. In my case I am using 64bit vpn client.



This PC > Desktop > REBEL-VPN-GW > WindowsAmd64

Name	Date modified	Type	Size
VpnClientSetupAmd64	27/07/2018 21:49	Application	202 KB

- After that, we can see new connection under windows 10 VPN page.



VPN

VPN

Advanced Options

Allow VPN over metered networks

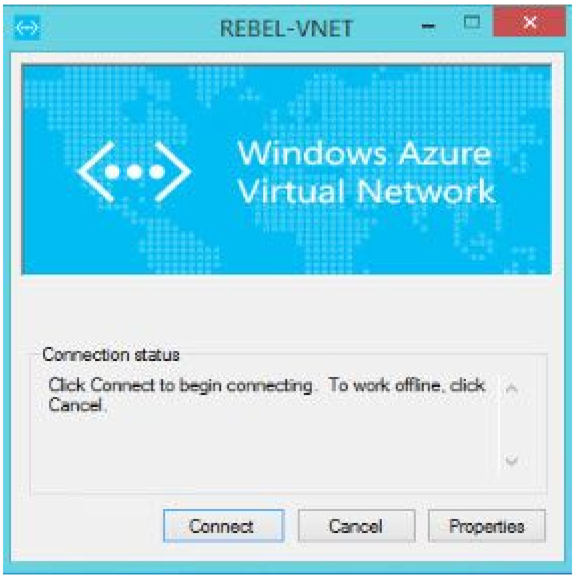
On

Allow VPN while roaming

On

Related settings

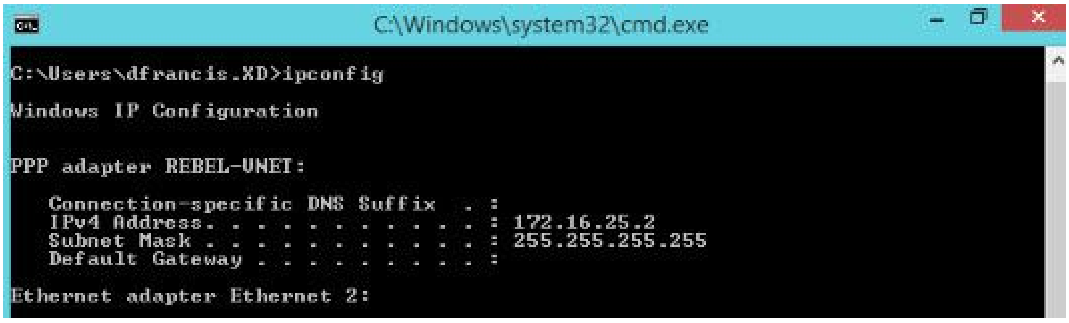
- Click on connect to VPN. Then it will open up this new window. Click on **Connect** in there.



Connection status

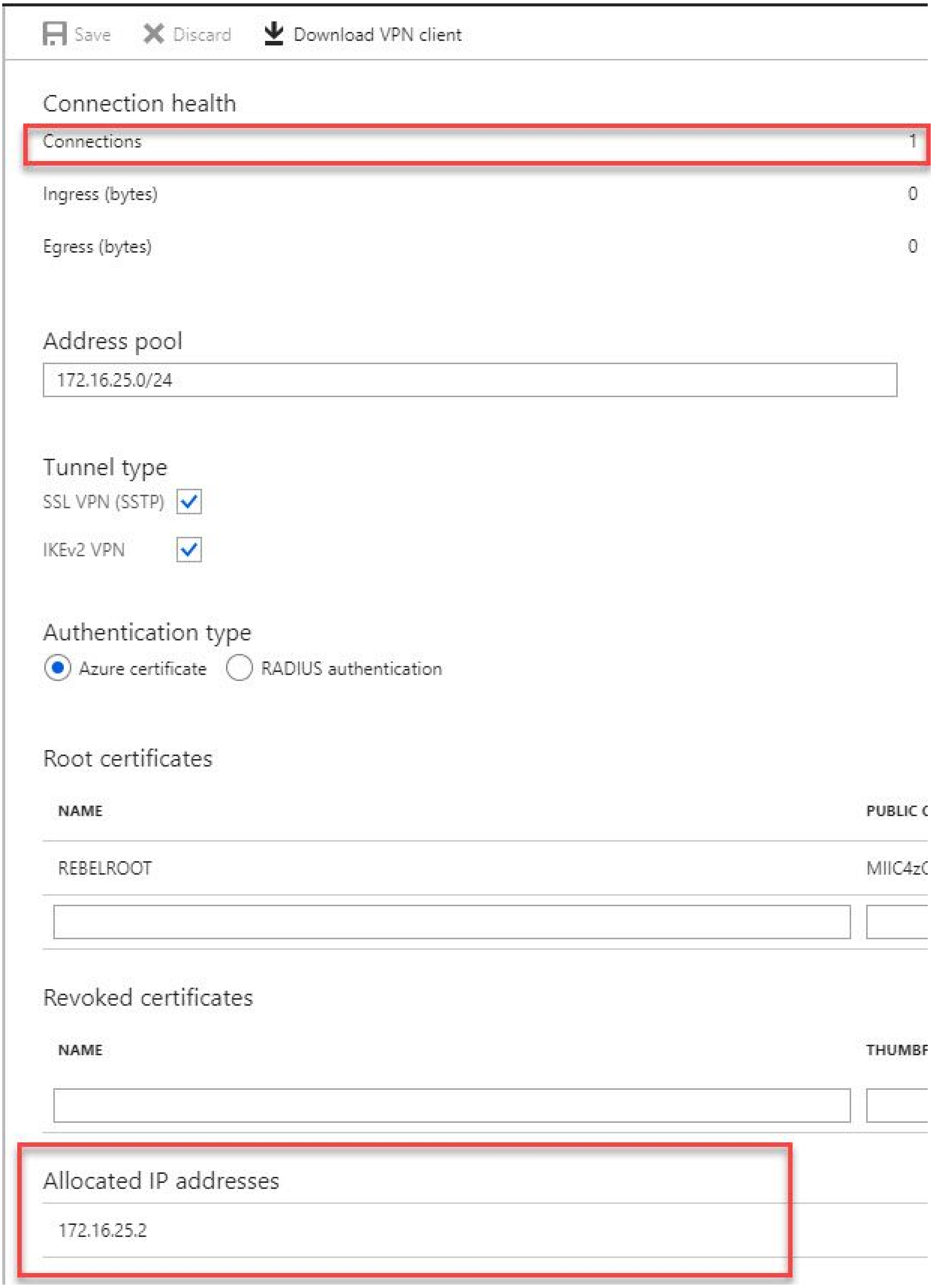
Click Connect to begin connecting. To work offline, click Cancel.

- Then run ip config to verify ip allocation from VPN address pool.



```
C:\Users\dfrancis.XD>ipconfig

Windows IP Configuration


PPP adapter REBEL-UNET:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 172.16.25.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 2:
```

- In VPN gateway page also, I can see one connection is made.



Connection health

Connections 1

Ingress (bytes) 0

Egress (bytes) 0

Address pool

172.16.25.0/24

Tunnel type

SSL VPN (SSTP) ☑

IKEv2 VPN ☑

Authentication type

● Azure certificate ○ RADIUS authentication

Root certificates

NAME	PUBLIC C
REBELROOT	MIIC4zC

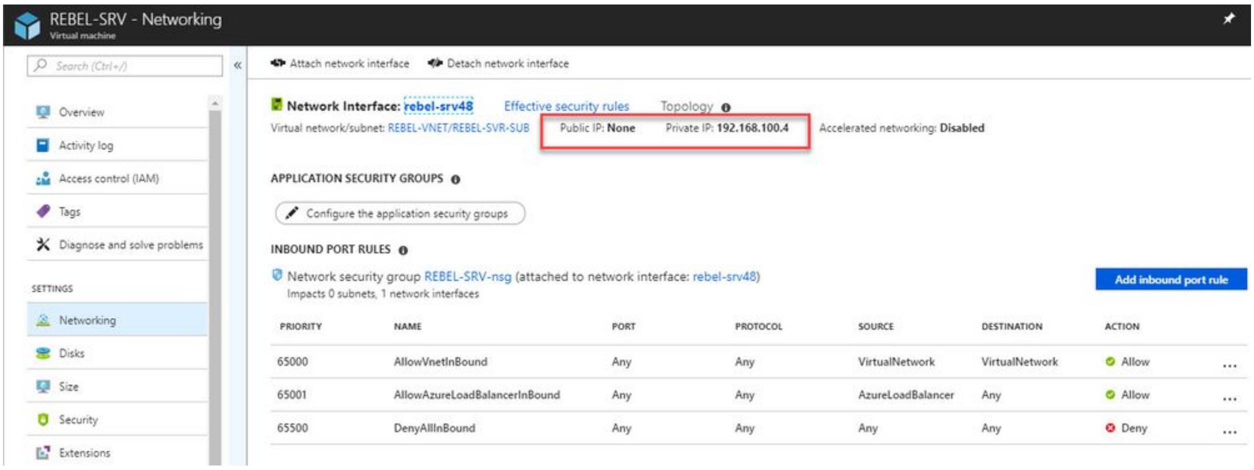
Revoked certificates

NAME	THUMBF

Allocated IP addresses

172.16.25.2

- I have a server setup under new virtual network we created. This server only has private ip and its 192.168.100.4



Network Interface: rebel-srv48

Virtual network/subnet: REBEL-VNET/REBEL-SVR-SUB   Public IP: None   Private IP: 192.168.100.4   Accelerated networking: Disabled

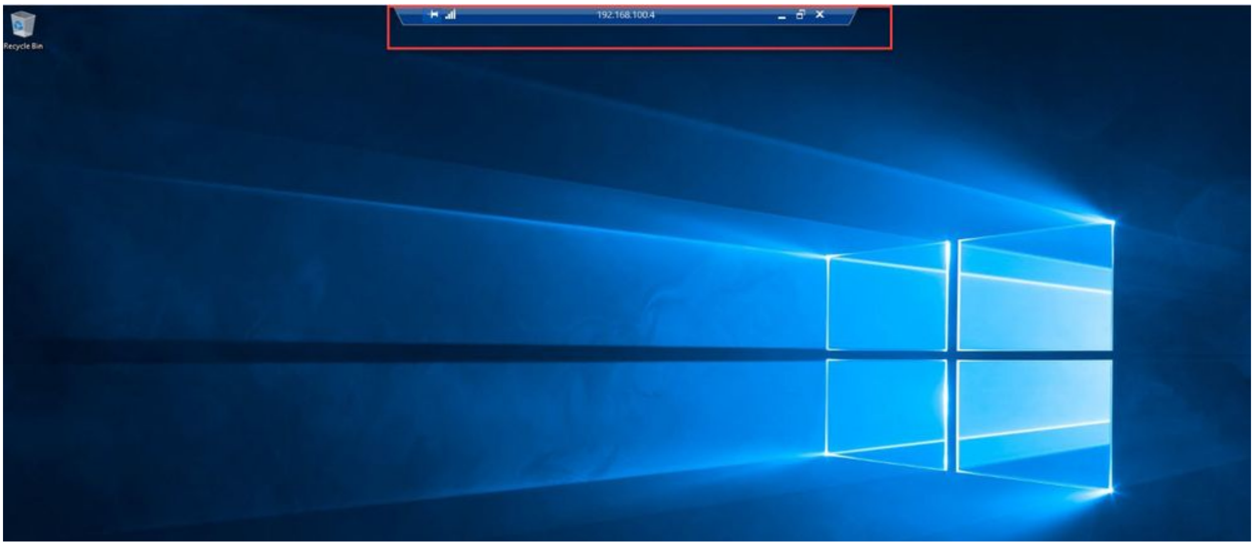
APPLICATION SECURITY GROUPS

INBOUND PORT RULES

Network security group REBEL-SRV-nsg (attached to network interface: rebel-srv48)
Impacts 0 subnets, 1 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✕ Deny

- As expected, I can RDP to this via VPN.


Recycle Bin
192.168.100.4