Question 1: R&D Document on How to setup Point to Site

Setting up a Point-to-Site (P2S) VPN allows individual clients to connect to a virtual network via a secure connection over the internet. This setup involves several steps, including configuring your network, setting up the VPN gateway, creating certificates, and configuring VPN clients. This document will guide you to set up P2S through the process.

# Point-to-Site VPN Setup Guide

**Table of Contents**

1. Prerequisites
2. Step-by-Step Setup
   1. Create a Virtual Network
   2. Create a gateway subnet
   3. Create a VPN Gateway
   4. Configure Point-to-Site VPN
   5. Generate and Upload VPN Client Configuration
   6. Download VPN Client
   7. Install the VPN Client
   8. Connect to the VPN
3. Verifying the Connection
4. Troubleshooting
5. Additional Considerations

## Prerequisites

1. Virtual Network: A VNet in your Azure environment.
2. Gateway Subnet: Created in your VNet.
3. Virtual Network Gateway: Configured in your VNet.

## Step-by-Step Setup

### Step 1: Create a Virtual Network

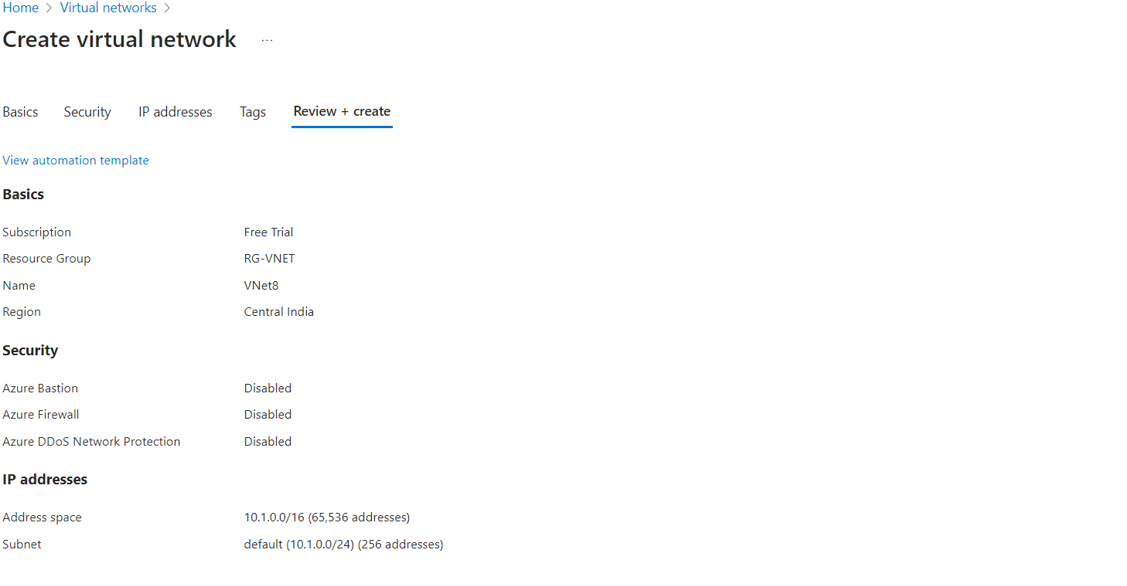
1. Log in to Azure Portal.
2. **Navigate to Virtual Networks:**

* Click "Create a resource" > "Networking" > "Virtual Network".

1. **Configure VNet:**

* **Name:** Provide a name for your virtual network e.g.VNet8.
* **Address Space:** Define the address space, e.g., 10.1.0.0/16.
* **Subnets:** Create a subnet, e.g., 10.1.0.0/24.

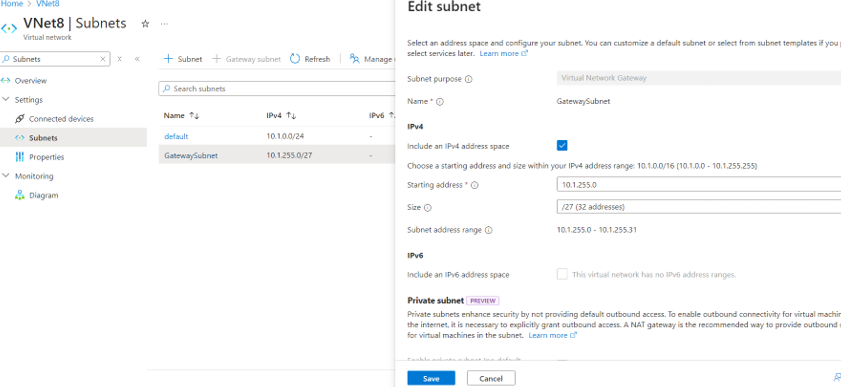
1. Review + Create: Verify the details and create the VNet.



### 

### Step 2: Create a gateway subnet

1. Open the page of your virtual network e.g., VNet8.
2. On the left pane select Subnets.
3. Select +GatewaySubnet.
4. Adjust the IP range value e.g., 10.1.255.0/27.
5. Click on Add/ Save button.



### 

### Step 3: Create a VPN Gateway

1. **Navigate to the Virtual Network Gateway:**

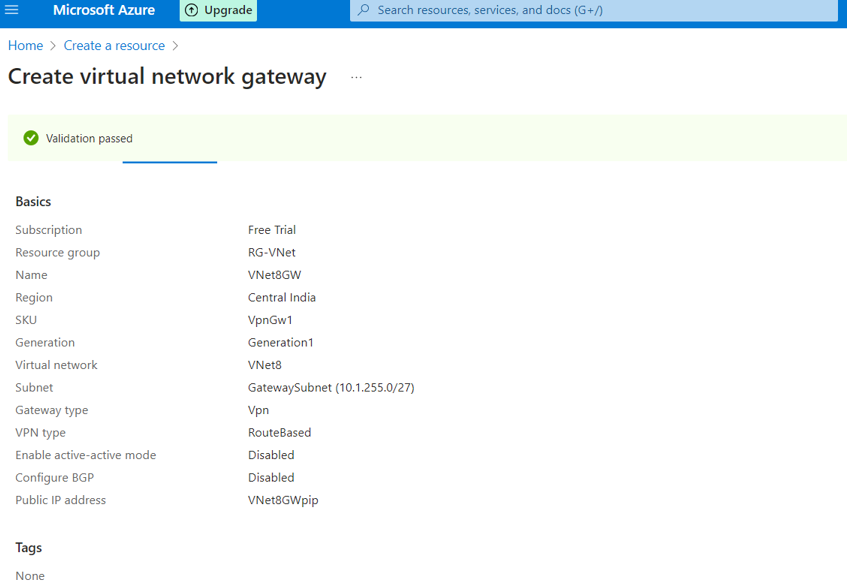
* Go to Create a resource > Networking > Virtual network gateway.

1. **Fill in the required fields:**

* **Name:** Enter a name for your VPN gateway e.g.VNet8GW.
* **Region:** Select the same region as your VNet.
* **Gateway type:** Select VPN.
* **SKU:** Choose the appropriate SKU based on your requirements (e.g., VpnGw1).
* **Virtual network:** Select the VNet you created.
* **Public IP address:** Create a new public IP address.

1. **Create the Gateway:**

* Click Review + create, then click on Create.



### Step 4: Configure Point-to-Site Configuration

1. **Navigate to the Virtual Network Gateway:**

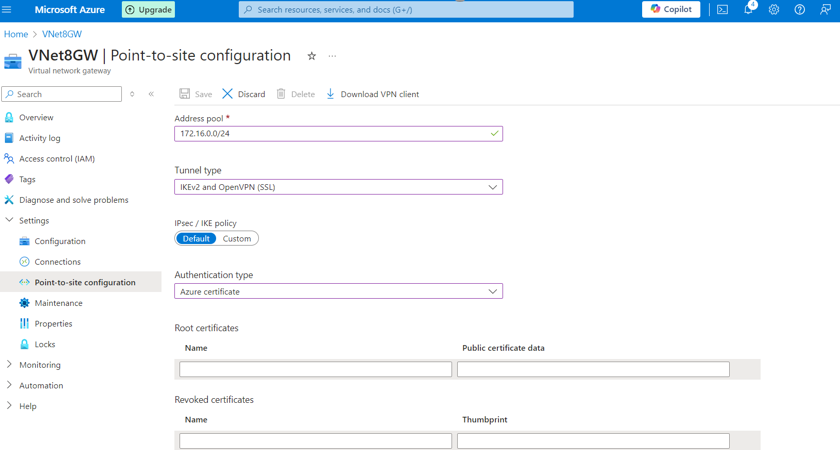
* Go to your Virtual Network Gateway (P2S-VPN-Gateway).

1. **Configure Point-to-Site:**

* Under Settings, select Point-to-site configuration.
* Click Configure now.

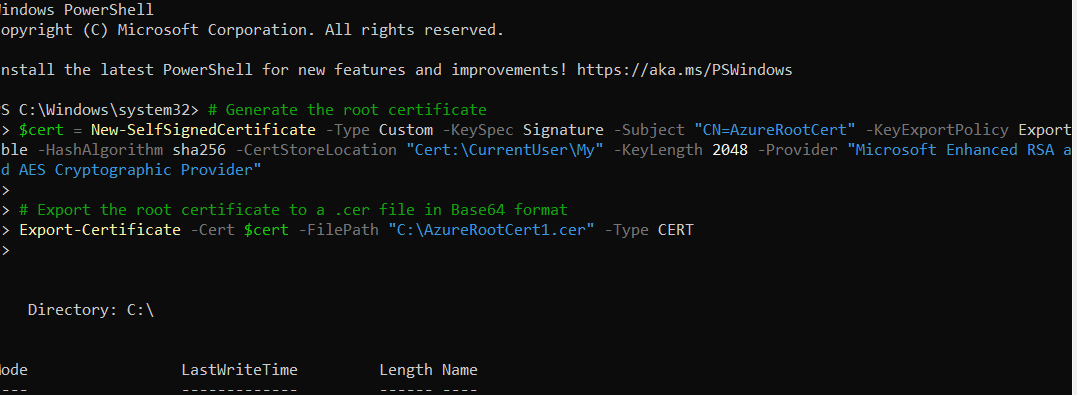
1. **Fill in the Required Information:**

* **Address pool:** Enter 172.16.0.0/24.
* **Tunnel type:** Select IKEv2 and OpenVPN (SSL).
* **Authentication type:** Choose Azure Certificate.



### Step 5: Generate and Upload VPN Client Configuration

1. **Generate Certificates:**

* On your local machine, open PowerShell and run the following commands to create a root certificate and client certificate:

1. **Upload the Root Certificate:**

* In the Certificates section of the Point-to-site configuration fill in root certificates.
* **Name:** Enter RootCert.
* **Public Certificate Data:** Open the C:\AzureRootCert.cer file in a text editor and copy the content. Paste it into the Public Certificate Data field.

1. Click Save.

### Step 6: Download VPN Client

1. **Download VPN Client:**

* Once the configuration is saved, click Download VPN client.

### Step 7: Install VPN Client

1. **Extract and Install:**

* Extract the downloaded VPN client package.
* Run the setup file for your operating system and follow the prompts to install the VPN client.

1. **Import Client Certificate:**

* Double-click the AzureClientCert.pfx file you created.
* Follow the prompts to import the certificate into the Personal certificate store. Use the password you specified during export.

### Step 8: Connect to the VPN

1. **Open VPN Client:**

* Open the installed VPN client (e.g., Azure VPN Client).

1. **Connect to the VPN:**

* Select the VPN profile you installed.
* Click Connect.

## Verify Connection

* Once connected, verify the connection by checking your IP address and accessing resources within the Azure VNet.
* Open a command prompt and run ipconfig to see the IP address assigned from the 172.16.0.0/24 range.

## Troubleshooting

* **Connection Issues:** Verify that the client configuration matches the VPN gateway settings.
* **Authentication Failures:** Ensure that the correct certificates or credentials are used.
* **Network Access Problems:** Check the routing and address pool configurations.

## Additional Considerations

* **Security:** Ensure that strong authentication methods are used and regularly updated.
* **Scalability:** Monitor usage and consider upgrading the VPN gateway SKU if necessary.
* **Compliance:** Adhere to organizational and regulatory requirements for data security and privacy.