# Point-to-Site (P2S) VPN

* A Point-to-Site VPN (or just P2S VPN) is a way to let individual devices like your laptop or PC connect securely to a private network (like your company’s or Azure’s) using the internet.
* How it works?
* Every device makes its own private connection to the Azure VPN gateway.
* The gateway checks if the device is allowed.
* Once verified, all the traffic from your device goes through a protected tunnel into your private network.
* No one outside can peek in.

# Step-by-Step Setup

* Step-1: creating a virtual network
* Open the **Virtual Network** section in Azure.
* Name it like Point-to-site-VNet.
* For address space, use 172.16.1.0/25.
* Add a subnet called VM-subnet with 172.16.1.0/26.
* Then, add another subnet, but this time select **Virtual Network Gateway** as its purpose.
* Address space: 172.16.1.4/27.
* Azure will name it Gateway Subnet by default.
* Create it and wait till it’s ready.
* Step-2: creating a VPN gateway
* Go to **Virtual Network Gateway** and click **Create**.
* Name it like VPN-Gateway.
* Choose **VPN** as the gateway type.
* Link it to the Point-to-site-VNet you made earlier.
* For Public IPs, name them VPN-PIP and VPN-PIP-2.
* Click **Review + Create**, then **Create**.
* Step-3: create Certificates
* Make a Root Certificate and Then export this certificate as a **Base-64 .cer** file.
* Write the following in powershell:

$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `

Subject "CN=AzureRootCert" -KeyExportPolicy Exportable `

HashAlgorithm sha256 -KeyLength 2048 `

CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign

* Make a Client Certificate and Export this one as a .pfx file (you’ll be asked to set a password).
* Write the following in powershell:

New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `

Subject "CN=AzureChildCert" -KeyExportPolicy Exportable `

HashAlgorithm sha256 -KeyLength 2048 `

CertStoreLocation "Cert:\CurrentUser\My" `

NotAfter (Get-Date). AddYears (6) `

Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")

* Step-4: Configure the VPN Gateway
* Open your VPN Gateway in Azure.
* Go to **Settings**, go to **Point-to-site configuration**.
* Set the address pool to something like 192.168.1.0/25.
* Tunnel type: select both **IKEv2** and **SSTP**.
* Auth type: choose **Azure certificate**.
* Create a new public IP, name it like VPN-PIP-3.
* Now add both certificates.
* Paste in the public part of the root and client certificates.
* Click **Save**.
* Step-5: Download the VPN Client Package
* After saving the config, there is **Download VPN Client** option.
* Click it.
* It will give a zip file with all the setup files.
* Share this with anyone who needs to connect.
* Step-6: Set Things Up on the User’s Device
* On the user’s computer, **import the .pfx certificate**.
* Then unzip the VPN client and install it.
* This creates the connection profile for Azure VPN.
* Step-7: Connect and Test
* Open the VPN client that was installed.
* Click **Connect**.
* Enter any needed credentials.
* Once connected, check if the IP is from 192.168.1.0/25.
* Try reaching internal servers or Azure resources.