Prepared by: Nandini Goyal
Intern at Celebal Technologies
Department: Cloud Infra & Security
Date: 25 July 2025

R&D Document

Setting up Point-to-Site VPN on Azure

Table of Contents

1. Introduction

A **Point-to-Site (P2S) VPN** connection allows you to securely connect an individual client computer to an Azure virtual network. It's suitable when you want to connect from a remote location and do not need a site-to-site connection.

2. Pre-requisites

- Azure Student Subscription
- Azure Resource Group
- Permissions to create virtual network, gateway, and certificates

3. Creating the Virtual Network Gateway

3.1 Create a Virtual Network

- Go to Azure Portal > Create a resource > Networking > Virtual Network
- Select region like `East US` or `Central India` (low quota usage)
- Configure address space (e.g., 10.0.0.0/16)
- Add a subnet (e.g., 10.0.0.0/24)

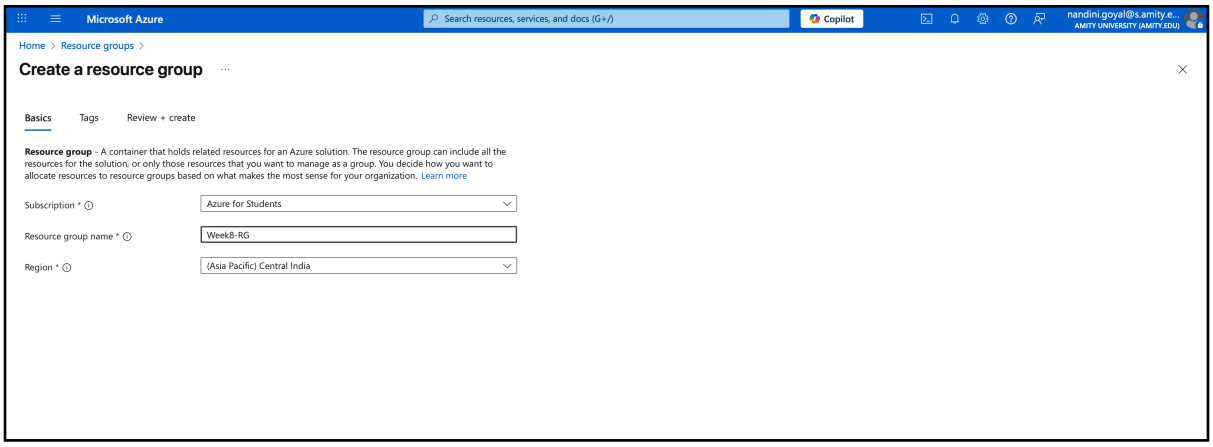

Figure 1: Resource Group

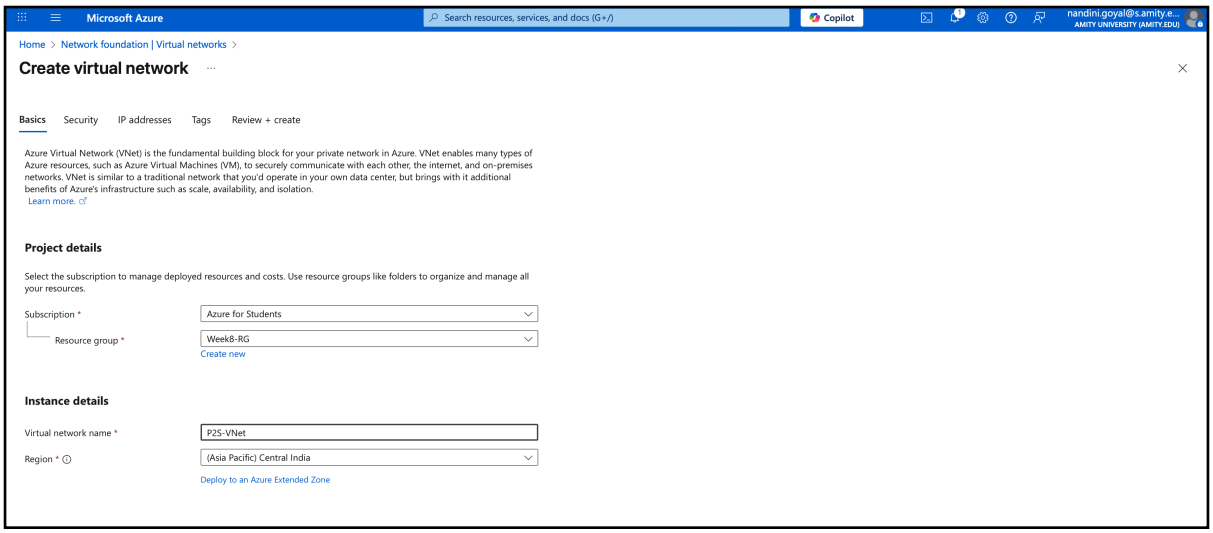

Figure 2: VNet Basics Tab

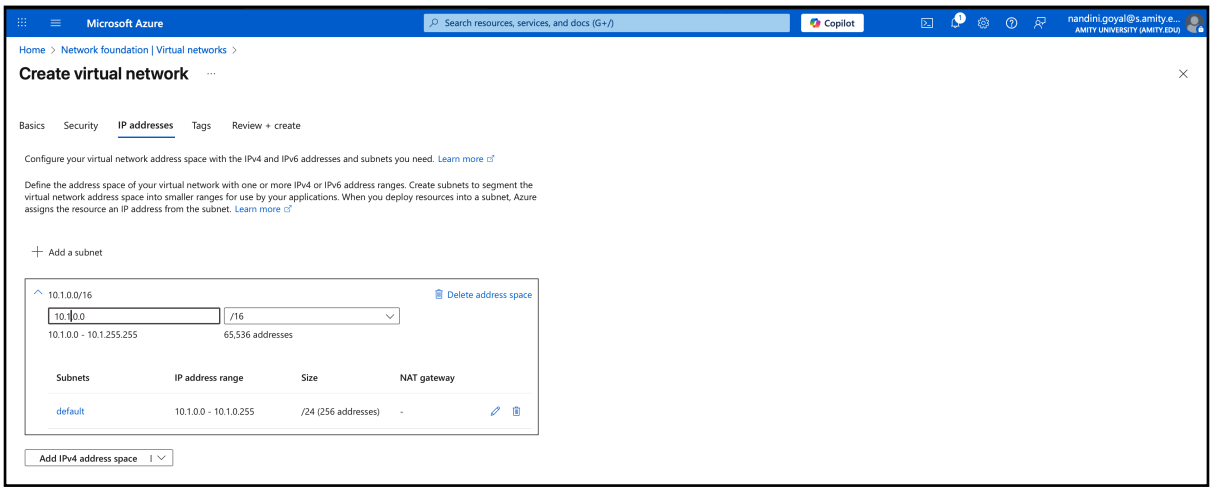

Figure 3: VNet IP Addresses Tab

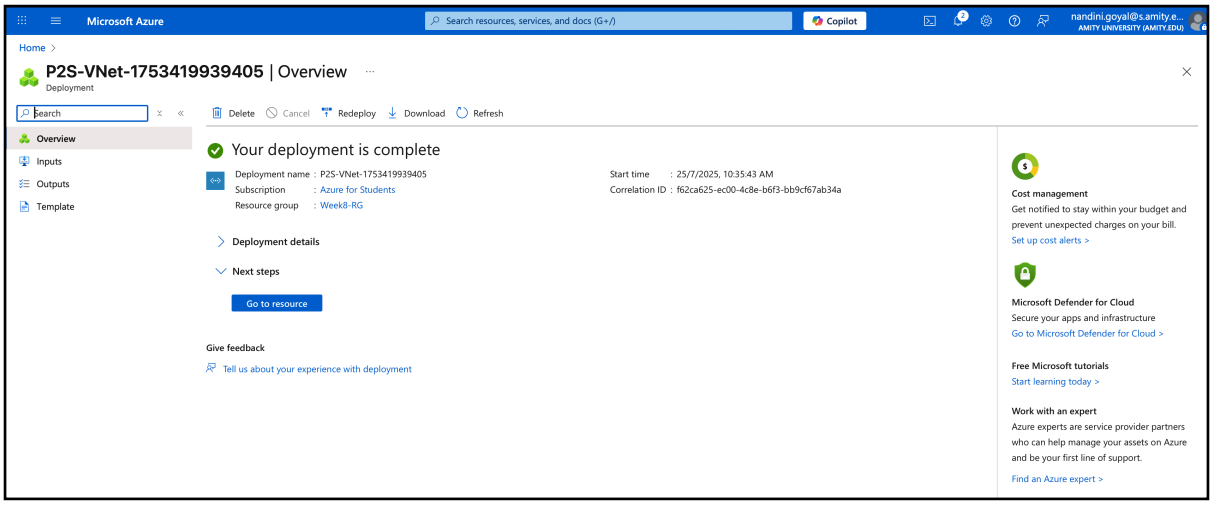

Figure 4: VNet Deployed

3.2 Create the VPN Gateway Subnet

- Go to Subnets under your VNet > Add Gateway Subnet
- Use address range like 10.0.1.0/24

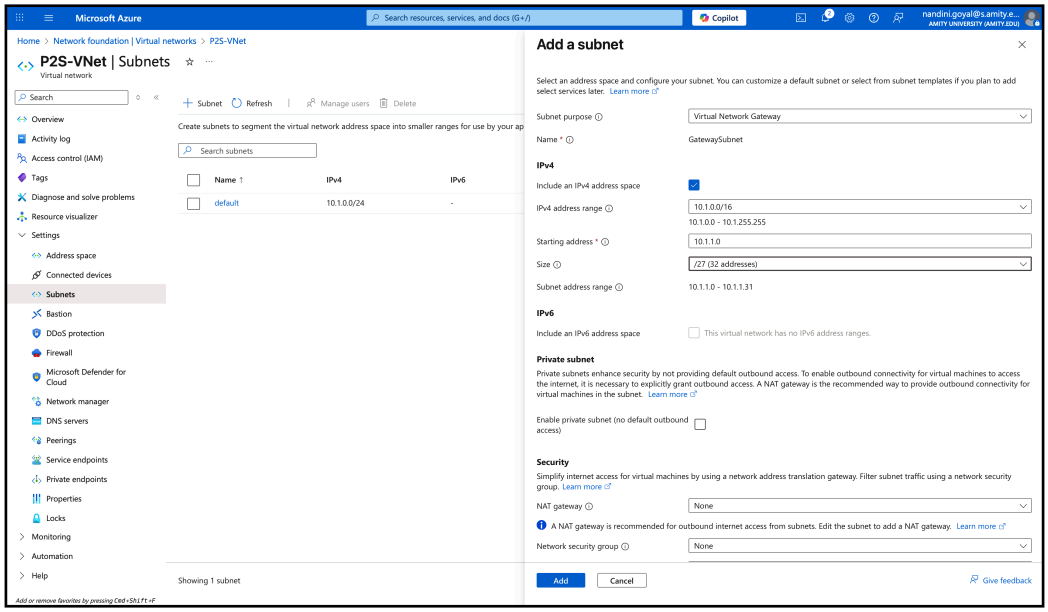

Figure 5: Gateway Subnet configuration

3.3 Create the Virtual Network Gateway

- Go to Create a resource > Networking > Virtual network gateway
- Choose VPN type: `Route-based`
- SKU: Use `Basic`
- Region must match VNet
- Associate with the created VNet

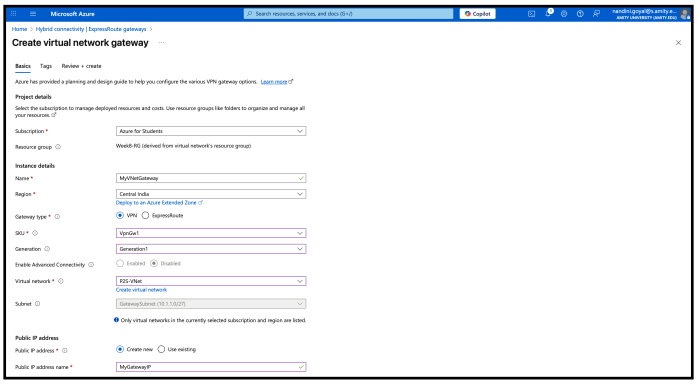

Figure 6: Virtual Network Gateway creation details

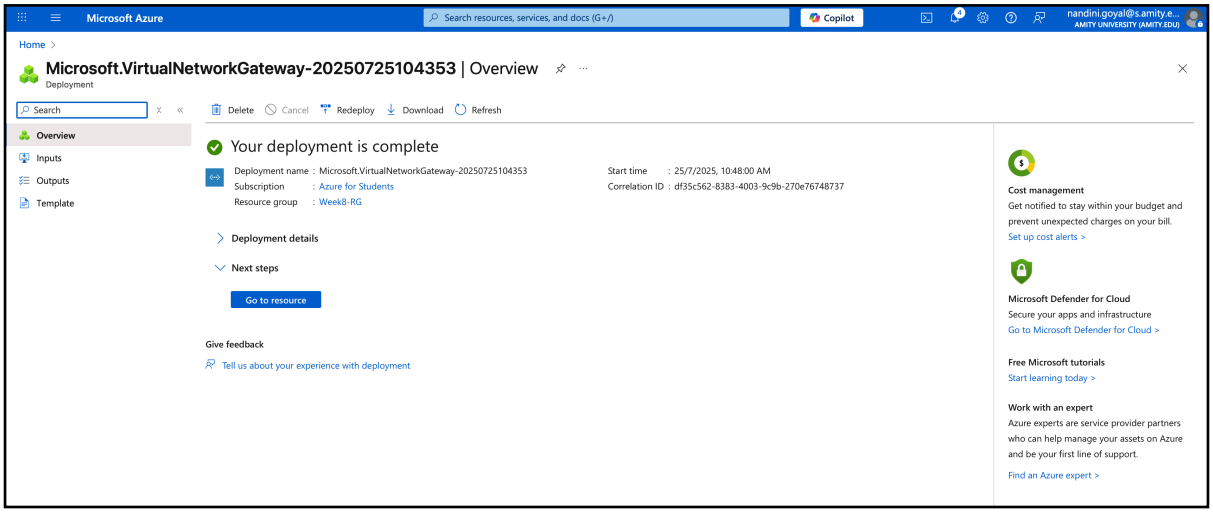

Figure 7: Virtual Network Gateway deployed

4. Generating Client Certificates

4.1 Root Certificate

- Use PowerShell on local system to generate a self-signed root certificate:

$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature -Subject "CN=AzureP2SRootCert" -KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation "Cert:\\CurrentUser\\My" -KeyUsageProperty Sign -KeyUsage CertSign

- Export the public key (.cer) and upload to Azure

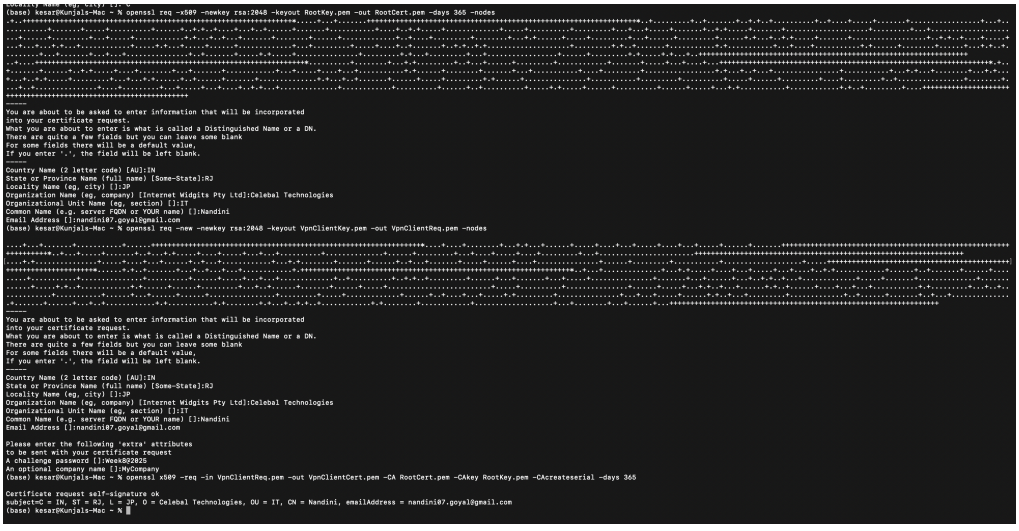

Figure 8: Terminal with root cert command

4.2 Client Certificate

$clientcert = New-SelfSignedCertificate -Type Custom -DnsName AzureP2SClient -KeySpec Signature -Subject "CN=AzureP2SClientCert" -KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation "Cert:\\CurrentUser\\My" -Signer $cert

5. Configuring Point-to-Site VPN

5.1 Configure P2S Parameters

- Go to the created Virtual Network Gateway > Point-to-site configuration > Configure now
- Address Pool: `172.16.201.0/24`
- Tunnel type: SSTP + IKEv2

5.2 Upload Root Certificate

- Upload `.cer` file generated in step 4

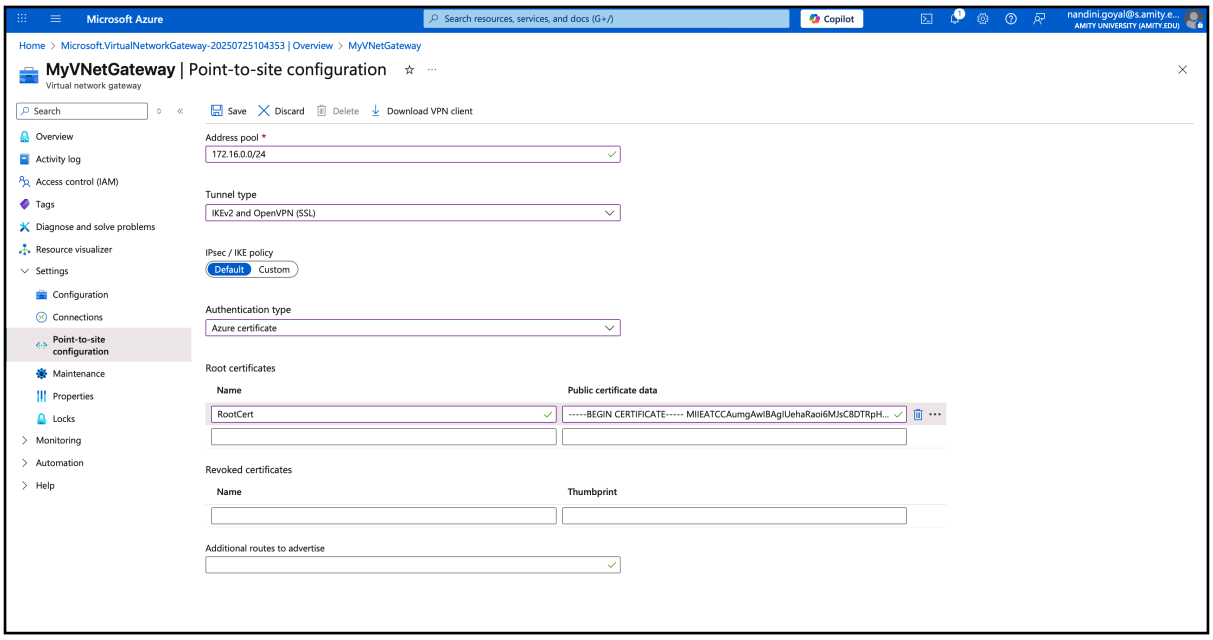

Figure 9: Upload root cert section in Azure

5.3 Download VPN Client

- Once configured, download VPN client specific to OS (Windows 64-bit)

6. Connecting from Client System

- Run the VPN client installer
- Connect to Azure VPN via installed profile
- Enter credentials when prompted

7. Verifying the Connection

* Ping the VNet IP address from your client
* Check Azure portal > Virtual Network Gateway > Connections to see status

8. Conclusion

Point-to-Site VPN on Azure provides secure, remote access for individual users. Using self-signed certificates and Azure's VPN gateway, you can test connectivity securely even with a student plan.

9. References

- Microsoft Docs: https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-certificate-gateway
- YouTube: https://youtu.be/luw2mlD7CGk
- Microsoft Certificate PowerShell Docs
- Additional: https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-point-to-site