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

R&D Document

Setting Up Site-to-Site VPN using Hyper-V and Azure

Table of Contents

1. Introduction

Site-to-Site (S2S) VPN allows a secure connection between your on-premises network (in this case, a Hyper-V machine) and Azure Virtual Network. It simulates a corporate hybrid cloud setup for learning or deployment purposes.

2. Pre-requisites

- Azure Student Subscription
- Hyper-V enabled system with Windows Server
- Public IP on the local machine or a simulated environment within Azure

3. Step-by-Step Setup

3.1 Create Resource Group

1. Go to Azure Portal.
2. Search for "Resource Groups" and click "Create".
3. Enter a name and choose Central India as the region.
4. Click Review + Create

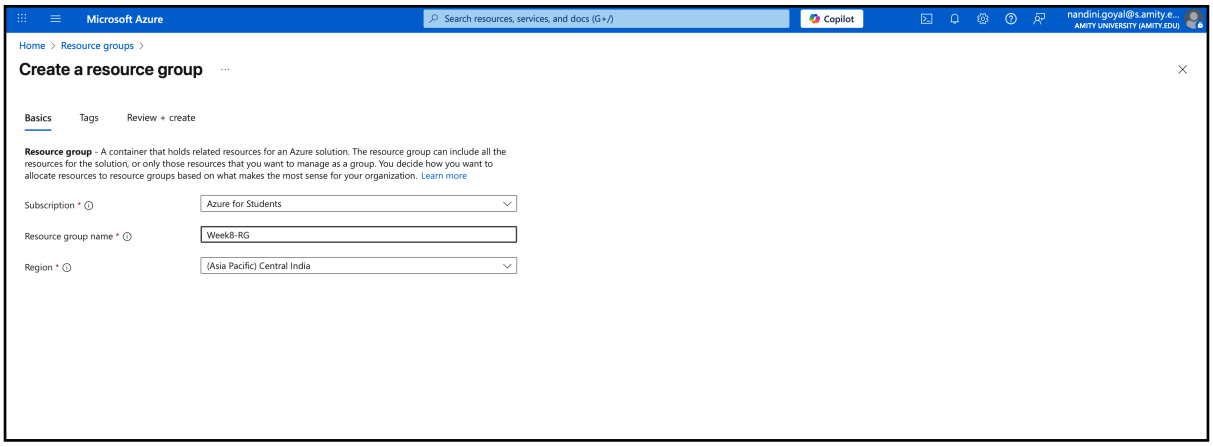

Figure 1: Resource Group

3.2 Create Virtual Network and Gateway Subnet

- Go to "Virtual Networks" > Click Create.
- Use the previously created Resource Group.
- Set the address space to `10.1.0.0/16`.
- Create a subnet (e.g., `10.1.0.0/24`).
- Add a Gateway Subnet with range `10.1.255.0/27`.

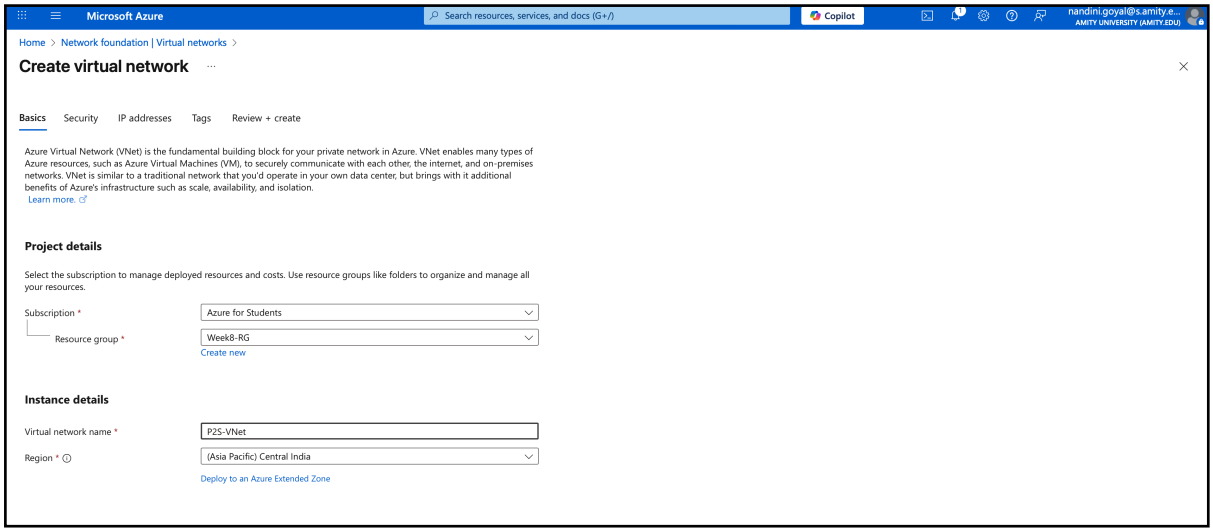

Figure 2: VNet Basics Tab

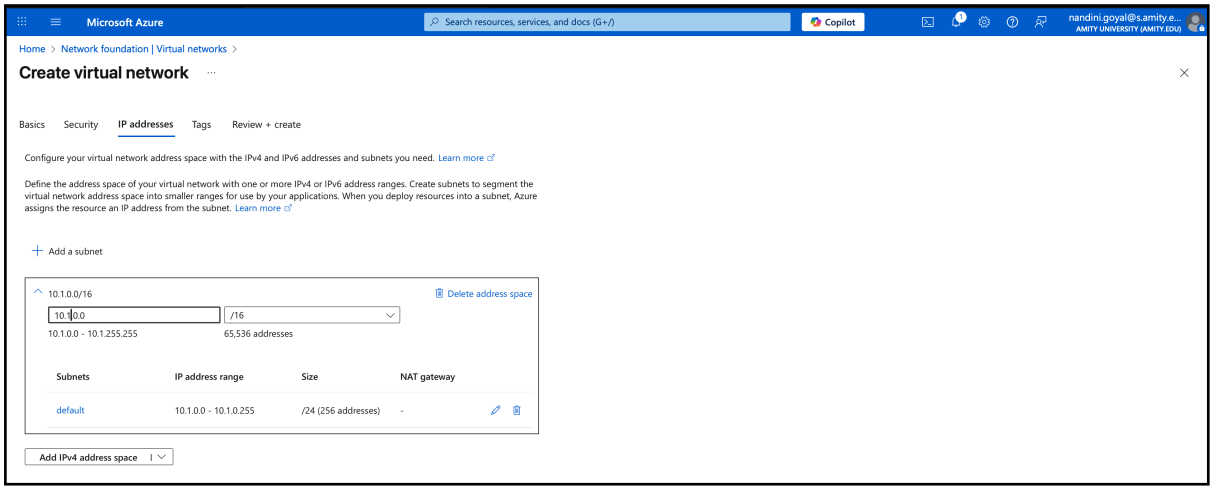

Figure 3: VNet IP Addresses Tab

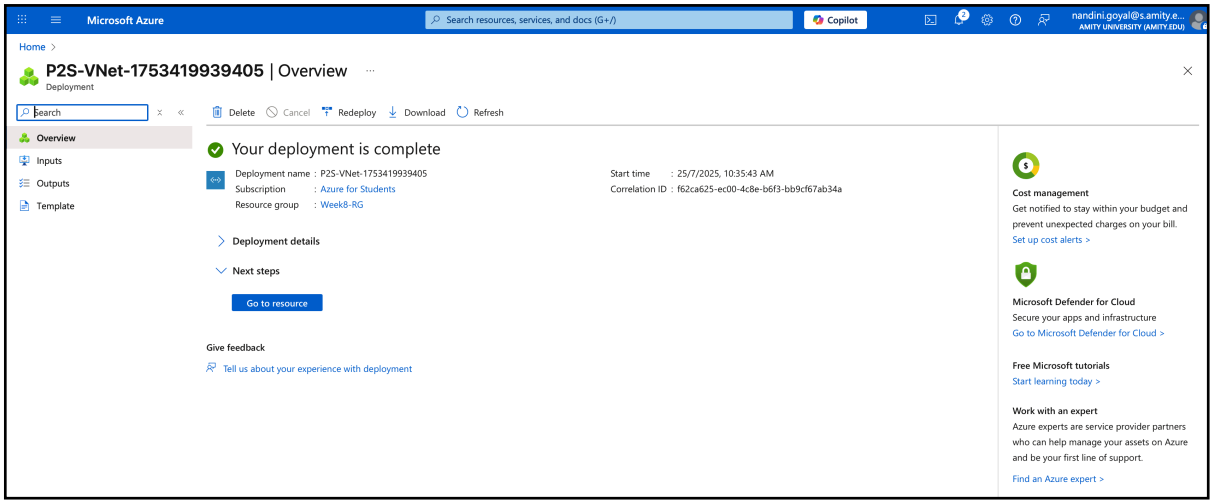

Figure 4: VNet Deployed

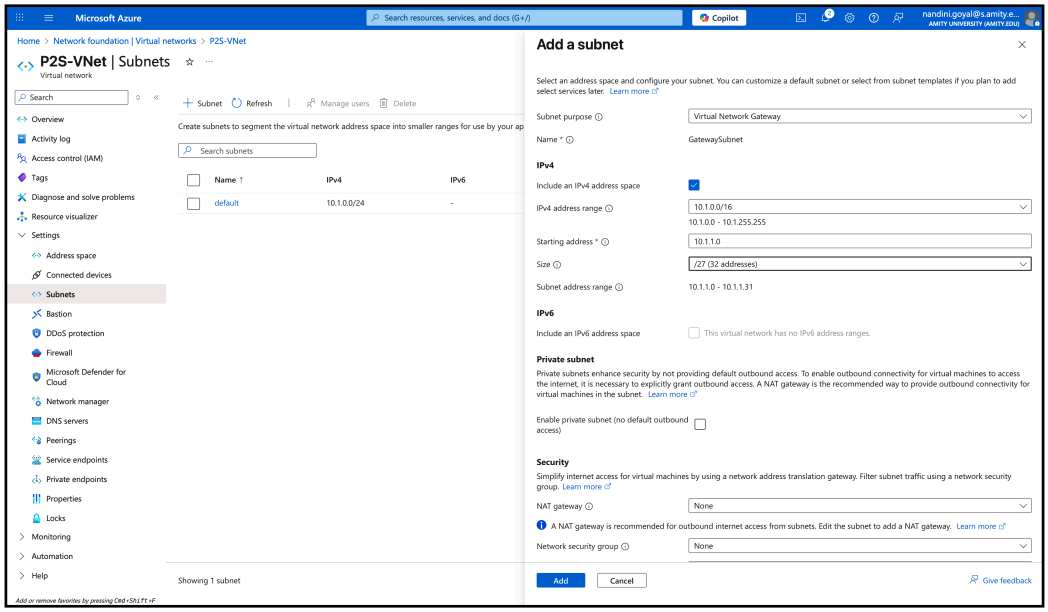

Figure 5: Gateway Subnet configuration

3.3 Create VPN Gateway

- Go to "VPN Gateways" > Click Create.
- Choose the VNet and Resource Group.
- Select Route-based, SKU: Basic.
- Assign a name and use Central India as region.

3.4 Create Local Network Gateway

1. Navigate to "Local Network Gateways" > Click Create.
2. Provide a name and use the public IP of your on-prem server (or dummy for testing).
3. Enter the address space of your on-prem network (e.g., `192.168.10.0/24`).

3.5 Configure VPN Connection

1. Go to "VPN Gateways" > Your Gateway > Connections > Click + Add.
2. Choose Site-to-Site (IPSec).
3. Link it to the Local Network Gateway.
4. Provide a shared key (e.g., `Azure123`).

3.6 Set up RRAS in Hyper-V Machine

1. On your Hyper-V Windows Server, install RRAS role.
2. Open RRAS > Configure and Enable Routing and Remote Access.
3. Select Custom Configuration → Check VPN Access and NAT.
4. Create a demand-dial interface:

- Destination: Azure VPN Gateway public IP
- Use the shared key configured earlier

3.7 Verify VPN Tunnel

1. Return to Azure → VPN Gateway → Connections.
2. Status should show Connected.
3. Use `ping`, `tracert`, or remote access tools to test the connection.

4. Conclusion

Setting up Site-to-Site VPN using Hyper-V and Azure allows students and professionals to simulate enterprise-level hybrid cloud environments. This method provides a deeper understanding of secure, persistent, cross-network communication.

5. References

- [Microsoft Docs - VPN Gateway](https://learn.microsoft.com/en-us/azure/vpn-gateway/)
- [YouTube - Site-to-Site VPN with Hyper-V](https://youtu.be/luw2mlD7CGk?si=SCpHq5xQgIddQNpq)
- [Azure VPN Gateway How-to](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal)

- [RRAS Setup - Microsoft](https://learn.microsoft.com/en-us/windows-server/remote/remote-access/ras/rras/rras-deploy)