

CELEBAL TECHNOLOGY INTERNSHIP (CSI)

Name: Harsh Tongariya

College: Arya College of Engineering Information Technology

Domain: Cloud Infra & Security

Student ID: CT\_CSI\_CI\_1160

**Research & Development Document**

Title: Setup of Site-to-Site VPN Using Hyper-V in Microsoft Azure

1. Objective

To establish a secure Site-to-Site (S2S) VPN connection between an on-premises network hosted in a Hyper-V virtualized environment and an Azure Virtual Network (VNet) using industry-standard IPSec/IKEv2 protocol. This configuration enables secure communication and seamless resource extension from on-premises to Azure.

**2. Components Required**

| Component | Description |
| --- | --- |
| Hyper-V Host | Windows Server 2016/2019/2022 with Hyper-V role enabled, acting as the local virtualization environment |
| RRAS VM | Windows Server virtual machine configured with Routing and Remote Access Service to function as the VPN gateway |
| Azure Virtual Network (VNet) | Logical isolation in Azure containing subnets and other resources |
| Azure VPN Gateway | Route-based VPN gateway resource enabling encrypted tunnels between Azure and on-premises |
| Public IP Address | Static IP used for Azure VPN Gateway and NAT IP used for the RRAS server |
| IPSec/IKE Protocols | Standard tunneling protocols used to encrypt and secure VPN traffic |

**3.Implementation Steps**

🔹 A. Azure Side Configuration

1. Create Virtual Network and Subnets

* Navigate to Azure Portal > Create Virtual Network
* Address space: 10.1.0.0/16
* Subnet (App): 10.1.1.0/24
* GatewaySubnet (mandatory): 10.1.255.0/27

2. Create Static Public IP

* Resource: Azure Public IP Address
* SKU: Standard
* Assignment: Static

3. Deploy Virtual Network Gateway

* VPN Type: Route-based
* SKU: VpnGw1 or higher
* Assign the previously created GatewaySubnet and Public IP
* Deployment may take 20–30 minutes

4. Create Local Network Gateway

* Define On-prem Public IP (NAT address used by RRAS)
* Define on-premises address range (e.g., 192.168.0.0/24)

5. Establish Site-to-Site VPN Connection

* Link the Azure VPN Gateway and Local Network Gateway
* Connection Type: Site-to-Site (IPSec)
* Enter a strong Shared Key (must match on-prem RRAS)
* Use protocol: IKEv2

🔹 B. On-Premises Configuration using Hyper-V and RRAS

1. Set Up the Hyper-V VM

* Install Windows Server on VM (name: RRAS-Gateway)
* Configure two NICs:
  + NIC1: External (with NAT/Public IP)
  + NIC2: Internal (connected to LAN)

2. Configure RRAS on the VM

* Open Server Manager > Add Roles and Features
* Select: Network Policy and Access Services > Routing and Remote Access
* Complete installation and open RRAS console

3. Enable VPN and NAT Routing

* Select Custom Configuration > Enable:
  + VPN Access
  + NAT Routing
* Start the RRAS service

4. Configure NAT

* In RRAS console, right-click server > Properties
* Set the external NIC to provide NAT

5. Create a Demand-Dial Interface

* RRAS > Network Interfaces > New Demand-dial Interface
* Name: Azure-S2S

Wizard Configuration:

| Configuration Step | Input |
| --- | --- |
| Connection Type | VPN |
| VPN Protocol | IKEv2 |
| Destination Address | Azure VPN Gateway Public IP |
| Authentication | Pre-Shared Key (same as Azure) |
| Static Routes | Add Azure VNet CIDR (e.g., 10.1.0.0/16) |

**4. Validation and Testing Procedures**

* Ensure VPN tunnel status is "Connected" in Azure Portal
* From on-prem VM: ping <Azure VM IP> and tracert
* From Azure VM: ping <on-prem resource IP>
* Run: route print, Get-NetRoute to confirm routing

**5. Security Best Practices**

* Use a strong and complex Pre-Shared Key (PSK)
* Use Network Security Groups (NSGs) to restrict inbound/outbound traffic
* Enable logging with Azure Network Watcher
* Keep RRAS Server patched and behind a firewall
* Consider deploying Azure Firewall for advanced inspection

**6. Estimated Costs**

| Azure Resource | Monthly Cost Estimate (INR) |
| --- | --- |
| VPN Gateway (VpnGw1) | ₹3,000 – ₹6,000 |
| Static Public IP | ₹200 |
| Virtual Network and Subnets | Free |
| RRAS VM (Hyper-V) | Local resource usage |

**7. Alternative Implementations**

* Use a dedicated hardware VPN device (e.g., Cisco, Juniper)
* Deploy Azure Virtual WAN for multi-branch scalability
* Replace RRAS with pfSense or MikroTik for advanced control

**8. References and Resources**

* [Microsoft Docs – Azure VPN Gateway S2S Setup](https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal)
* [RRAS Installation Guide](https://learn.microsoft.com/en-us/windows-server/remote/remote-access/ras/ras-install)
* [Hyper-V Networking Overview](https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/networking/hyper-v-networking-overview)
* https://youtu.be/luw2mlD7CGk