

Step-by-Step Configuration

1. Configure Azure Virtual Network and Gateway

- Create a Virtual Network and Gateway Subnet
- Deploy a VPN Gateway: Use VpnGw1 SKU or above
- Allocate a public IP for the gateway
- Note down the public IP address of Azure VPN Gateway

2. Install and Configure RRAS on Hyper-V Server

- Install the RRAS role via Server Manager
- Open RRAS and configure a new demand-dial interface

3. Create Demand-Dial Interface on RRAS

- In RRAS console, right-click 'Network Interfaces' > 'New Demand-Dial Interface'
- Name the interface e.g., 'AzureVPN'

- Choose 'Connect using VPN' and select 'IKEv2'
- Enter Azure VPN Gateway public IP
- Use a static route: Destination = Azure VNet address space; Mask = appropriate subnet mask
- Enter pre-shared key (must match Azure local network gateway configuration)

4. Configure Azure Local Network Gateway

- Go to Azure > Create Local Network Gateway
- Specify the on-premises public IP and address space
- Associate it with the Azure VPN Gateway connection

5. Create Site-to-Site Connection in Azure

- Go to Azure VPN Gateway > Connections > Add
- Connection type: Site-to-site (IPSec)
- Link to Local Network Gateway
- Enter pre-shared key

6. Verify the Connection

- Initiate the connection from RRAS using the demand-dial interface
- Check the status in Azure VPN Gateway > Connections
- Ping Azure VMs from your on-premises network

Verification Steps

- From on-premises, ping Azure VMs using private IP
- Use `tracert` to verify the routing through the VPN tunnel
- Monitor connection status in Azure portal and RRAS logs

References

CSI ASSIGNMENT 8

Microsoft Docs:

<https://learn.microsoft.com/en-us/azure/vpn-gateway/>

Video Guide:

<https://www.youtube.com/watch?v=luw2mID7CGk>