SITE TO SITE

Setting up a Site-to-Site VPN between Azure and Hyper-V :

We will configure a Windows Server Virtual Machine on Hyper-V to act as the "on-premises" VPN device using Routing and Remote Access Service (RRAS), and an Azure VPN Gateway as the cloud endpoint.

Instead of the expensive Azure VPN Gateway, we will deploy a Windows Server VM in Azure and configure it with RRAS (Routing and Remote Access Service) to act as the VPN endpoint, while being much more cost-effective as you can stop the VM when not using it.

Step 1.1: Prepare the Azure Virtual Network and Subnet:

- Create an Azure Resource Group: RG-S2S-HyperV-Lab
- VNET: VNet-S2S-Azure (10.0.0.0/16), a subnet: VM-Subnet (10.0.1.0/24)
- This VM-Subnet is designated to host our Azure RRAS VM, instead of a traditional Azure VPN Gateway.

Step 1.2: Deploy the Azure-Side Windows Server VM for RRAS:

- Instead of an Azure VPN Gateway, a standard Windows Server VM was deployed to run the RRAS to establish the Site-to-Site VPN.
- VM name: Azure-RRAS-SVR, Image: Win2019Datacenter.
- VM Size: Standard_B2s
- Public IP named PublicIP-AzureRRAS (4.213.137.9)
- NSG: NSG-AzureRRAS was created and associated with the VM.
    - NSG Rules: Inbound rules to allow: RDP (Port 3389), IPsec (UDP Ports 500 and 4500), ICMP (Ping).

Phase 2: Azure RRAS In-VM Configuration :

Step 2.1: Install Routing and Remote Access Role on Azure-RRAS-SVR:

- The "Remote Access" role was installed on the Azure-RRAS-SVR VM, including the DirectAccess and VPN (RAS) and Routing role services.

Step 2.2: Configure Routing and Remote Access Service on Azure-RRAS-SVR:

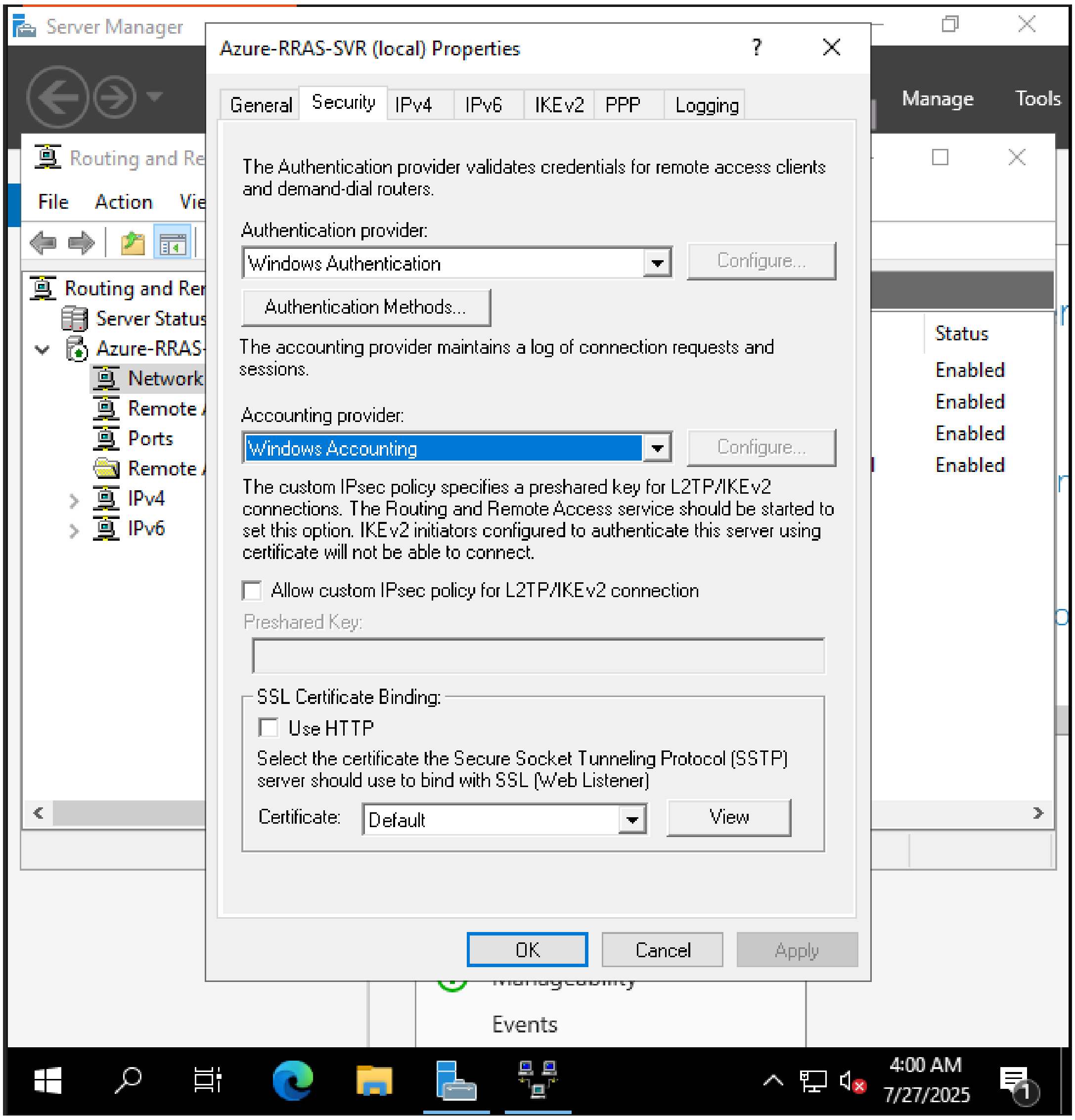
- Selected "Custom configuration" and enabled both "VPN access" and "LAN routing", The RRAS service was successfully started.

Step 2.3: Create Demand-Dial Interface (S2S-to-OnPrem) on Azure-RRAS-SVR:

- The VPN type was specified as IKEv2 (Internet Key Exchange version 2).

Step 2.4: Add Static Route for On-Premises Network on Azure-RRAS-SVR:

- This route directs traffic destined for your on-premises network (e.g., 192.168.1.0/24) through the S2S-to-OnPrem VPN interface.



Azure-RRAS-SVR (local) Properties

General | Security | IPv4 | IPv6 | IKEv2 | PPP | Logging

The Authentication provider validates credentials for remote access clients and demand-dial routers.

Authentication provider: Windows Authentication

Authentication Methods...

The accounting provider maintains a log of connection requests and sessions.

Accounting provider: Windows Accounting

The custom IPsec policy specifies a preshared key for L2TP/IKEv2 connections. The Routing and Remote Access service should be started to set this option. IKEv2 initiators configured to authenticate this server using certificate will not be able to connect.

☐ Allow custom IPsec policy for L2TP/IKEv2 connection

Preshared Key:

SSL Certificate Binding:

☐ Use HTTP

Select the certificate the Secure Socket Tunneling Protocol (SSTP) server should use to bind with SSL (Web Listener)

Certificate: Default

Status
Enabled
Enabled
Enabled
Enabled

Phase 3: On-Premises Hyper-V RRAS Configuration (In-VM):

Step 3.1: Prepare On-Premises Windows Server VM for RRAS:

- Windows Server VM: OnPrem-RRAS-Server was ready in Hyper-V environment.
- This VM was configured with at least two network adapters: one external (public-facing for internet access) and one internal.

Step 3.2: Install Routing and Remote Access Role on OnPrem-RRAS-Server:

- The "Remote Access" role was installed on the OnPrem-RRAS-Server VM, including DirectAccess and VPN (RAS) and Routing role services.

Step 3.3: Configure RRAS on OnPrem-RRAS-Server:

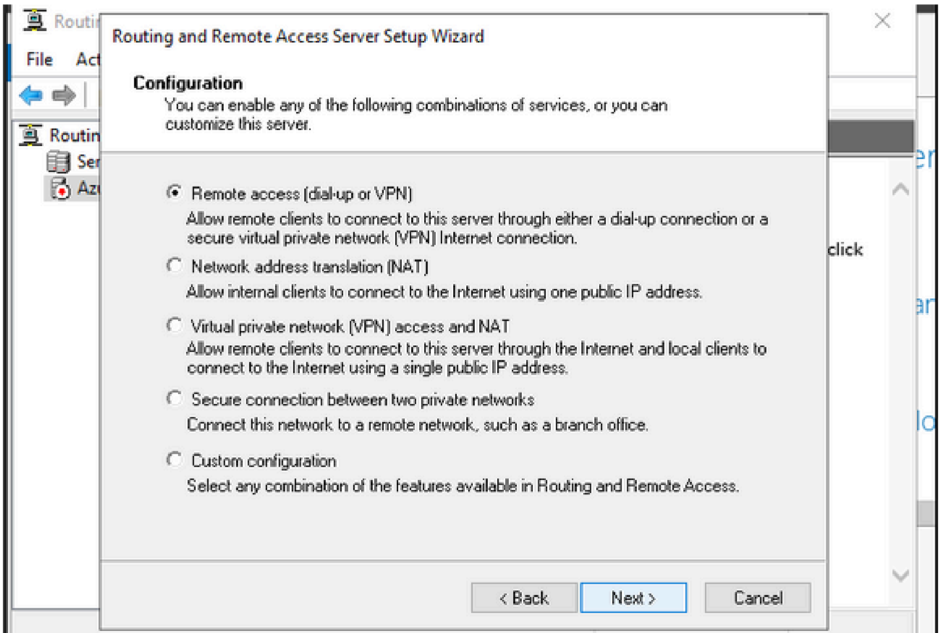
- The RRAS service was configured using "Custom configuration" with "VPN access" and "LAN routing" enabled, then started successfully.

Step 3.4: Create Demand-Dial Interface on OnPrem-RRAS-Server:

- The VPN type was set to IKEv2.
- The Destination Address was set to: 4.213.137.9.
- The Pre-Shared Key (PSK) was configured on this interface.

Step 3.5: Add Static Route for Azure VNet on OnPrem-RRAS-Server:

- A static route was added in the RRAS console to direct traffic for the Azure VNet (10.0.0.0/16) through the S2S-to-Azure VPN interface.



Routing and Remote Access Server Setup Wizard

Configuration

You can enable any of the following combinations of services, or you can customize this server.

● Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.

○ Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.

○ Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.

○ Secure connection between two private networks
Connect this network to a remote network, such as a branch office.

○ Custom configuration
Select any combination of the features available in Routing and Remote Access.

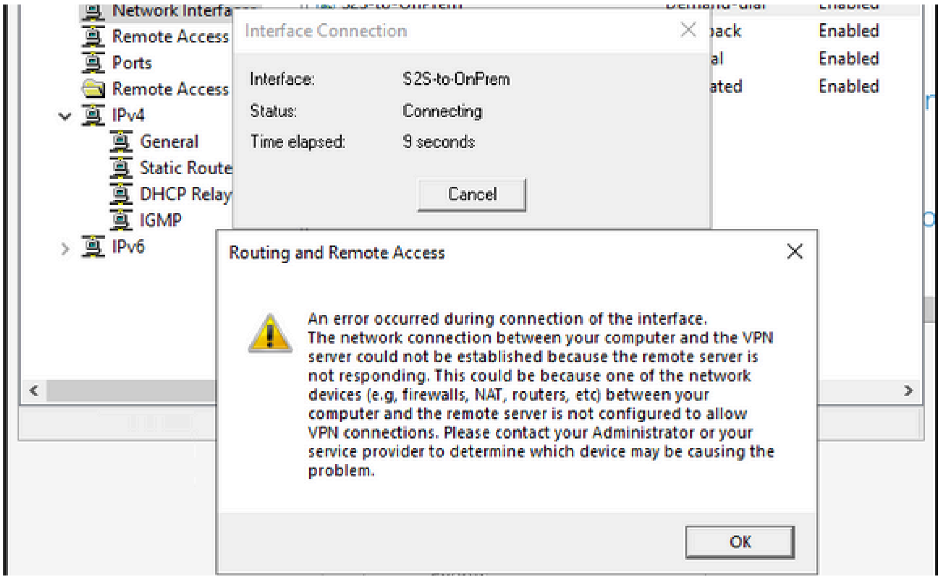
Phase 4: VPN Connection Testing & Current Limitation:

Step 4.1: Attempt to Connect VPN and Troubleshooting:

- An attempt was made to connect the VPN interface from the Azure-RRAS-SVR side.
- Initial errors like "remote access server did not resolve" were encountered, indicating an issue with the Azure VM being able to find the on-premises public IP.
- After ensuring the destination IP was the correct on-premises public IP, the error changed to "remote server is not responding".

Step 4.2: Identification of Hotspot Limitation:

- The primary reason for the "remote server is not responding" error was identified: using a phone hotspot for internet connection.
- Most phone hotspots utilize Carrier-Grade NAT (CGNAT), which prevents direct inbound connections and port forwarding (specifically UDP 500 and 4500) from the internet to devices behind the hotspot. This means the Azure RRAS server cannot initiate and establish the VPN tunnel with your OnPrem-RRAS-Server.
- It means the process and all the steps above are correctly executed and the test will be passed if the internet connection was changed.



Interface Connection

Interface: S2S-to-OnPrem

Status: Connecting

Time elapsed: 9 seconds

Routing and Remote Access

An error occurred during connection of the interface.
The network connection between your computer and the VPN server could not be established because the remote server is not responding. This could be because one of the network devices (e.g, firewalls, NAT, routers, etc) between your computer and the remote server is not configured to allow VPN connections. Please contact your Administrator or your service provider to determine which device may be causing the problem.

CONCLUSION

Did:

- Deployed Azure network resources and a Windows Server VM using Azure CLI.
- Configured Routing and Remote Access Service (RRAS) on both the Azure VM and an on-premises Hyper-V VM for a Site-to-Site VPN.
- Set up VPN interfaces (IKEv2, PSK) and static routes on both ends.
- Troubleshooted Azure deployment errors (memory, IP conflicts) and RRAS connection issues.

Learned:

- Practical Azure CLI deployment for networking and VMs.
- How to configure Windows Server RRAS for Site-to-Site VPNs.
- The critical roles of IP Forwarding, NSG rules, and static routes in VPN connectivity.
- Major impact of network limitations like Carrier-Grade NAT (CGNAT) from phone hotspots, which ultimately prevented the VPN from establishing due to blocked inbound connections, despite correct configurations.
- Essential troubleshooting skills for hybrid cloud networking.

Submitted by:

Sambit Kumar Panda

References:

https://learn.microsoft.com/en-us/azure/virtual-network/

https://learn.microsoft.com/en-us/windows-server/remote/remote-access/get-started-install-ras-as-vpn

https://www.google.com/search?q=https://learn.microsoft.com/en-us/windows-server/remote/remote-access/rras/routing-and-remote-access

https://www.draytek.co.uk/information/blog/what-is-cgnat