# Week – 8 Assignment

## Setting Up Site-to-Site VPN Using Hyper-V

### Introduction

A Site-to-Site (S2S) VPN allows you to connect two separate networks over the internet securely. This is commonly used to connect a branch office network to a company headquarters network. In this guide, we will set up an S2S VPN using Hyper-V.

### Objectives

- Understand the requirements for setting up an S2S VPN.
- Set up a Hyper-V virtual machine (VM) to act as a VPN gateway.
- Configure the VPN gateway and establish a site-to-site VPN connection.

### Prerequisites

- Two separate networks with internet connectivity.
- Windows Server with Hyper-V installed.
- Administrative rights to perform actions on the server.

### Steps to Set Up Site-to-Site VPN Using Hyper-V using Azure GUI mode

### 1. Set Up Hyper-V Virtual Machines

1. **Install Hyper-V**:
    - Ensure that the Hyper-V role is installed on your Windows Server.
    - Open **Server Manager**, go to **Manage** > **Add Roles and Features** > **Role-based or feature-based installation**.
    - Select **Hyper-V** and follow the prompts to complete the installation.
2. **Create Virtual Machines**:
    - Open **Hyper-V Manager**.
    - Right-click on your server and select **New** > **Virtual Machine**.
    - Follow the prompts to create two VMs, one for each network you wish to connect.

### 2. Configure the Virtual Network Adapters

1. **Create Virtual Switches**:
    - In **Hyper-V Manager**, go to **Virtual Switch Manager**.
    - Create an external virtual switch for each network interface on the server.

2. **Assign Network Adapters to VMs**:
    - Go to each VM's settings.
    - Add network adapters and connect them to the appropriate virtual switches.

**3. Install Routing and Remote Access Service (RRAS)**

1. **Install RRAS on Each VM**:
    - Log in to each VM.
    - Open **Server Manager**, go to **Manage** > **Add Roles and Features**.
    - Install the **Remote Access** role and **Routing** role service.
2. **Configure RRAS**:
    - Open **Routing and Remote Access** from the **Administrative Tools**.
    - Right-click on the server name and select **Configure and Enable Routing and Remote Access**.
    - Choose **Custom Configuration** > **VPN Access** and **LAN Routing**.
    - Start the service after configuration.

**4. Set Up VPN on RRAS**

1. **Configure VPN Properties**:
    - In **Routing and Remote Access**, right-click the server name and select **Properties**.
    - Go to the **Security** tab, configure authentication methods, and ensure **Allow custom IPsec policy for L2TP/IKEv2 connection** is enabled.
    - Set up a pre-shared key for IPsec.
2. **Configure IP Address Assignment**:
    - Go to the **IPv4** tab and configure the static address pool for VPN clients.
    - Ensure that IP forwarding is enabled between network interfaces.

**5. Configure Static Routes**

1. **Add Static Routes on Each VM**:
    - In **Routing and Remote Access**, expand **IP Routing** > **Static Routes**.
    - Add routes to direct traffic between the two networks.

**6. Establish Site-to-Site VPN Connection**

1. **Configure Demand-Dial Interface**:

- In **Routing and Remote Access**, right-click **Network Interfaces** and select **New Demand-Dial Interface**.
- Follow the wizard to create a demand-dial interface, specifying the IP address of the remote VPN gateway.

2. **Configure VPN Credentials**:
   - Set up the authentication credentials to match the settings on the remote VPN gateway.
   - Ensure the pre-shared key matches the one configured earlier.
3. **Test the Connection**:
   - Start the demand-dial interface and verify the connection.
   - Check the status and logs for any errors.

**Testing the Connection**

- Verify that you can ping resources on the remote network from each side.
- Test access to network services to ensure full connectivity.

**Troubleshooting Tips**

- Ensure that firewalls on both sides allow VPN traffic.
- Verify that network adapters are correctly configured.
- Check RRAS logs for any connection issues.
- Ensure that routing tables are correctly set up.

**Steps to Set Up Site-to-Site VPN Using Hyper-V using Azure CLI mode**

**1. Create a Resource Group**

```
az group create --name MyResourceGroup --location eastus
```

**2. Create a Virtual Network**

```
az network vnet create --resource-group MyResourceGroup --name MyVNet --address-prefix 10.0.0.0/16 --subnet-name MySubnet --subnet-prefix 10.0.0.0/24
```

**3. Create a Virtual Network Gateway**

First, create a public IP address for the gateway:

```
az network public-ip create --resource-group MyResourceGroup --name MyVNetGatewayIP --allocation-method Dynamic
```

Then, create the virtual network gateway:

```
az network vnet-gateway create --resource-group MyResourceGroup --name MyVNetGateway --public-ip-address MyVNetGatewayIP --vnet MyVNet --gateway-type Vpn --vpn-type RouteBased --sku VpnGw1 --no-wait
```

**4. Create a Local Network Gateway**

```
az network local-gateway create --resource-group MyResourceGroup --name MyLocalGateway --gateway-ip-address <OnPremPublicIP> --local-address-prefixes <OnPremNetworkCIDR>
```

**5. Create the VPN Connection**

```
az network vpn-connection create --resource-group MyResourceGroup --name MyConnection --vnet-gateway1 MyVNetGateway --local-gateway2 MyLocalGateway --shared-key "YourSharedKey"
```

**On-Premises Hyper-V Configuration**

**1. Install and Configure RRAS**

On the Hyper-V host, install and configure RRAS to function as a VPN gateway.

1. **Install RRAS**
    - Open Server Manager, go to Manage -> Add Roles and Features.
    - Select Role-based or feature-based installation.
    - In the Roles section, select Remote Access.
    - In the Features section, ensure DirectAccess and VPN (RAS) is checked.
    - Complete the installation.
2. **Configure RRAS**
    - Open the RRAS console.
    - Right-click your server and select Configure and Enable Routing and Remote Access.
    - Choose Custom configuration, then select VPN access and LAN routing.
    - Complete the configuration and start the service.
3. **Set Up the VPN Connection**
    - Right-click your server in the RRAS console, go to Properties.
    - Under the Security tab, ensure that Allow custom IPsec policy for L2TP/IKEv2 connection is checked.
    - Enter the Pre-shared key used in the Azure VPN connection setup.
4. **Add Static Routes**

- Add static routes to the RRAS server to route traffic to the Azure virtual network.

route -p add <AzureNetworkCIDR> mask 255.255.255.0 <OnPremGatewayIP>

**Verify the Connection**

1. **Check the Connection Status**
   - In the Azure portal, navigate to your virtual network gateway.
   - Check the connection status to ensure it is Connected.
2. **Verify Traffic Flow**
   - Test the connectivity by pinging VMs in the Azure virtual network from your on-premises network and vice versa.

**Conclusion**

Setting up a Site-to-Site VPN using Hyper-V involves creating virtual machines, configuring RRAS, and establishing a VPN connection between two networks. By following this guide, you can set up a secure connection to link two separate networks, enabling seamless communication and resource sharing.