Celebal Assignment - 8

How to setup Point to Site

To set up a Point-to-Site (P2S) VPN connection with certificate authentication using the Azure portal, follow these steps:

1. Azure Subscription: Ensure you have an active Azure subscription. You can sign up for a free account if you don't have one.

Example Values

Virtual Network (VNet) Configuration:

- VNet Name: VNet1
- Address Space: 10.1.0.0/16
- Subnet Name: FrontEnd
- Subnet Address Range: 10.1.0.0/24
- Resource Group: TestRG1
- Location: East US

Virtual Network Gateway Configuration:

- Name: VNet1GW
- Gateway Type: VPN
- VPN Type: Route-based (required for P2S)
- SKU: VpnGw2
- Generation: Generation2
- Gateway Subnet Address Range: 10.1.255.0/27
- Public IP Address Name: VNet1GWpip

Connection Type and Client Address Pool:

- Connection Type: Point-to-site
- Client Address Pool: 172.16.201.0/24

Steps to Configure P2S VPN with Certificate Authentication

1. Create a VNet

1. Sign in to the Azure portal.

2. In the search bar, type "virtual network" and select Virtual network from the results.
3. Click Create.
4. On the Basics tab, configure the following settings:
   - Subscription: Select your subscription.
   - Resource Group: Select TestRG1 or create a new one.
   - Name: Enter VNet1.
   - Region: Select East US.
5. Click Next: IP Addresses.
6. Configure the IP address settings:
   - IPv4 Address Space: Add 10.1.0.0/16.
   - Subnet: Click + Add subnet, enter FrontEnd for the subnet name, and 10.1.0.0/24 for the subnet address range.
7. Click Review + create, then Create.

2. Create a Gateway Subnet

1. Go to your VNet VNet1.
2. In the left pane, select Subnets.
3. Click + Gateway subnet.
4. Enter 10.1.255.0/27 for the address range.
5. Click Save.

3. Create the VPN Gateway

1. In the search bar, type "virtual network gateway" and select Virtual network gateway.
2. Click Create.
3. On the Basics tab, configure the following settings:
   - Subscription: Select your subscription.
   - Resource Group: Select TestRG1.
   - Name: Enter VNet1GW.
   - Region: Select East US.
   - Gateway Type: Select VPN.
   - VPN Type: Select Route-based.
   - SKU: Select VpnGw2.
   - Generation: Select Generation2.
4. Configure the Virtual Network:
   - Virtual Network: Select VNet1.
   - Gateway Subnet: Should be autofilled with 10.1.255.0/27.
5. Configure the Public IP Address:
   - Public IP Address: Select Create new.
   - Name: Enter VNet1GWpip.
6. Click Review + create, then Create.

4. Generate Certificates

Root Certificate

1. Obtain a .cer file for the root certificate:
- Use an enterprise solution or generate a self-signed certificate.
- Export the public certificate data as a Base64 encoded X.509 .cer file.

Client Certificate

1. Generate a client certificate from the root certificate and install it on each client computer:
- Use Power Shell, Make Cert, or Open SSL to generate client certificates.

5. Configure P2S VPN in Azure

1. Go to your VPN gateway VNet1GW.
2. In the left pane, select Point-to-site configuration.
3. Click Configure now.
4. Enter 172.16.201.0/24 for the client address pool.
5. Select IKEv2 and Open VPN(SSL) for the tunnel type.
6. Select Azure certificate for the authentication type.
7. Upload the public root certificate data:
- Open the .cer file in a text editor.
- Copy the certificate data and paste it into the Public certificate data field.
- Name the certificate.
8. Click Save.

6. Download VPN Client Configuration

1. On the Point-to-site configuration page, click Download VPN client.
2. Unzip the downloaded file and use the configuration files to configure your VPN client.

7. Connect VPN Client to Azure

1. Use the appropriate VPN client software based on your operating system and the selected tunnel type.
2. Install the client certificate on your client computer.
3. Configure the VPN client using the downloaded configuration files.
4. Connect to the VPN and verify the connection by checking the assigned IP address.

Verify Connection

1. Open an elevated command prompt and run `ip config /all`.

2. Check that the IP address is within the client address pool range (e.g., 172.16.201.x).

Connect to a Virtual Machine (VM)

1. Locate the private IP address of the VM in the Azure portal or via Power Shell.
2. Open Remote Desktop Connection and enter the private IP address of the VM to connect.

By following these steps, you can create a P2S VPN configuration using certificate authentication and the Azure portal.

How to setup Site to Site using Hyper-V

Setting up a Site-to-Site (S2S) VPN using Hyper-V involves configuring a VPN gateway on both sides of the connection—your on-premises network and the Azure network. Here's a step-by-step guide to help you set up a Site-to-Site VPN using Hyper-V:

1. Azure Subscription: Ensure you have an active Azure subscription.
2. On-Premises Network: You need a network infrastructure with Hyper-V enabled.
3. VPN Device: A compatible VPN device or Windows Server with Routing and Remote Access Service (RRAS) configured as a VPN server.

Step 1: Create a Virtual Network in Azure

1. Sign in to the Azure portal: [Azure Portal](https://portal.azure.com)
2. Create a Virtual Network:
- In the portal, search for "Virtual network" and click on "Create".
- Fill in the necessary details like `Name`, `Address space`, `Resource group`, `Location`, etc.
- Example:
- `Name`: VNet1
- `Address space`: 10.1.0.0/16
- `Subnet name`: FrontEnd
- `Subnet address range`: 10.1.0.0/24

Step 2: Create a Gateway Subnet in Azure

1. Add Gateway Subnet:
- Go to the created virtual network (VNet1).
- Click on "Subnets" and then "+ Gateway subnet".
- Specify the `Address range` (e.g., 10.1.255.0/27) and click "Save".

Step 3: Create the VPN Gateway in Azure

1. Create VPN Gateway:
- In the portal, search for "Virtual network gateway" and click on "Create".
- Fill in the required details:
- `Name`: VNet1GW
- `Region`: (Same as your VNet)

- `Gateway type`: VPN
- `VPN type`: Route-based
- `SKU`: VpnGw2
- `Generation`: Generation2
- `Virtual network`: Select VNet1
- `Gateway subnet address range`: 10.1.255.0/27
- `Public IP address`: Create a new one, e.g., VNet1GWpip

- Click "Review + create" and then "Create".

Step 4: Configure the On-Premises VPN Device or RRAS

1. Install RRAS on Windows Server (if using Windows Server):
   - Open Server Manager.
   - Add the `Remote Access` role and `Routing`.
   - Configure RRAS and set up as a VPN Server.

2. Configure S2S VPN on RRAS:
   - Open the RRAS console.
   - Right-click on the server name and select "Configure and Enable Routing and Remote Access".
   - Select "Custom configuration" and choose "VPN access" and "LAN routing".
   - Right-click on the server name again, go to "Properties", and configure the `Security` tab to enable IKEv2.
   - Configure the `IP` tab to set up the IP address assignment.

3. Configure S2S Connection:
   - Go to "Network Interfaces", right-click and select "New Demand-dial Interface".
   - Follow the wizard to configure the connection:
     - `Connection name`: AzureS2S
     - `VPN Type`: IKEv2
     - `IP Address of Azure VPN Gateway`: (e.g., 52.174.34.24 from Azure)
     - `Credentials`: Use shared key from Azure.

Step 5: Configure the Local Network Gateway in Azure

1. Create Local Network Gateway:
   - In the portal, search for "Local network gateway" and click on "Create".
   - Fill in the required details:
     - `Name`: OnPremGateway
     - `IP address`: Public IP of your on-premises VPN device
     - `Address space`: On-premises network address range (e.g., 192.168.1.0/24)
   - Click "Review + create" and then "Create".

Step 6: Create the VPN Connection in Azure

1. Create VPN Connection:
- **Go to the created Virtual Network Gateway (VNet1GW).**
- **Click on "Connections" and then "+ Add".**
- **Fill in the required details:**
  - **`Name`: VNet1-to-OnPrem**
  - **`Connection type`: Site-to-site (IPsec)**
  - **`Virtual network gateway`: VNet1GW**
  - **`Local network gateway`: OnPremGateway**
  - **`Shared key (PSK)`: Same as configured in RRAS**

Step 7: Verify the VPN Connection

1. Check Connection Status:
- **In the Azure portal, go to "Virtual network gateways" -> "Connections".**
- **Verify that the connection status is "Connected".**
- **On the RRAS server, check the connection status in the "Routing and Remote Access" console.**