Week – 8 Assignment

A. Setting Up Point-to-Site VPN

Introduction

A Point-to-Site (P2S) VPN allows you to create a secure connection to your virtual network from an individual client computer. This setup is commonly used when you need to connect to your virtual network from a remote location, such as from home or on the road.

Objectives

- Understand the requirements for setting up a P2S VPN.
- Set up a P2S VPN in an Azure environment.
- Test the connection from a client computer.

Prerequisites

- An active Azure subscription.
- A configured virtual network (VNet).
- A configured subnet within the VNet.
- Administrative rights to perform actions in the Azure portal.

Steps to Set Up Point-to-Site VPN using Azure GUI mode

1. Create a Virtual Network Gateway

1. **Navigate to the Azure Portal**:
    - Go to the Azure portal (https://portal.azure.com/).
2. **Create a Virtual Network Gateway**:
    - Select **Create a resource** > **Networking** > **Virtual Network Gateway**.
    - Fill in the required details:
        - **Name**: Enter a name for your gateway.
        - **Region**: Select the region where your resources are located.
        - **Gateway type**: Select **VPN**.
        - **VPN type**: Select **Route-based**.
        - **SKU**: Choose the appropriate SKU based on your bandwidth requirements.
        - **Virtual network**: Select your virtual network.
        - **Public IP address**: Create a new public IP address.

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

2. Configure Point-to-Site VPN

1. **Navigate to the Virtual Network Gateway**:
    - Go to **Virtual Network Gateways** and select your newly created gateway.
2. **Configure P2S Settings**:
    - In the **Settings** section, select **Point-to-site configuration**.
    - Click **Configure now**.
3. **Fill in the Point-to-site Configuration**:
    - **Address pool**: Enter an IP address range for the VPN clients, e.g., 172.16.0.0/24.
    - **Tunnel type**: Select **OpenVPN (SSL)**, **IKEv2**, or both.
    - **Authentication type**: Select **Azure Certificate** or **Azure Active Directory**.
    - **Root certificate**: Upload or generate a root certificate.
    - **Client certificate**: Generate and upload a client certificate if required.

3. Generate and Upload Certificates

1. **Generate a Self-Signed Root Certificate** (if not using Azure AD):
    - Use PowerShell or OpenSSL to generate a self-signed root certificate.
    - Export the root certificate in Base-64 encoded X.509 (.cer) format.
2. **Generate a Client Certificate**:
    - Use the root certificate to generate a client certificate.
    - Export the client certificate in PFX format.
3. **Upload the Certificates**:
    - Upload the root certificate to the Azure portal under the **Point-to-site configuration** section.

4. Download the VPN Client Configuration

1. **Navigate to the Virtual Network Gateway**:
    - Go to **Virtual Network Gateways** and select your gateway.
2. **Download VPN Client**:
    - In the **Settings** section, select **Point-to-site configuration**.
    - Click **Download VPN client**.

3. **Install the VPN Client**:
    - Download the appropriate VPN client configuration file for your operating system.
    - Install the VPN client on your local machine.

5. Connect to the VPN

1. **Install the Client Certificate** (if using certificates):
    - Install the client certificate on your local machine.
2. **Connect to the VPN**:
    - Open the installed VPN client.
    - Enter the connection details provided in the configuration file.
    - Connect to the VPN.

Testing the Connection

- Verify that the client machine has received an IP address from the address pool configured in the P2S setup.
- Test connectivity to resources within the virtual network.

Troubleshooting Tips

- Ensure that the virtual network gateway is correctly configured and in a running state.
- Verify that the client certificate is installed correctly on the client machine.
- Check the VPN client's log for any error messages.
- Ensure that the firewall on the client machine is not blocking the VPN connection.

Steps to Set Up Point-to-Site VPN 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 MyGatewayIP --allocation-method Dynamic
```

Then, create the gateway:

```
az network vnet-gateway create --resource-group MyResourceGroup --name MyGateway --public-ip-address MyGatewayIP --vnet MyVnet --gateway-type Vpn --vpn-type RouteBased --sku VpnGw1 --no-wait
```

4. Configure the Point-to-Site VPN

Generate VPN Client Root Certificate and Client Certificate

You need to create a root certificate and a client certificate. You can do this using OpenSSL or makecert on Windows.

For example, using OpenSSL:

1. Create a Root Certificate

   ```
   openssl req -x509 -newkey rsa:2048 -keyout VPNRootPrivateKey.pem -out VPNRootCertificate.pem -days 365 -nodes -subj "/CN=MyVPNRootCA"
   ```

2. Create a Client Certificate

   ```
   openssl req -newkey rsa:2048 -keyout VPNClientPrivateKey.pem -out VPNClientCertificate.csr -nodes -subj "/CN=MyVPNClient"
   ```

   ```
   openssl x509 -req -in VPNClientCertificate.csr -CA VPNRootCertificate.pem -CAkey VPNRootPrivateKey.pem -CAcreateserial -out VPNClientCertificate.pem -days 365
   ```

Upload the Root Certificate

Convert the root certificate to Base64 and upload it:

```
ROOT_CERT_DATA=$(cat VPNRootCertificate.pem | base64 | tr -d '\n')
```

```
az network vnet-gateway root-cert create --resource-group MyResourceGroup --gateway-name MyGateway --name MyRootCert --public-cert-data "$ROOT_CERT_DATA"
```

5. Configure the VPN Client Address Pool

```
az network vnet-gateway update --resource-group MyResourceGroup --name MyGateway --set vpnClientAddressPool=172.16.201.0/24
```

6. Generate VPN Client Configuration

After the gateway is created, generate and download the VPN client configuration:

```
az network vnet-gateway vpn-client generate --resource-group MyResourceGroup --name MyGateway --authentication-method EAPTLS --client-root-cert MyRootCert --no-wait
```

7. Install VPN Client on Your Computer

Download the VPN client configuration package from the Azure portal or using Azure CLI. The package includes the necessary configuration files for connecting to the VPN from your computer.

8. Connect to the VPN

1. Install the VPN client on your computer using the downloaded configuration package.
2. Use the VPN client to connect to the Azure VPN.

This process sets up a Point-to-Site VPN connection in Azure using Azure CLI. Ensure you have the necessary permissions and environment set up before proceeding with these steps.

Conclusion

Setting up a Point-to-Site VPN in Azure allows secure remote access to your virtual network. By following the steps outlined in this document, you can create and configure a P2S VPN using GUI and CLI mode, generate necessary certificates, and test the connection from a client machine. This setup is essential for providing secure and flexible remote access to your network resources.