**R&D Document: Setting Up Point-to-Site (P2S) VPN**

**1. Introduction**

A Point-to-Site (P2S) VPN connection enables you to create a secure connection to your Azure Virtual Network (VNet) from an individual client computer. This is useful for remote workers who need to access resources in Azure securely.

**2. Prerequisites**

* **Azure Subscription**: Ensure you have an active Azure subscription.
* **Virtual Network**: You should have an existing VNet.
* **VPN Client**: The client computer needs a VPN client installed.

**3. Step-by-Step Setup**

**Step 1: Create a Virtual Network**

1. **Navigate to Azure Portal**:
   * Go to the Azure portal.
2. **Create a VNet**:
   * In the left-hand menu, select "Create a resource" > "Networking" > "Virtual network".
   * Enter the following details:
     + **Name**: MyVNet
     + **Address space**: 10.1.0.0/16
     + **Subnet name**: Subnet1
     + **Subnet address range**: 10.1.0.0/24
   * Click "Review + create" and then "Create".

**Step 2: Create a Virtual Network Gateway**

1. **Navigate to Virtual Network Gateways**:
   * In the left-hand menu, select "Create a resource" > "Networking" > "Virtual network gateway".
2. **Configure the Virtual Network Gateway**:
   * Enter the following details:
     + **Name**: MyVNetGateway
     + **Region**: Same as your VNet
     + **Gateway type**: VPN
     + **VPN type**: Route-based
     + **SKU**: Select an appropriate SKU (e.g., VpnGw1)
     + **Virtual network**: Select MyVNet
     + **Public IP address**: Create a new one, name it MyVNetGatewayIP
   * Click "Review + create" and then "Create".
   * Note: It can take 45 minutes or more for the gateway to be created.

**Step 3: Configure Point-to-Site VPN**

1. **Navigate to the Virtual Network Gateway**:
   * In the left-hand menu, select "Virtual network gateways", then select MyVNetGateway.
2. **Configure Point-to-Site Settings**:
   * In the settings section, select "Point-to-site configuration".
   * Click on "Configure now" and enter the following details:
     + **Address pool**: 172.16.0.0/24 (This is the range of IP addresses that will be assigned to VPN clients)
     + **Tunnel type**: Select SSTP (SSL) or IKEv2
     + **Authentication type**: Azure certificate or Azure Active Directory
     + **Root certificate**: Upload the root certificate in Base-64 format (if using certificate-based authentication)

**Step 4: Generate and Upload Certificates (if using Certificate-based Authentication)**

1. **Generate a Self-Signed Root Certificate**:
   * On a Windows machine, open PowerShell as an administrator and run:

powershell

Copy code

$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature -Subject "CN=MyRootCert" -KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign -NotAfter (Get-Date).AddYears(5)

1. **Export the Root Certificate**:
   * Open certmgr.msc, find MyRootCert under Personal > Certificates, right-click and select "Export".
   * Choose "Base-64 encoded X.509 (.CER)" and save the file.
2. **Upload the Root Certificate**:
   * In the Azure portal, under "Point-to-site configuration", upload the .cer file.
3. **Generate a Client Certificate**:
   * Run the following PowerShell command:

powershell

Copy code

$clientCert = New-SelfSignedCertificate -Type Custom -DnsName MyClientCert -KeySpec Signature -Subject "CN=MyClientCert" -KeyExportPolicy Exportable -HashAlgorithm sha256 -KeyLength 2048 -CertStoreLocation "Cert:\CurrentUser\My" -Signer $cert -KeyUsageProperty Sign -KeyUsage CertSign -NotAfter (Get-Date).AddYears(5)

1. **Export the Client Certificate**:
   * Open certmgr.msc, find MyClientCert under Personal > Certificates, right-click and select "Export".
   * Choose "Yes, export the private key" and follow the steps to export as .pfx file.

**Step 5: Download and Install the VPN Client**

1. **Download the VPN Client**:
   * In the Azure portal, navigate to "Point-to-site configuration" of MyVNetGateway and click "Download VPN client".
2. **Install the VPN Client**:
   * Extract the downloaded file and run the VPN client installer on your client machine.
3. **Configure the VPN Client**:
   * If using certificate-based authentication, import the .pfx client certificate to the client machine.
   * Open the VPN client and connect to the Azure VPN.

**Step 6: Verify the VPN Connection**

1. **Verify the Connection**:
   * Once connected, verify that the client machine has an IP address from the P2S address pool.
   * Test connectivity to resources in the Azure VNet.

**4. Best Practices**

* **Use Strong Authentication**: Prefer using Azure Active Directory for authentication over certificates for added security.
* **Monitor VPN Connections**: Use Azure Monitor to keep track of active VPN connections and any potential issues.
* **Regularly Rotate Certificates**: If using certificate-based authentication, ensure certificates are rotated regularly to maintain security.

**5. Conclusion**

Setting up a Point-to-Site VPN allows secure remote access to Azure resources. Following the steps outlined ensures a secure and reliable connection for remote users. This setup enhances security, provides flexibility, and ensures that remote workers can access necessary resources efficiently.

**References**

* [Azure Virtual Network Documentation](https://docs.microsoft.com/en-us/azure/virtual-network/)
* [Point-to-Site VPN Overview](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal)

This R&D document provides a comprehensive guide to setting up a Point-to-Site VPN, ensuring secure remote access to Azure resources.