**Point-to-Site VPN**

**What Is Point-to-Site (P2S) VPN?**

* A Point-to-Site (P2S) VPN is a secure VPN connection that allows individual client devices (such as laptops or PCs) to connect to a remote network, typically a corporate or cloud environment, over the internet. P2S is designed for remote workers or individual users to securely access organizational resources as if they were on-site.

**How It Works?**

* Each client device establishes its own VPN tunnel to the remote network gateway.
* The VPN gateway authenticates the client (usually with certificates or other secure methods).
* After authentication, the client's traffic is securely tunneled to the internal network.

**Steps to set up Point-to-Site:**

1. **Create a Virtual Network**

* Go to the Virtual Network console.
* And fill all the configurations of the Virtual Network.
* Specify the name of the Virtual network is Point-to-site-VNet.
* Fill the address space of the Virtual Network as 172.16.1.0/25.
* Create a subnet named as VM-subnet and the address space will be 172.16.1.0/26.
* Then create another subnet, click on add a subnet and then in the Subnet purpose section select Virtual Network Gateway and the address space of the subnet will be 172.16.1.4/27 and it will be named as GatewaySubnet by default.
* Deploy the Virtual Network.

1. **Create a Virtual Network Gateway**

* Go to Virtual Network Gateway.
* Click on create.
* Specify the name of the virtual network gateway as VPN-Gateway.
* Select the region same as Virtual Network.
* Gateway type: VPN.
* In the Virtual Network section, select the Point-to-site-VNet.
* The Virtual Network gateway will be selected by default.
* In the Public IP address section, specify the name of the Public IP address as VPN-PIP and in the Second public IP address section, specify the name of the Public IP address as VPN-PIP-2.
* Then click on review + create and then create.

1. **Generate Certificates**

* P2S VPNs often use certificate-based authentication. You need:
  + A root certificate (uploaded to the gateway to trust clients).
  + A client certificate (derived from the root, installed on user devices).

1. Generate root certificate (Windows PowerShell)

* To generate root certificate, open the PowerShell and use the below command:

$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `

-Subject "CN=AzureRootCert" -KeyExportPolicy Exportable `

-HashAlgorithm sha256 -KeyLength 2048 `

-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign

* Export the root certificate as Base-64 .cer file.

1. Generate Client Certificate

* To generate client certificate, open the powershell and use the below command:

New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `

-Subject "CN=AzureChildCert" -KeyExportPolicy Exportable `

-HashAlgorithm sha256 -KeyLength 2048 `

-CertStoreLocation "Cert:\CurrentUser\My" `

-NotAfter (Get-Date).AddYears(6) `

-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")

* Export client certificate as .pfx (password protected).

1. **Configure point to site on VPN gateway.**

* Go to the VPN gateway, under the settings section click on Point-to-site configuration.
* Specify the address pool as 192.168.1.0/25 - the range clients will get IPs from.
* Select the tunnel type as IKEv2 and SSTP.
* Select the authentication type as Azure Certificate.
* Create new Public IP address and specify its name as VPN-PIP-3.
* In the root certificates section add the two certificates that we generated root certificate and client certificate and in the public certificate data section of both certificates, enter the values in the certificates.
* Click on save.

1. **Download VPN Client Software**

* From the Point-to-Site configuration page, download the VPN client package generated for your setup.
* Distribute to users.

1. **Install Certificates and VPN Client on User Devices**

* Import the client certificate (.pfx) on the endpoint device (Current User location)
* Extract/install the VPN client hardware.
* Run the client and ensure it creates the intended VPN connection profile.

1. **Connect and Validate**

* On the user’s device, initiate the VPN connection.
* Authenticate as prompted.
* After connection, verify IP is from the address pool and try to access cloud/internal resources.