Notes on Point-to-Site VPN connections

**Notes on Point-to-Site VPN Connection**

A Point-to-Site VPN connection is used to establish a secure connection between multiple client machines an an Azure virtual network via the Internet.

Below is a diagram from the Microsoft documentation on a sample scenario

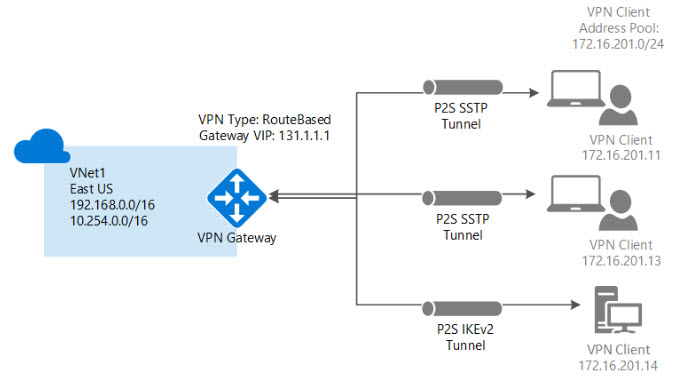


Image reference -<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal>

* This sort of connection is based off certificates for authentication.
* You need to have a root certificate in place that needs to be uploaded to Azure for the point-to-site connection.
* A client certificate needs to be generated from the root certificate. This client certificate needs to be on each client computer that needs to connect to the Azure virtual network via the Point-to-Site connection.
* To generate the certificates, you can use a Certificate authority or generate a self-signed certificate using PowerShell. Some commands are given below

**// To generate the root certificate**

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

-Subject "CN=RootCertificate" -KeyExportPolicy Exportable `

-HashAlgorithm sha256 -KeyLength 2048 `

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

**// To generate the client certificate**

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

-Subject "CN=ClientCertificate" -KeyExportPolicy Exportable `

-HashAlgorithm sha256 -KeyLength 2048 `

-CertStoreLocation "Cert:\CurrentUser\My" `

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