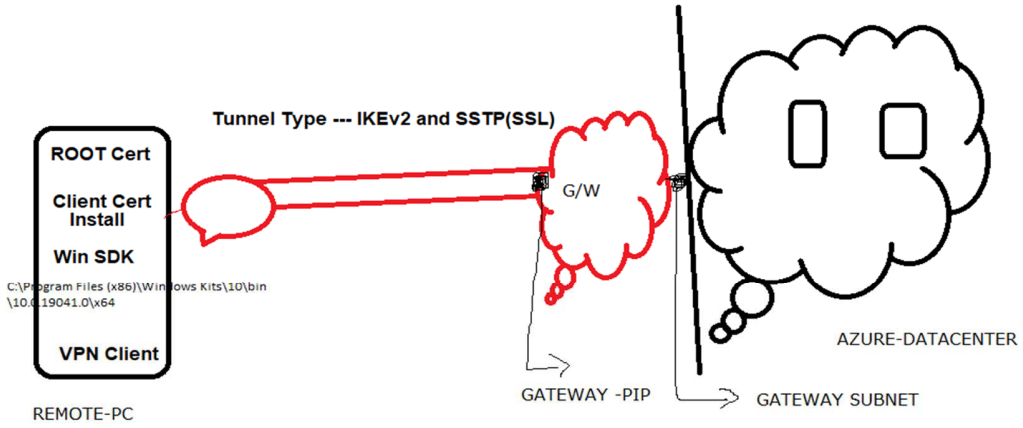
STEP BY STEP – POINT TO SITE



POINT TO SITE-

A Point-to-Site (P2S) VPN gateway lets you create a secure connection to your Azure virtual network from an individual client computer, Point-to-Site VPN connections are useful when you want to connect to your Azure VNet from remote locations such as your home or hotel.

P2S VPN is also a useful solution to use instead of S2S VPN when you have only a few clients that need to connect to a VNet.

Virtual Private Network (VPN) device
It is a device or service that provides external connectivity to the local area network. The Virtual Private Network (or VPN) device can be a hardware device or a software solution such as the Routing and Remote Access Service (RRAS) in Windows Server 2012.
Virtual network
The application in the cloud and the components of Azure VPN Gateway are in the same virtual network.
Azure VPN Gateway
The VPN Gateway service allows you to connect the virtual network to the local area network using a VPN device. This service includes the following elements:
Virtual network gateway. The resource that provides a virtual VPN device for the virtual network. It is responsible for routing traffic from the local area network to the virtual network.
Local area network gateway. Abstraction of the local VPN device. Network traffic from the application in the cloud to the local area network is routed through this gateway.
Connection. The connection has properties that specify the type of connection (IPSec) and the shared key with the local VPN device to encrypt traffic.
Gateway subnet. The virtual network gateway is maintained on its own subnet.

Point-to-Site (Point-To-Site)
This type of connection is made through SSTP (Secure Sockets Tunnel Protocol). It allows you to configure an interconnection to the Azure Network individually, from a specific Client Team, in order to access its resources. Point-to-Site connections do not need a VPN dial-up device but work with a VPN client installed on the Device. However, only such equipment can connect to Azure resources. In the case that there are several teams that need access to these resources, each of them must mark a Point-to-Site VPN.

- Before you start this Lab , Please Create One Vnet – 10.0.0.0/16 AND One Subnet- 10.0.0.0/24 and One Azure VM Installed – Example – VM1-PROD – IP – 10.0.0.4

HIGH LEVEL STEPS –

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

1. CREATE GATEWAY SUBNET .

2. CREATE VNET-GATEWAY - 30 MINS

3. TAKE ANY REMOTE MACHINE - WIN10 (WEST-US - VNET-WEST-US- 172.16.0.0/16 - SUBNET1- 172.16.0.4)

4. WIN10 - INSTALL SDK TOOL --- GIVES ME MAKECERT.EXE - RUN 2 COMMANDS - TWO CERTIFICATES - ROOT , CLIENT -

5. ROOT - EXPORT - WITHOUT PRIVATE KEY

6. CLIENT - EXPORT - WITH PRIVATE KEY

7. CLIENT - INSTALL ON WIN-10 MACHINE

8. ROOT - OPEN VIA NOTEPAD - THUMBPRINT - SINGLE LINE -* - COPY

9. GATEWAY - ENABLE POINT TO SITE -

> 192.168.0.0/24 -VPN

> CERTIFACTE NAME -ROOT

> THUMBPRINT VALUE - PASTE

> SAVE - 10 SECONDS- NO ERROR .

10. DOWNLOAD SCRIPT - POINT TO SITE PORTAL --- SCRIPT INSTALL AND CONNECT - WINDOWS 10 .

STEP-1- CREATE GATEWAY SUBNET
Resource Group > VNET>SUBNETS> GATEWAY SUBNETS>ADD – 172.16.2.0/24 (Available Free Subnet).

STEP-2 Create Gateway-

Create Gateway > Azure>New> Network>Virtual Network Gateway>Name> VPN>ROUTE BASED>SKU-SPEED(STANDARD)> SELECT VIRTUAL NETWORK (CREATED IN STEP 1) > PUBLIC IP- NEW – NAME-PIP>FINISH .

STEP -3- Prepare Remote Machine –
We don't have Any Remote Machine in Lab Environment so Lets use Azure WEST-US region and Create one WIN-10 VM and Treat this VM as Official Laptop – working from Home .

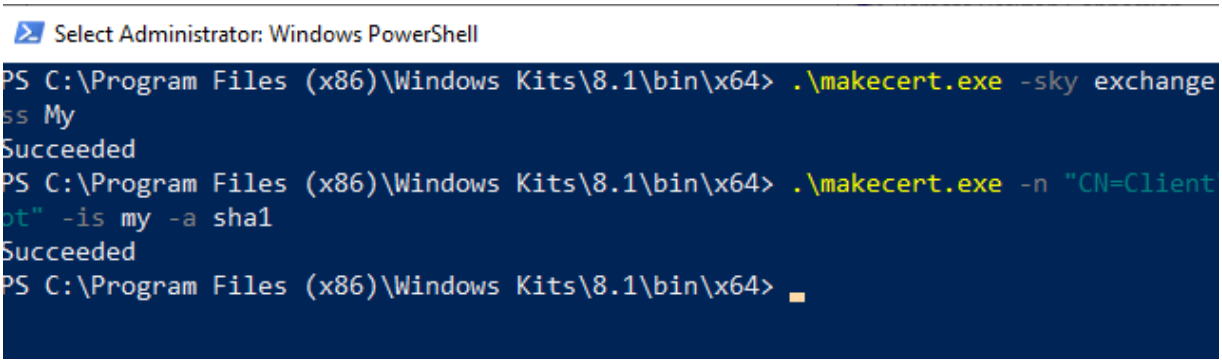
1. CREATE ONE RESOURCE GROUP – RG-2-WESTUS
2. CREATE ONE VNET IN WEST US – NAME WEST-VNET – ADDRESS SPACE – 172.16.0.0/16 – SUBNET1-172.16.0.0/24 .
3. CREATE ONE WIN-10 VM – NAME REMOTE-10 INTO WEST US . YOU WILL GET DEFAULT IP – 172.16.0.4

STEP NO 4 – INTALL SDK TOOL INTO REMOTE-WIN-10 MACHINE

https://go.microsoft.com/fwlink/p/?linkid=2120843

C:\Program Files (x86)\Windows Kits\10\bin\10.0.19041.0\x64

1. DOWNLOAD SKD FORM One Drive + WINRAR Tool .
2. Install SDK – Next next – Default Path .
3. SDK Path – for SDK - C:\Program File X86\WINDOWS KITS\8.1\BIN\X64.
4. Open Powershell RUN AS Admin – CD \
5. C:\ C:\Program File X86\WINDOWS KITS\8.1\BIN\X64



7. Under this Path, Run Two Commands to Create Two Certificates – One is Root and one is Client.

.\makecert .exe -sky exchange -r -n "CN=root" -pe -a sha1 -len 2048 -ss My

.\makecert.exe -n "CN=Client" -pe -sky exchange -m 96 -ss My -in "root" -is my -a sha1

STEP-5- EXPORT ROOT-

RUN>MMC> ADD/ SNAP IN> ADD- CERTIFICATES > USERS > OK >UNDER CURRENT USER CERTIFICATES>PERSONAL> CERTIFICATE* you will get two certificates created during step 5.

Right click-Root>All Task > Export > Do not Export with Private Key >Select Base X64.CER Option> Next> Location >C:\Root>Save.

STEP-6 - EXPORT CLIENT-

Right client >Client certificate > Export> Export with Private Key > Password > Location > C:\CLIENT. * Extension of this certificate should be .PFX.

STEP-7- INSTALL – CLIENT CERTIFICATE – REMOTE-WIN-10

RIGHT CLICK CLIENT.PFX INSTALL > Client.PFX > NEXT > DEFAULT PATH- YES .

STEP -8 – OPEN ROOT CERTICATE VIA NOTEPAD

1. Open saved Certificate> Root * >Open via Notepad > you will get Thumbprint of the certificates > Format > remove word wrap
2. Delete Top and Bottom Two Line - -----BEGIN CERTIFICATE----- and End Certificate ********** > Change Entire Thumbprint into Single line> Copy >
3. Remove WORD WRAP AND USE BACK SPACE.

STEP-9- ENABLE POINT TO SITE -

Azure Portal >Gateway> USE VPN CONFIGURATION> Point to site> CONFIGURE NOW > Add Address Pool Example- 192.168.0.0/24 (Free Subnet)>Name – Root > Public Certificate Data > Paste (Thumbprint)>Tunnel Type > IKEV2 &SSTP > Save. WAIT FOR 2-3 MINUTES.

Once Configuration is saved . Under Same Console> Top Side of Azure under Gateway >Download VPN Client option is visible>Click Download And Wait for 2 MINUTES TO GET .ZIP File > Save .

STEP-10 – INSTALL CLIENT SCRIPT – CONNECT - TEST

1. DOWNLOAD> EXTRAT THE ZIP CLIENT SCRIPT > UNDER- WindowsAmd64> RUN X64 BIT SCRIPT- RIGHT CLICK RUN AS ADMIN .
2. RUN > NCPA.CPL > YOU WILL GET CONNECTION BASED ON VNET NAME - K-VNET > RIGHT CLICK CONNECT – NEXT NEXT – CONNECT .
3. TESTING – TURN OFF THE WINDOWS FIREWALL OF EAST-US PRODVM AND TRY TO PING 10.0.0.4 FROM REMOTE PC .
4. MSTSC – TRY TO TAKE RDP FROM WIN-10 PC TO PROD VM – 10.0.0.4

https://infra.engineer/azure/26-azure-point-to-site-client-vpn