VPN gateway

Functionalities provided

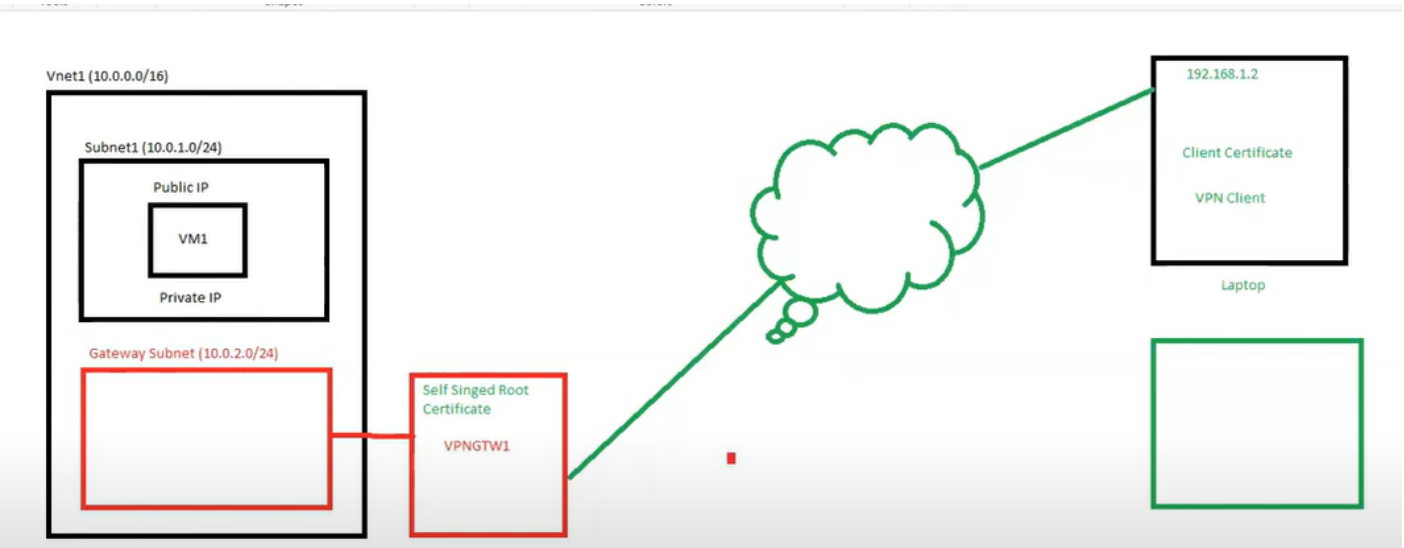
- creating a secure channel.
- Authenticating users
- Providing an IP address (static IP address).
- DNS resolution
- access control

- ! Creating secure channels between users, networks, or systems over the internet.
- The way tunnel is established and secured depends on the selected VPN protocol, such as openVPN, IPsec, or IKEv2.
  - ? secure access to local systems for remote users would often be encrypted via the IKEv2 protocol.
  - ? site-to-site connections connecting two branches would rely on the IPsec protocol.
  - ? modern protocols, like OpenVPN or Wireguard are equally suited for all VPN use cases.
- Another task of VPN gateway is authenticating users.
- authentication process

Requirements to create P2S

- VPN gateway - need to attach to the Vnet where the VM exists.
- whenever we connect Gateway with a Vnet. we require a *GatewaySubnet* subnet
- connecting between Gateway with the Gateway Subnet.
- Need to give an IP pool (IP range) to the VPN gateway, one IP is assigned to the Local machine.
  - Then both VPN gateway and Local machine will be in the same network.
  - Connection established
- Need an Authentication process to connect the VPN gateway.
  - In youtube (self Signed Root Certificate - authentication process) inside the VPN gateway.
  - Create a Client Certificate - deployed in the local machine.
- Need a VPN client (software) installed in the Local machine to initiate the VPN connection.

- now VPN gateway is a gateway to enter inside the Vnet.



Self Signed root certificate

- powershell script

```
$params = @{
    Type = 'Custom'
    Subject = 'CN=P2SRootCert'
    KeySpec = 'Signature'
    KeyExportPolicy = 'Exportable'
    KeyUsage = 'CertSign'
    KeyUsageProperty = 'Sign'
    KeyLength = 2048
    HashAlgorithm = 'sha256'
    NotAfter = (Get-Date).AddMonths(24)
    CertStoreLocation = 'Cert:\CurrentUser\My'
}
$cert = New-SelfSignedCertificate @params
```

- Locating the certificate - `certmgr.msc`, console to manage your certificates
- `Personal` > `Certificates`
- P2SRootCert file is created (valid for 1 year)
- Exporting - right-click > All tasks > Export > NExt > Next > Base-64 encoded, 509 (.CER)

Generate a Client Certificate

- powershell script

```
$params = @{
        Type = 'Custom'
        Subject = 'CN=P2SChildCert'
        DnsName = 'P2SChildCert'
        KeySpec = 'Signature'
        KeyExportPolicy = 'Exportable'
        KeyLength = 2048
        HashAlgorithm = 'sha256'
        NotAfter = (Get-Date).AddMonths(18)
        CertStoreLocation = 'Cert:\CurrentUser\My'
        Signer = $cert
        TextExtension = @(
         '2.5.29.37={text}1.3.6.1.5.5.7.3.2')
    }
    New-SelfSignedCertificate @params
```

- Exporting - Export the private key > create a password > and save it.
- extention - .pfx

Download VPN client

- unzip it.
- run the exe as administrator

---

important resources

About Azure VPN Gateway | Microsoft Learn
VPN protocols compared
IP Whitelisting
active-active, actice-standby
