Exercice - Créer une passerelle VPN Azure

40 minutes

Vous souhaitez être sûr de pouvoir connecter des clients ou des sites de votre environnement à Azure à l'aide de tunnels chiffrés via le réseau Internet public. Dans cette unité, vous allez créer une passerelle VPN de point à site, puis vous allez vous connecter à cette passerelle à partir de votre ordinateur client. Vous allez utiliser des connexions d'authentification par certificat Azure natif pour la sécurité.

Vous allez procéder comme suit :

1. Créez une passerelle VPN RouteBased.
2. Téléchargez la clé publique d'un certificat racine à des fins d'authentification.
3. Générez un certificat client à partir du certificat racine, puis installez le certificat client sur chaque ordinateur client qui se connectera au réseau virtuel à des fins d'authentification.
4. Créez les fichiers config du client VPN, qui contiennent les informations nécessaires au client pour se connecter au réseau virtuel.

Configuration

Pour effectuer ce module, vous allez utiliser Azure PowerShell à partir de votre ordinateur Windows 10 local.

Nous allons commencer par définir les variables à utiliser au moment de créer un réseau virtuel. Ouvrez une nouvelle session PowerShell et créez les variables suivantes :

PowerShell Copier

```
$VNetName  = "VNetData"
$FESubName = "FrontEnd"
$BESubName = "Backend"
```

```
$GWSubName = "GatewaySubnet"
$VNetPrefix1 = "192.168.0.0/16"
$VNetPrefix2 = "10.254.0.0/16"
$FESubPrefix = "192.168.1.0/24"
$BESubPrefix = "10.254.1.0/24"
$GWSubPrefix = "192.168.200.0/26"
$VPNClientAddressPool = "172.16.201.0/24"
$ResourceGroup = "VpnGatewayDemo"
$Location = "East US"
$GWName = "VNetDataGW"
$GWIPName = "VNetDataGWPIP"
$GWIPconfName = "gwipconf"
```

Configurer un réseau virtuel

1. Créez un groupe de ressources.

   PowerShell — Copier

   ```
   New-AzResourceGroup -Name $ResourceGroup -Location $Location
   ```

2. Définissez des configurations de sous-réseau pour le réseau virtuel. Elles ont les noms **FrontEnd, BackEnd** et **GatewaySubnet**. Tous ces sous-réseaux existent au sein du préfixe de réseau virtuel.

   PowerShell — Copier

   ```
   $fesub = New-AzVirtualNetworkSubnetConfig -Name $FESubName -Address-
   Prefix $FESubPrefix
   $besub = New-AzVirtualNetworkSubnetConfig -Name $BESubName -Address-
   Prefix $BESubPrefix
   $gwsub = New-AzVirtualNetworkSubnetConfig -Name $GWSubName -Address-
   Prefix $GWSubPrefix
   ```

3. Ensuite, créez le réseau virtuel en utilisant les valeurs de sous-réseau et un serveur DNS statique.

   PowerShell — Copier

   ```
   New-AzVirtualNetwork -Name $VNetName -ResourceGroupName $Resource-
   Group -Location $Location -AddressPrefix $VNetPrefix1,$VNetPrefix2 -
   Subnet $fesub, $besub, $gwsub -DnsServer 10.2.1.3
   ```

4. À présent, spécifiez les variables pour le réseau que vous venez de créer.

PowerShell Copier

```
$vnet = Get-AzVirtualNetwork -Name $VNetName -ResourceGroupName $Re-
sourceGroup
$subnet = Get-AzVirtualNetworkSubnetConfig -Name "GatewaySubnet" -
VirtualNetwork $vnet
```

5. Demandez une adresse IP publique attribuée dynamiquement.

PowerShell Copier

```
$pip = New-AzPublicIpAddress -Name $GWIPName -ResourceGroupName $Re-
sourceGroup -Location $Location -AllocationMethod Dynamic
$ipconf = New-AzVirtualNetworkGatewayIpConfig -Name $GWIPconfName -
Subnet $subnet -PublicIpAddress $pip
```

Créer la passerelle VPN

Lorsque vous créez cette passerelle VPN :

- GatewayType doit avoir la valeur Vpn
- VpnType doit avoir la valeur RouteBased

> **Notes**
>
> Notez que cette partie de l'exercice peut durer jusqu'à 45 minutes.

1. Pour créer la passerelle VPN, exécutez la commande suivante et appuyez sur Entrée.

PowerShell Copier

```
New-AzVirtualNetworkGateway -Name $GWName -ResourceGroupName $Re-
sourceGroup `
  -Location $Location -IpConfigurations $ipconf -GatewayType Vpn `
  -VpnType RouteBased -EnableBgp $false -GatewaySku VpnGw1 -Vpn-
ClientProtocol "IKEv2"
```

2. Attendez que la sortie de commande apparaisse.

Ajouter le pool d'adresses des clients VPN

1. Exécutez la commande suivante, puis appuyez sur Entrée.

```powershell
$Gateway = Get-AzVirtualNetworkGateway -ResourceGroupName $Resource-
Group -Name $GWName
Set-AzVirtualNetworkGateway -VirtualNetworkGateway $Gateway -Vpn-
ClientAddressPool $VPNClientAddressPool
```

2. Attendez que la sortie de commande apparaisse.

Générer un certificat client

L'infrastructure réseau étant créée sur Azure, nous devons créer un certificat client auto-signé sur notre machine locale. Cette opération s'effectue de la même façon sur la plupart des systèmes d'exploitation, mais nous allons voir comment générer un certificat client sur Windows 10 à l'aide de PowerShell avec le module Azure PowerShell et l'utilitaire Windows **Gestionnaire de certificats**.

1. La première étape consiste à créer le certificat racine auto-signé. Exécutez la commande ci-dessous.

```powershell
$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
-Subject "CN=P2SRootCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -
KeyUsage CertSign
```

2. Ensuite, générez un certificat client signé par votre nouveau certificat racine.

```powershell
New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeyS-
pec Signature `
-Subject "CN=P2SChildCert" -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")
```

Nos certificats étant générés, nous devons exporter la clé publique de notre certificat racine.

1. Exécutez `certmgr` à partir de PowerShell pour ouvrir le Gestionnaire de certificats.
2. Accédez à **Personnel** > **Certificats**. Recherchez et cliquez avec le bouton droit sur le certificat **P2SRootCert** dans la liste, puis sélectionnez **Toutes les tâches** > **Exporter**.
3. Dans l'Assistant Exportation de certificat, cliquez sur **Suivant**.
4. Assurez-vous que l'option **Non, ne pas exporter la clé privée** est sélectionnée, puis cliquez sur **Suivant**.
5. Dans la page **Format de fichier d'exportation**, vérifiez que l'option **X.509 encodé en base 64 (.CER)** est sélectionnée, puis cliquez sur **Suivant**.
6. Dans la page **Fichier à exporter**, sous **Nom de fichier**, accédez à un emplacement dont vous vous souviendrez et enregistrez le fichier sous **P2SRootCert.cer**, puis cliquez sur Suivant.
7. Dans la page **Fin de l'Assistant Exportation du certificat**, cliquez sur **Terminer**.
8. Dans la boîte de message **Assistant d'exportation de certificat**, cliquez sur **OK**.

Charger les informations de la clé publique du certificat racine

1. Dans la fenêtre PowerShell, exécutez la commande suivante afin de déclarer une variable pour le nom du certificat :

   PowerShell | Copier

   ```
   $P2SRootCertName = "P2SRootCert.cer"
   ```

2. Remplacez l'espace réservé `<cert-path>` par l'emplacement d'exportation de votre certificat racine, puis exécutez la commande suivante :

   Copier

PowerShell

```
$filePathForCert = "<cert-path>\P2SRootCert.cer"
$cert = new-object System.Security.Cryptography.X509Certifi-
cates.X509Certificate2($filePathForCert)
$CertBase64 = [system.convert]::ToBase64String($cert.RawData)
$p2srootcert = New-AzVpnClientRootCertificate -Name $P2SRootCertName
-PublicCertData $CertBase64
```

3. Le nom du groupe étant défini, chargez le certificat sur Azure à l'aide de la commande suivante.

PowerShell | Copier

```
Add-AzVpnClientRootCertificate -VpnClientRootCertificateName
$P2SRootCertName -VirtualNetworkGatewayname $GWName -ResourceGroup-
Name $ResourceGroup -PublicCertData $CertBase64
```

Azure reconnaîtra désormais ce certificat comme certificat racine approuvé pour notre réseau virtuel.

Configurer le client VPN natif

1. Exécutez la commande suivante pour créer des fichiers de configuration de client VPN au format .ZIP.

PowerShell | Copier

```
$profile = New-AzVpnClientConfiguration -ResourceGroupName $Resource-
Group -Name $GWName -AuthenticationMethod "EapTls"
$profile.VPNProfileSASUrl
```

2. Copiez l'URL retournée dans la sortie de cette commande et collez-la dans votre navigateur. Votre navigateur doit commencer le téléchargement d'un fichier .ZIP. Extrayez le contenu de l'archive et placez-le à un emplacement approprié.

> **Notes**
>
> Certains navigateurs tenteront initialement de bloquer le téléchargement de ce fichier ZIP sous prétexte qu'il s'agit d'un téléchargement dangereux.

Vous devrez ignorer cet avertissement dans votre navigateur afin de pouvoir extraire le contenu de l'archive.

3. Dans le dossier extrait, accédez au dossier **WindowsAmd64** (pour les ordinateurs Windows 64 bits) ou au dossier **WindowsX86** (pour les ordinateurs 32 bits).

   ⓘ **Notes**

   Si vous souhaitez configurer un VPN sur un ordinateur non Windows, vous pouvez utiliser le certificat et les fichiers de paramètres du dossier **Generic**.

4. Double-cliquez sur le fichier **VpnClientSetup{architecture}.exe**, `{architecture}` reflétant votre architecture.
5. Dans l'écran **Windows a protégé votre PC**, cliquez sur **Plus d'informations**, puis sur **Exécuter quand même**.
6. Dans la boîte de dialogue **Contrôle de compte d'utilisateur**, cliquez sur **Oui**.
7. Dans la boîte de dialogue **VNetData**, cliquez sur **Oui**.

Connexion à Azure

1. Appuyez sur la touche Windows, tapez **Paramètres** et appuyez sur ENTRÉE.
2. Dans la fenêtre **Paramètres**, cliquez sur **Réseau et Internet**.
3. Dans le volet gauche, cliquez sur **VPN**.
4. Dans le volet de droite, cliquez sur **VNetData**, puis cliquez sur **Se connecter**.
5. Dans la fenêtre VNetData, cliquez sur **Se connecter**.
6. Dans la prochaine fenêtre VNetData, cliquez sur **Continuer**.
7. Dans la boîte de message **Contrôle de compte d'utilisateur**, cliquez sur **Oui**.

ⓘ **Notes**

Si ces étapes ne fonctionnent pas, vous devrez peut-être redémarrer votre ordinateur.

Vérifier votre connexion

1. À une nouvelle invite de commandes Windows, exécutez `IPCONFIG /ALL`.
2. Copiez l'adresse IP sous l'adaptateur PPP VNetData, ou notez-la.
3. Vérifiez que l'adresse IP est dans le **plage VPNClientAddressPool de 172.16.201.0/24**.
4. Vous avez réussi à établir une connexion à la passerelle VPN Azure.

Vous venez de configurer une passerelle VPN, ce qui vous permet d'établir une connexion client chiffrée à un réseau virtuel dans Azure. Cette approche convient parfaitement aux ordinateurs clients et aux connexions de site à site plus petites.

Unité suivante: Explorer Azure ExpressRoute

Continuer >