ChatGPT

Guide de configuration d'un VPN site-à-site (Telma ↔ Azure)

Ce guide détaille les étapes de configuration d'un VPN site-à-site entre un réseau local (sous-réseau 192.168.X.X, connecté via Telma) et Azure, afin que les machines locales accèdent à une base Cosmos DB PostgreSQL hébergée. Nous utilisons l'**Azure CLI** pour toutes les commandes. Les contraintes d'une box Telma (équipement tiers potentiellement non configurable avec IP dynamique) sont abordées, ainsi qu'une solution de secours (VPN point-à-site) si le VPN site-à-site n'est pas possible.

1. Créer le réseau virtuel et sous-réseau dans Azure

1. **Créer un groupe de ressources** pour isoler les ressources :

   ```
   az group create --name MonRG --location eastus
   ```

   Exemple Azure CLI : création du groupe de ressources MonRG dans la région "eastus" [1] .
2. **Créer le VNet et un sous-réseau** (choisir un réseau IP qui n'empiète pas sur le local 192.168.X.X). Par exemple, un espace `10.0.0.0/16` :

   ```
   az network vnet create \
     --resource-group MonRG \
     --name MonVNet \
     --address-prefix 10.0.0.0/16 \
     --subnet-name FrontEnd \
     --subnet-prefix 10.0.0.0/24
   ```

   Cette commande crée le VNet « MonVNet » (10.0.0.0/16) avec un sous-réseau « FrontEnd » (10.0.0.0/24) [2] .
3. **Ajouter le sous-réseau de passerelle** (`GatewaySubnet`). Ce sous-réseau réservé permettra de déployer la passerelle VPN Azure :

   ```
   az network vnet subnet create \
     --resource-group MonRG \
     --vnet-name MonVNet \
     --name GatewaySubnet \
     --address-prefix 10.0.255.0/27
   ```

   Le nom doit être exactement "GatewaySubnet" et la taille recommandée ≥ /27 [3] .

2. Configurer la passerelle VPN Azure

1. **Demander une adresse IP publique** pour la passerelle VPN Azure :

```
az network public-ip create \
  --resource-group MonRG \
  --name MonGWpip \
  --allocation-method Static \
  --sku Standard
```

Cette adresse IP publique statique sera assignée à la passerelle VPN lors de sa création [4].

2. **Créer la passerelle VPN (Virtual Network Gateway)**. Choisir un SKU adapté (ex. `VpnGw2Az` pour redondance avec génération 2). Exemple en mode actif-standby (une seule IP publique) :

```
az network vnet-gateway create \
  --resource-group MonRG \
  --name MaPasserelleVPN \
  --public-ip-addresses MonGWpip \
  --vnet MonVNet \
  --gateway-type Vpn \
  --vpn-type RouteBased \
  --sku VpnGw2AZ \
  --generation Generation2 \
  --no-wait
```

Cette commande crée une passerelle VPN route-based, génération 2, SKU VpnGw2AZ [5]*. La création peut prendre 20–45 minutes.*

3. Créer la connexion site-à-site dans Azure

1. **Créer le Local Network Gateway**, qui représente le site local. Indiquez l'IP publique du routeur local (ou FQDN s'il est dynamique) et le préfixe local (par ex. `192.168.1.0/24`) :

```
az network local-gateway create \
  --resource-group MonRG \
  --name MonSiteLocal \
  --gateway-ip-address <IP_publique_local> \
  --local-address-prefixes 192.168.1.0/24
```

Cette commande définit le site local « MonSiteLocal » avec son IP publique et son réseau interne [6]*. Azure attend normalement une IP fixe ; on peut aussi spécifier un FQDN si on utilise un service DNS dynamique* [7].

2. **Créer la connexion VPN** entre la passerelle Azure et le site local. Choisir une clé partagée (PSK) robuste. Exemple :

```
az network vpn-connection create \
  --resource-group MonRG \
  --name ConnexionS2S \
  --vnet-gateway1 MaPasserelleVPN \
  --shared-key MaCleSecrete123 \
  --local-gateway2 MonSiteLocal
```

Cette commande établit le tunnel IPsec/IKE avec la clé "MaCleSecrete123" (doit correspondre à celle configurée sur l'équipement local) [8] .

4. Configuration côté local (routeur Telma ou équipement tiers)

- **Adresse publique** : le routeur local doit avoir une IP publique fixe. Si l'IP change (cas des connexions domestiques Telma), Azure permet d'utiliser un nom DNS (FQDN) mis à jour via un service DDNS [7] .
- **Algorithmes/IPsec** : configurer l'équipement VPN local en mode *route-based* (IKEv2) avec des paramètres compatibles Azure (par ex. IKE 2.0, chiffrement AES256, SHA256, DH Group 2 et IPsec AES256-GCM) [9] .
- **Clé partagée** : utiliser la même PSK que pour la connexion Azure (`MaCleSecrete123` dans l'exemple).
- **Adresse du tunnel** : indiquer l'adresse IP publique (ou le FQDN) de la passerelle VPN Azure. Si la passerelle est en mode actif-actif, on configure les deux adresses IP publiques disponibles.
- **Ouverture de ports** : autoriser UDP 500 et 4500 (NAT-T) sur le routeur.
- **Routes** : s'assurer que le trafic destiné au réseau `10.0.0.0/16` (VNet Azure) passe par le tunnel IPsec. Sur certains équipements, ajouter une route statique vers le réseau Azure via l'interface VPN.

Remarque : si l'équipement Telma n'est pas modifiable (ni accès admin ni IP fixe), un VPN site-à-site peut être impossible. Dans ce cas, on pourra envisager un VPN **point-à-site** (P2S) Azure (voir section suivante).

5. Tester la connectivité

- **Statut de la connexion VPN** : sur Azure, vérifier l'état du tunnel avec :

```
az network vpn-connection show \
  --resource-group MonRG \
  --name ConnexionS2S
```

Le champ `connectionStatus` doit passer à `Connected` lorsque le tunnel est établi [10] .

- **Test depuis le réseau local** : depuis une machine locale (192.168.X.X), tenter un **ping** vers une ressource du VNet Azure (par exemple un VM dans le sous-réseau). Si ce ping passe, le tunnel fonctionne.
- **Test de la base Cosmos DB PostgreSQL** : une fois le tunnel établi, depuis la machine locale exécuter une commande psql vers l'endpoint Cosmos (en supposant que la base soit accessible via le VNet). Par exemple :

```
psql "host=moncosmos.postgres.database.azure.com user=utilisateur
dbname=maBD sslmode=require"
```

Cela vérifie l'accès à la base via le VPN. (Si CosmosDB a un firewall, ajouter l'adresse IP du VNet Azure aux règles d'accès.)

6. Alternative : VPN Point-à-Site (P2S) si S2S impossible

Si le VPN site-à-site n'est pas réalisable (par ex. IP locale dynamique, équipement non accessible), on peut configurer un VPN **point-à-site** Azure. Le P2S permet à des postes distants de se connecter individuellement à la VNet via un client VPN. C'est recommandé « lorsque vous avez seulement quelques clients à connecter » [11]. Par exemple, on peut réutiliser la même passerelle réseau virtuel :

```
az network vnet-gateway update \
  --resource-group MonRG \
  --name MaPasserelleVPN \
  --client-protocol IkeV2 \
  --address-prefixes 192.168.100.0/24
```

Ici on active le P2S (IKEv2) sur la passerelle existante et on réserve l'espace d'adresses 192.168.100.0/24 pour les clients VPN [12]. Il faudra alors générer des certificats ou utiliser Azure AD pour authentifier les utilisateurs. Chaque client importera une configuration VPN (fournie par Azure) et pourra se connecter.

En résumé, ce guide configure le réseau virtuel et la passerelle VPN Azure par Azure CLI, crée le tunnel site-à-site et présente les paramètres à appliquer sur l'équipement local. Il explique aussi les contraintes possibles (IP dynamique Telma) et l'option P2S si besoin. Avec le tunnel actif, les machines locales pourront atteindre l'instance Cosmos DB PostgreSQL sur Azure via le réseau privé établi.

Sources : Documentation Azure VPN (CLI) [2] [5] [8] [10] [9] [7] [11] [12].

---

[1] [3] [4] [5] Create a virtual network gateway - CLI - Azure VPN Gateway | Microsoft Learn
https://learn.microsoft.com/en-us/azure/vpn-gateway/create-routebased-vpn-gateway-cli

[2] az network vnet | Microsoft Learn
https://learn.microsoft.com/en-us/cli/azure/network/vnet?view=azure-cli-latest

[6] [8] Create S2S VPN connection - shared key authentication - Azure CLI - Azure VPN Gateway | Microsoft Learn
https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-cli

[7] How to create a site to site VPN when local network has dynamic public IP - Microsoft Q&A
https://learn.microsoft.com/en-us/answers/questions/1186022/how-to-create-a-site-to-site-vpn-when-local-networ

[9] About VPN devices for connections - Azure VPN Gateway | Microsoft Learn
https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices

[10] Verify a gateway connection - Azure VPN Gateway | Microsoft Learn
https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-verify-connection-resource-manager

[11] About Azure Point-to-Site VPN connections - Azure VPN Gateway | Microsoft Learn
https://learn.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about

[12] az network vnet-gateway | Microsoft Learn
https://learn.microsoft.com/en-us/cli/azure/network/vnet-gateway?view=azure-cli-latest