

---

*TP - Connexion VPN inter site Azure GCP*

---

**Site Azure première partie :**

1. Création d'un groupe de ressources
2. Création du réseau virtuel
3. Ajout d'un sous-réseau Gateway dans le réseau virtuel
4. Création de la machine virtuelle
  - 4.1. Ouverture des ports dans la machine virtuelle
5. Création de la passerelle de réseau virtuel (VPN)

**Site Google :**

1. Création d'un réseau VPC
2. Création d'une connectivité hybride (VPN)
3. Création de la machine virtuelle
4. Ouverture des ports pour le RDP et l'ICMP

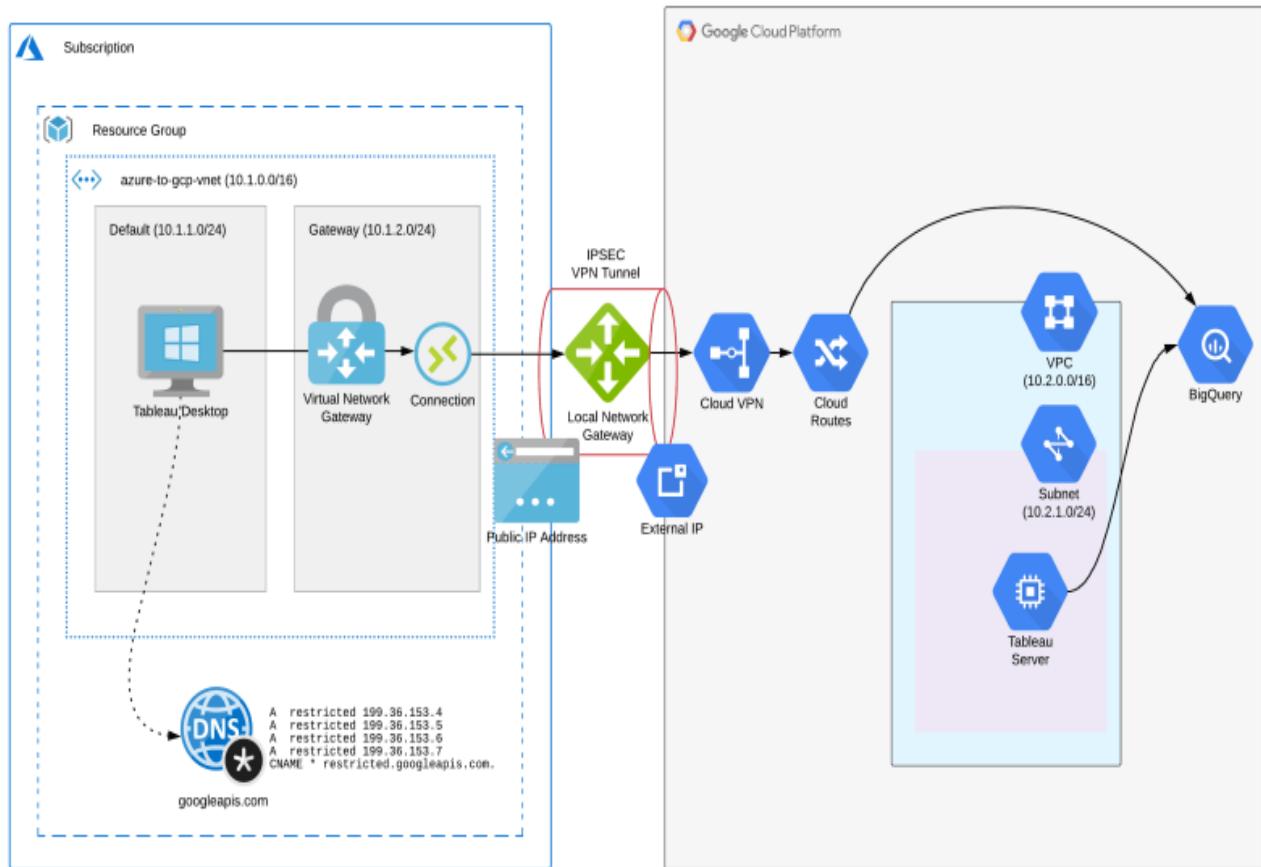
**Site Azure deuxième partie :**

1. Création de la passerelle de réseau local
2. Création de la connexion (Tunnel)
3. Vérifications de communication

---

*Schéma du TP*

---



---

*Source*

---

**Site Azure :**

Espace d'adressage du réseau Azure (Vnet) : 172.32.0.0/16

Espace d'adressage des sous-réseaux d'Azure :

- Serveurs : 172.32.0.0/24
- GatewaySub : 172.32.1.0/24

Machine virtuelle : 2K19SRV-DC01

OS Windows (Windows Server 2019 Datacenter)

Taille A2 standard v2 (2 processeurs virtuels, 4 Gio de mémoire)

@IP Publique pour accès en RDP : 51.103.114.52

**Site Google :**

Espace d'adressage du réseau Google (VPC) : 10.10.0.0/16

@IP de la passerelle : 10.10.0.1

Machine virtuelle : googlevms

@IP Publique pour accès en RDP : 35.210.157.220

---

## Site Azure – Partie 1

---

### I- Création d'un groupe de ressource

Créer un nouveau groupe de ressource nommé « **SiteAzure** »

Accueil > Groupes de ressources >

### Créer un groupe de ressources

De base    Étiquettes    Vérifier + créer

**Groupe de ressources**- Un conteneur qui contient les ressources associées à une solution Azure. Le groupe de ressources peut inclure toutes les ressources de la solution, ou uniquement les ressources que vous voulez gérer en tant que groupe. Vous choisissez la façon dont vous voulez allouer des ressources aux groupes de ressources en fonction de ce qui est le plus adapté à votre organisation. [En savoir plus](#)

#### Détails du projet

Abonnement \* [\(i\)](#)

Azure subscription 1

Groupe de ressources \* [\(i\)](#)

SiteAzure

**✖ Un groupe de ressources avec le même nom existe déjà dans l'abonnement sélectionné Azure subscription 1.**

#### Détails de la ressource

Région \* [\(i\)](#)

(Europe) France Central

[Vérifier + créer](#)

[< Précédent](#)

[Suivant : Étiquettes >](#)

## II- Création d'un réseau Virtuel

Accueil > Réseaux virtuels >

### Créer un réseau virtuel

De base Adresses IP Sécurité Étiquettes Vérifier + créer

Réseau virtuel Azure (VNet) est le composant fondamental de votre réseau privé dans Azure. VNet permet à de nombreux types de ressources Azure, notamment des machines virtuelles Azure, de communiquer de manière sécurisée entre elles, avec Internet et sur les réseaux locaux. VNet est similaire à un réseau traditionnel que vous opérez dans votre propre centre de données, avec en plus les avantages de l'infrastructure Azure comme la mise à l'échelle, la disponibilité et l'isolation.  
[En savoir plus sur le réseau virtuel](#)

**Détails du projet**

Abonnement \* (i) Azure subscription 1

Groupe de ressources \* (i) SiteAzure [Créer nouveau](#)

**Détails de l'instance**

Nom \* SiteAzure   
 ✖ Il existe déjà une ressource ayant le même nom et le même type dans le groupe de ressources actuel.

Région \* France Central

**Vérifier + créer** < Précédent Suivant : Adresses IP > Télécharger un modèle pour automation

Ajouter un Espace d'adressage IPV4 et ajouter un sous-réseau

De base    **Adresses IP**    Sécurité    Étiquettes    Vérifier + créer

Espace d'adressage du réseau virtuel, spécifié sous la forme d'un ou plusieurs prefixes d'adresse en notation CIDR (par exemple, 192.168.1.0/24).

Espace d'adressage IPv4

✓ ✖

**⚠️** L'espace d'adressage « 172.32.0.0/16 (172.32.0.0 - 172.32.255.255) » chevauche l'espace d'adressage « 172.32.0.0/16 (172.32.0.0 - 172.32.255.255) » du réseau virtuel « SiteAzure ». Les réseaux virtuels avec des espaces d'adressage qui se chevauchent ne peuvent pas être appariés. Si vous voulez appairer ces réseaux virtuels, changez l'espace d'adressage « 172.32.0.0/16 (172.32.0.0 - 172.32.255.255) ». [En savoir plus](#)

**⚠️** Les plages d'adresses entrées « 172.32.0.0/16 » peuvent ne pas fonctionner correctement. Il est recommandé d'utiliser des plages d'adresses dans l'espace d'adressage privé non routable défini dans RFC 1918. [En savoir plus](#)

Ajouter un espace d'adressage IPv6  ⓘ

Plage d'adresses du sous-réseau en notation CIDR (par exemple, 192.168.1.0/24). Elle doit faire partie de l'espace d'adressage du réseau virtuel.

+ Ajouter un sous-réseau ✖ Supprimer le sous-réseau

<input type="checkbox"/> Nom de sous-réseau	Espace d'adressage de sous-réseau	Passerelle NAT
<input type="checkbox"/> Serveurs	172.32.0.0/24	-

**Vérifier + créer**    < Précédent    Suivant : Sécurité >    Télécharger un modèle pour automation

On ira ensuite dans notre groupe de ressources > SiteAzure > Sous-réseaux > Sous-réseau de passerelle et on indique la plage 172.32.1.0/24.

### III-    Création de la machine virtuelle

De base    Disques    Mise en réseau    Administration    Monitoring    Paramètres avancés    Étiquettes    Vérifier + créer

Créez une machine virtuelle qui exécute Linux ou Windows. Sélectionnez une image dans la Place de marché Azure ou utilisez une image personnalisée. Renseignez l'onglet De base et sélectionnez Vérifier + créer pour provisionner une machine virtuelle avec des paramètres par défaut, ou passez en revue chaque onglet pour une personnalisation complète. [En savoir plus](#)

**ⓘ** Cet abonnement peut ne pas être éligible pour déployer des machines virtuelles de certaines tailles dans certaines régions.

**Détails du projet**

Sélectionnez l'abonnement pour gérer les coûts et les ressources déployées. Utilisez les groupes de ressources comme les dossiers pour organiser et gérer toutes vos ressources.

Abonnement \*  ⓘ

Groupe de ressources \*  ⓘ  ✖ [Créer nouveau](#)

**Détails de l'instance**

Nom de la machine virtuelle \*  ⓘ  ✖ **Le nom de la machine virtuelle doit être unique dans le groupe de ressources actuel.**

Région \*  ⓘ

Options de disponibilité  ⓘ

**Vérifier + créer**    < Précédent    Suivant : Disques >

## Créer une machine virtuelle

Taille \*

Voir toutes les tailles

Compte d'administrateur

Nom d'utilisateur \*

Mot de passe \*

Confirmer le mot de passe \*

Règles des ports d'entrée

Selectionnez les ports réseau de machine virtuelle accessibles publiquement à partir d'Internet. Vous pouvez spécifier un accès réseau plus limité ou granulaire sous l'onglet Mise en réseau.

Ports d'entrée publics \*  Aucun  Autoriser les ports sélectionnés

Selectionner des ports d'entrée \*

**⚠ Cela permet à toutes les adresses IP d'accéder à votre machine virtuelle.**  
Ceci est recommandé uniquement pour les tests. Utilisez les contrôles avancés de l'onglet Mise en réseau pour créer des règles afin de limiter le trafic entrant sur les adresses IP connues.

## Gestion des licences

**Vérifier + créer**

&lt; Précédent

Suivant : Disques &gt;

## Créer une machine virtuelle

De base Disques Mise en réseau Administration Monitoring Paramètres avancés Étiquettes Vérifier + créer

Définissez la connectivité réseau de votre machine virtuelle en configurant les paramètres de la carte d'interface réseau. Vous pouvez contrôler les ports et la connectivité entrante/sortante avec des règles de groupe de sécurité, ou placer derrière une solution d'équilibrage de charge existante. [En savoir plus](#)

Interface réseau

Quand vous créez une machine virtuelle, une interface réseau est créée pour vous.

Réseau virtuel \*

Sous-réseau \*

Adresse IP publique

**⚠ 1 adresse IP publique est nécessaire pour cette configuration, mais 0 (sur 3) reste dans votre abonnement « Azure subscription 1 ». Pour atteindre votre quota, vous pouvez choisir une adresse IP publique existante ou supprimer la nouvelle adresse IP publique pour passer en dessous de la limite.**

Groupe de sécurité réseau de la carte réseau  Aucun  De base  Paramètres avancés

Ports d'entrée publics \*  Aucun  Autoriser les ports sélectionnés

**Vérifier + créer**

< Précédent

Suivant : Administration >

## IV- Ouverture des ports

On se rendra dans l'onglet toutes les ressources on cliquera sur le groupe de sécurité Windows, on se rendra sur Règles de sécurité de trafic entrant et il y aura seulement la règle ICMP à ajouter.

<input type="text" value="Filtrer par nom"/> Port == tout Protocole == tout Source == tout Destination == tout Action == tout						
Priorité ↑↓	Nom ↑↓	Port ↑↓	Protocole ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
▼ Règles de sécurité de trafic entrant						
300	<span style="color: orange;">⚠</span> <a href="#">RDP</a>	3389	TCP	N'importe lequel	N'importe lequel	<input checked="" type="checkbox"/> Allow
320	<span style="color: orange;">⚠</span> <a href="#">HTTP</a>	80	TCP	N'importe lequel	N'importe lequel	<input checked="" type="checkbox"/> Allow
340	<span style="color: orange;">⚠</span> <a href="#">HTTPS</a>	443	TCP	N'importe lequel	N'importe lequel	<input checked="" type="checkbox"/> Allow
360	<span style="color: orange;">⚠</span> <a href="#">SSH</a>	22	TCP	N'importe lequel	N'importe lequel	<input checked="" type="checkbox"/> Allow
370	<span style="color: orange;">⚠</span> <a href="#">ICMP</a>	N'importe lequel	ICMP	N'importe lequel	N'importe lequel	<input checked="" type="checkbox"/> Allow

## V- Création de la passerelle de réseau virtuel (VPN)

## Créer une passerelle de réseau virtuel ...

Abonnement \*

Azure subscription 1

Groupe de ressources

SiteAzure (dérivé du groupe de ressources du réseau virtuel)

Détails de l'instance

Nom \*

VPN

Région \*

France Central

Type de passerelle \*

VPN  ExpressRoute

Type de VPN \*

Basé sur itinéraires  Basé sur des stratégies

RÉFÉRENCE (SKU) \*

VpnGw1

Génération

Generation1

Réseau virtuel \*

SiteAzure

[Créer un réseau virtuel](#)

✖ Le réseau virtuel comporte déjà une passerelle de ce type ou la passerelle existante dans le réseau virtuel ne prend pas en charge la coexistence.

Sous-réseau

GatewaySubnet (172.32.1.0/24)

✖ Seuls les réseaux virtuels dans l'abonnement et la région sélectionnés sont listés.

Type d'IP publique \*

Créer  Utiliser l'existante

Nom de l'adresse IP publique \*

SiteAzure

✖ Il existe déjà une ressource ayant le même nom et le même type dans le groupe de ressources actuel.

[Vérifier + créer](#)[Précédent](#)[Suivant : Étiquettes >](#)[Télécharger un modèle pour automation](#)

Nous avons terminé la première partie sur Azure, nous allons passer à la partie GCP

Cette partie GCP se fera sur <https://console.cloud.google.com/>

## I- Création d'un réseau VPC

**Créer un réseau VPC**

**Nom:** google-vpc Ce nom est déjà utilisé.

**Description:**

**Plage d'adresses IPv6 Intégrées ULA du réseau VPC:** Activé

Activation de cette fonctionnalité attribue un bloc /48 à partir du préfixe ULA défini par Google réseau.

Activé  Désactivé

**Sous-réseaux:**

Les sous-réseaux vous permettent de créer votre topologie cloud privée dans Google Cloud. Cliquez sur "Automatique" pour créer un sous-réseau dans chaque région ou sur "Personnalisé" pour définir manuellement les sous-réseaux. [En savoir plus](#)

**Mode de création du sous-réseau:** Personnalisé

Personnalisé  Automatique

**Nouveau sous-réseau:**

**Nom:** google-sub Ce nom est déjà utilisé.

**Description:**

**Région:** europe-west1

**Type de piste d'adresses IP:** IPv4 (piste unique)

IPv4 (piste unique)  IPv4 et IPv6 (double piste)

**Plage IPv4:** 10.0.0.0/16

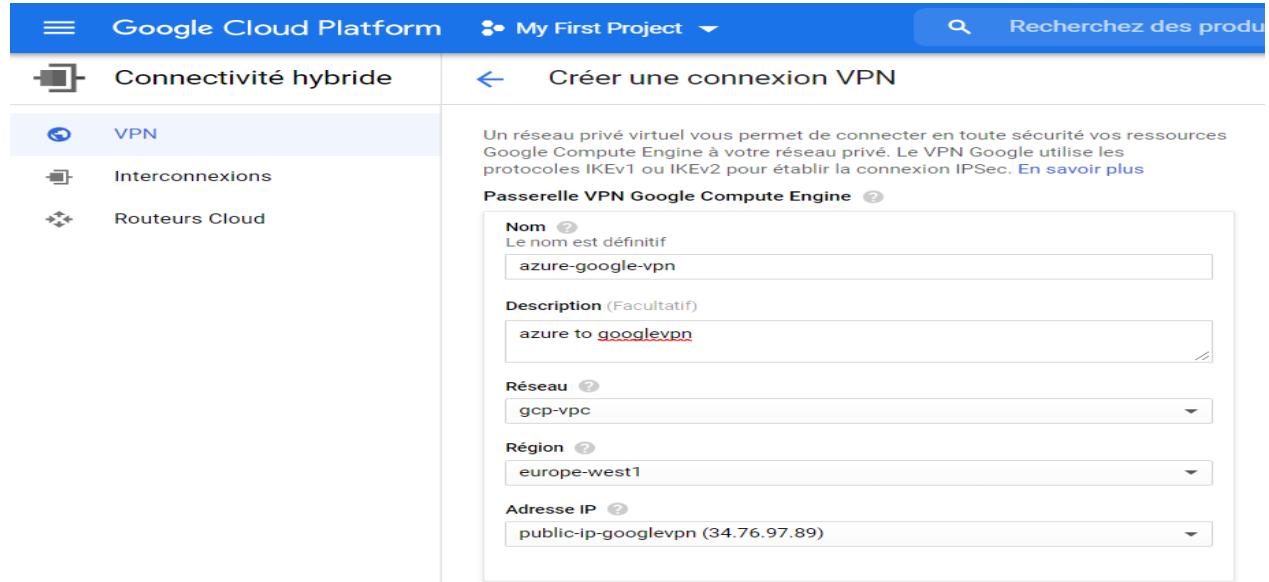
**Mode de routage dynamique:**

Régional Les routeurs cloud hébergent que les routes de la région dans laquelle ils ont été créés.

Mondial Le mode mondial vous permet d'obtenir de manière dynamique les routes vers et depuis l'ensemble des régions, à l'aide d'un seul VPN ou d'une interconnexion de Cloud Router.

## II- Création d'une connectivité hybride (VPN)

On créera un VPN Standard



Créer une connexion VPN

Passerelle VPN Google Compute Engine

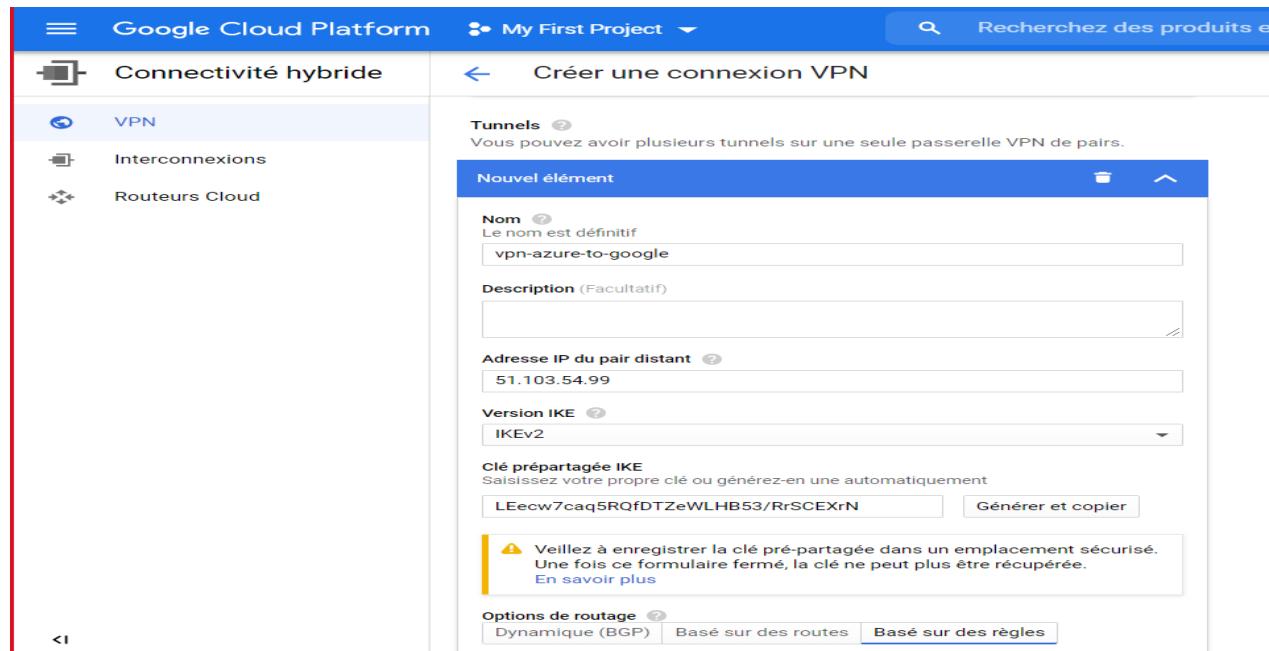
**Nom** Le nom est définitif  
azure-google-vpn

**Description (Facultatif)**  
azure to googlevpn

**Réseau** gcp-vpc

**Région** europe-west1

**Adresse IP** public-ip-googlevpn (34.76.97.89)



Créer une connexion VPN

**Tunnels** Vous pouvez avoir plusieurs tunnels sur une seule passerelle VPN de pairs.

**Nouvel élément**

**Nom** Le nom est définitif  
vpn-azure-to-google

**Description (Facultatif)**

**Adresse IP du pair distant** 51.103.54.99

**Version IKE** IKEv2

**Clé prépartagée IKE** Saisissez votre propre clé ou générez-en une automatiquement  
LEecw7caq5RQfDTZeWLH53/RrSCEXrN Générer et copier

**Options de routage** Dynamique (BGP) Basé sur des routes Basé sur des règles

⚠ Bien noter la clef pré-partagée IKE

### III- Crédit de la machine virtuelle

Élément	Estimation mensuelle
2 vCPU + 4 GB memory	26.91 SUS
Premium image usage fee*	33.58 SUS
Disque persistant standard de 50 Go	2,00 SUS
Sustained use discount	-0,00 SUS
Total	62.49 SUS

**Google Cloud** My First Project

[Créer une instance](#)

Pour créer une instance de VM, sélectionnez l'une de ces options :

- Nouvelle instance de VM**  
Créer entièrement une instance de VM unique
- Nouvelle instance de VM à partir d'un modèle**  
Créer une instance de VM unique à partir d'un modèle existant
- Nouvelle instance de VM à partir d'une image système**  
Créer une instance de VM unique à partir d'une image système existante
- Marketplace**  
Déployer une solution prête à l'emploi sur une instance de VM

**Disque de démarrage**

Nom	googlevms
Type	Nouveau disque persistant standard
Taille	50 Go
Type de licence	Palement à l'usage
Image	Windows Server 2019 Datacenter

[MODIFIER](#)

Si vous utilisez Windows et que vous avez l'intention d'exécuter des logiciels Microsoft supplémentaires, veuillez remplir le [formulaire de vérification des licences](#).

[En savoir plus](#) sur les exigences concernant la mobilité des licences Microsoft

**Identité et accès à l'API**

Comptes de service

Compte de service

Compute Engine default service account

Vous devez définir le rôle "Utilisateur du compte de service" (roles/iam.serviceAccountUser) pour les utilisateurs qui souhaitent accéder aux VM avec ce compte de service. [En savoir plus](#)

Niveaux d'accès

Autoriser l'accès par défaut

Autoriser l'accès complet à l'ensemble des APIs Cloud

Définir l'accès pour chaque API

**Pare-feu**

Ajouter des tags et des règles de pare-feu pour autoriser un trafic réseau spécifique provenant d'Internet

Autoriser le trafic HTTP

Autoriser le trafic HTTPS

**Options avancées**

**Mise en réseau**

Nom d'hôte et interfaces réseau

Tags réseau: **azuretogooglenet**

Nom d'hôte: **MyVM**

Définissez un nom d'hôte personnalisé pour cette instance ou laissez-le par défaut. Ce choix est définitif.

Transfert IP

Activer

Configuration des performances du réseau

Carte d'interface réseau: **-**

Bande passante réseau

Augmenter la bande passante de sortie totale

Bandes passantes réseau sortante maximale : 2 Gbit/s

Interfaces réseau

L'interface réseau est définitive

Modifier l'interface réseau

Réseau: **gcp-vpc**

Sous-réseau: **google-sub IPv4 (10.10.0.0/16)**

Type de pile d'adresses IP

IPv4 (pile unique)

IPv4 et IPv6 (double pile)

Adresse IP interne principale: **Éphémère (automatique)**

Plages d'adresses IP d'alias

[+ AJOUTER UNE PLAGE D'ADRESSES IP](#)

Adresse IPv4 externe: **Éphémère**

Niveau de service réseau

Premium

Standard (europe-west1)

Enregistrement PTR du DNS public

Activer pour IPv4

Nom de domaine PTR: **MyVM**

[OK](#)

Après ça on peut valider la création de la VM.

---

## Site Azure – Partie 2

---

### I- Crédation de la Passerelle de réseau local

Accueil > Passerelles de réseau local > **Créer une passerelle de réseau local** ...

De base   Avancé   Vérifier + créer

Une passerelle de réseau local est un objet spécifique qui représente un emplacement local (le site) à des fins de routage. [En savoir plus.](#)

**Détails du projet**

Abonnement \*

Groupe de ressources \*   [Créer nouveau](#)

**Détails de l'instance**

Région \*

Nom \*   ✖ Une passerelle de réseau local portant ce nom existe déjà dans le groupe de ressources actuel.

Point de terminaison

Adresse IP \*

Espaces d'adressage

---

### II- Crédation de la connexion (Tunnel)

## Créer une connexion

...

De base Paramètres Étiquettes Vérifier + créer

Créez une connexion sécurisée à votre réseau virtuel en utilisant VPN Gateway ou ExpressRoute.

[En savoir plus sur VPN Gateway](#)[En savoir plus sur ExpressRoute](#)

## Détails du projet

Abonnement \*

Azure subscription 1

Groupe de ressources \*

SiteAzure

[Créer nouveau](#)

## Détails de l'instance

Type de connexion \* ⓘ

Site à site (IPsec)

Nom \*

AzureVPN

✖ Il existe déjà une ressource ayant le même nom et le même type dans le groupe de ressources actuel.

Région \*

France Central

## Créer une connexion

...

De base Paramètres Étiquettes Vérifier + créer

## Passerelle de réseau virtuel

Pour pouvoir utiliser un réseau virtuel avec une connexion, le réseau doit être associé à une passerelle de réseau virtuel.

Passerelle de réseau virtuel \*

VPN

Passerelle de réseau local \*

localGW

✖ Il existe déjà une connexion « AzureVPN » de la passerelle « VPN » à la passerelle « localGW ».

Clé partagée (PSK) \*

LEecw7caq5RQfDTZeWLHB53/RrSCEXrN

Protocole IKE ⓘ

 IKEv1  IKEv2

Utiliser l'adresse IP privée Azure ⓘ

Activer BGP ⓘ

Stratégie IPsec/IKE ⓘ

 Par défaut  Personnalisé

Utiliser le sélecteur de trafic basé sur une stratégie ⓘ

 Activer  Désactiver

Délai d'expiration de DPD en secondes \*

45

Mode de connexion ⓘ

 Default  InitiatorOnly  ResponderOnly

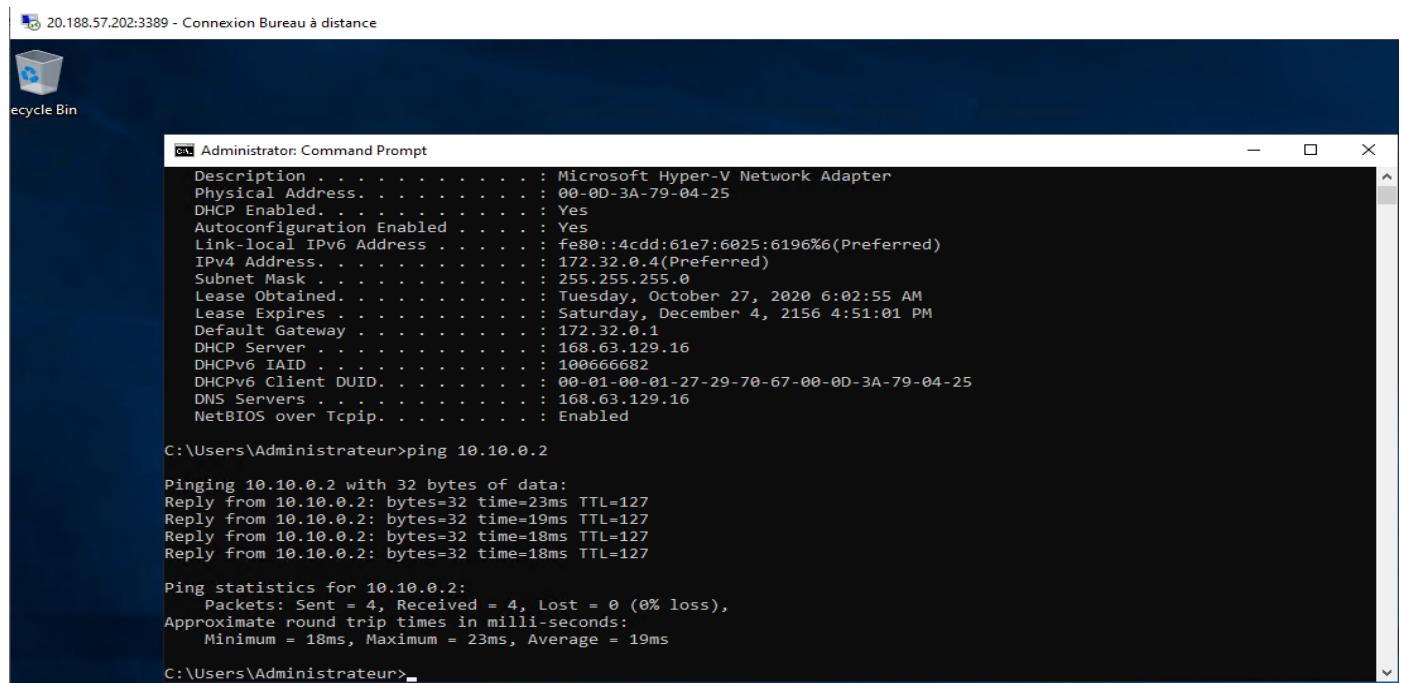
On pensera bien à insérer la clef pré-partagée IKE (P.10)

## III- Vérification de communication

On peut désormais se connecter en RDP aux deux serveurs et directement se rendre dans les règles de firewall entrante (et sortante) et activer l'ICMP :

Diagnostics de réseau de base - Demande d'écho ICMP (ICMPv4-Entrant)	Diagnostics de réseau de base	Domaine	Non	Autoriser
Diagnostics de réseau de base - Demande d'écho ICMP (ICMPv4-Entrant)	Diagnostics de réseau de base	Privé, Public	Non	Autoriser

On peut maintenant tester le Ping entre les machines



20.188.57.202:3389 - Connexion Bureau à distance

cycle Bin

Administrator: Command Prompt

```
Description . . . . . : Microsoft Hyper-V Network Adapter
Physical Address . . . . . : 00-0D-3A-79-04-25
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::4cdd:61e7:6025:6196%6(PREFERRED)
IPv4 Address. . . . . : 172.32.0.4(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, October 27, 2020 6:02:55 AM
Lease Expires . . . . . : Saturday, December 4, 2156 4:51:01 PM
Default Gateway . . . . . : 172.32.0.1
DHCP Server . . . . . : 168.63.129.16
DHCPv6 IAID . . . . . : 100666682
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-29-70-67-00-0D-3A-79-04-25
DNS Servers . . . . . : 168.63.129.16
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Administrateur>ping 10.10.0.2

Pinging 10.10.0.2 with 32 bytes of data:
Reply from 10.10.0.2: bytes=32 time=23ms TTL=127
Reply from 10.10.0.2: bytes=32 time=19ms TTL=127
Reply from 10.10.0.2: bytes=32 time=18ms TTL=127
Reply from 10.10.0.2: bytes=32 time=18ms TTL=127

Ping statistics for 10.10.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 23ms, Average = 19ms

C:\Users\Administrateur>
```