Configuration d’un VPN site-à-site

FOUR Lucas
Conseil départemental de la Drôme

Table des matières

Cahier des charges – Expression des besoins

| Descriptif de l'existant |

L'infrastructure de départ étant inexistante, je ne dispose d'aucun service réseau préconfiguré. Mon environnement se limite à un accès à Internet via le réseau local (LAN) du GRETA, qui me permet de télécharger les ressources nécessaires à la mise en place du projet.

| Besoin(s) |

Ce travail pratique a pour objectif la mise en place d'une solution de réseau privé virtuel (VPN) site-à-site. Le besoin est de permettre à deux réseaux géographiquement distants de communiquer entre eux de manière sécurisée et transparente, comme s'ils faisaient partie d'un même réseau local. Les machines de chaque site doivent pouvoir accéder aux ressources de l'autre site tout en garantissant la confidentialité et l'intégrité des échanges.

| Contrainte(s) |

La réalisation de ce travail pratique est soumise aux contraintes suivantes :

- **Contrainte de temps** : le déploiement complet de l'infrastructure doit être réalisé en huit heures.
- **Contrainte technique** : le protocole utilisé pour le tunnel VPN doit être WireGuard.
- **Contrainte de sécurité** : l'authentification entre les deux sites doit reposer sur un échange de clés cryptographiques.
- **Contrainte de routage** : les règles de routage nécessaires à l'acheminement du trafic entre les deux réseaux doivent être configurées.
- **Contrainte de validation** : le TP sera considéré comme réussi uniquement si le tunnel est correctement établi et que les machines de chaque réseau peuvent accéder aux ressources de l'autre réseau de manière sécurisée.

Ressources

| Ressources mises à disposition |

Pour la réalisation de ce travail pratique, j'utilise un environnement virtualisé sous Hyper-V. Les machines virtuelles sont configurées avec deux interfaces réseau distinctes : une interface WAN, connectée au commutateur virtuel externe afin d'accéder au réseau du GRETA et d'établir le tunnel VPN, et une interface LAN, connectée à un commutateur virtuel privé représentant le réseau interne. Cette architecture permet de simuler deux réseaux d'entreprise distincts reliés par un VPN site-à-site. Le protocole WireGuard est utilisé pour établir un tunnel chiffré entre les deux machines, permettant ainsi aux équipements de chaque réseau d'accéder aux ressources de l'autre de manière sécurisée, comme s'ils étaient connectés au même réseau local.

| Ressources nécessaires à la mise en place |

Pour la mise en œuvre de ce travail pratique, plusieurs éléments matériels et logiciels sont nécessaires :

- **Matériel :** Une machine hôte performante avec Hyper-V activé.
- **Logiciel :** Un système d'exploitation pour les machines virtuelles ainsi que WireGuard pour la mise en place du tunnel VPN et la gestion des clés d'authentification
- **Réseau :** Deux commutateurs virtuels (un "Externe" pour le WAN, un "Privé" pour le LAN).

| Gestion des ressources |

Le temps imparti pour ce TP étant d'environ huit heures, installation comprise, j'ai anticipé la préparation de l'environnement nécessaire à la mise en place du VPN. Cette préparation permet de se concentrer rapidement sur l'essentiel : la configuration du tunnel WireGuard entre les deux machines. L'objectif est d'assurer l'installation des machines virtuelles, le paramétrage du tunnel sécurisé ainsi que la configuration des règles de routage permettant la communication entre les deux réseaux. La validation du TP consiste à vérifier l'établissement du tunnel et la capacité des machines de chaque site à communiquer entre elles de manière sécurisée en fin de séance.

Analyse

Solutions	OpenVPN	WireGuard
Coûts	Gratuit (open source)	Gratuit (open source)
OS d'installation	Multi-plateforme (Linux, Windows, macOS, BSD, Android, iOS)	Multi-plateforme (Linux, Windows, macOS, BSD, Android, iOS)
Points forts	Très mature et éprouvé, très compatible, beaucoup d'options (TLS, certificats, profils), fonctionne bien en environnements "contraints" (proxy/ports variés)	Très léger et très performant, latence faible, configuration simple, très bon pour les mobiles (reconnexion rapide), code plus petit donc souvent plus facile à auditer
Interface / utilisation	Souvent géré via fichiers .ovpn + clients GUI selon l'OS ; administration serveur flexible mais peut être plus "verbeuse"	Configuration très directe (pairs/clefs), outils simples (GUI dispo selon OS), logique "peer-to-peer" facile à maintenir
Mise en place	Setup solide mais parfois long (PKI, certificats, paramètres TLS/chiffrement)	Mise en place rapide (génération de clefs + peers), peu de paramètres, déploiement facile
Communauté / Support	Très grande communauté, documentation et tutos abondants, très répandu en entreprise	Communauté très active, doc claire, adoption très large ces dernières années

Idéal pour	Entreprise, accès distant robuste, compatibilité maximale, scénarios avancés (TLS, auth, politiques, contournement réseaux restrictifs)	VPN site-à-site, accès distant rapide, performances, mobiles, lab/PME, déploiements simples et modernes
Limites	Configuration parfois complexe, plus "lourd" (CPU/overhead), perf souvent inférieure à WireGuard	Moins adapté aux besoins très avancés (certificats/TLS), gestion d'identités/accès plus basique, nécessite une bonne gestion des clefs

| Choix d'une solution – Argumentation |

J'ai choisi d'utiliser WireGuard comme solution VPN, car il s'agit d'une technologie moderne offrant de hautes performances, une grande simplicité de configuration et un niveau de sécurité élevé. WireGuard repose sur des mécanismes de chiffrement modernes et utilise un système d'authentification basé sur des paires de clés cryptographiques, ce qui permet de sécuriser efficacement les communications entre les différents sites. De plus, WireGuard se distingue par sa légèreté et sa facilité de déploiement comparé à d'autres solutions VPN plus complexes. Sa configuration simple permet de mettre en place rapidement un tunnel sécurisé entre deux réseaux tout en garantissant la confidentialité et l'intégrité des échanges. Enfin, WireGuard est compatible avec de nombreux systèmes d'exploitation tels que Windows, Linux, macOS, Android et iOS, ce qui facilite son utilisation dans différents environnements. Cette solution répond donc aux besoins de sécurité, de performance et de simplicité d'administration, essentiels pour la mise en place d'un VPN site-à-site efficace et facilement maintenable.

| Plan d'adressage réseau |

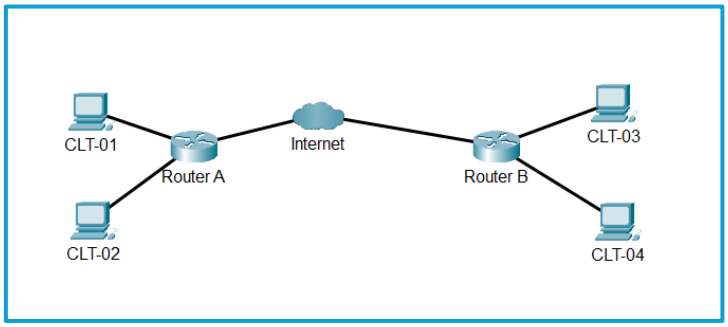
Tableau d'adressage :

Nom du réseau	Adresse réseau	Masque de sous réseau	Première adresse	Dernière adresse	Adresse de broadcast
WAN	172.26.0.0	255.255.254.0	172.26.0.1	172.26.1.254	172.26.1.255
LAN	10.0.0.0	255.255.555.0	10.0.0.1	10.0.0.254	10.0.0.254

Tableau des adresses IP :

Réseau	Machines	Adresse IP	Masque de sous réseau	Passerelle par défaut	DNS
172.31.10.0	GW-Siège	172.31.10.254	255.255.255.0	X	172.31.10.10
172.31.10.0	Serveur AD	172.31.10.10	255.255.255.0	172.31.10.254	172.0.0.1
172.31.20.0	GW-Agence	172.31.20.254	255.255.255.0	X	172.31.10.10
172.31.20.0	PC Agence	172.31.20.10	255.255.255.0	172.31.20.254	172.31.10.10

Schéma réseau :



| Etude de l'impact sur le SI existant |

Étant donné que ce travail s'inscrit dans un contexte de formation, il n'existe aucun système d'information (SI) préexistant, à l'exception de l'accès à Internet. L'ensemble de l'infrastructure nécessaire doit donc être entièrement créé et configuré dans le cadre de ce travail pratique. La mise en place de WireGuard permet de sécuriser les communications en établissant un tunnel VPN chiffré entre deux réseaux distants. Cette solution repose sur un système d'authentification par clés cryptographiques et permet de relier plusieurs machines ou sites à travers Internet de manière sécurisée, tout en assurant la confidentialité et l'intégrité des échanges. Dans un contexte professionnel, le déploiement de WireGuard au sein d'une entreprise permettrait de sécuriser les interconnexions entre différents sites ou réseaux distants, de protéger les échanges transitant sur Internet et de simplifier l'administration grâce à une configuration légère et efficace. Cette solution offre ainsi une alternative moderne, performante et facilement maintenable pour la mise en place de VPN site-à-site.

| Phasage de l'intervention |

Dans un premier temps, je procéderai à la création et à la préparation des machines virtuelles nécessaires au fonctionnement de l'infrastructure réseau dans l'environnement Hyper-V. Chaque machine sera configurée avec les interfaces réseau adaptées : une interface reliée au commutateur virtuel externe pour l'accès au réseau et à Internet, et une interface reliée au commutateur virtuel privé pour représenter le réseau interne. Dans un second temps, je mettrai en place le VPN à l'aide de WireGuard. Je générerai les paires de clés cryptographiques nécessaires pour chaque machine, puis je configurerai les interfaces WireGuard en définissant les adresses IP du tunnel ainsi que les paramètres des pairs (peers) afin d'établir la communication entre les deux réseaux. Une fois la configuration terminée, je mettrai en place les règles de routage permettant aux machines des deux réseaux de communiquer entre elles à travers le tunnel VPN. Enfin, je réaliserai plusieurs tests de connectivité afin de vérifier que le tunnel est correctement établi et que les machines de chaque réseau peuvent accéder aux ressources de l'autre réseau de manière sécurisée.

| Prévision des tests et validation |

Lors de la configuration de WireGuard, je procéderai à plusieurs vérifications afin de m'assurer de son bon fonctionnement. Je vérifierai tout d'abord que l'interface WireGuard est correctement activée sur chaque machine et que les paramètres du tunnel (adresse IP du tunnel et port d'écoute) sont correctement configurés. Je contrôlerai ensuite que les paires de clés cryptographiques sont correctement générées et associées aux différents pairs (peers), et que les réseaux autorisés (AllowedIPs) correspondent bien aux sous-réseaux qui doivent transiter par le tunnel VPN. Après cela, je vérifierai que les règles de routage et de pare-feu permettent la communication entre les deux réseaux à travers le tunnel. Enfin, je testerai la connectivité en établissant la communication entre les deux machines afin de m'assurer que le tunnel WireGuard est bien actif. Je vérifierai notamment que les machines obtiennent un accès au réseau distant et que les échanges (tests de ping ou accès aux services) fonctionnent correctement. Ces différentes vérifications permettront de valider le bon fonctionnement du VPN site-à-site mis en place avec WireGuard.

Mise en place

| Installation du service WireG |

La première étape consiste à installer **WireGuard** sur les deux passerelles Debian.

WireGuard est un protocole VPN moderne intégré au noyau Linux, offrant :

- Un chiffrement performant
- Une configuration simple
- Une faible consommation de ressources.

Sur les deux machines, on commence par mettre à jour la liste des paquets puis installer WireGuard :

```bash
sudo apt update
sudo apt install wireguard -y
```

Ce paquet installe également l'outil **wireguard-tools,** qui permet de :

- Générer les clés
- Créer les interfaces VPN
- Gérer la configuration du tunnel.

Une fois installé, le système est prêt à créer l'interface VPN virtuelle appelée **wg0.**

| Génération des clés cryptographique |

WireGuard utilise un système de cryptographie asymétrique basé sur une paire de clés :

- **Clé privée** : conservée secrètement sur la machine
- **Clé publique** : partagée avec le pair distant.

Chaque passerelle génère sa propre paire de clés avec la commande suivante :

```bash
wg genkey | tee privatekey | wg pubkey > publickey
```

Cette commande réalise plusieurs actions :

- **wg genkey** génère une clé privée.
- **tee privatekey** enregistre cette clé dans un fichier.
- **wg pubkey** génère automatiquement la clé publique correspondante.
- La clé publique est enregistrée dans le fichier **publickey.**

À la fin de cette étape, chaque machine possède :

```
privatekey
publickey
```

La clé publique du Site A devra être copiée sur le Site B, et inversement, afin d'établir la relation de confiance entre les deux passerelles.

| Configuration du VPN sur le site B (Siège) |

Sur la passerelle **GW-Siège**, on crée le fichier de configuration :

```
/etc/wireguard/wg0.conf
```

Configuration :

```ini
[Interface]
Address = 172.31.0.1/24
ListenPort = 51820
PrivateKey = CLE_PRIVEE_SITE_B

[Peer]
PublicKey = CLE_PUBLIQUE_SITE_A
AllowedIPs = 172.31.20.0/24
Endpoint = 172.31.1.90:51820
PersistentKeepalive = 25
```

| Activation du routage IPv4 |

Par défaut, un système Linux ne transmet pas les paquets entre ses interfaces.

Pour que la passerelle puisse transférer les paquets :

LAN ↔ VPN

Il faut activer le **IP forwarding**.

Commande :

```bash
sysctl -w net.ipv4.ip_forward=1
```

Pour rendre ce paramètre permanent :

Modifier le fichier :

```
/etc/sysctl.conf
```

Et ajouter ou décommenter :

```
net.ipv4.ip_forward=1
```

Cette étape est **indispensable pour que les machines du LAN puissent utiliser le tunnel VPN**.

| Démarrage du tunnel VPN |

Une fois la configuration terminée, on active l'interface **WireGuard :**

```bash
wg-quick up wg0
```

Cette commande :

- Crée l'interface réseau virtuelle **wg0**
- Applique la configuration
- Établit le tunnel VPN.

Pour vérifier l'état du VPN :

```bash
wg show
```

Cette commande affiche :

- Les clés utilisées
- L'adresse du peer
- Le **dernier handshake**
- Le volume de données échangé.

La présence d'un **handshake récent** confirme que la connexion VPN est active.

| Vérification de la connectivité |

Sur la passerelle Debian, la commande suivante permet de vérifier que le tunnel WireGuard est actif :

```bash
wg show
```

Résultat attendu :

- Présence du **peer distant**
- Affichage d'un **latest handshake récent**
- Échange de données (transfer).

Cela confirme que le tunnel VPN est bien établi entre les deux passerelles.

Depuis la passerelle du **Site A**, on teste la connexion avec l'interface VPN du Site B :

```bash
ping 172.31.0.1
```

Résultat attendu :

Réception de réponses ICMP indiquant que la communication fonctionne à travers le tunnel VPN.

Depuis la passerelle du **Site B**, on vérifie l'accès à la passerelle du Site A :

```bash
ping 172.31.20.254
```

Résultat attendu :

Réponse du ping confirmant que le routage entre les deux réseaux est fonctionnel.

Depuis un **poste client du Site A**, on teste l'accès au serveur du siège :

```bash
ping 172.31.10.10
```

Résultat attendu :

Le poste client du Site A reçoit une réponse du serveur du Site B, ce qui confirme que :

- Le tunnel VPN fonctionne
- Le routage entre les deux LAN est correct
- La communication inter-sites est opérationnelle.

Conclusion

La mise en place et la configuration du VPN avec WireGuard m'ont permis de déployer une solution de communication sécurisée entre deux réseaux distincts. En configurant les interfaces réseau des machines virtuelles ainsi que les paramètres du tunnel WireGuard, j'ai pu établir une connexion chiffrée permettant aux machines de chaque réseau de communiquer entre elles de manière sécurisée.s

Auto-évaluation

Le temps imparti de quatre heures a été respecté grâce à une bonne préparation en amont, notamment la préparation de l'environnement de virtualisation et la connaissance préalable des différentes étapes de configuration. Cette anticipation m'a permis d'optimiser le déroulement du TP et de me concentrer rapidement sur la mise en place et la configuration du VPN avec WireGuard. Ainsi, les différentes étapes, de la création des machines virtuelles à l'établissement du tunnel sécurisé et aux tests de connectivité, ont pu être réalisées dans les délais prévus.