



Republique Democratique Du Congo

UNIVERSITE DE KINSHASA



FACULTE DES SCIENCES ET TECHNOLOGIES

DEPARTEMENT DE MATHÉMATIQUE, INFORMATIQUE ET STATISTIQUE

Systeme d'exploitation Groupe 29
« Création d'un Serveur VPN avec OpenVPN ou
WireGuard. »

Fait par :

- ✓ EMPAMPOSA BOSINGA BENJAMIN
- ✓ NGONGO NGOYI MOISE
- ✓ KANDONGO MAKINGA DON
- ✓ MUTOMBO DINANGA ELVIS
- ✓ NIMI MANANGA TIMOTHEE
- ✓ GILANGU NZAMBA EMMANUEL
- ✓ NGANGU KITSHAMA DANIEL
- ✓ MEBUO MENGWE NICOLAS

PROF/ KASENGEDIA

ANNEE ACADEMIQUE 2024-2025

1. Introduction

Dans un monde numérique où la sécurité des communications est primordiale, les VPN (Virtual Private Network) s'imposent comme une solution indispensable. Ce projet vise à mettre en œuvre un serveur VPN sécurisé avec WireGuard ou OpenVPN, un protocole moderne, léger et rapide. L'objectif est de comprendre le fonctionnement d'un tunnel chiffré et de maîtriser la mise en place d'une architecture sécurisée de communication sur une machine Linux virtuelle.

Pré requis

On a besoin des différents matériels et logiciels pour la création d'un Serveur VPN avec un Linux Ubuntu.

- Un Pc sous Linux Ubuntu ou une VM
- Le logiciel [WireGuard](#)

2. Objectifs du Projet

- Créer un serveur VPN sécurisé avec WireGuard.
- Comprendre la logique de chiffrement et d'authentification.
- Tester et valider la connectivité via une machine virtuelle.

Qu'est-ce qu'un VPN ?

Est un service utilisé pour protéger votre connexion Internet contre tout accès non autorisé avec le moyen de chiffrement. Il peut également faire office de mécanisme d'arrêt, en mettant fin à des programmes présélectionnés en cas d'activité suspecte sur Internet, réduisant ainsi la probabilité que les données soient compromises.

Comment ça marche ?

Un VPN masque votre adresse IP en redirigeant votre connexion vers un serveur distant spécialement configuré et géré par l'hôte du VPN. Cela signifie que si vous surfez en ligne au moyen d'un VPN, le serveur VPN devient la source de vos données. Ainsi, votre fournisseur d'accès Internet (FAI) et d'autres tiers ne peuvent pas connaître les sites Web que vous visitez ni les données que vous envoyez et recevez en ligne. Un VPN fonctionne comme un filtre qui transforme toutes vos données en « charabia ». Même si quelqu'un parvenait à accéder à vos données, celles-ci seraient inexploitable.

Qu'est-ce qu'un serveur ?

Un serveur est un ordinateur ou un système qui met des ressources, des données, des services ou des logiciels à la disposition d'autres ordinateurs, appelés « clients », sur un réseau. En théorie, un ordinateur est considéré comme un serveur à partir du moment où il partage des ressources avec une machine cliente.

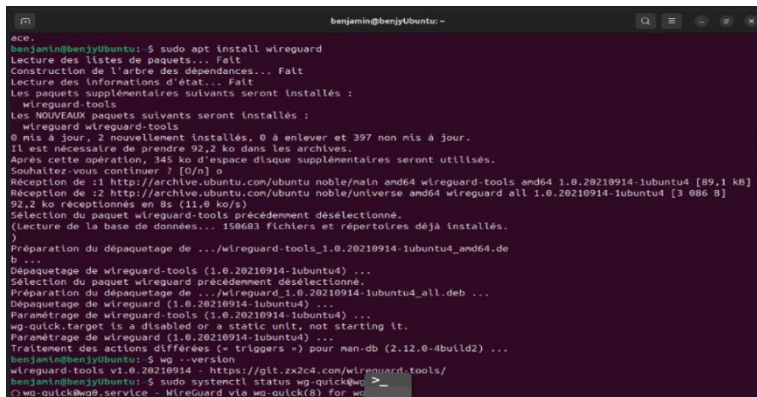
Qu'est-ce que WireGuard ?

WireGuard est un protocole VPN avancé et moderne, facile à configurer, offrant une vitesse fulgurante. Il est considéré comme plus sécurisé qu'IPsec grâce à une cryptographie de pointe. La fonctionnalité de WireGuard VPN fonctionne généralement mieux que celle d'OpenVPN, bien connu dans le domaine.

4. Démarche de Réalisation

4.1. Installation de WireGuard

`sudo apt install wireguard`



```
benjamin@benjyUbuntu: ~$ sudo apt install wireguard
benjamin@benjyUbuntu: ~$ sudo apt install wireguard
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  wireguard-tools
Les NOUVEAUX paquets suivants seront installés :
  wireguard wireguard-tools
0 mis à jour, 2 nouvellement installés, 0 à enlever et 397 non mis à jour.
Il est nécessaire de prendre 92,2 ko dans les archives.
Après cette opération, 345 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://archive.ubuntu.com/ubuntu noble/main amd64 wireguard-tools amd64 1.0.20210914-1ubuntu4 [89,1 kB]
Réception de :2 http://archive.ubuntu.com/ubuntu noble/universe amd64 wireguard all 1.0.20210914-1ubuntu4 [3 886 B]
92,2 ko réceptionnés en 8s (11,0 ko/s)
Sélection du paquet wireguard-tools précédemment désélectionné.
(Lecture de la base de données... 156683 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../wireguard-tools_1.0.20210914-1ubuntu4_amd64.de
b ...
Dépaquetage de wireguard-tools (1.0.20210914-1ubuntu4) ...
Sélection du paquet wireguard précédemment désélectionné.
Préparation du dépaquetage de .../wireguard_1.0.20210914-1ubuntu4_all.deb ...
Dépaquetage de wireguard (1.0.20210914-1ubuntu4) ...
Paramétrage de wireguard-tools (1.0.20210914-1ubuntu4) ...
wg-quick.target is a disabled or a static unit, not starting it.
Paramétrage de wireguard (1.0.20210914-1ubuntu4) ...
Traitement des actions différées (= triggers =) pour man-db (2.12.0-4build2) ...
benjamin@benjyUbuntu: ~$ wg --version
wireguard-tools v1.0.20210914 - https://git.zx2c4.com/wireguard-tools/
benjamin@benjyUbuntu: ~$ sudo systemctl status wg-quick@wg0
wg-quick@wg0.service - WireGuard via wg-quick(8) for wg0
```

4.2. Génération des clés

Les clés servent à chiffrer les connexions VPN.



```
benjamin@benjyUbuntu: ~$ wg genkey | sudo tee /etc/wireguard/privatekey
wIbrrPNrYbEo6MRkc4V632L0CW0wTz2rnccEsLqwm3E=
benjamin@benjyUbuntu: ~$ nano wg.conf
benjamin@benjyUbuntu: ~$ sudo nano /etc/wireguard/wg.conf
benjamin@benjyUbuntu: ~$ wg genkey | sudo tee /etc/wireguard/publickey
YKjWw6iqMv8P91Hq3M2KrfkxaVEEWYCXJSTbIjzVTwk=
```

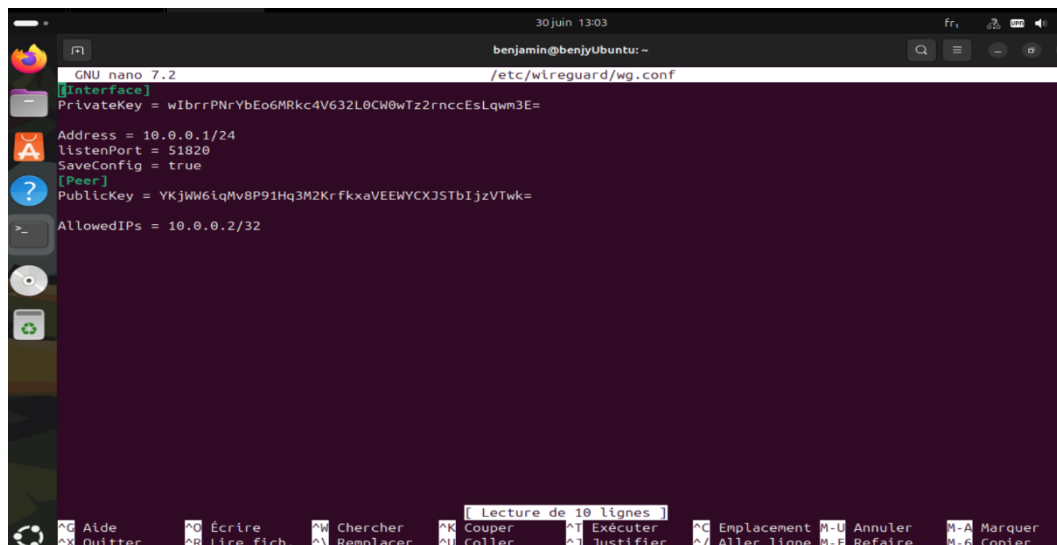
La clé privée (privateKey) est l'identité secrète de l'interface wireguard(client ou serveur), nous allons l'utiliser pour chiffrer les données

La clé publique (publicKey) est la clé dérivée de la clé privée ; la clé est partageable aux correspondants(clients ou serveurs distants), elle permet de vérifier les signatures et de déchiffrer les messages.

4.3. Configuration du serveur (/etc/wireguard/wg.conf)

a) Création le fichier de configuration

```
benjamin@benjyUbuntu:~$ sudo nano /etc/wireguard/wg.conf
```



```
GNU nano 7.2 /etc/wireguard/wg.conf
[Interface]
PrivateKey = wIbrrPNrYbEo6MRkc4V632L8CW0wTz2rnccESLqwm3E=
Address = 10.0.0.1/24
ListenPort = 51820
SaveConfig = true
[Peer]
PublicKey = YKjWM6iqMv8P91Hq3M2KrfkxavEEWYCXJSTbIjzVTwk=
AllowedIPs = 10.0.0.2/32
```

[Interface]

Cette section définit l'interface VPN locale, c'est-à-dire le serveur WireGuard lui-même.

PrivateKey = wIbrrPNrYbEo6MRkc4VG32L8CW0wTz2rnccESLqwm3E=*

- C'est la clé privée du serveur.

Address = 10.0.0.1/24

- C'est l'adresse IP interne que le serveur VPN aura dans le tunnel.
- /24 signifie que le sous-réseau inclura les IP allant de 10.0.0.1 à 10.0.0.254.

ListenPort = 51820

- Port UDP sur lequel le serveur écoute les connexions entrantes.
- C'est le port par défaut de WireGuard.

► **SaveConfig** = true

Option qui permet à WireGuard de sauvegarder automatiquement les modifications.

[Peer]

Cette section représente un client distant qui se connectera à ton serveur.

PublicKey = YKjJW461qMv8P91Hq3M2KrfkxaVEEWYCXJSTbIJ2VTwk=

- C'est la clé publique du client
- Elle permet au serveur de vérifier l'identité du client.

AllowedIPs = 10.0.0.2/32

- Cela veut dire que le client aura l'adresse privée 10.0.0.2 dans le tunnel VPN.
- /32 signifie "juste cette adresse précise".
- C'est aussi une règle de routage : le serveur saura que tout trafic vers 10.0.0.2 doit aller vers ce client.

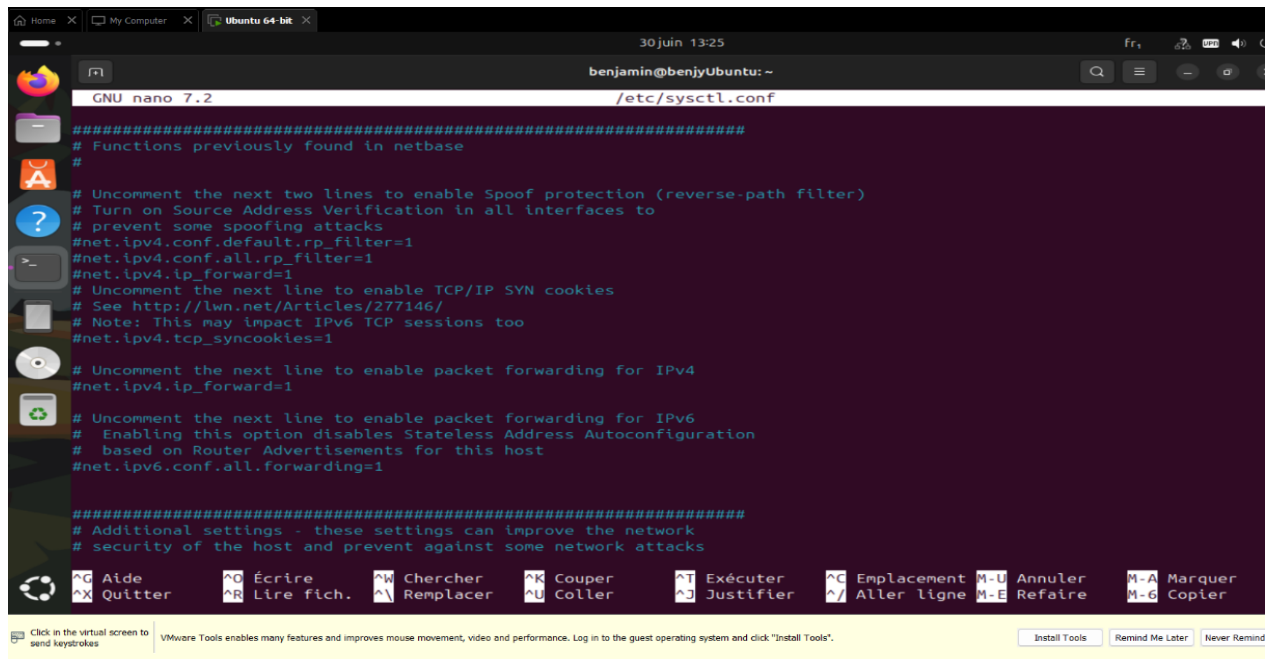
4.4. Activation du routage IP

Certains aspects de la configuration réseau du serveur doivent être modifiés afin que WireGuard puisse acheminer correctement le trafic à travers le VPN. Le premier d'entre eux est le transfert IP, une méthode permettant de déterminer où le trafic IP doit être acheminé. Ceci est essentiel pour la fonctionnalité VPN que notre serveur fournira. Editer le fichier sysctl.conf.

Nous avons accédé au fichier sysctl.conf via la commande

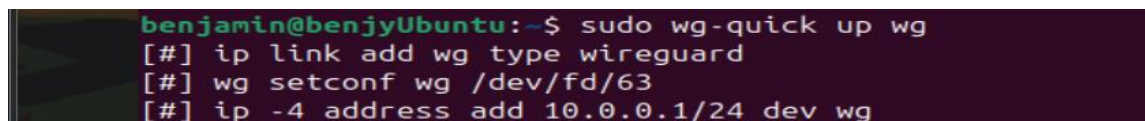
```
benjamin@benjyUbuntu:~$ sudo nano /etc/sysctl.conf
```

Que nous avons ajouter `ipv4.ip_forward=1`

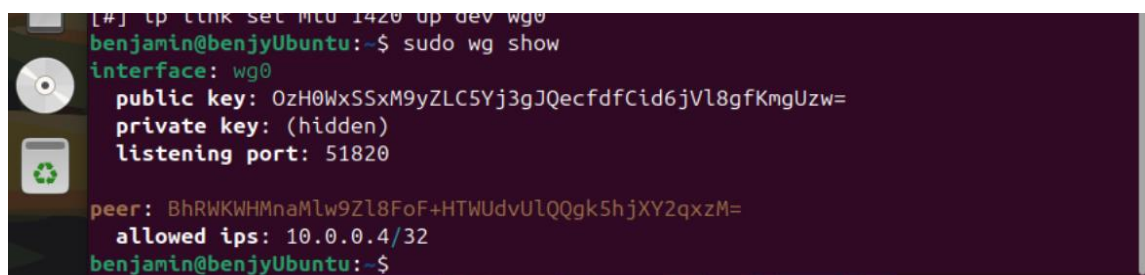


4.5. Démarrage du VPN

`sudo wg-quick up wg`



Vérification de l'activation de l'interface



6. Conclusion

La mise en place d'un serveur VPN avec WireGuard a permis de renforcer la sécurité des communications sur Internet tout en offrant une solution simple et efficace pour masquer l'identité numérique des utilisateurs. Ce projet a non seulement permis de comprendre les principes fondamentaux des VPN, mais aussi d'acquérir des compétences pratiques en matière de configuration et de gestion des serveurs VPN.

7. Bibliographie

1. Système d'exploitation note de cours L2 lmd informatique – Professeur Kasengedi Motumbe Pierre
2. WireGuard Documentation Officielle – WireGuard
(<https://www.wireguard.com/>)
3. Ubuntu Manual Pages – Ubuntu Manpages
(<https://manpages.ubuntu.com/>)
4. Installation d'un serveur Wireguard sous debian 10
(<https://www.gdidees.eu/userfiles/file/docs/Installation-ServeurWIREGUARD-Debian10.pdf>)