INSTALLATION D'UN SERVEUR WIREGUARD AVEC EASY WG QUICK SOUS DEBIAN 10

Debian Buster

Configuration de base

Tutoriel **WIREGUARD** – DEBIAN 10

David GOÏTRÉ

Table des matières

Introduction 1

1. Pré requis 1

2. Paramétrage du serveur 2

3. Paramétrage de connexion au serveur 2

4. Installer le serveur WireGuard 3

5. Activer le transfert IP 3

5. Création des utilisateurs 4

6. Démarrer le service WireGuard 5

7. Connecter le client Windows au VPN 5

8. Connecter le client à l'aide du qrcode 5

9. Configurer le routage à l'aide de UFW 6

10. Commandes Linux Debian 6

11. Utilisation local du VPN 6

12. Conclusion 7

Introduction

Un réseau privé virtuel (VPN) est un protocole utilisé pour ajouter la sécurité et la confidentialité aux réseaux privés et publics. Les VPN envoient du trafic entre deux ou plusieurs appareils sur un réseau dans un tunnel chiffré. Une fois la connexion VPN établie, tout le trafic réseau est chiffré du côté du client. Les VPN masquent votre adresse IP de sorte que nos actions en ligne sont pratiquement introuvables.

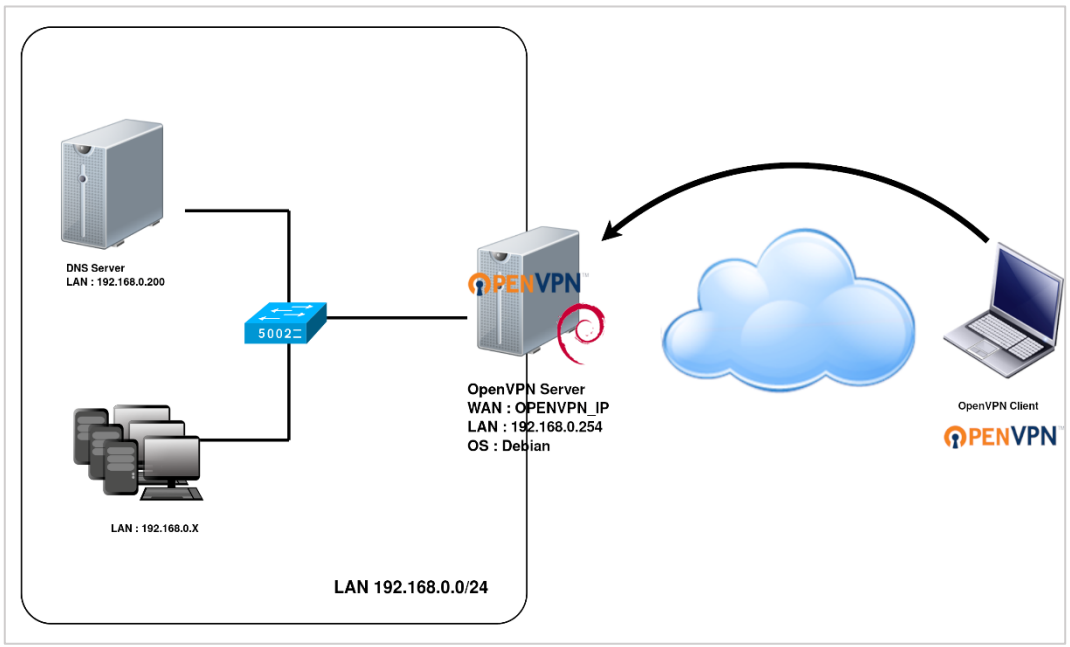
Il fournit le cryptage et l'anonymat, protège nos activités en ligne, nos achats en ligne, l'envoi d'e-mails et aide également à garder notre navigation Web anonyme.

1. Pré requis

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

- Un ou des PC client sous Windows
- Une Box (Free, Orange, Sfr…)
- Le logiciel WireGuard pour les clients
- Le logiciel Putty pour se connecter en SSH au serveur VPN
- Connaitre l'interface réseau (eth0, br0, enp0s3, ens3…) via la commande : **ip a**
  Pour notre test c'est **l'interface eth0** qui sera utilisée

Voici le schéma que l'on doit obtenir une fois le serveur VPN mise en place :



Ce schéma n'est qu'un exemple. Il n'est pas essentiel de posséder une machine Serveur DNS, ni d'avoir plusieurs PC Client sur le réseau LAN.

2. Paramétrage du serveur

Avant d'aller plus loin, il nous faut connaître l'interface réseau de notre serveur **Debian** et lui attribuer une adresse IP fixe.

a) Lister les interfaces

```
$ ip link | awk '{ print $2}'   # liste les interfaces
# ethtool <interface> | grep detected   # détecte l'interface connectée
```

b) Définir une adresse IP fixe

```
# nano /etc/network/interfaces   # ouvre le fichier des interfaces
```

c) Copier le texte ci-dessous dans le fichier **interfaces**

```
# Interface reseau de bouclage
auto lo
iface lo inet loopback
# Interface reseau principale
allow-hotplug eth0
iface eth0 inet static
address 192.xxx.xxx.xxx
netmask 255.255.255.0
gateway 192.xxx.xxx.xxx
```

d) Rebooter le serveur

```
# systemctl restart networking
# systemctl reboot
```

3. Paramétrage de connexion au serveur

a) Créer **une redirection de port** sur la box (Free, Orange…) vers votre serveur **Debian**.

- **port** : 51820
- **Protocole** : UDP

b) Activer le **SSH** sur le serveur. Pour ce faire, ouvrir le dossier **Boot**, de la carte SD du **Debian** via l'explorateur de Windows et créer un fichier **ssh** (sans extension) dans ce **dossier**.

c) Ouvrir **Putty** et se connecter au serveur VPN avec les identifiants créés lors de l'installation de Linux

b) Mettre à jour les packages du système vers la dernière version. Exécuter la commande suivante pour mettre à jour et mettre à niveau les packages de votre système :

```
# apt-get update -y
# apt-get upgrade -y
```

4. Installer le serveur WireGuard

Le référentiel de **Easy-Wg-Quick** est disponible sur Github. Le script a été adapté pour les besoins du tutorial.

a) Télécharger le script d'installation et le rendre exécutable

```
# https://www.gdidees.eu/userfiles/file/easy-wgquick.zip
# mkdir /wgquick  # décompresser le fichier dedans
# chmod +x easy-wg-quick
```

b) Installer Wireguard VPN Server et Qrencode

```
# sudo apt install wireguard-tools mawk grep iproute2 qrencode
```

c) Installer Dkms, Tools et headers

```
# apt-get install wireguard wireguard-tools net-tools linux-headers-`uname -r`
# apt-get install wireguard-dkms wireguard-tools linux-headers-$(uname -r)
```

d) Vérifier que le module noyau Wireguard est correctement installé. Cela devrait afficher les détails du module, comme le nom de fichier, la description, l'auteur

```
# /sbin/modinfo wireguard
```

5. Activer le transfert 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**

```
# nano /etc/sysctl.conf
```

a) Décommenter la ligne suivante

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

b) Vérifier que **l'ip_forward** est activé

```
# sudo sysctl -p   # active l'ip_forward
# cat /proc/sys/net/ipv4/ip_forward   # affiche le résultat
```

Installer d'autres outils (optionnel) :

```
# apt-get install git
# apt-get install python3-qrcode
```

5. Création des utilisateurs

a) Editer le fichier **easy-wg-quick** et renseigner les variables suivantes :

```
WG_IPHOST="86.xxx.xxx.xxx"          #@IP DU ROUTEUR
WG_IPSRV="10.0.0."                  #@IP DU VPN
WG_ALLOWEDIPS="0.0.0.0/0, ::/0"     #@IP DU TRAFIC RESEAU
WG_DNS="192.xxx.xxx.xxx"            #DNS IPV4
WG_DNS_NET6="xxxx:xxxx"             #DNS IPV6
WG_PORT="45698"                     #PORT DE REDIRECTION APPLIQUE AU ROUTEUR
```

b) Lancer le script **easy-wg-quick** pour générer un utilisateur

```
# cd /wgquick
# ./easy-wg-quick  # créer le fichier wgclient_10.conf
# ./easy-wg-quick theo  # créer le fichier wgclient_theo.conf
```

c) Un résultat s'affiche comme ci-dessous

```
No seqno.txt... creating one!
No wgpsk.key... creating one!
No wghub.key... creating one!
No wghub.conf... creating one!
Wireguard hub address is 10.13.1.140: 51820 on wlp9s0.
Note: customize [Interface] section of wghub.conf if required!
Note: passing argument to script creates client configuration with supplied
    name to help remembering which config was for which device. If you
    didn't pass any argument you can still rename created file manually
    with command:
 mv -vi wgclient_10.conf wgclient_name.conf
No wgclient_10.conf... creating one!
```

```
Scan QR code with your phone or use "wgclient_10.conf" file.
Updating wghub.conf... done!
Important: Deploy updated wghub.conf configuration to wireguard with wg-quick:
 sudo wg-quick down ./wghub.conf # if already configured
 sudo wg-quick up ./wghub.conf
 sudo wg show # to check status
```

d) Le fichier **wghub.conf** est créé. Lancer la configuration à chaque création d'un utilisateur

```
# sudo wg-quick down ./wg0.conf  # if already configured
# sudo wg-quick up ./wg0.conf
```

e) Exécuter la commande suivante pour vérifier l'état du service Wireguard :

```
# sudo wg show
```

On doit obtenir la sortie suivante :

```
interface: wghub
 public key: 9swxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx=
 private key: (hidden)
 listening port: 45968

peer: eiMxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx =
 preshared key: (hidden)
 allowed ips: 10.0.0.10/32, fd22:1807:5920:9756::10/128
```

6. Démarrer le service WireGuard

On peut maintenant démarrer le service WireGuard et l'activer après le redémarrage du système à l'aide des commandes suivantes :

```
# cp wghub.conf /etc/wireguard/wghub.conf
# systemctl enable wg-quick@wghub
# systemctl status wg-quick@wghub  #Vérifie le status
```

7. Connecter le client Windows au VPN

Il faut transférer le fichier de configuration sur le PC Client à l'aide d'un logiciel FTP.

a) Se connecter au serveur via **FileZilla** avec les mêmes identifiants utilisés dans Putty.
b) Ouvrir le dossier et récupérer le fichier

```
$ /home/user/wgquick/wgclient_10.conf
```

c) Copier le fichier dans le dossier souhaité **C:\Documents\confs**
d) Ouvrir le client WireGuard
e) Importer le fichier **wgclient_10.conf**, puis cliquer sur le bouton **Activer**

8. Connecter le client à l'aide du qrcode

a) Photographier le **QRCode** (affiché suite à l'exécution du script) avec l'application WireGuard du smartphone

9. Configurer le routage à l'aide de UFW

Par défaut, le pare-feu UFW n'est pas installé dans Debian 10. On peut l'installer avec la commande suivante :

```
# apt-get install ufw -y
```

Après avoir installé le pare-feu UFW, vous devrez ajouter des règles de pare-feu pour activer le masquage afin que vos clients VPN accèdent à Internet.

a) Tout d'abord, on doit configurer UFW pour accepter les paquets transférés

```
# sudo ufw allow 51820/udp
```

b) Ensuite, recharger le pare-feu UFW à l'aide de la commande suivante:

```
# sudo ufw disable
# sudo ufw enable
```

10. Commandes Linux Debian

a) Liste des commandes basique à la gestion du serveur Linux Debian

```
# wg-quick up ./wg0.conf   # activer WireGuard
# wg-quick down ./wg0.conf   # désactiver WireGuard
# systemctl start wg-quick@wg0   # démarrer WireGuard
# systemctl stop wg-quick@wg0   # arrêter WireGuard
# systemctl poweroff   # éteint le serveur en toute sécurité
# systemctl reboot   # redémarre le serveur en toute sécurité
# apt install xrdp   # install le bureau à distance RDP
# systemctl enable xrdp   # active xrdp en tant que service système
# apt install openssh-server  # installe le SSH
# systemctl enable sshd.service  # active le service SSH au démarrage
##### Désactive la mise en veille #####
# systemctl mask sleep.target suspend.target hibernate.target hybrid-sleep.target
```

11. Utilisation local du VPN

Une fois connecté au VPN **via un PC local**, impossible d'accéder aux périphériques réseaux locaux sans ajouter une route spécifique.

a) Ouvrir une invite de commande

b) Saisir la commande : **route -p add 192.168.1.X/24 10.0.0.2** (@IP du périphérique / @IP du VPN)

c) Mapper les périphériques via leur adresse IP

12. Conclusion

WireGuard est installé et configuré avec succès sur le serveur **Linux Debian 10**. On peut désormais accéder à Internet en toute sécurité et protéger son identité.

Destiné à Linux Debian, **WireGuard** fonctionne aussi parfaitement sur une distribution Fedora, Ubuntu ou Mint en mode VPS ou sur un ordinateur personnel.