

01/05/2023

# Mise en place d'un VPN

## Itinérant

### Atelier



# Table des matières

Travail à faire :..... 2

Installation et Config du serveur Wireguard :..... 3

Configuration du Client Wireguard : ..... 8

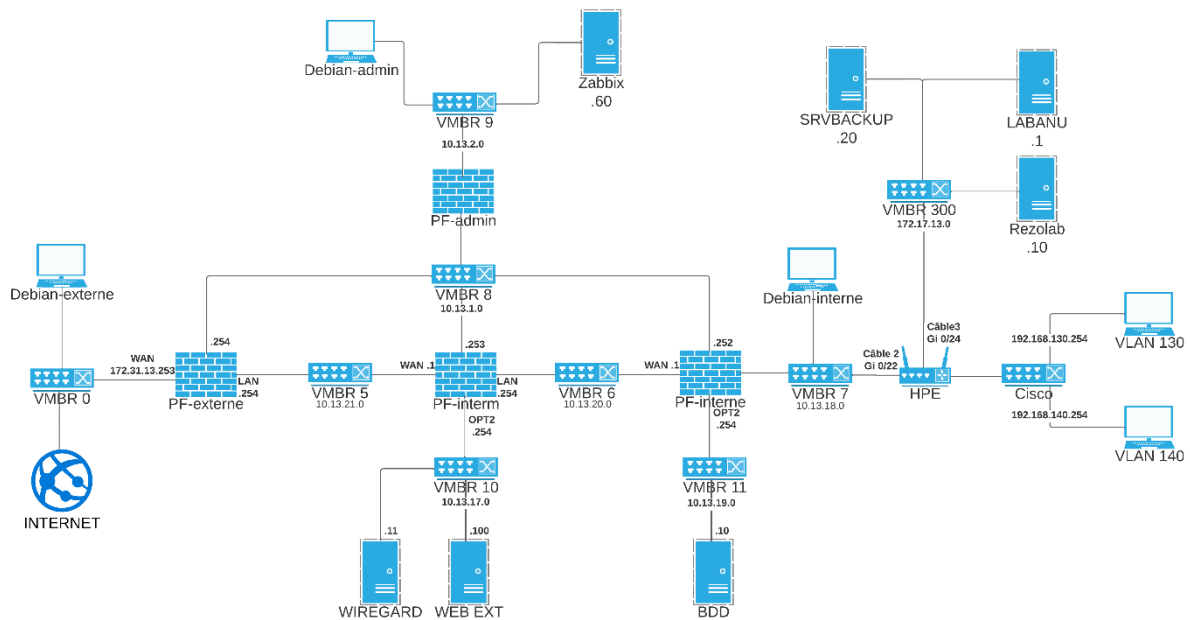
LES TEST :..... 13

# Travail à faire :

Dans ce TP nous allons créer un VPN Afin que un utilisateur distant a accès à ses fichiers depuis chez lui.

Pour cela nous allons mettre en place un serveur VPN WIREGUARD qui tourne sur du Debian 11.

Voici le schéma final :



# Installation et Config du serveur

## Wireguard :

Bon pour commencer il nous faut une Debian 11 installer et paramétrer afin que l'on puisse commencer.

Pour l'exemple la machine virtuel WIREGARD a comme IP 10.13.17.11 attentions il est fortement conseiller de faire un accès SSH mais il faut créer les routes depuis la PF-admin pour et passer par la PF-interm.

Pour ma part les routes étaient déjà créées grâce à un autre TP. (Oublie pas qu'il faut créer les règles pour le SSH sur le PF-Admin et PF-Interm).

Enfin on peut débiter il faut d'abord mettre à jour :

`apt-get update`

Puis après Install wireguard :

`apt-get install wireguard`

La partie logicielle de wireguard est installer mais il lui faut deux trois autres choses pour pouvoir fonctionner :

Maintenant il nous faut la commande wg qui va nous générer des clés privées comme public

`wg genkey | sudo tee /etc/wireguard/wg-private.key | wg pubkey | sudo tee /etc/wireguard/wg-public.key`

Normalement la clé publique sera écrite sur la console il nous faut ajouter notre clé privée dans le dossier de wireguard :

```
sudo cat /etc/wireguard/wg-private.key
```

Maintenant il créer un fichier de configuration que nous allons appelez wg0.conf :

```
sudo nano /etc/wireguard/wg0.conf
```

Dans ce fichier il faut rajouter le contenu suivant (on viendrait le complété par la suite)

```
[Interface]
```

```
Address = 10.7.0.1
```

```
SaveConfig = true
```

```
ListenPort = 51820
```

```
PrivateKey = <clé privée du serveur>
```

Alors La section [Interface] sert à déclarer la partie serveur. Voici quelques informations :

- Address : l'adresse IP de l'interface WireGuard au sein du tunnel VPN (sous-réseau différent du LAN distant)

- SaveConfig : la configuration est mise en mémoire (et protégée) tout le temps que l'interface est active

- ListenPort : le port d'écoute de WireGuard, ici c'est 51820 qui est le port par défaut, mais je vous invite à le personnaliser

- PrivateKey : la valeur de la clé privée de notre serveur (wg-private.key)

Maintenant nous allons démarrer cette interface avec la commande :

```
sudo wg-quick up wg0
```

Puis nous allons vérifier si tout est bon avec :

`ip a`

Normalement voici le résultat :

```
valid_lft forever preferred_lft forever
3: wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state UNKNOWN
up default qlen 1000
    link/none
    inet 10.7.0.1/24 scope global wg0
        valid_lft forever preferred_lft forever
```

En même temps nous allons en profiter pour afficher la config de wg0 :

`sudo wg show wg0`

Voici le résultat :

```
interface: wg0
  public key: byF3zSV9rMrqlgR3PFaOFAq6G8SpSit+9k7ePb9y8B8=
  private key: (hidden)
  listening port: 51820
```

Après cela il faut juste faire la commande suivante afin que l'interface wg0 soit actif au démarrage de la Debian.

`sudo systemctl enable wg-quick@wg0.service`

Bon c'est là que cela devient un peu compliqué il faut activer l'ip forwarding afin que la Debian puisse router les paquets entre les différents réseaux comme un routeur :

`sudo nano /etc/sysctl.conf`

Il faut ajouter à la fin du fichier cette ligne :

`net.ipv4.ip_forward = 1`

Après il faut activer l'IP Masquerade pour faire simple c'est activer le NAT sur la Debian (Comme un pare-feu linux) on va utiliser la commande ufw il faut l'installer pour commencer :

```
apt install ufw
```

On va faire c'est commande à une pour autoriser le SSH et l'autre pour activer le port 51820 (le wireguard) :

```
sudo ufw allow 22/tcp
```

Puis

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

Ensuite il nous faut le nom de l'interface de base de debian on la trouve grâce la commande ip a :

```
valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
rnp default qlen 1000
link/ether 32:67:3c:0b:00:00 brd ff:ff:ff:ff:ff:ff
```

Grace a cette info peut s'en servir pour édit le fichier suivant :

```
nano /etc/ufw/before.rules
```

et il faut ajouter ces lignes a la fin du fichier :

```
# NAT - IP masquerade
```

```
*nat
```

```
:POSTROUTING ACCEPT [0:0]
```

```
-A POSTROUTING -o ens18 -j MASQUERADE
```

```
# End each table with the 'COMMIT' line or these rules won't be
processed
```

```
COMMIT
```



Et toujours dans le même fichier on va déclarer le réseau interne de l'entreprise (mais je vais l'adapter pour seulement un hôte mais cela est pareil pour un réseau il faut juste adapter le /32 en /24 ou autre) :

# autoriser le forwarding pour le réseau distant de confiance (+ le réseau du VPN)

-A ufw-before-forward -s 172.17.13.1/32 -j ACCEPT

-A ufw-before-forward -d 172.17.13.1/32 -j ACCEPT

-A ufw-before-forward -s 10.13.17.11/32 -j ACCEPT

-A ufw-before-forward -d 10.13.17.11/32 -j ACCEPT

-A ufw-before-forward -s 10.7.0.2/32 -j ACCEPT

-A ufw-before-forward -d 10.7.0.2/32 -j ACCEPT

Bon il ne reste plus qu'à appliquer nos changements et à redémarrer les services avec les commandes suivantes :

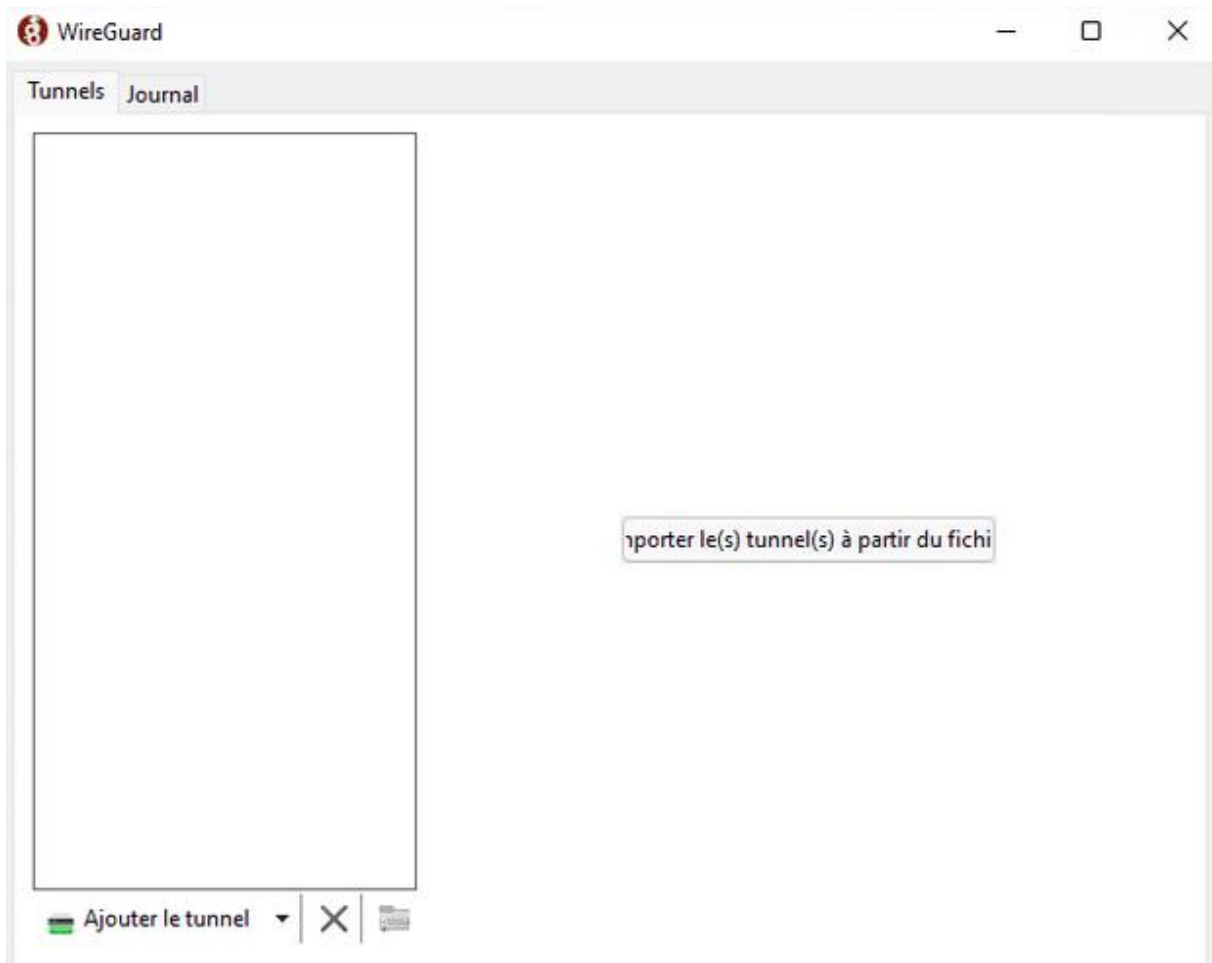
sudo ufw enable

sudo systemctl restart ufw

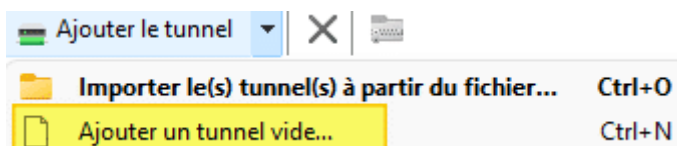


# Configuration du Client Wireguard :

Le client wireguard doit être télécharger sur site officiel puis installer après cela vous allez arriver sur cela :



Nous allons créer un nouveau tunnel vide il faut faire ajouter un tunnel puis ajouter un tunnel vide :



Nous allons créer un peer un serveur à distance ce qu'il faut savoir c'est que le logiciel wireguard va chercher de bloc un qui se nomme « [interface] » et l'autre « [Peer] » les crochet son très important

donc je vais donner les deux blocs et vous aurez juste à remplacer avec votre valeur cela sera plus simple.

[Interface]

PrivateKey = OP6dceP4+C5QwSFXg0uXcQ2PiLG9gJpgTW1Hte+4q2s=

Address = 10.7.0.2/24

DNS = 8.8.8.8

[Peer]

PublicKey = byF3zSV9rMrglgR3PFaOFAq6G8SpSit+9k7ePb9y8B8=

AllowedIPs = 10.7.0.2/24, 10.13.17.11/32, 172.17.13.1/32

Endpoint = 172.31.13.253:51820

Memo :

- PublicKey : il s'agit de la clé publique du serveur WireGuard Debian 11 (vous pouvez obtenir sa valeur via la commande "sudo wg")

- AllowedIPs : il s'agit des adresses IP / des sous-réseaux accessibles via ce réseau VPN WireGuard, ici il s'agit du sous-réseau propre à mon VPN WireGuard (10.7.0.2/24) et de mon LAN distant (172.17.13.1/32)

- Endpoint : il s'agit de l'adresse IP de l'hôte Debian 11 puisque c'est notre point de liaison WireGuard (il faudra préciser l'adresse IP publique)

Bon il ne reste plus qu'à déclarer le nouveau client wireguard et le nat sur les pf-externe et pf-interm et tout sera bon :

On va d'abord finir avec le client wireguard il reste plus que a déclarer le peer sur le serveur Debian il faut d'abord stopper l'interface wg 0 :

```
sudo wg-quick down /etc/wireguard/wg0.conf
```

Ensuite modifier le fichier précédemment créé :

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

dans le fichier a la suite du bloc « [interface] » on va rajouter cela :

```
[Peer]
```

```
PublicKey = PbkwKFpLaqXINQWeu7ycaWz0dRsA3OCyu4j5p6EGNTA=
```

```
AllowedIPs = 10.7.0.2/32
```

Ce bloc contient la clé publique de win 10 ainsi que l'adresse ip de son interface alloué à lui.

Il ne reste plus qu'à sauvegarder le fichier et a relancez l'interface « wg0 » :

```
wg-quick up /etc/wireguard/wg0.conf
```

Pour voir si tout est bon on va faire une Verif.

```
interface: wg0
  public key: byF3zSV9rMrglgR3PFaOFAq6G8SpSit+9k7ePb9y8B8=
  private key: (hidden)
  listening port: 51820




peer: PbkwKFpLaqXINQWeu7ycaWz0dRsA3OCyu4j5p6EGNTA=
  preshared key: (hidden)
  endpoint: 172.31.13.110:55532
  allowed ips: 10.7.0.2/32
```

Pour finir la config, on va sécuriser les fichiers de configuration pour limiter l'accès à "root" :




```
sudo chmod 600 /etc/wireguard/ -R
```

Bon il nous reste plus que les PF-sense et c'est bon :

Pour la PF-externe :

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	51820	10.13.21.1	51820	WIREGUARD	  

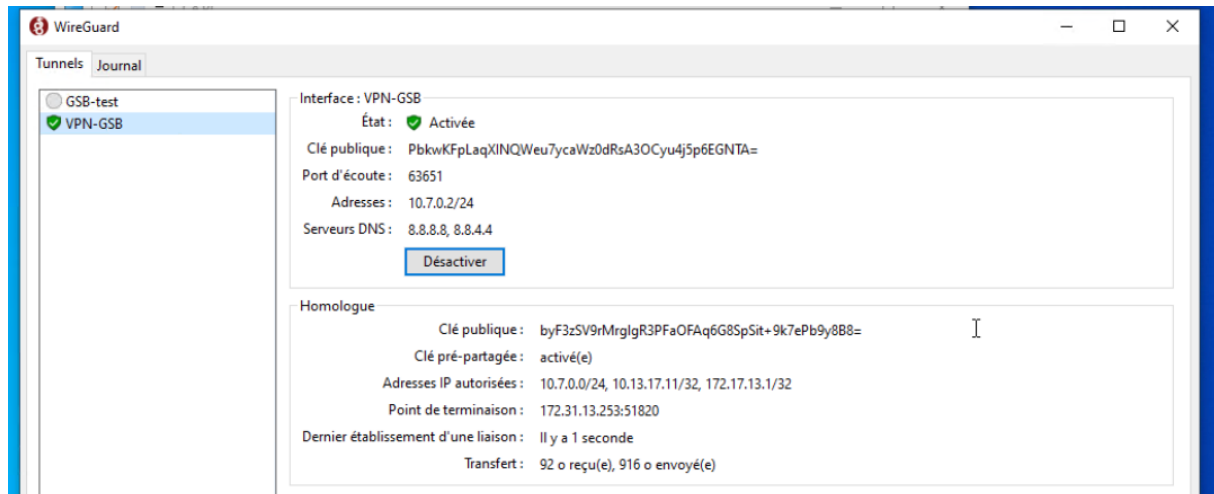
Pour la PF-interm :

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	51820	10.13.17.11	51820	WIREGUARD	  

Bon pour faire simple j'ai fait Deux NAT un de la wan pf-externe a la wan de la pf-interm et un deuxième du wan de interm vers le serveur wireguard.

## LES TEST :

On va l'activer et on peut voir que c'est bon :

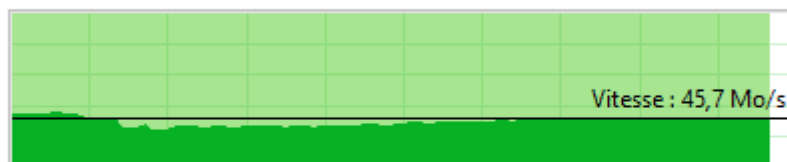


On va faire un test de déplacement pour voir le débit :

Copie d'un élément de Téléchargements vers Partage

94% terminé

II X



Nom : VMware-ESXi-7.0U3b-18905247-depot.zip

Temps restant : Environ 5 secondes

Éléments restants : 1 (20,5 Mo)

**WireGuard VPN**

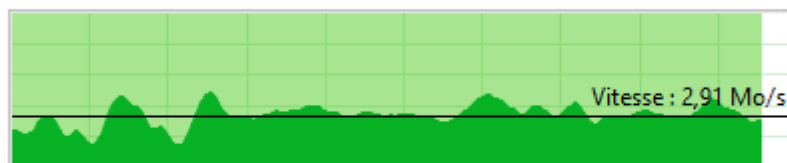
^ Moins de détails

Si on regarde le même test avec de l'openVPN :

Copie d'un élément de Téléchargements vers Partage

95% terminé

II X



Nom : VMware-ESXi-7.0U3b-18905247-depot.zip

Temps restant : Environ 10 secondes

Éléments restants : 1 (16,5 Mo)

**OpenVPN**

^ Moins de détails