



Procédure mise en place d'un VPN

Mise en place d'un serveur VPN avec Wireguard

Procédure mise en place d'un VPN.....	1
1- Prérequis.....	1
2- Installation des packages.....	1
3- Configuration d'un tunnel VPN	2
4- Configuration du « Peer »	3
5- Fichier de configuration côté client.....	5
6- Tests	6
7- Conclusion.....	7

1-Prérequis

J'ai utilisé mon PfSense pour mettre en place le VPN.

Il nous faut aussi un client externe à notre réseau.

2-Installation des packages

Nous allons commencer par installer le package Wireguard sur notre PfSense :

System => Package Manager :

The screenshot shows the PfSense Package Manager interface. A single package, 'WireGuard', is selected from the 'net' category. The version listed is '0.2.1'. The description text provides a brief overview of the WireGuard VPN protocol, highlighting its speed, security, and cross-platform compatibility.

✓ WireGuard net 0.2.1

WireGuard(R) is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPSec, while avoiding the massive headache. It intends to be considerably more performant than OpenVPN. WireGuard is designed as a general purpose VPN for running on embedded interfaces and super computers alike, fit for many different circumstances. Initially released for the Linux kernel, it is now cross-platform and widely deployable. It is currently under heavy development, but already it might be regarded as the most secure, easiest to use, and simplest VPN solution in the industry.

Il nous suffit maintenant d'activer Wireguard :

VPN > Wireguard > Settings > Enable Wireguard



Notre Package Wireguard est désormais activé.

Nous allons maintenant passer à la configuration.

3-Configuration d'un tunnel VPN

Nous allons commencer par créer un nouveau tunnel que l'on utilisera pour les échanges à travers le VPN.

Activons le tunnel pour commencer

Nous allons lui donner un nom parlant



Laisser le port par défaut qui est le 51820

Et affecter une adresse IP qui sera utilisée pour le VPN (il faut une adresse IP, et non une adresse réseau)

Ensuite, nous allons devoir générer une paire de clé depuis notre PfSense, en cliquant sur « **Generate** ». Il faut copier cette clé publique, et la garder de côté.

4-Configuration du « Peer »

Nous allons maintenant devoir configurer notre pair (Peer), afin de pouvoir utiliser le VPN sur un client.

Peer Configuration	
Enable	<input checked="" type="checkbox"/> Enable Peer <small>Note: Uncheck this option to disable this peer without removing it from the list.</small>
Tunnel	tun_wg1 (Tunnel_VPN) <small>WireGuard tunnel for this peer. (Create a New Tunnel)</small>
Description	WIN_CLT <small>Peer description for administrative reference (not parsed).</small>
Dynamic Endpoint	<input checked="" type="checkbox"/> Dynamic <small>Note: Uncheck this option to assign an endpoint address and port for this peer.</small>
Keep Alive	25 <small>Interval (in seconds) for Keep Alive packets sent to this peer. Default is empty (disabled).</small>

Commençons par activer le pair.

Nous devons ensuite lui affecter un tunnel (ici le tunnel créé à l'étape précédente)

Laissons activer le Dynamic Endpoint, au cas où nous utilisons du DHCP sur notre Client.

Entrer la valeur « 25 » dans le champ Keep Alive.



Address Configuration

Hint Allowed IP entries here will be transformed into proper subnet start boundaries prior to validating and saving. These entries are used for multiple peers on the same tunnel. Otherwise, traffic to the conflicting networks will only be routed to the last peer in the list.

Allowed IPs 10.12.12.0 / 24 Description
IPv4 or IPv6 subnet or host reachable via this peer. Description for administrative reference (not parsed).

Add Allowed IP **+ Add Allowed IP**

Nous devons enfin lui affecter une adresse IP dans le même réseau que celle assignée au tunnel

Public Key Xxc1fA50s5alN/aweb55S1WzqHAxe07bxD+QgzoUtxc=

WireGuard public key for this peer.

Nous devons ensuite insérer la clé publique du poste client que nous allons utiliser .

Il nous faut nous munir de notre client, installer Wireguard depuis ce lien :

<https://www.wireguard.com/install/>

Ensuite il nous faut créer un tunnel vide afin que Wireguard nous affecte une clé publique

Nous devons ensuite lui affecter un tunnel (ici le tunnel créé à l'étape précédente)

Puis copier notre clé publique :

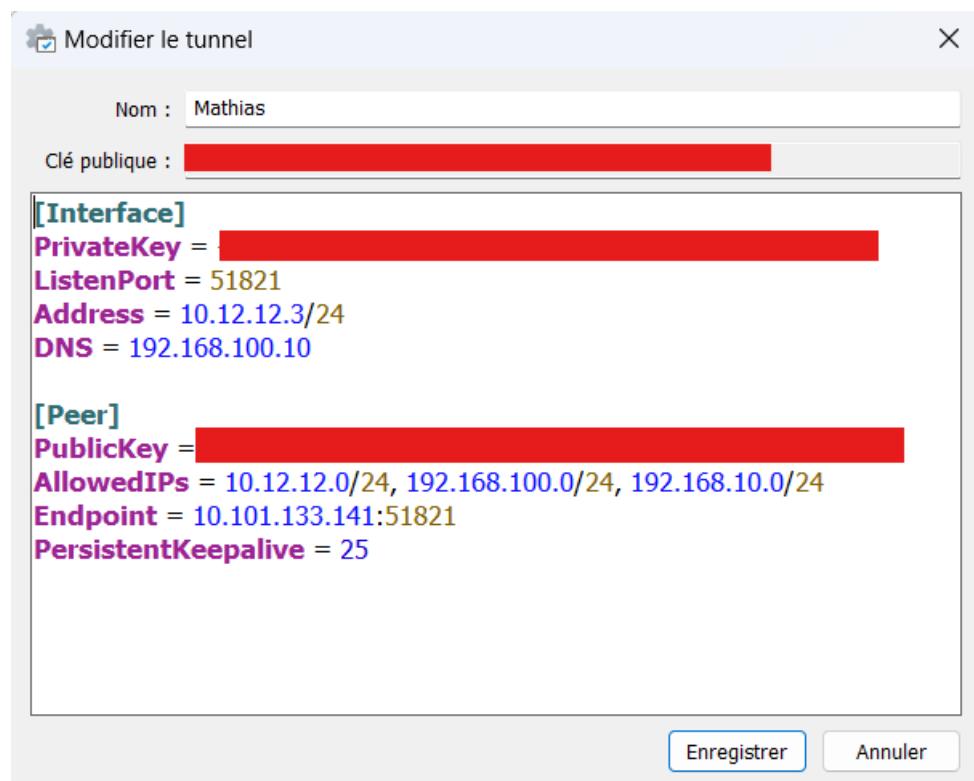
Clé publique : 0+j+UVKZ1WWbaZrCuTishsupF02EYiAV/CNTBj0BsSE=

Et l'insérer dans la configuration du pair dans PfSense.



5-Fichier de configuration côté client

Nous allons maintenant devoir modifier le fichier de conf du côté client.
Il doit ressembler à ceci :



Une autre solution est d'exporter la configuration du tunnel directement depuis PfSense, l'importer sur le poste client, puis d'y rajouter les informations manquantes (clé publique PfSense par exemple)

tun_wg1	Tunnel_VPN	kpdXzgjOvxcVBWRdiA6wQqmVcLPmqRxN...	10.12.12.1/24	51821	2			
---------	------------	-------------------------------------	---------------	-------	---	--	--	--



6-Tests

Nous allons maintenant nous connecter au VPN, puis teste si nous avons bien accès :

Interface : Mathias

État : Éteinte

Clé publique : KUZYE500CMUA89NOF+eobwhLuPrWQpXnuBOnvCkaO
hc=

Port d'écoute : 51821

Adresses : 10.12.12.3/24

Serveurs DNS : 192.168.100.10

Activer

Je récupère bien l'IP

Je ping bien mes serveurs

```
C:\Users\mathi>ping 192.168.100.10

Envoi d'une requête 'Ping' 192.168.100.10 avec 32 octets de données :
Réponse de 192.168.100.10 : octets=32 temps<1ms TTL=127
Réponse de 192.168.100.10 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.100.10 : octets=32 temps=1 ms TTL=127
```

Je résous bien mes nom DNS :

```
C:\Users\mathi>nslookup glpi.vetele.mv
Serveur :      SRV1.vetele.mv
Address: 192.168.100.10

Nom :      glpi.vetele.mv
Address: 192.168.100.50
```



J'arrive bien à me connecter en SSH à mes serveurs :

```
To delete this message, delete the /etc/p
.
Last login: Thu Apr 24 12:09:38 2025 from 10.12.12.3
root@CentreonDebian11:~# |
```

7-Conclusion

Nous avons mis en place une solution VPN afin de sécuriser un trafic entre un client physique, externe à mon réseau, et mon infrastructure réseau virtuelle.