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

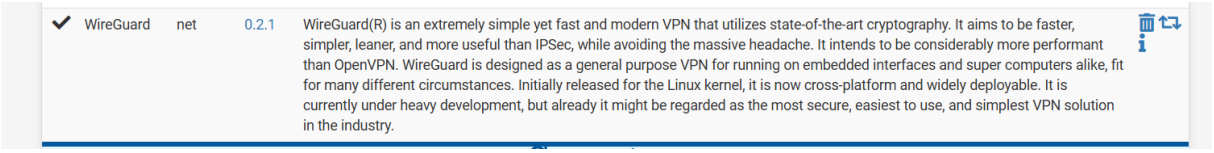
1-Prérequis

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

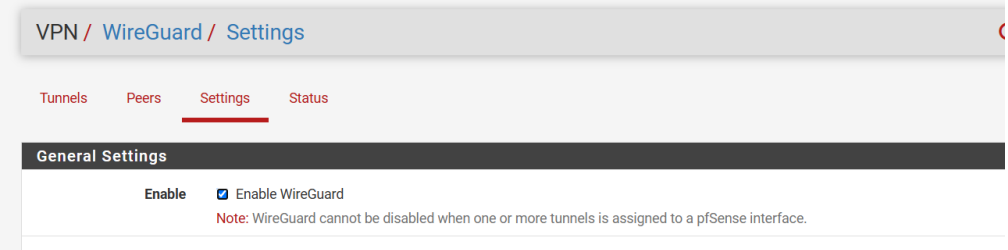
Nous allons commencer par installer le package Wireguard sur notre PfSense :

System => Package Manager :



Il nous suffit maintenant d'activer Wireguard :

VPN > Wireguard > Settings > Enable Wireguard

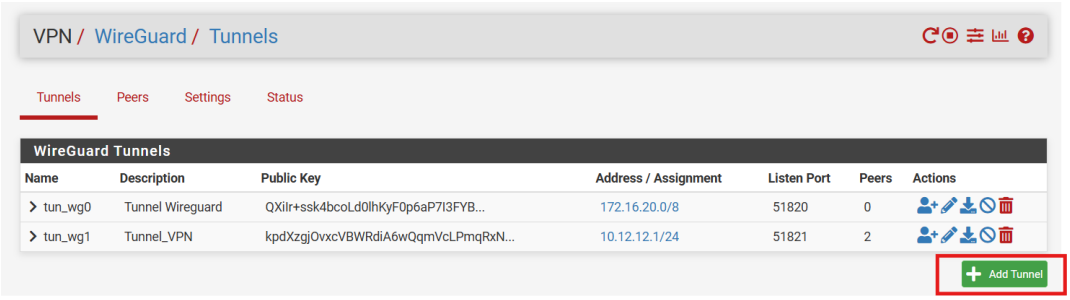


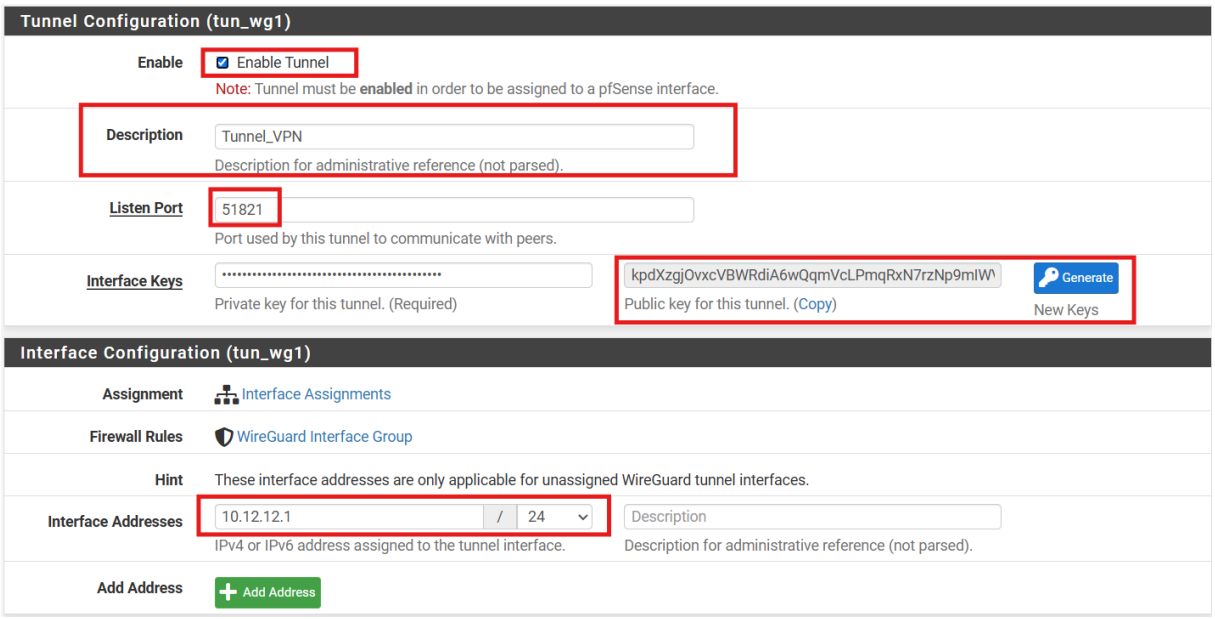
Notre Package Wireguard est désormais activé.

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

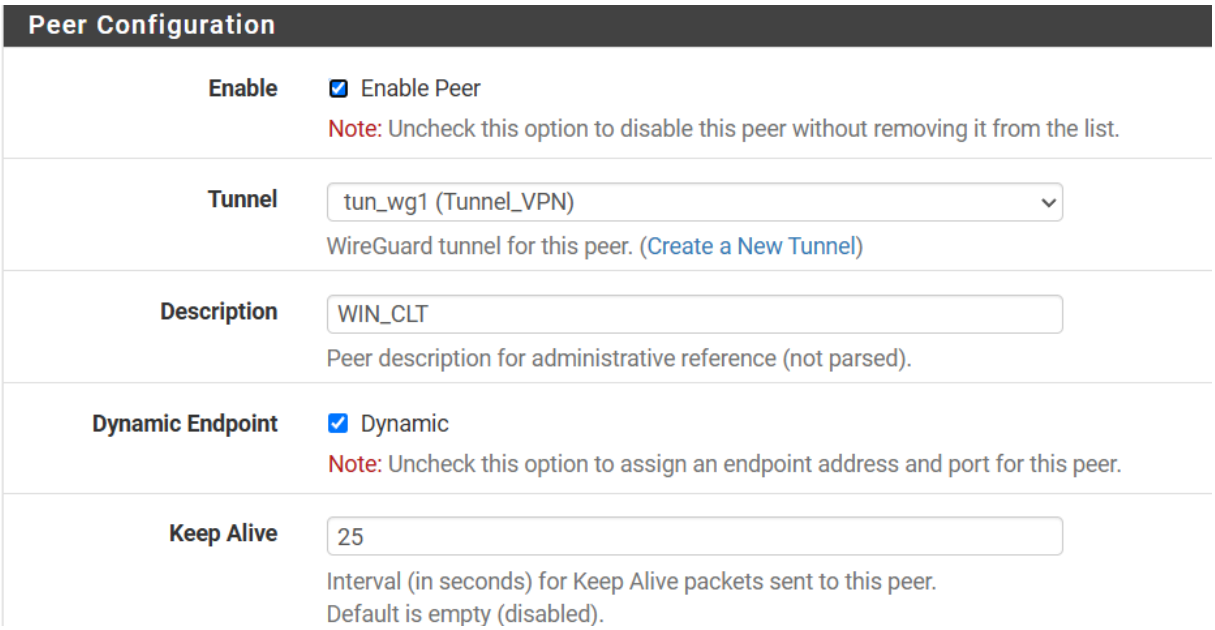
Laisser le port par défaut qui est le 51820

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 cliquand 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.

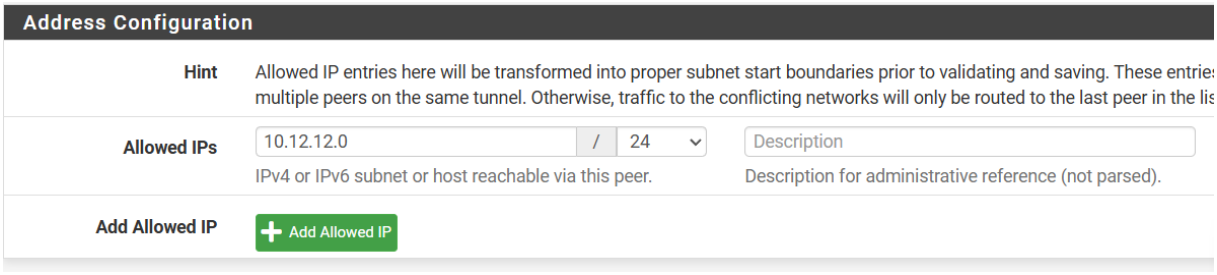


Commençons par activer le pair.

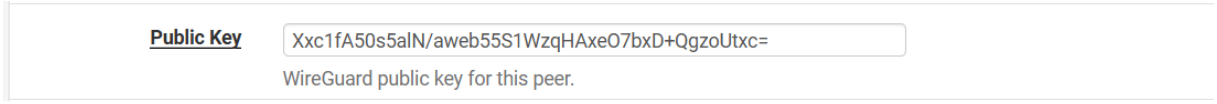
Nous devons ensuite lui affecter un tunnel (ici le tunnel crée à l'étape précédente)

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

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



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

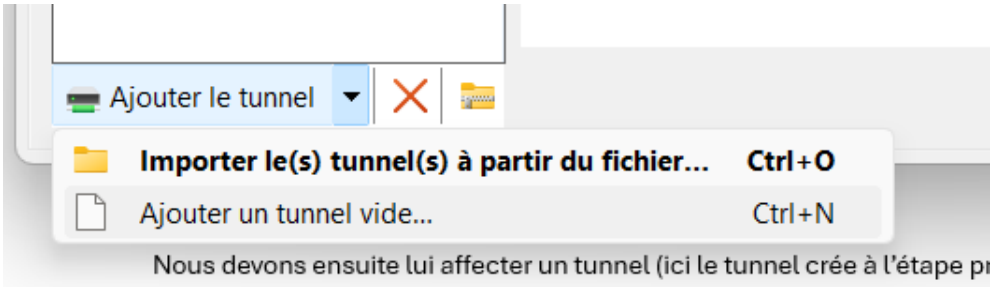


Nous devons ensuite insérer la clé publique du poste client que nous allons utiliser .

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

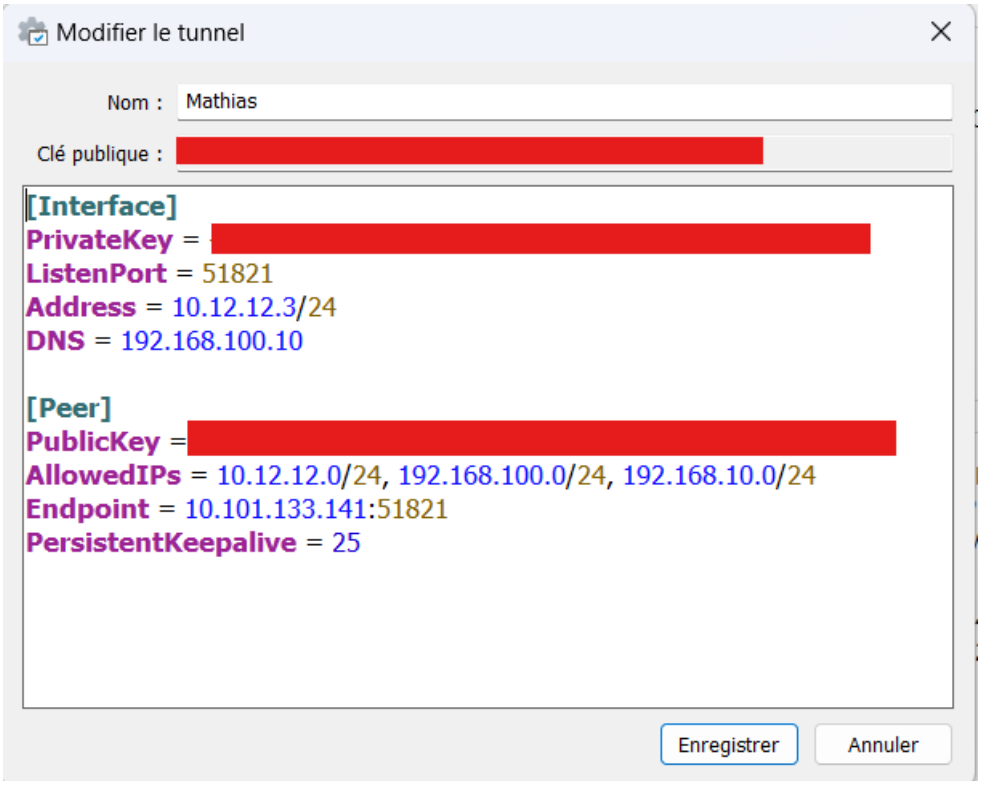


Puis copier notre clé publique :

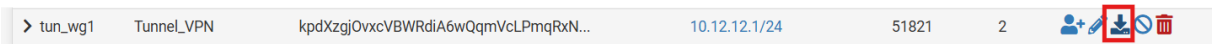
Et l'insérer dans la configuration du pair dans PfSense.

5-Fichier de configuration côté client

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

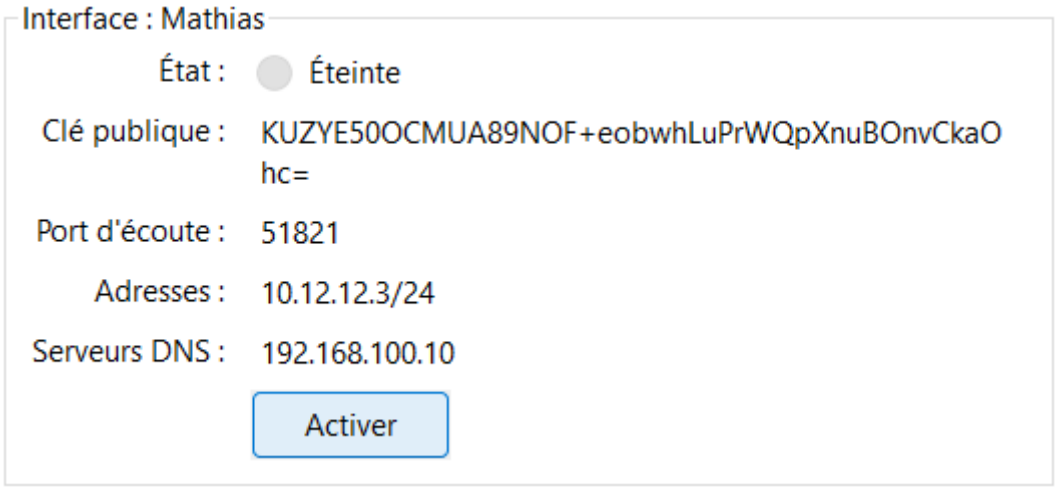


Une autre solution est d'exporter la configuration du tunnel directement depuis PfSense, l'importer sur le poste client, puise d'y rajouter les informations manquantes (clé publique PfSense par exemple)



6-Tests

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



Je récupère bien l'IP

```
Carte inconnue Mathias :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv4. . . . . . . . . . . . . .: 10.12.12.3
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :
```

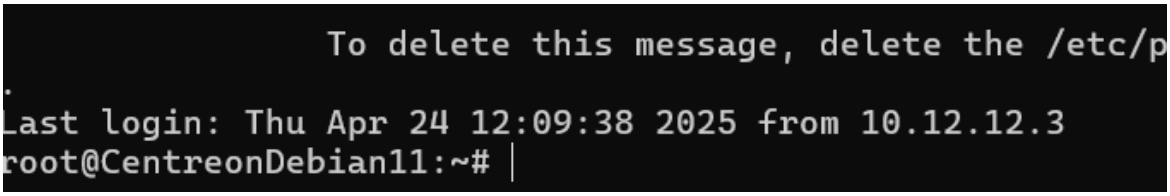
Je ping bien mes serveurs

```
:\Users\mathi>ping 192.168.100.10

nvoi d'une requête 'Ping'  192.168.100.10 avec 32 octets de données :
éponse de 192.168.100.10 : octets=32 temps<1ms TTL=127
éponse de 192.168.100.10 : octets=32 temps=1 ms TTL=127
éponse 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 :



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.