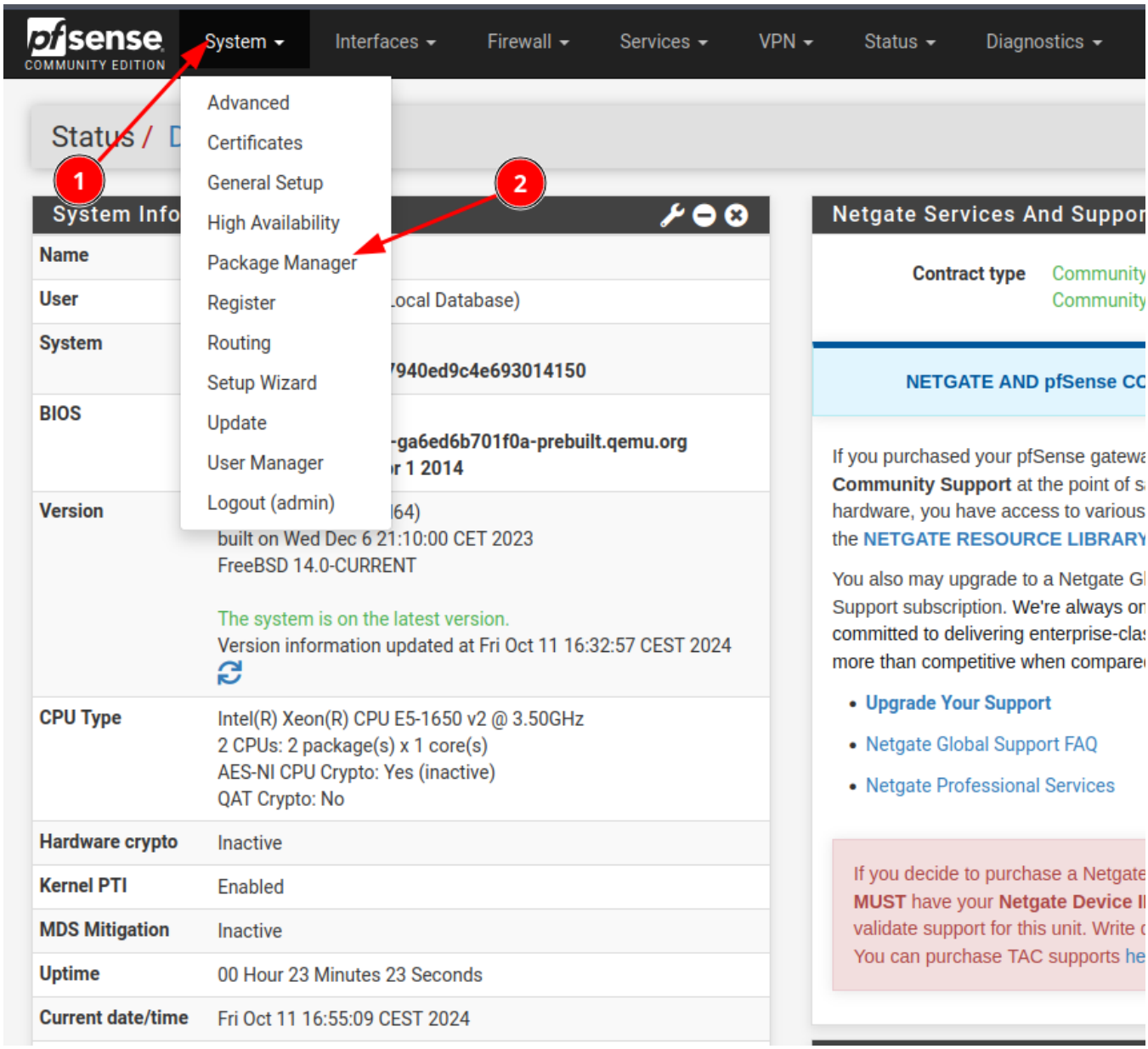
Mise en place de WIREGUARD

Prérequis:

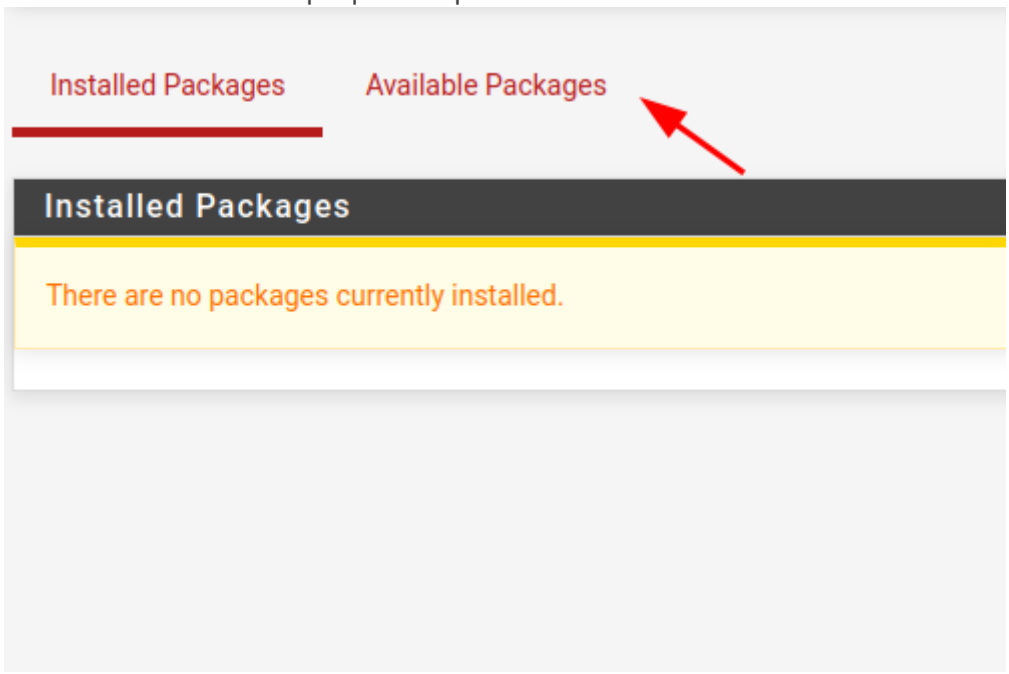
- Avoir une connexion internet (ping 8.8.8.8 et résolution de goolge.fr)
- Avoir installé pfsense

Installation du paquet Wireguard:

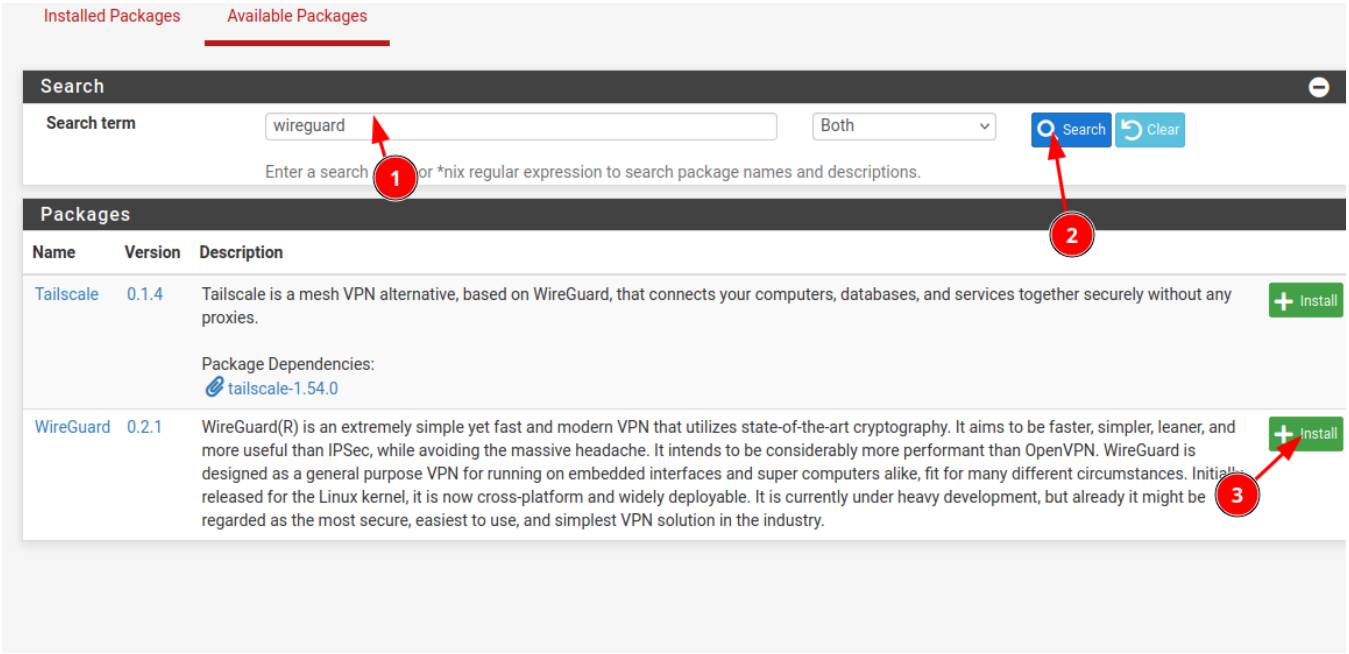
1. Se rendre dans la partie Package Manager



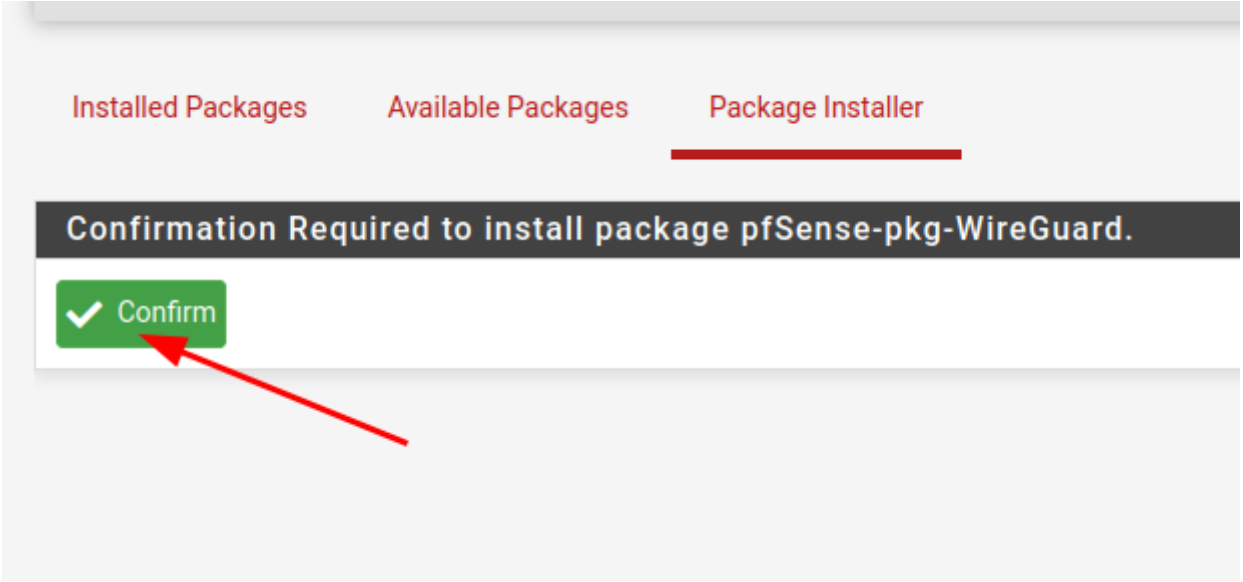
2. Aller dans la section paquet disponible



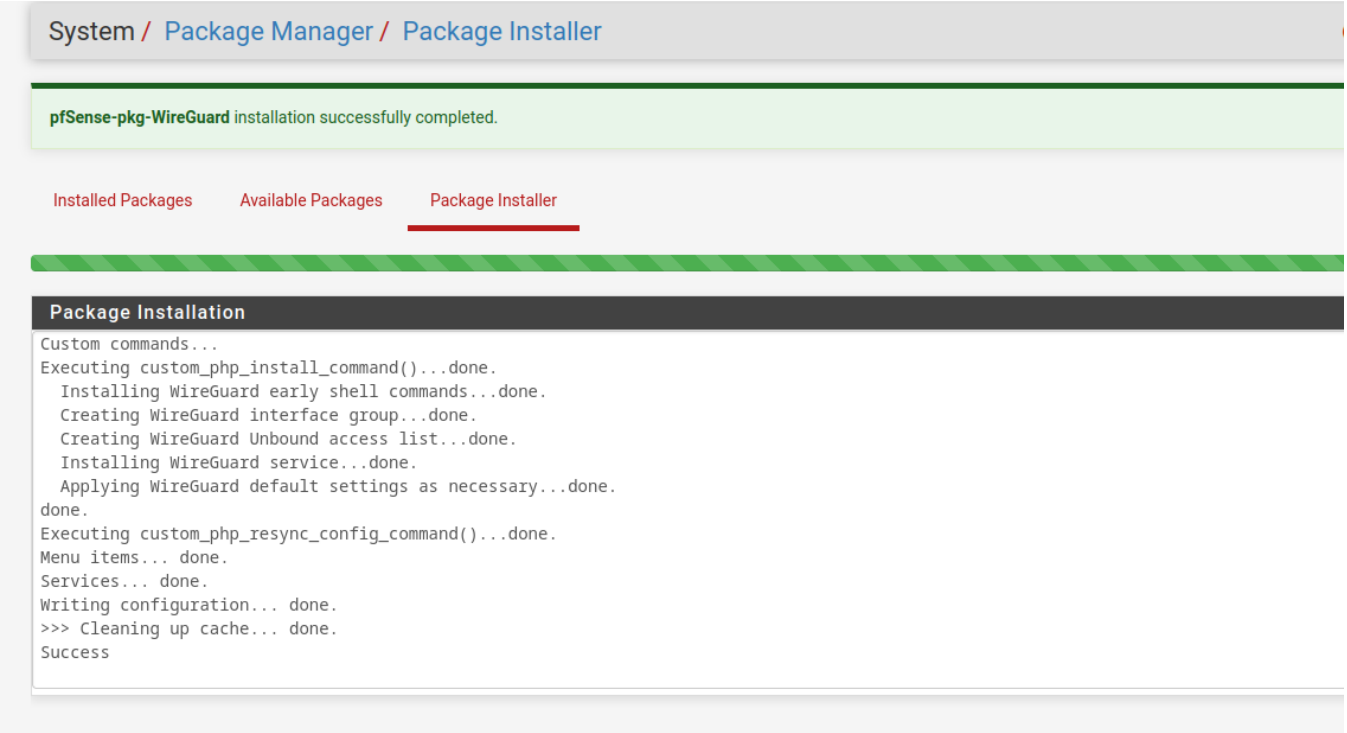
3. Chercher et installer WIREGUARD


Installed Packages
Available Packages
Search
Search term
wireguard
Both
Search
Clear
Enter a search string or *nix regular expression to search package names and descriptions.
1
2
Packages
Name
Version
Description
Tailscale
0.1.4
Tailscale is a mesh VPN alternative, based on WireGuard, that connects your computers, databases, and services together securely without any proxies.
Package Dependencies:
tailscale-1.54.0
Install
WireGuard
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.
Install
3

4. Confirmer

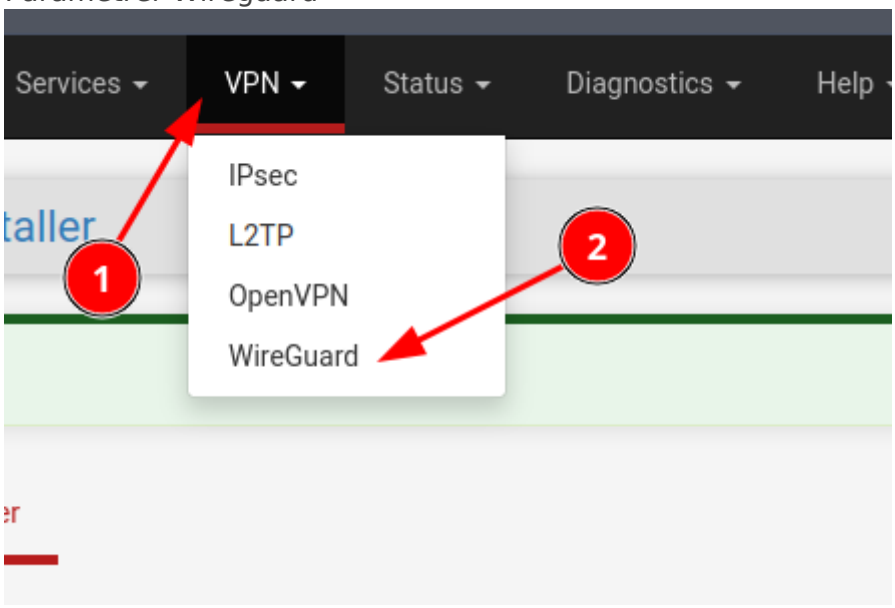

Installed Packages
Available Packages
Package Installer
Confirmation Required to install package pfSense-pkg-WireGuard.
Confirm

5. Attendre l'installation

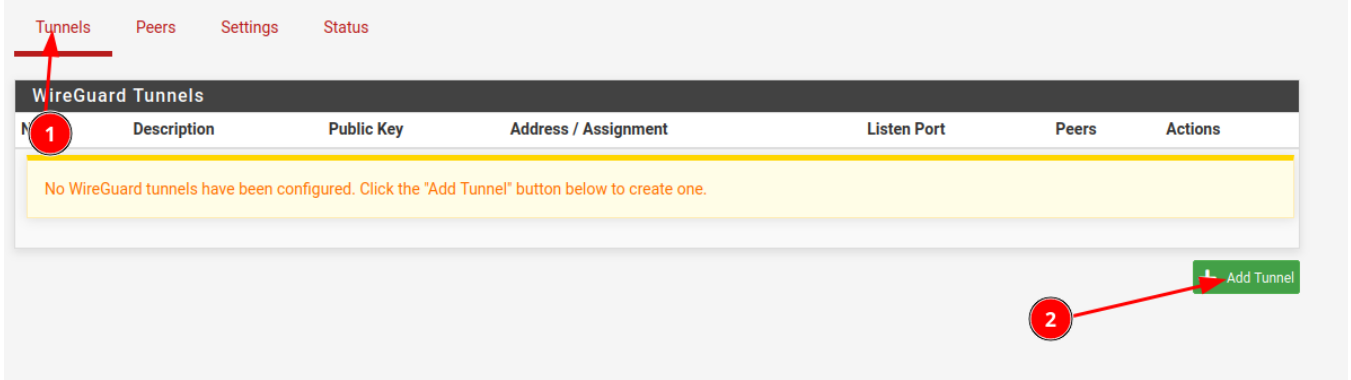


Paramétrage de Wireguard:

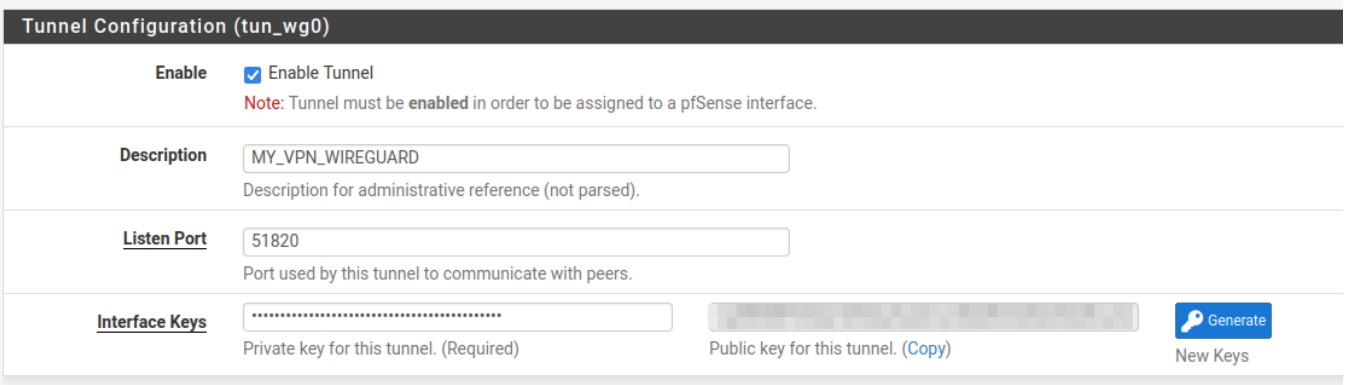
1. Paramétrer Wireguard



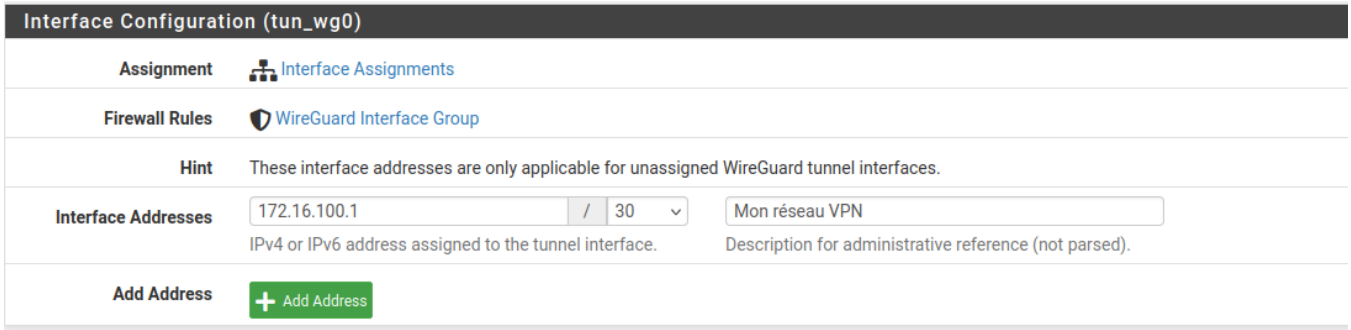
2. Ajouter un tunnel



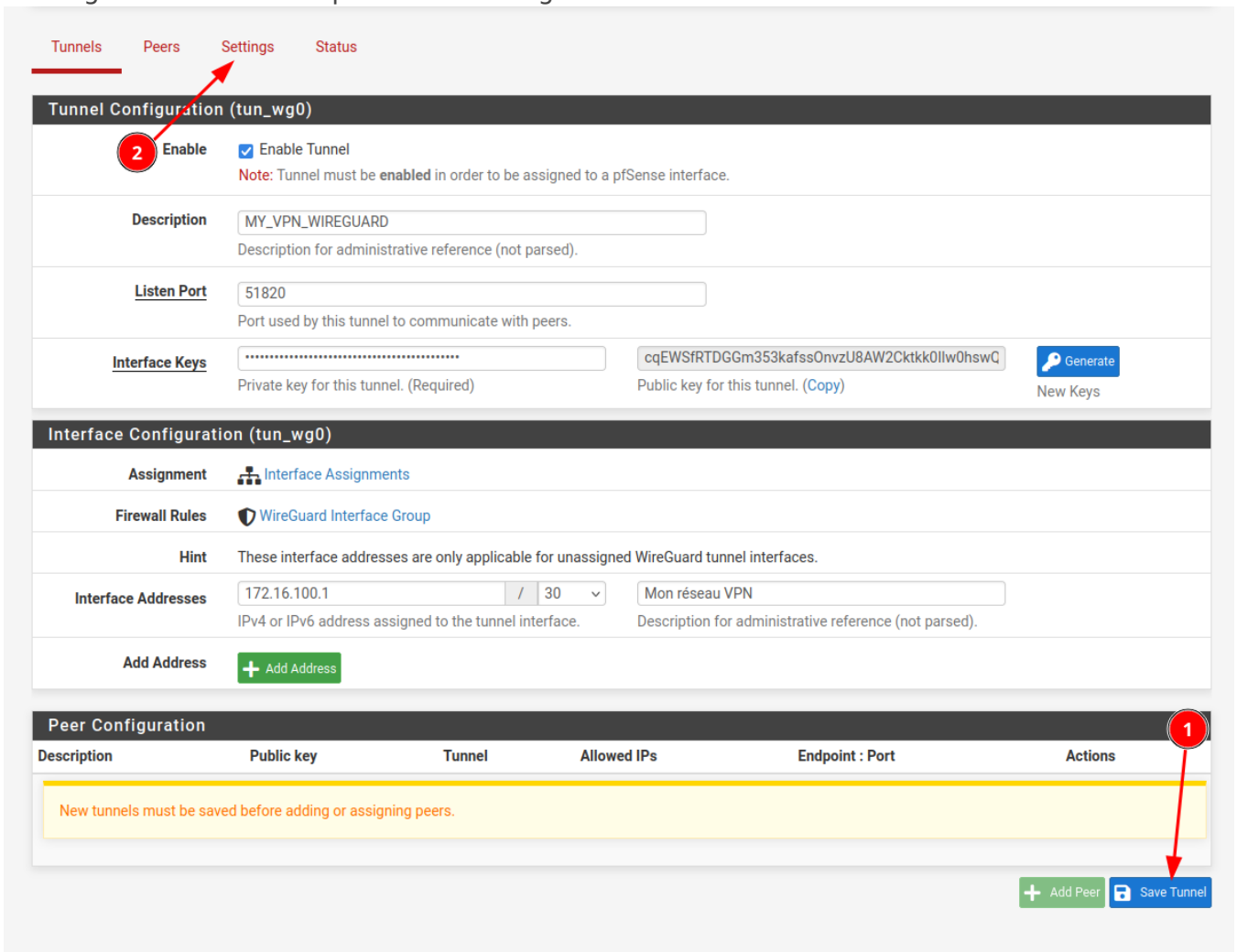
3. Mettre une description, le port que l'on souhaite utiliser et générer un paire de clé. Attention il faut garder la clé publique.



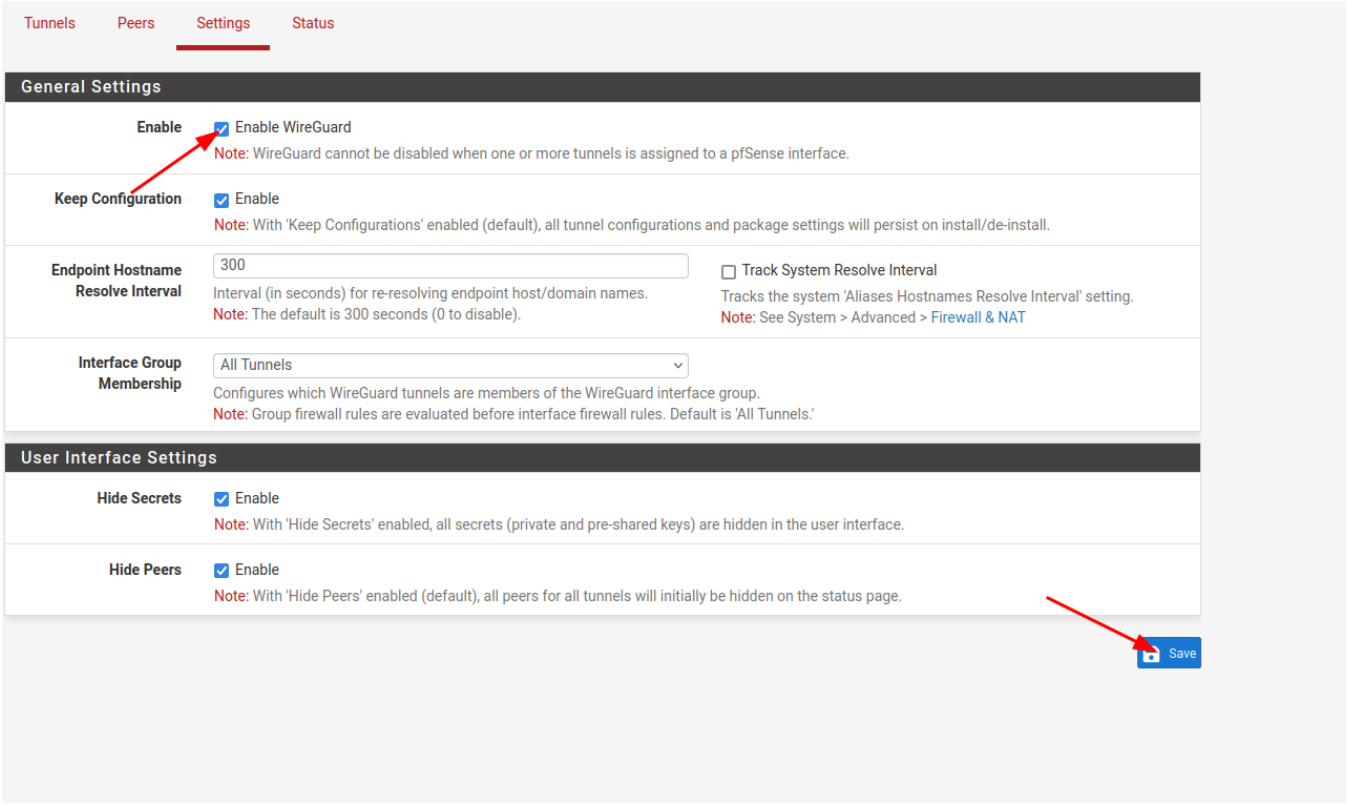
4. Paramétrer la partie réseau mettre un réseau qui n'est pas dans l'infrastructure actuelle



5. Sauvegarder le tunnel et passer au settings



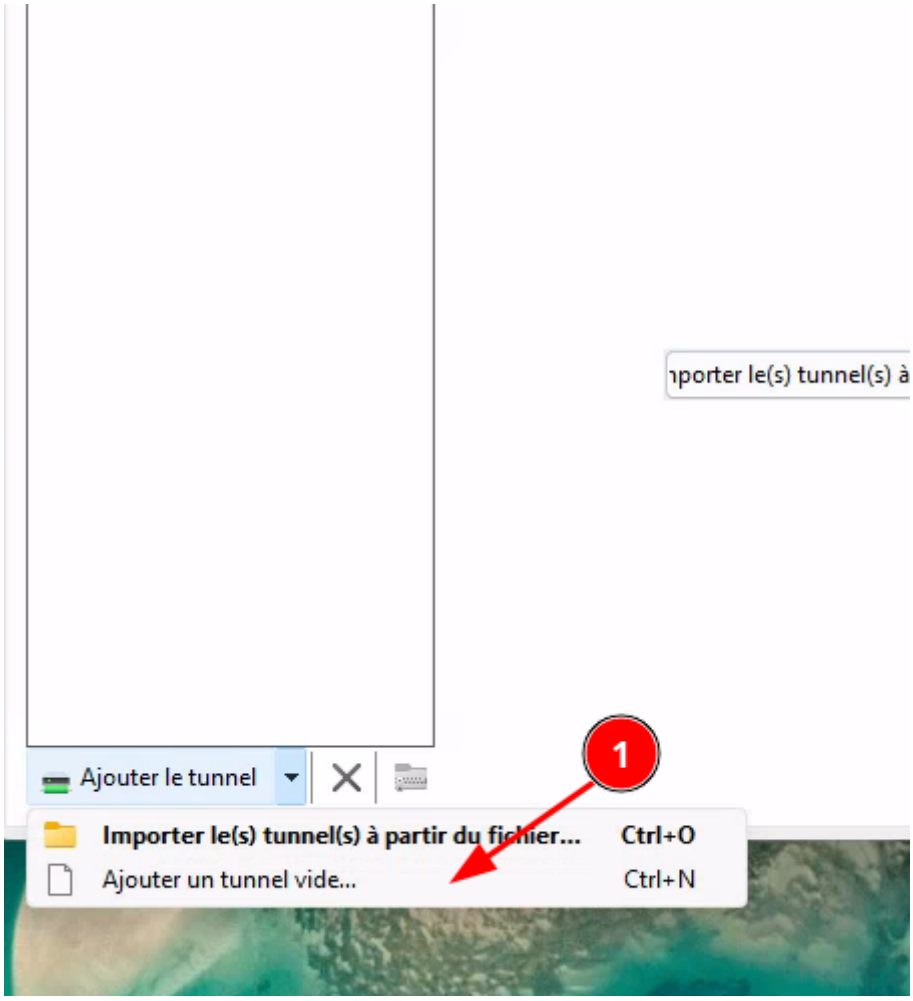
6. Activer Wireguard



7. Installation du paquet pour la génération de la paire de clé (Sur un Linux)

```
apt install wireguard
umask 077
wg genkey > privatekey
wg pubkey < privatekey > publickey
```

8. Démarrage du client WIREGUARD (Windows) et ajouter un nouveau tunnel
9. Ajouter un tunnel vide



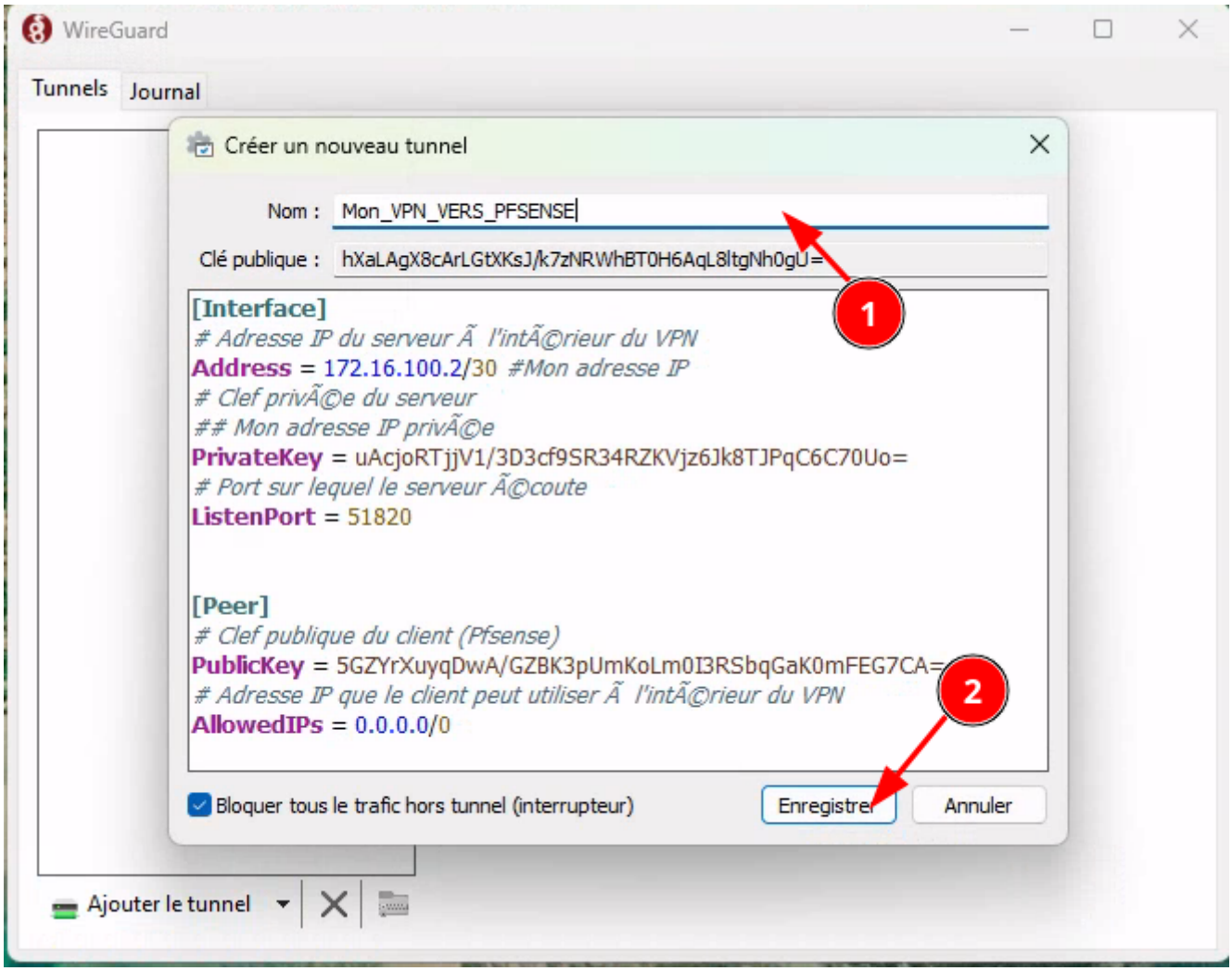
10. Ajouter la configuration

```
[Interface]
# Adresse IP du serveur à l'intérieur du VPN
Address = 172.16.100.2/30 #Mon adresse IP
# Clef privée du serveur
PrivateKey = uAcjoRTjjV1/3D3cf9SR34RZKVjz6Jk8TJPqC6C70Uo=
# Port sur lequel le serveur écoute
ListenPort = 51820
# DNS
DNS = 172.16.1.62, 1.1.1.1

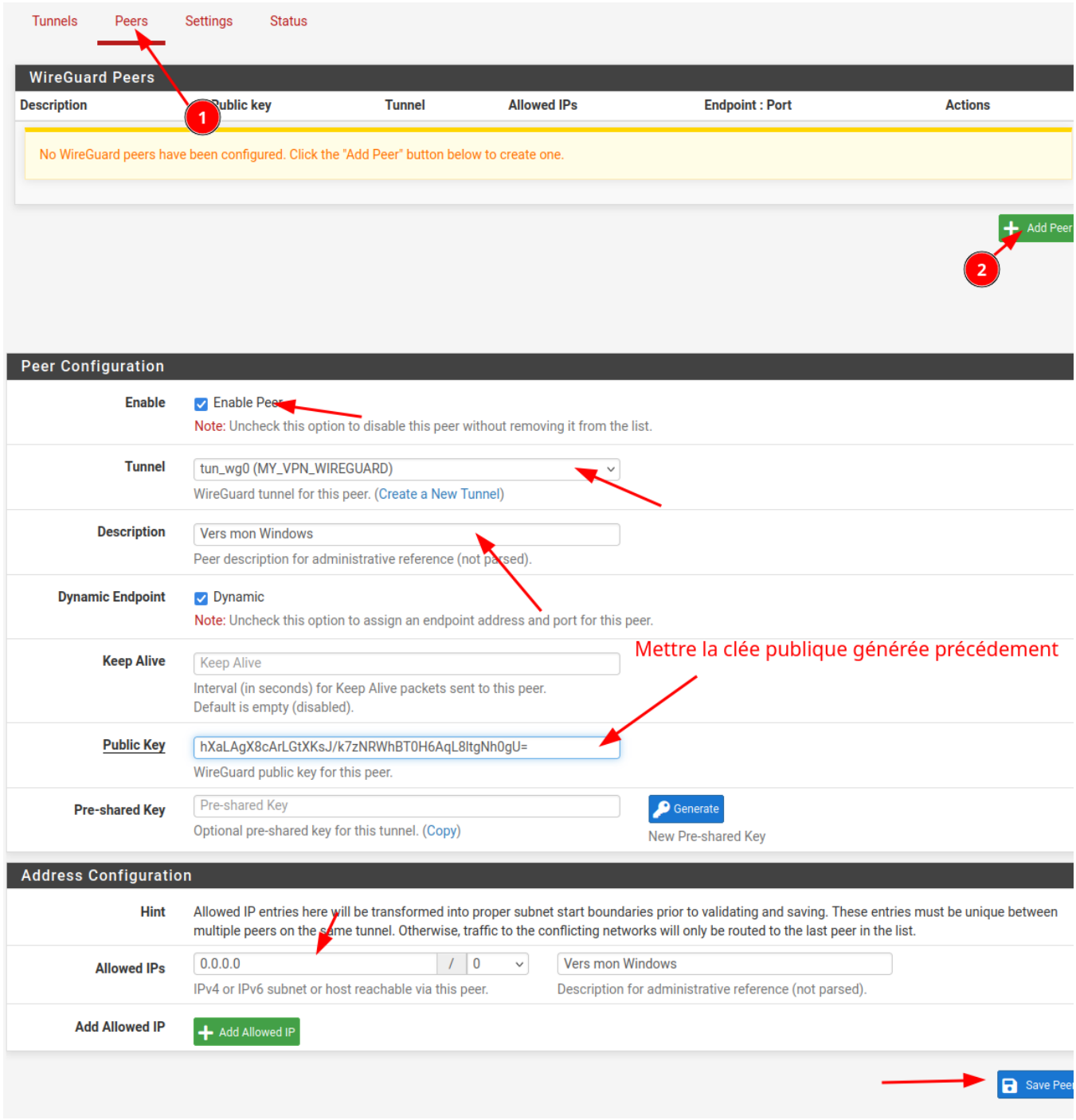


[Peer]
# Clef publique du client (Pfsense)
PublicKey = 5GZYrXuyqDwA/GZBK3pUmKoLm0I3RSbqGaK0mFEG7CA=
# Adresse IP que le client peut utiliser à l'intérieur du VPN
AllowedIPs = 0.0.0.0/0
#Ip du serveur distant
Endpoint = 192.168.1.112:51820
```

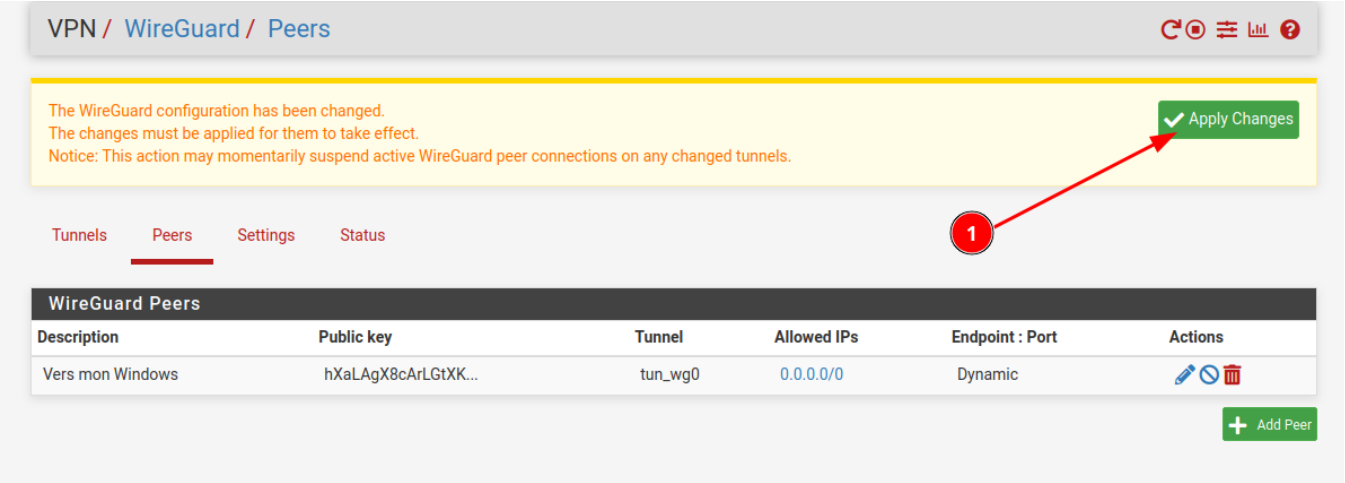
```
PersistentKeepalive = 15
```



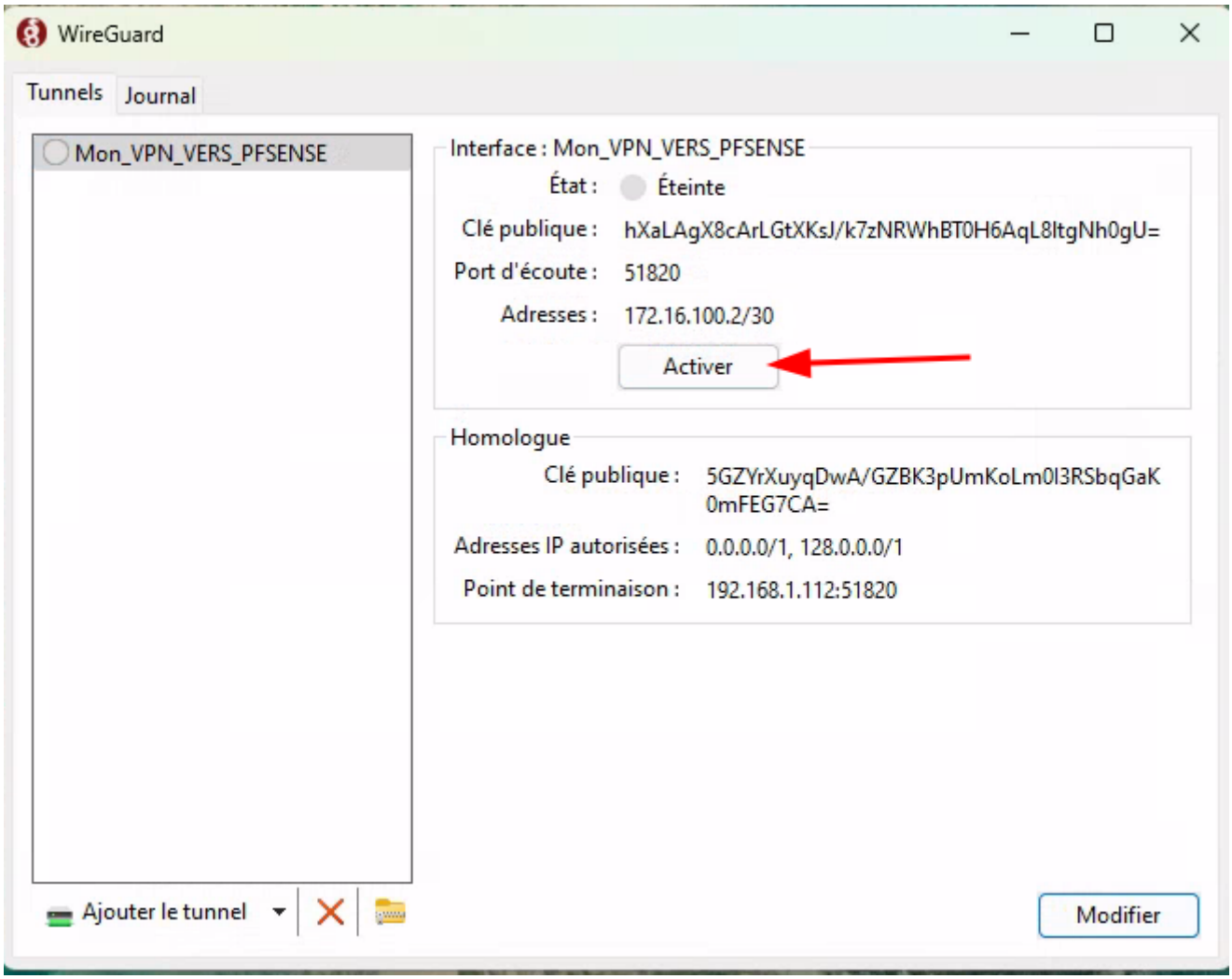
11. Passer à la partie Pfsense (ajouter un pair)



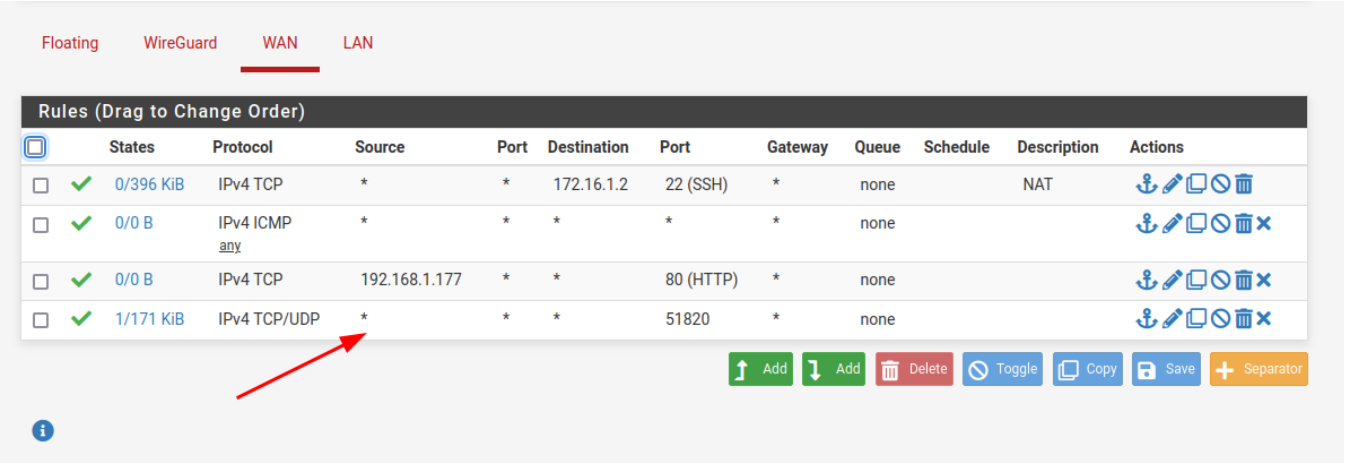
12. Appliquer les changements



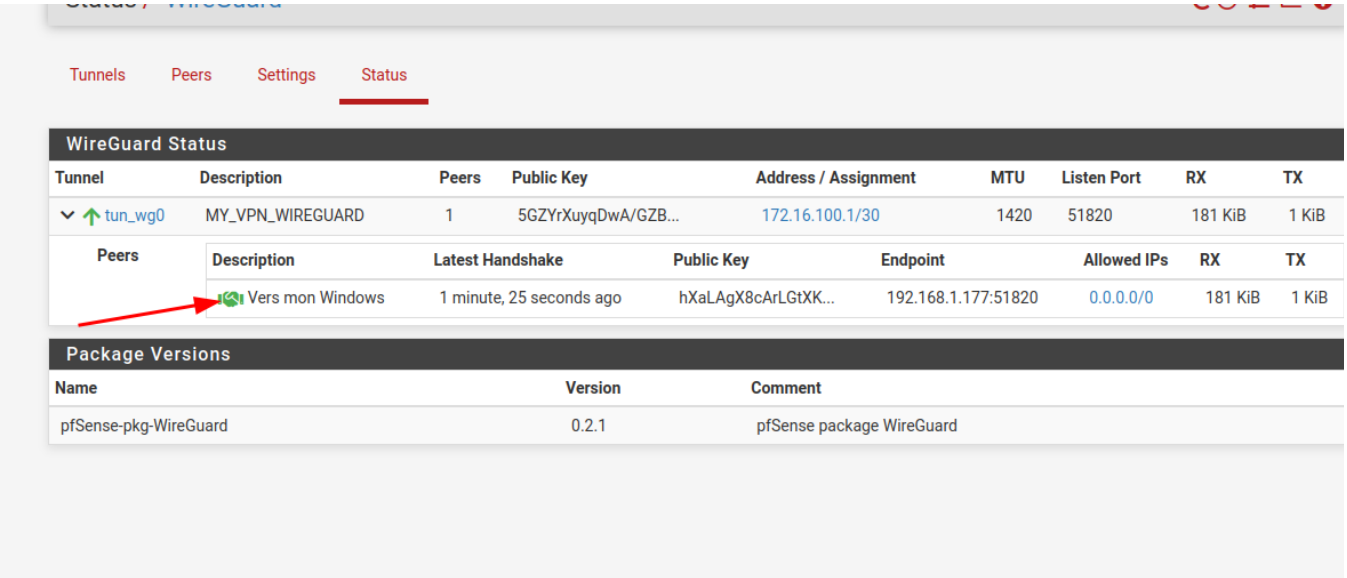
13. Activer le VPN (Windows)

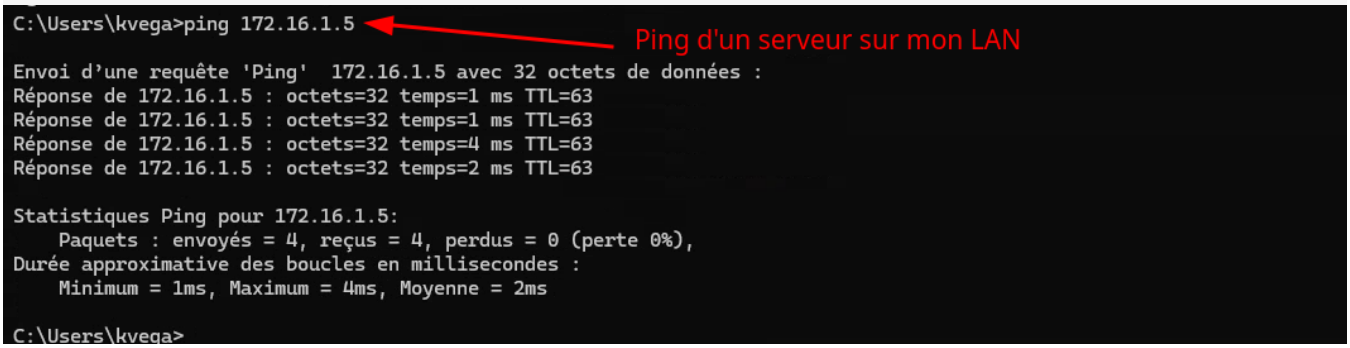


14. Mettre en place un Régle de pare feu sur l'interface WAN

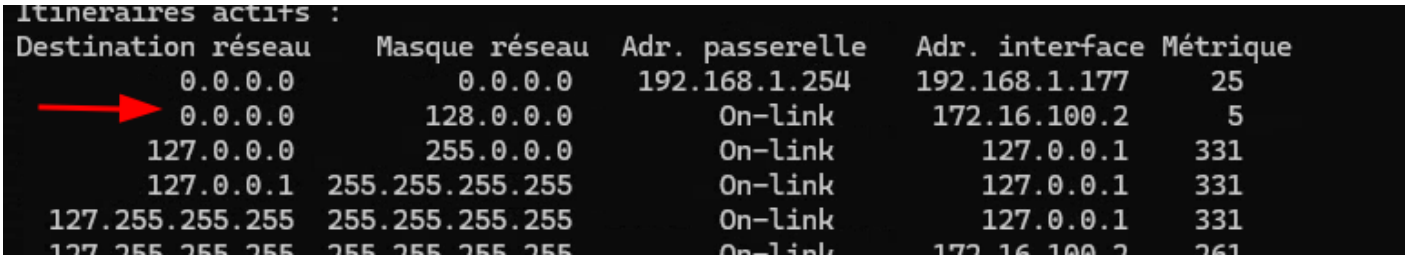


15. Vérifier que le VPN est bien connecté





16. Nous aurions pu aussi dans le configuration du client WIREGUARD spécifier les réseau auxquels Ont peut se connecter car en l'état actuel les routes ajoutées sont :



> Exemple de configuration que l'on pouvait mettre en place

```
[Interface]
# Adresse IP du serveur à l'intérieur du VPN
Address = 172.16.100.2/30 #Mon adresse IP
# Clef privée du serveur
## Mon adresse IP privée
PrivateKey = uAcjoRTjjV1/3D3cf9SR34RZKVjz6Jk8TJPqC6C70Uo=
# Port sur lequel le serveur écoute
ListenPort = 51820



[Peer]
# Clef publique du client (Pfsense)
PublicKey = 5GZYrXuyqDwA/GZBK3pUmKoLm0I3RSbqGaK0mFEG7CA=
# Adresse IP que le client peut utiliser à l'intérieur du VPN
AllowedIPs = 172.16.1.0/26
#Ip du serveur distant
Endpoint = 192.168.1.112:51820
```

Revision #10
Created 2024-10-14 11:44:45 UTC by kvega
Updated 2024-10-14 19:38:04 UTC by kvega