

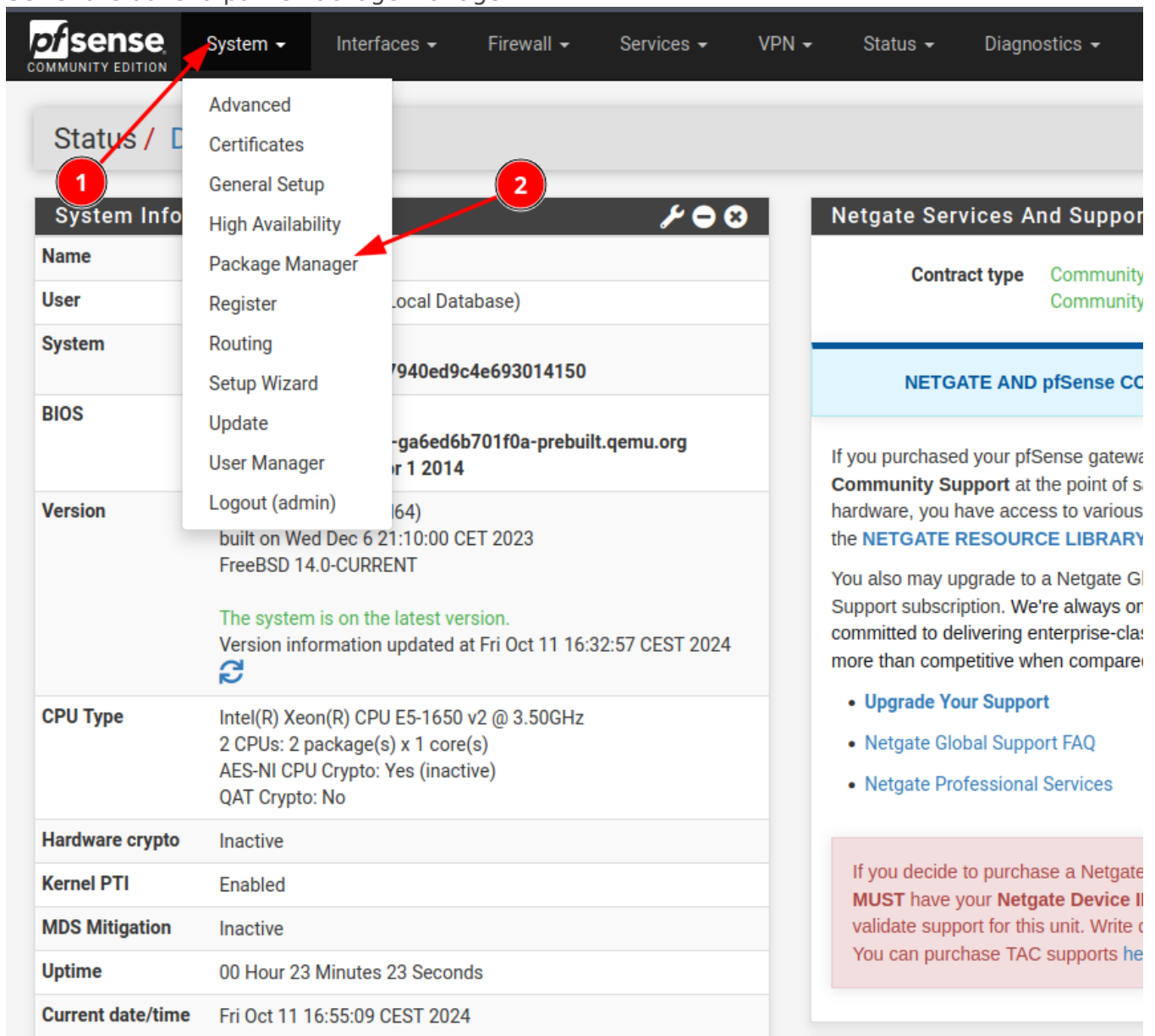
Mise en place de WIREGUARD

Prérequis:

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

Installation du paquet Wireguard:

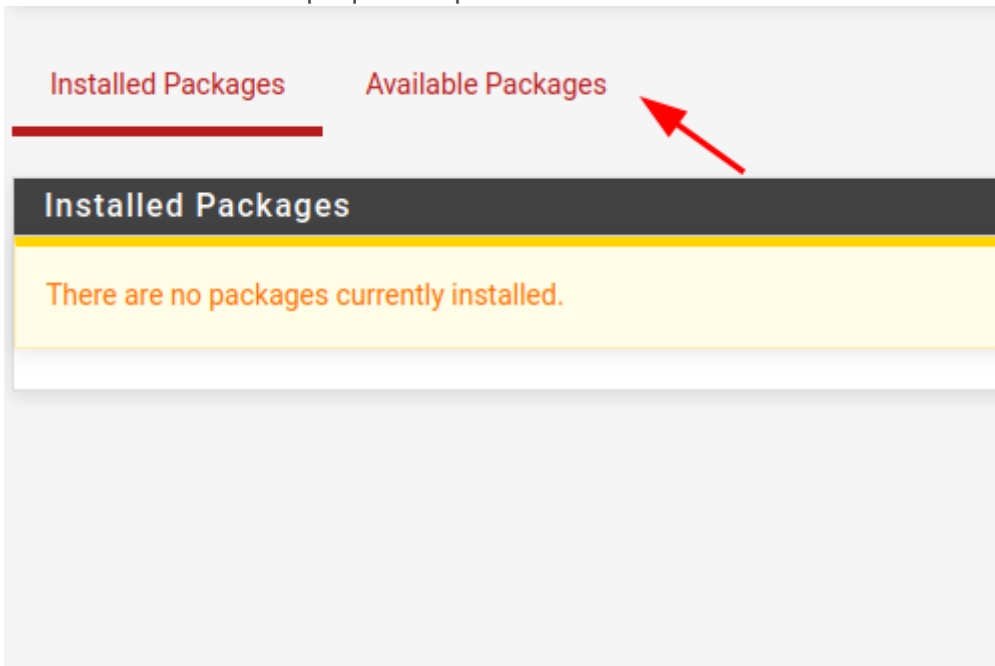
1. Se rendre dans la partie Package Manager



The screenshot shows the pfSense web interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', and 'Diagnostics'. The 'System' menu is open, showing options like 'Advanced', 'Certificates', 'General Setup', 'High Availability', 'Package Manager', 'Register', 'Routing', 'Setup Wizard', 'Update', 'User Manager', and 'Logout (admin)'. A red circle with the number '1' is placed over the 'System' menu, and another red circle with the number '2' is placed over the 'Package Manager' option. The main content area shows system information, including CPU type, hardware crypto, kernel PTI, MDS Mitigation, uptime, and current date/time. A sidebar on the right contains 'Netgate Services And Support' information.

System Info	Value
Name	
User	
System	
BIOS	
Version	built on Wed Dec 6 21:10:00 CET 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Fri Oct 11 16:32:57 CEST 2024
CPU Type	Intel(R) Xeon(R) CPU E5-1650 v2 @ 3.50GHz 2 CPUs: 2 package(s) x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 23 Minutes 23 Seconds
Current date/time	Fri Oct 11 16:55:09 CEST 2024

2. Aller dans la section paquet disponible



3. Chercher et installer WIREGUARD

The screenshot shows the same web interface as above, but with the 'Available Packages' tab selected. A search bar is visible with the text 'wireguard' entered. A red circle with the number '1' is around the search bar. To the right of the search bar is a dropdown menu set to 'Both' and a blue 'Search' button with a magnifying glass icon. A red circle with the number '2' is around the 'Search' button. Below the search bar is a table of packages. The table has columns for 'Name', 'Version', and 'Description'. The first row is for 'Tailscale' (version 0.1.4) and the second row is for 'WireGuard' (version 0.2.1). A red circle with the number '3' is around the 'Install' button for the 'WireGuard' package. The 'Install' button is a green square with a white plus sign and the text 'Install'.

Installed Packages Available Packages

Search

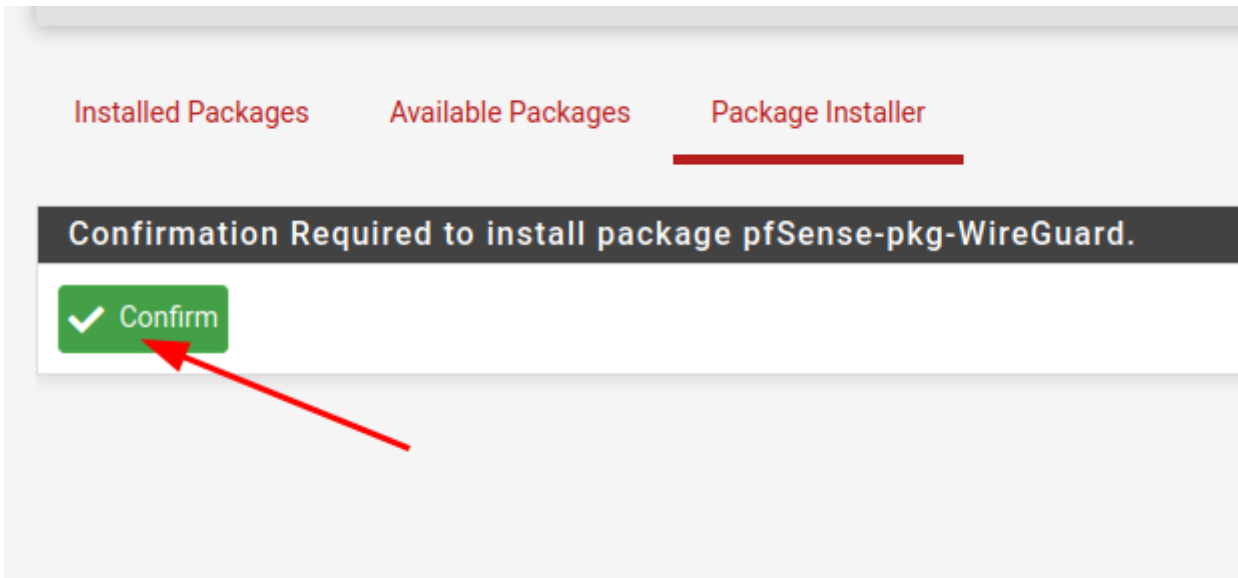
Search term wireguard Both Search Clear

Enter a search **1** or *nix regular expression to search package names and descriptions.

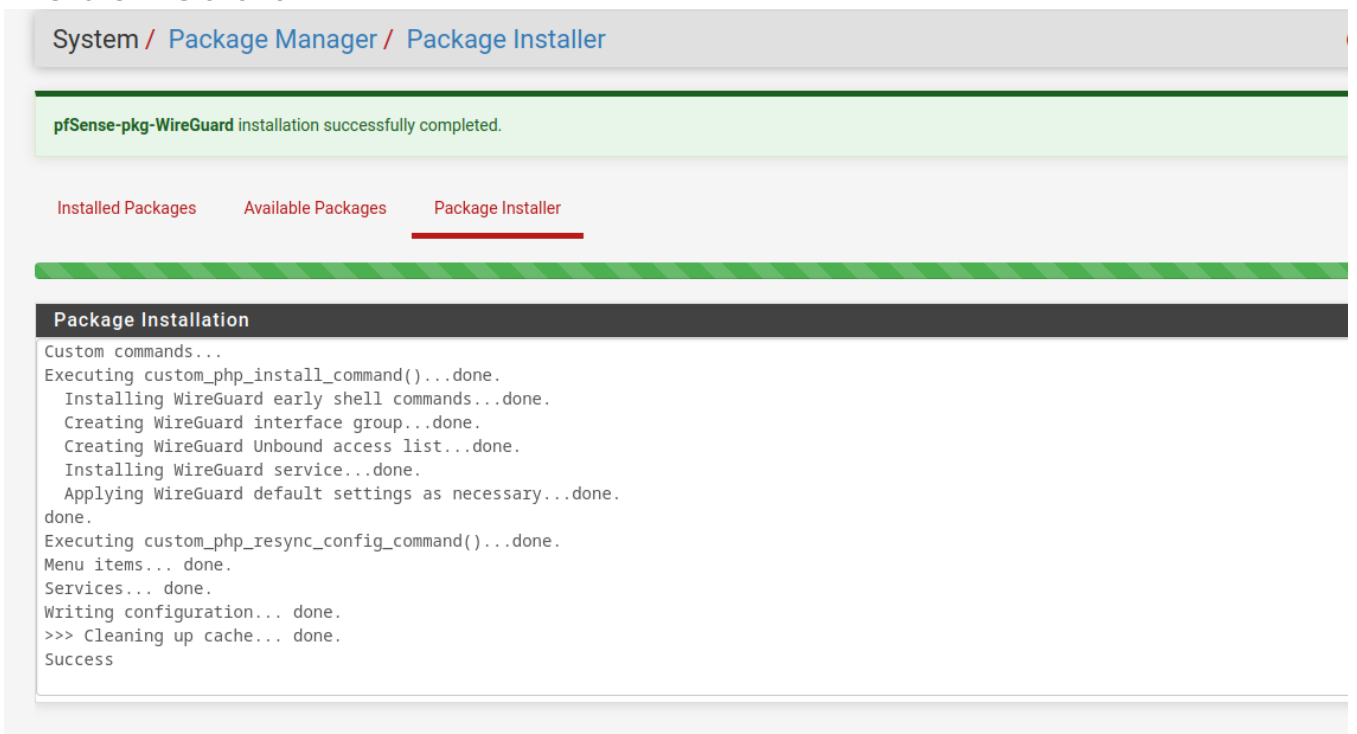
Packages

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

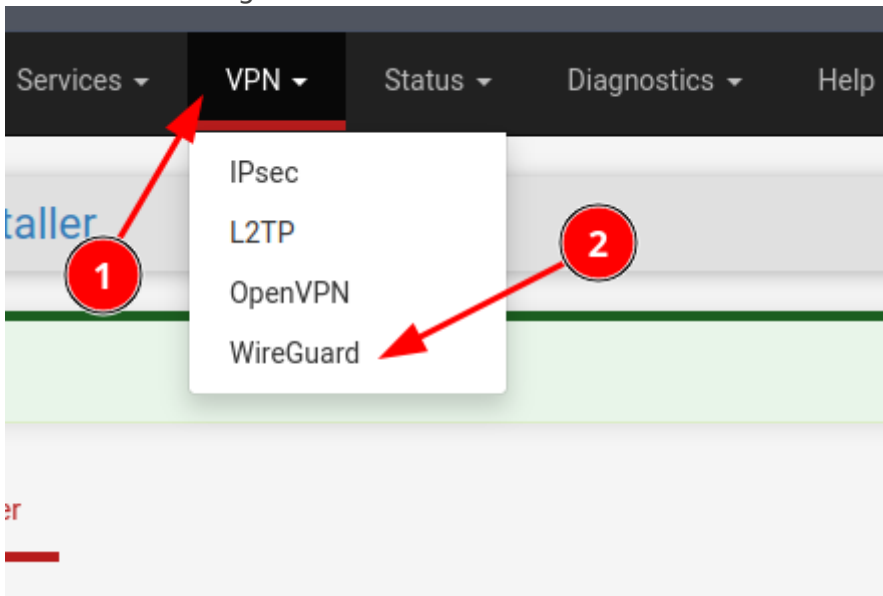


5. Attendre l'installation

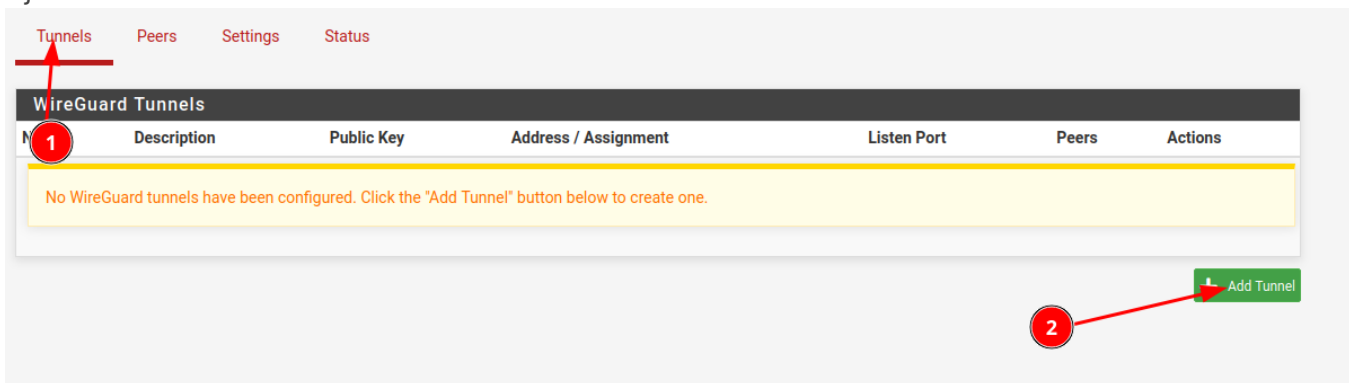


Paramétrage de Wireguard:

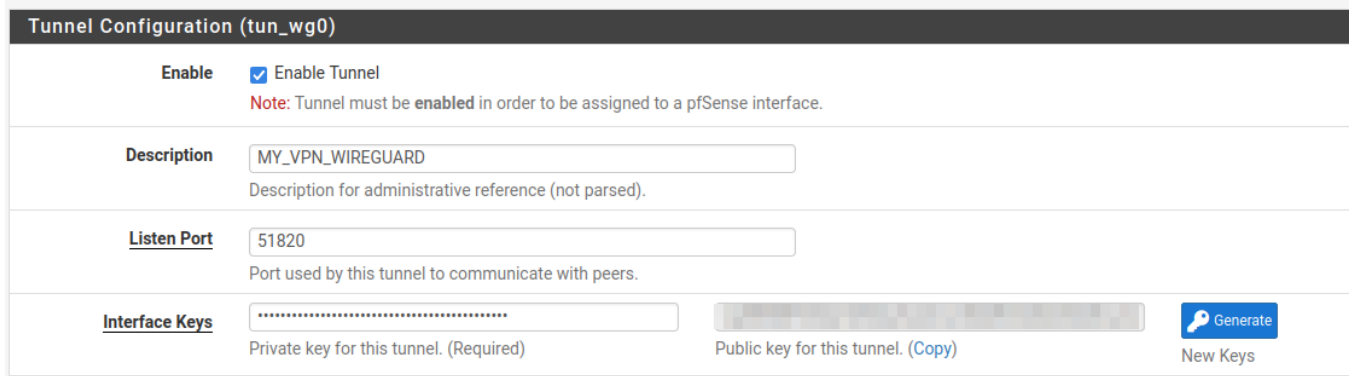
1. Paramétrer Wireguard



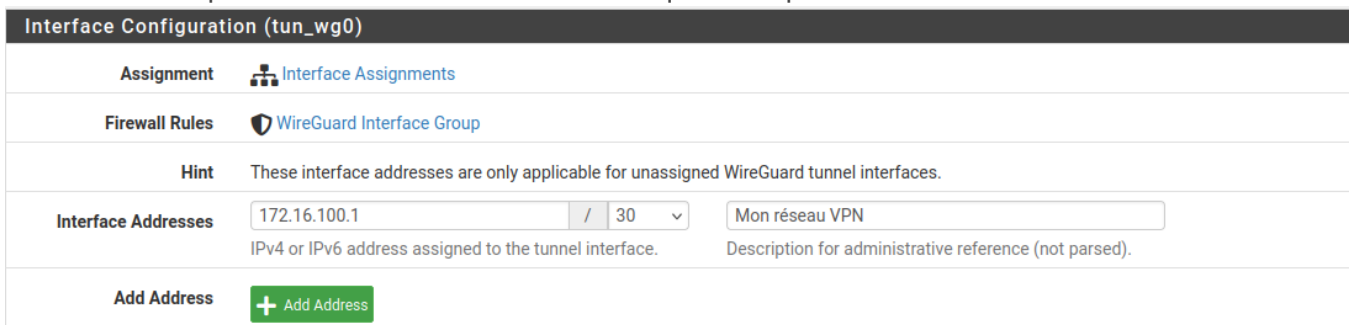
2. Ajouter un tunnel



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

Tunnels Peers **Settings** Status

Tunnel Configuration (tun_wg0)

2 Enable Enable Tunnel
 Note: Tunnel must be enabled in order to be assigned to a pfSense interface.

Description
 Description for administrative reference (not parsed).

Listen Port
 Port used by this tunnel to communicate with peers.

Interface Keys
 Private key for this tunnel. (Required) Public key for this tunnel. (Copy) New Keys

Interface Configuration (tun_wg0)

Assignment [Interface Assignments](#)

Firewall Rules [WireGuard Interface Group](#)

Hint These interface addresses are only applicable for unassigned WireGuard tunnel interfaces.

Interface Addresses /
 IPv4 or IPv6 address assigned to the tunnel interface. Description for administrative reference (not parsed).

Add Address

Peer Configuration

Description	Public key	Tunnel	Allowed IPs	Endpoint : Port	Actions
New tunnels must be saved before adding or assigning peers.					

1

6. Activer Wireguard

Tunnels Peers **Settings** Status

General Settings

Enable Enable WireGuard
 Note: WireGuard cannot be disabled when one or more tunnels is assigned to a pfSense interface.

Keep Configuration Enable
 Note: With 'Keep Configurations' enabled (default), all tunnel configurations and package settings will persist on install/de-install.

Endpoint Hostname Track System Resolve Interval
 Interval (in seconds) for re-resolving endpoint host/domain names. Tracks the system 'Aliases Hostnames Resolve Interval' setting.
 Note: The default is 300 seconds (0 to disable). Note: See System > Advanced > Firewall & NAT

Interface Group
 Membership Configures which WireGuard tunnels are members of the WireGuard interface group.
 Note: Group firewall rules are evaluated before interface firewall rules. Default is 'All Tunnels.'

User Interface Settings

Hide Secrets Enable
 Note: With 'Hide Secrets' enabled, all secrets (private and pre-shared keys) are hidden in the user interface.

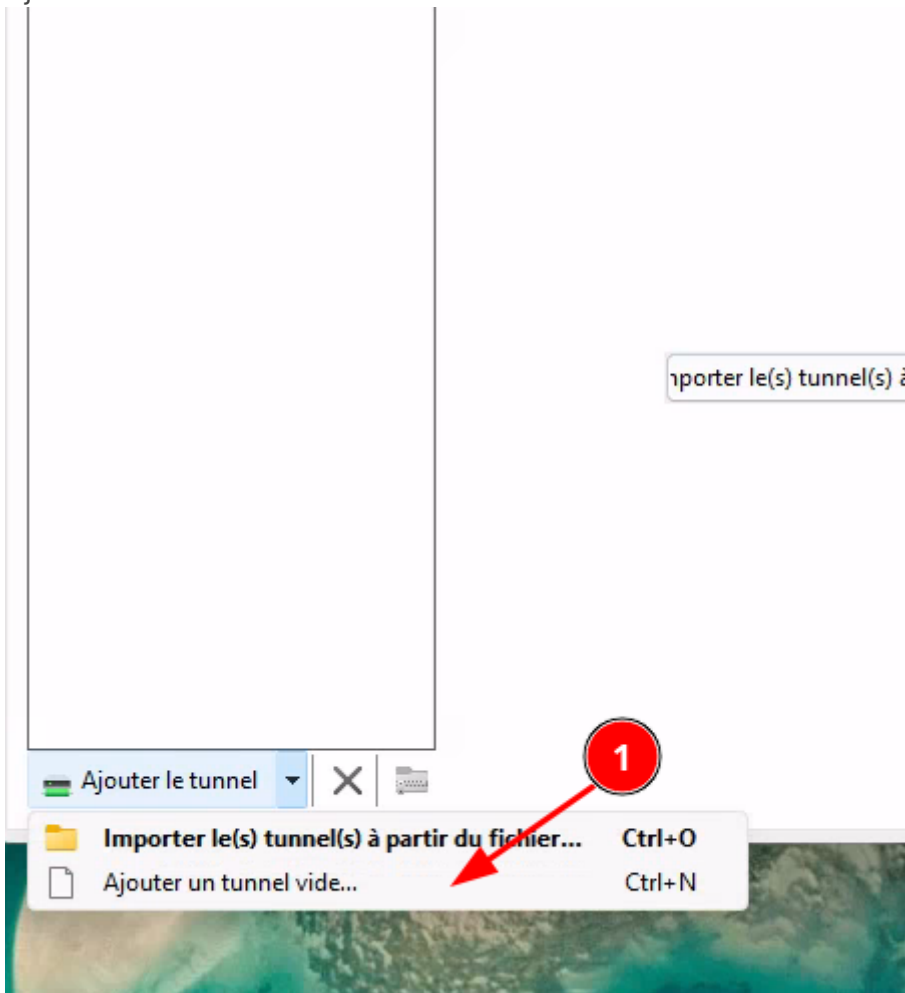
Hide Peers Enable
 Note: With 'Hide Peers' enabled (default), all peers for all tunnels will initially be hidden on the status page.

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

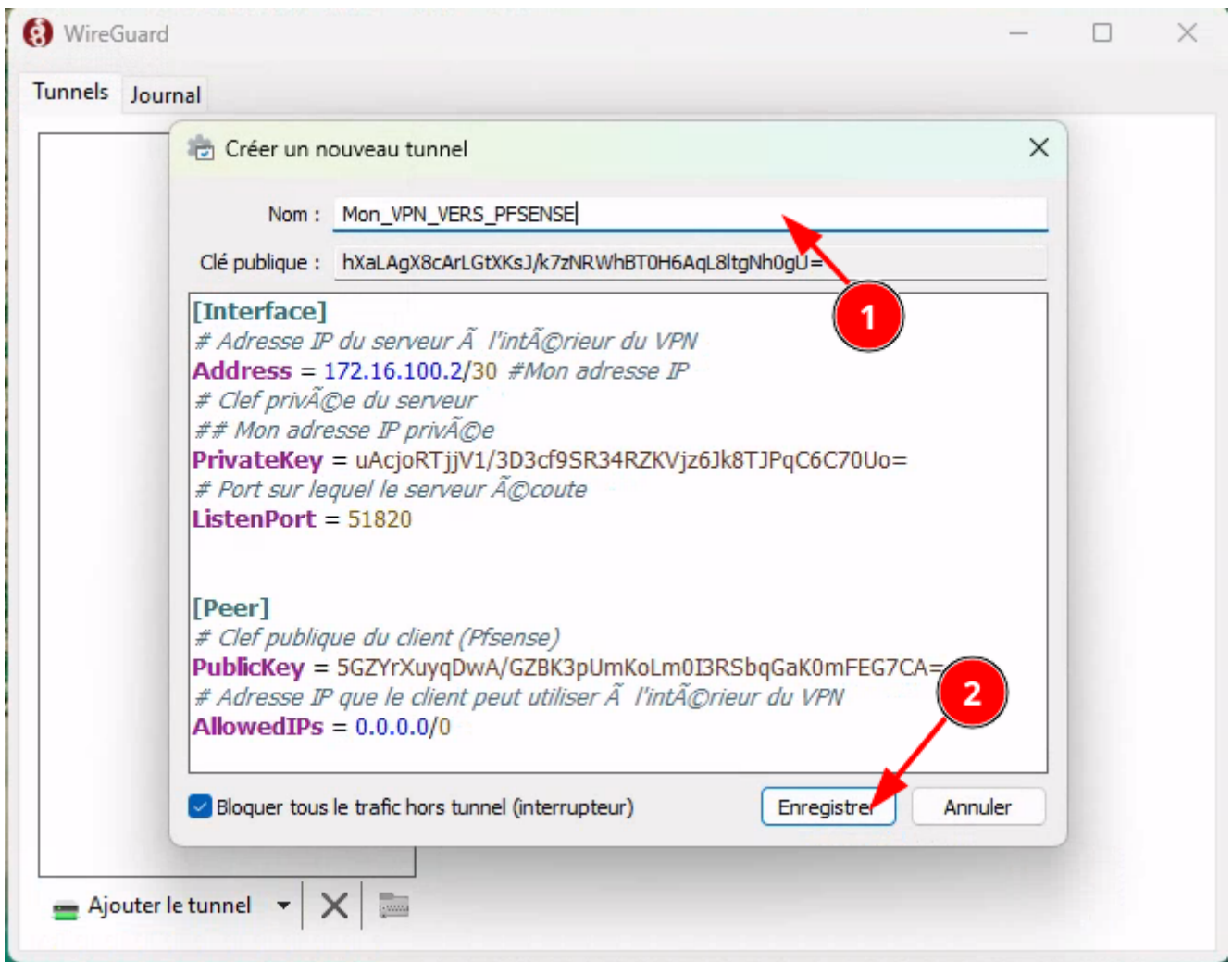
9. Ajouter un tunnel vide



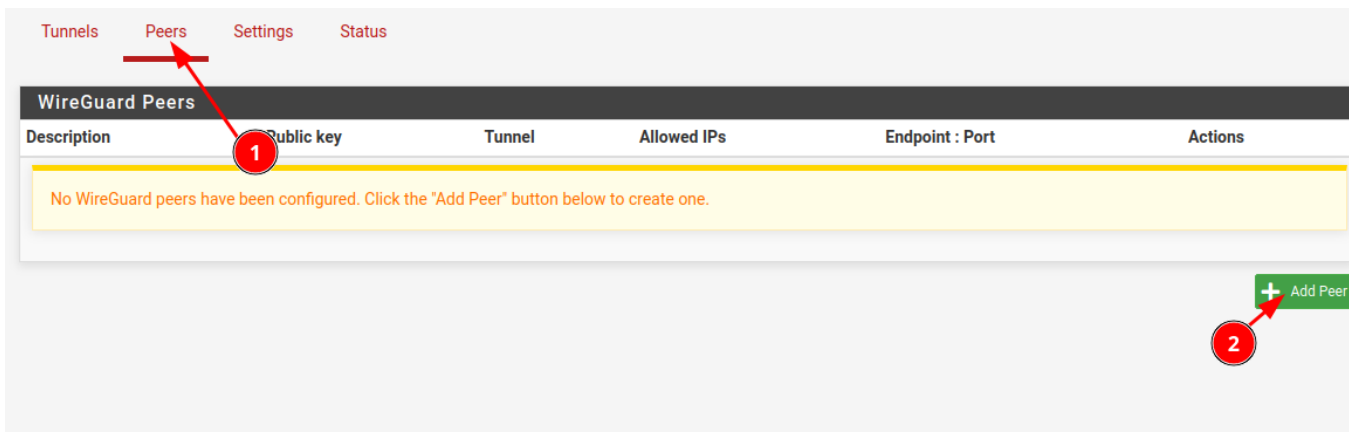
10. Ajouter la configuration

```
[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)



Peer Configuration

Enable Enable Peer
 Note: Uncheck this option to disable this peer without removing it from the list.

Tunnel tun_wg0 (MY_VPN_WIREGUARD)
 WireGuard tunnel for this peer. (Create a New Tunnel)

Description Vers mon Windows
 Peer description for administrative reference (not parsed).

Dynamic Endpoint Dynamic
 Note: Uncheck this option to assign an endpoint address and port for this peer.

Keep Alive Keep Alive
 Interval (in seconds) for Keep Alive packets sent to this peer. Default is empty (disabled).

Public Key hXaLAgX8cArLgTtXKsJ/k7zNRWhBTOH6AqL8ltgNh0gU=
 WireGuard public key for this peer.

Pre-shared Key Pre-shared Key
 Optional pre-shared key for this tunnel. (Copy) New Pre-shared Key

Address Configuration

Hint Allowed IP entries here will be transformed into proper subnet start boundaries prior to validating and saving. These entries must be unique between 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 0.0.0.0 / 0
 IPv4 or IPv6 subnet or host reachable via this peer. Description for administrative reference (not parsed).

Add Allowed IP

12. Appliquer les changements

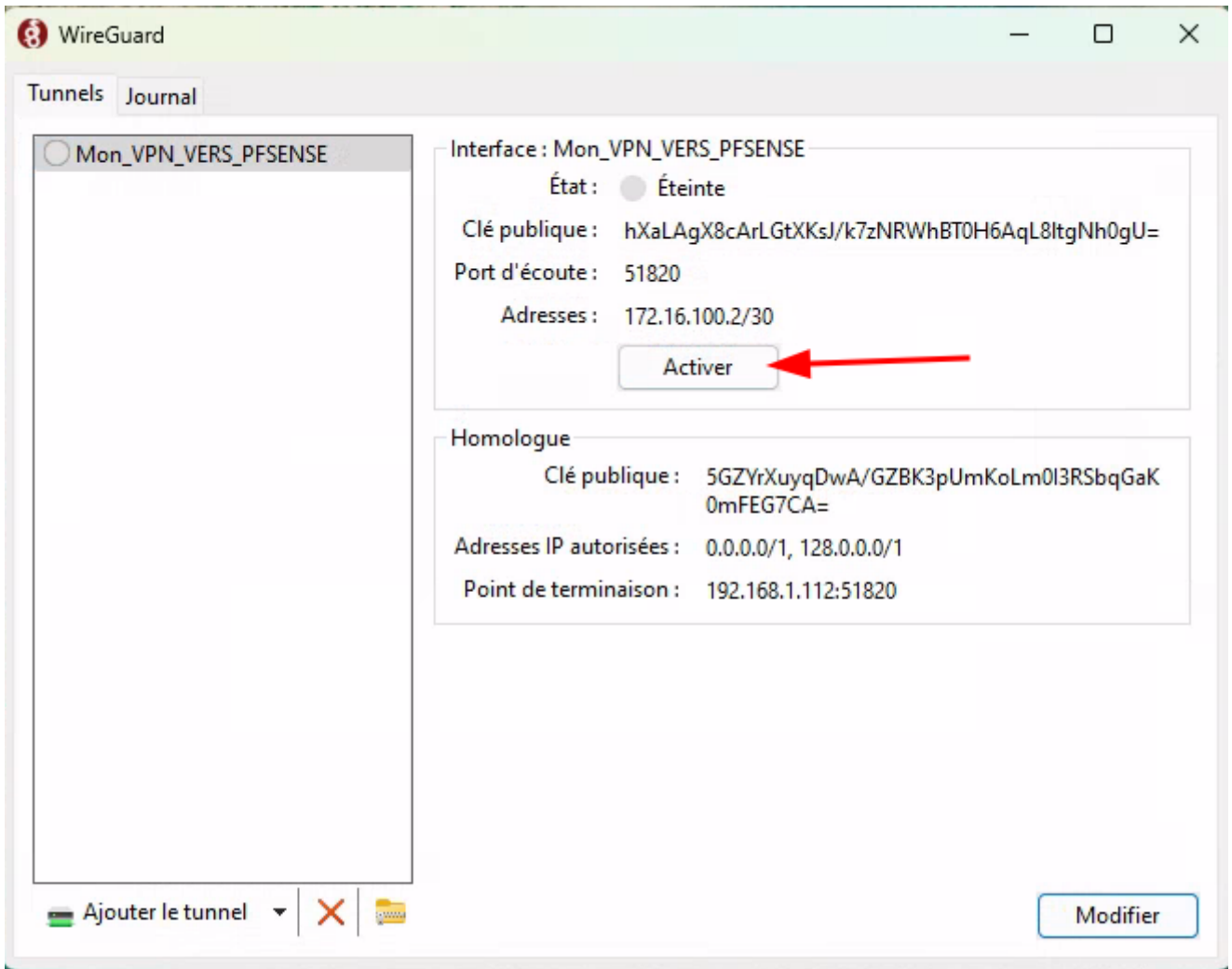
VPN / WireGuard / Peers

The WireGuard configuration has been changed.
 The changes must be applied for them to take effect.
 Notice: This action may momentarily suspend active WireGuard peer connections on any changed tunnels.

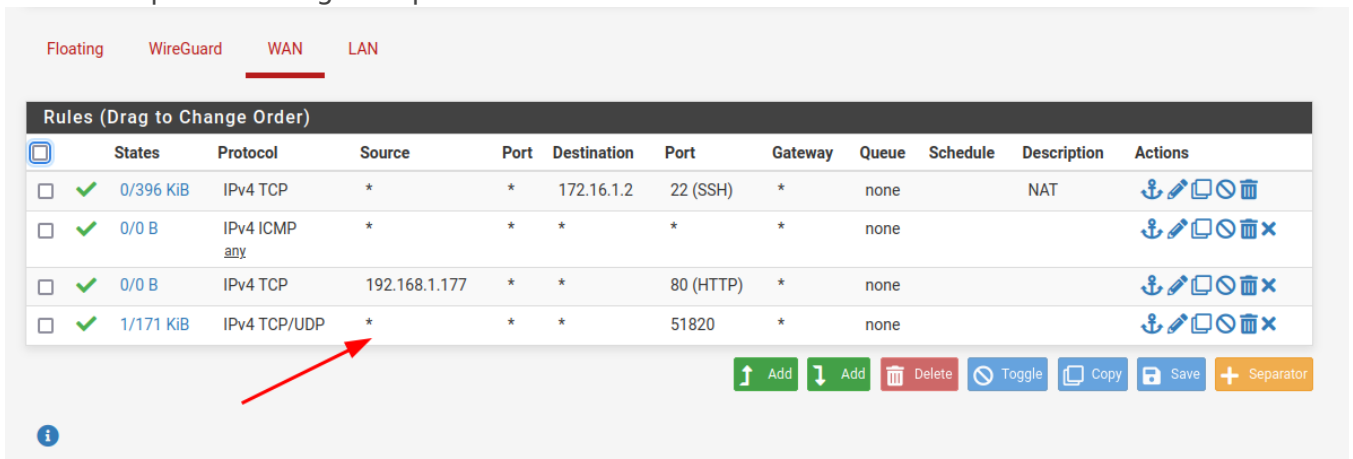
Tunnels **Peers** Settings Status

WireGuard Peers					
Description	Public key	Tunnel	Allowed IPs	Endpoint : Port	Actions
Vers mon Windows	hXaLAgX8cArLgTtXK...	tun_wg0	0.0.0.0/0	Dynamic	<input type="button" value="edit"/> <input type="button" value="stop"/> <input type="button" value="delete"/>

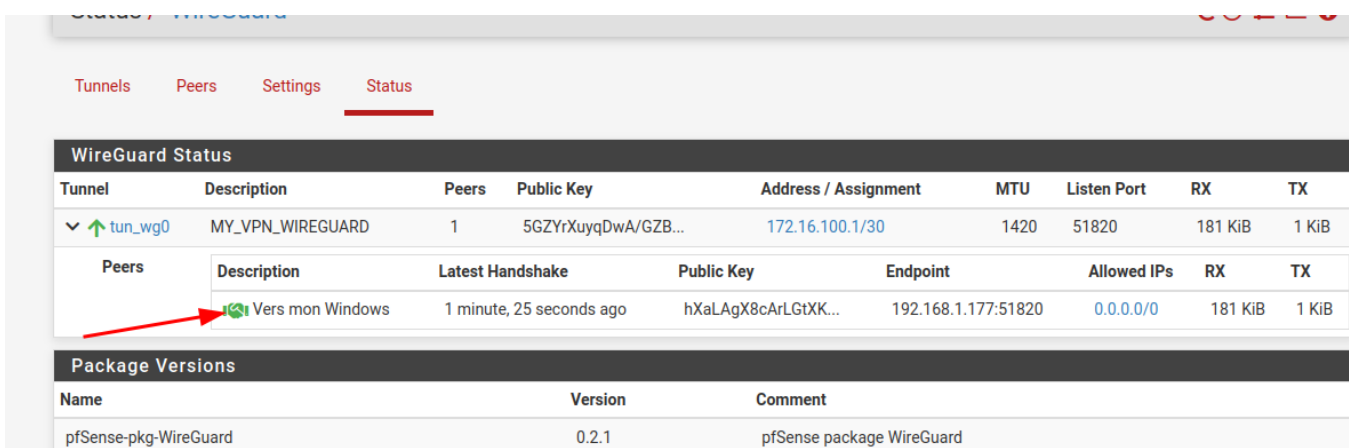
13. Activer le VPN (Windows)



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



15. Vérifier que le VPN est bien connecté



```
C:\Users\kvega>ping 172.16.1.5 ← Ping d'un serveur sur mon LAN
Envoi d'une requête 'Ping' 172.16.1.5 avec 32 octets de données :
Réponse de 172.16.1.5 : octets=32 temps=1 ms TTL=63
Réponse de 172.16.1.5 : octets=32 temps=1 ms TTL=63
Réponse de 172.16.1.5 : octets=32 temps=4 ms TTL=63
Réponse de 172.16.1.5 : octets=32 temps=2 ms TTL=63

Statistiques Ping pour 172.16.1.5:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 4ms, Moyenne = 2ms

C:\Users\kvega>
```

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

```
Itinéraires actifs :
Destination réseau      Masque réseau  Adr. passerelle  Adr. interface  Métrique
0.0.0.0                 0.0.0.0       192.168.1.254   192.168.1.177   25
→ 0.0.0.0                 128.0.0.0      On-link         172.16.100.2    5
127.0.0.0               255.0.0.0     On-link         127.0.0.1       331
127.0.0.1               255.255.255.255 On-link         127.0.0.1       331
127.255.255.255         255.255.255.255 On-link         127.0.0.1       331
127.255.255.255         255.255.255.255 On-link         172.16.100.2    261
```

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
```