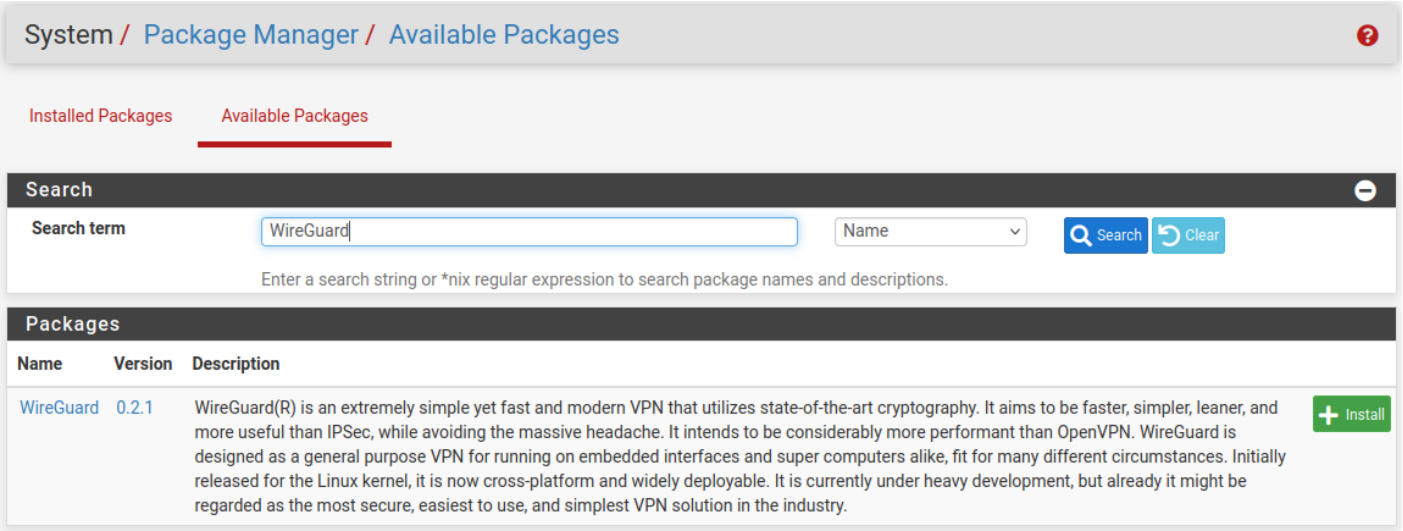
[pfSense] Wireguard

Introduction

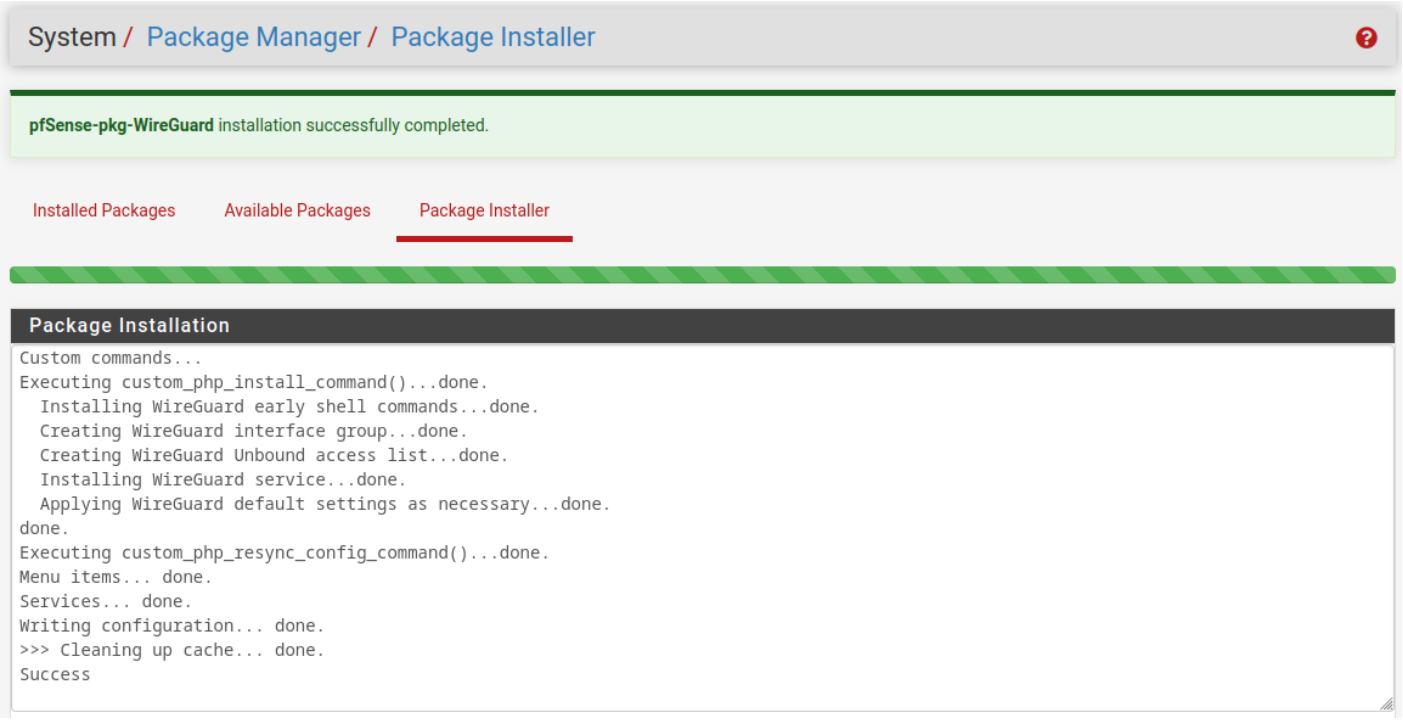
Wireguard supporte depuis récemment l'installation d'un VPN wiregard qui est le plus rapide et performant du marché des VPNs open source.

Installation

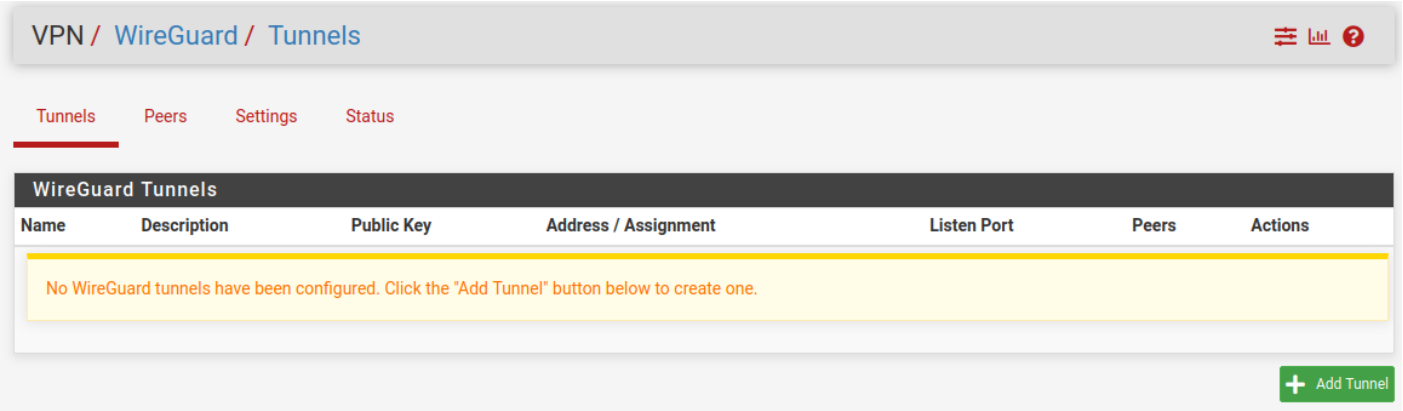
Tout d'abord, installez le paquet **WireGuard** depuis le menu **System > Package Manager > Available Packages** :



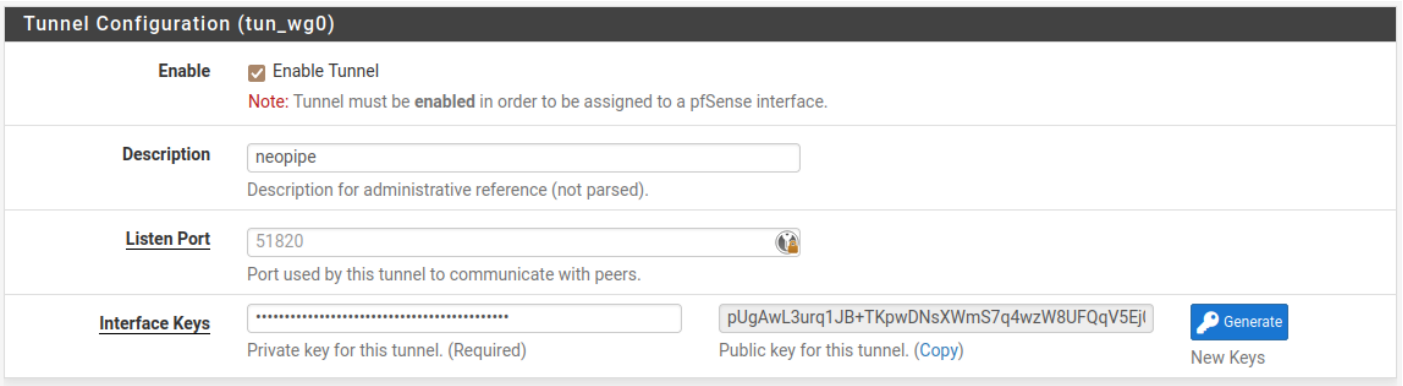
Cliquez sur **Install** puis **Confirm** et attendez que le message suivant apparaisse :



Ensuite, rendez vous dans l'onglet **VPN > Wireguard** et cliquez sur **Add tunnel** :

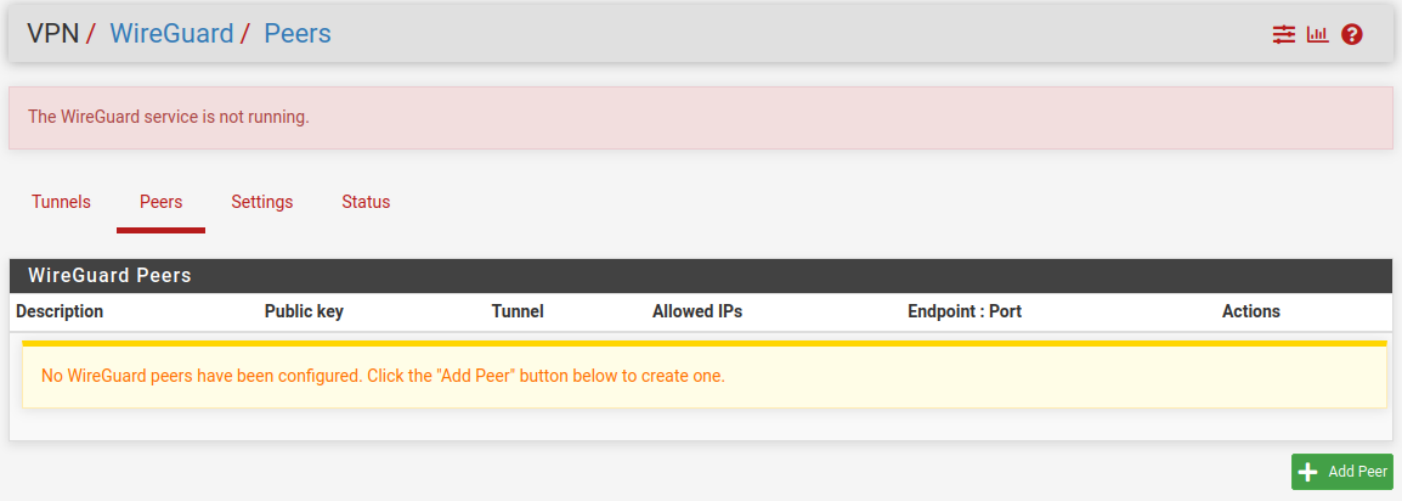


Pour la configuration du tunnel, saisissez en **description** le nom de votre VPN puis générez une paire de clés en cliquant sur **Generate** :

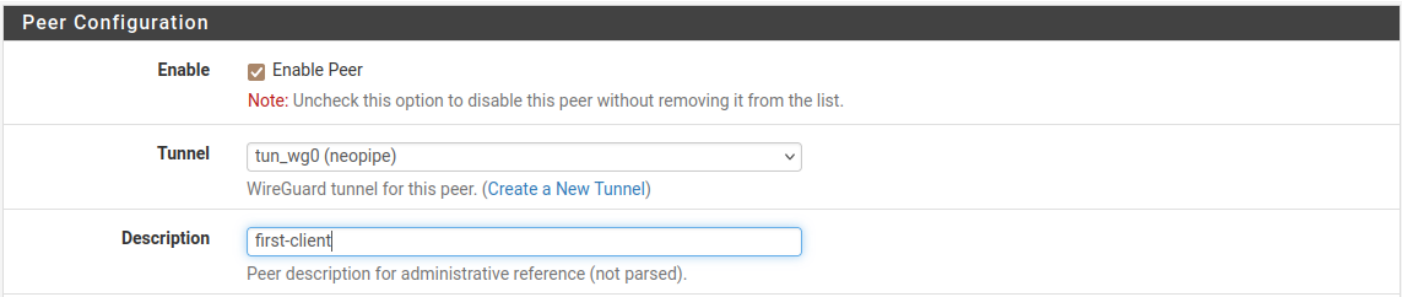


Dans la configuration de l'interface, saisissez l'adresse IP privée du routeur associée à l'interface du tunnel :

Cliquez sur **Save** et rendez vous dans l'onglet **Peer** puis cliquez sur **Add Peer** :



Sélectionnez votre **Tunnel** dans le menu déroulant et mettez le nom de votre client en **Description** :



Depuis votre client Wireguard, générez une paire de clés publique/privée :

```
[~/tmp]$ wg genkey | tee wg-private.key
EJUzxJoaNo3SfxjF0iyrxcT3kRcROaPBzoKBG6NKEm4=
```

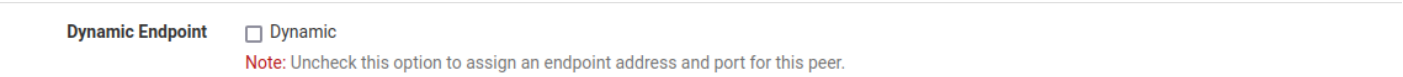
```
[~/tmp]$ cat wg-private.key| wg pubkey | tee wg-public.key
QNQJsUuG9SfsMCR4cYj9O/fr5uSL+qM1kgjLah+MZmc=
```

wg genkey | tee wg-private.key

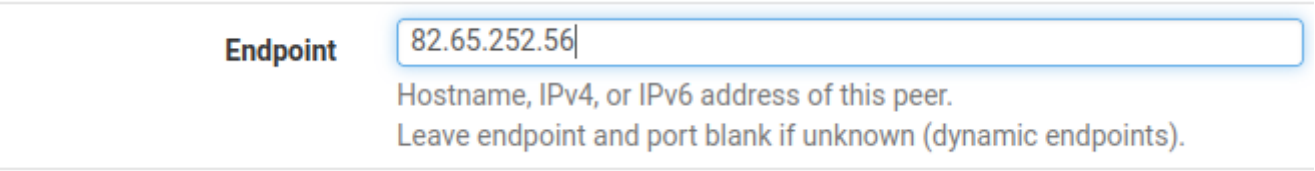
cat wg-private.key | wg pubkey | tee wg-public.key

Et renseignez la clé publique dans la configuration du peer sur pfsense :

Et n'oubliez pas de décocher **Dynamic Endpoint** :

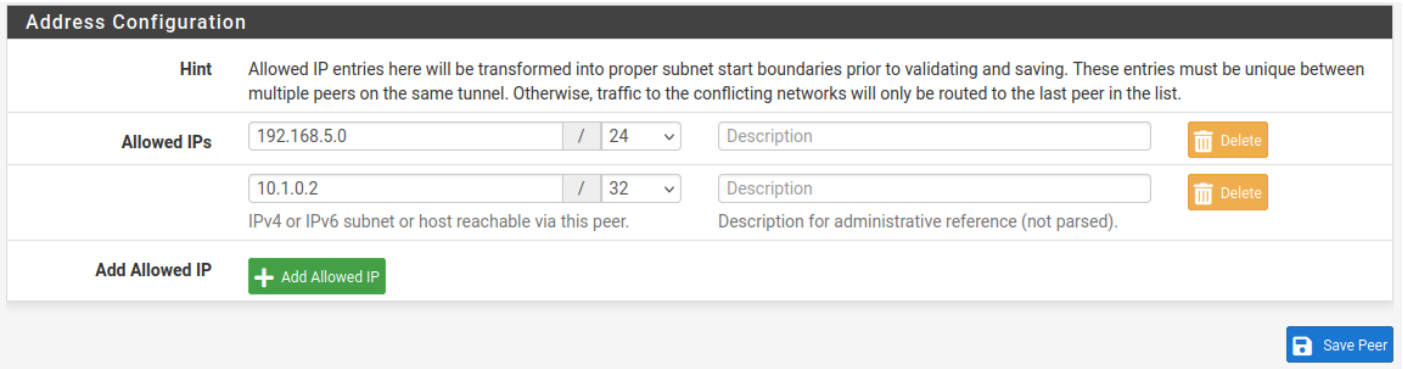


Saisissez ensuite l'adresse IP de l'**Endpoint** (IP publique de votre routeur qui sera atteinte pour se connecter au VPN) :

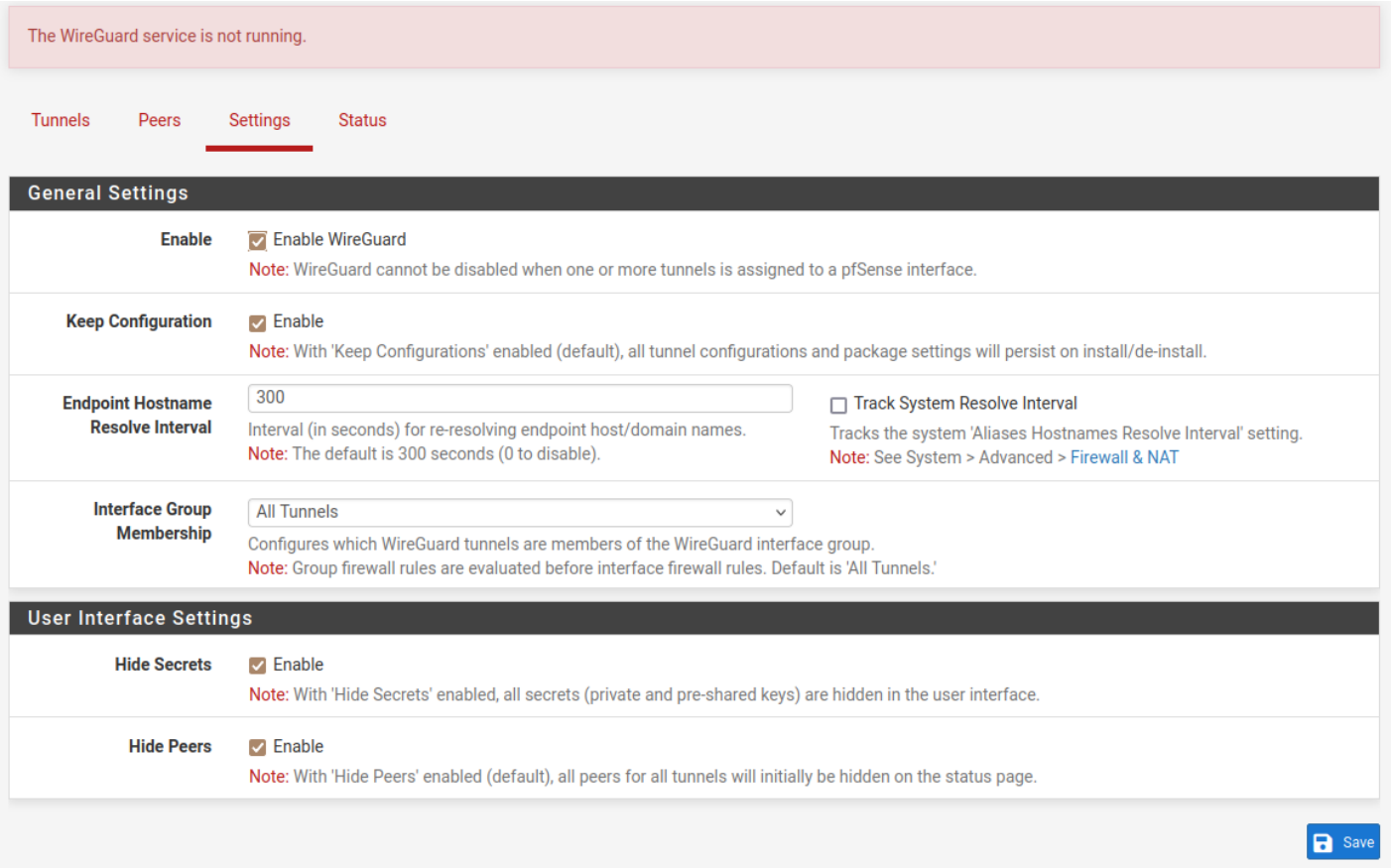


Dans la configuration d'adressage, vous pouvez choisir les réseaux accessibles via le VPN.

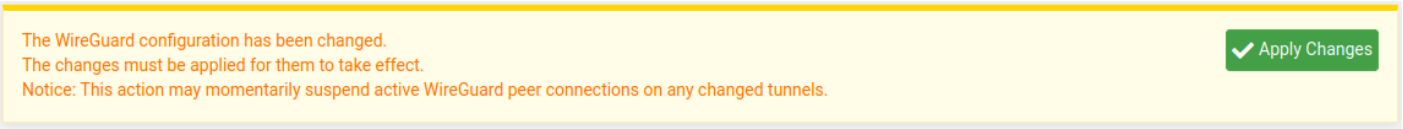
Vous devez saisir l'IP du peer ainsi que les sous-réseaux de destination que vous souhaitez autoriser :



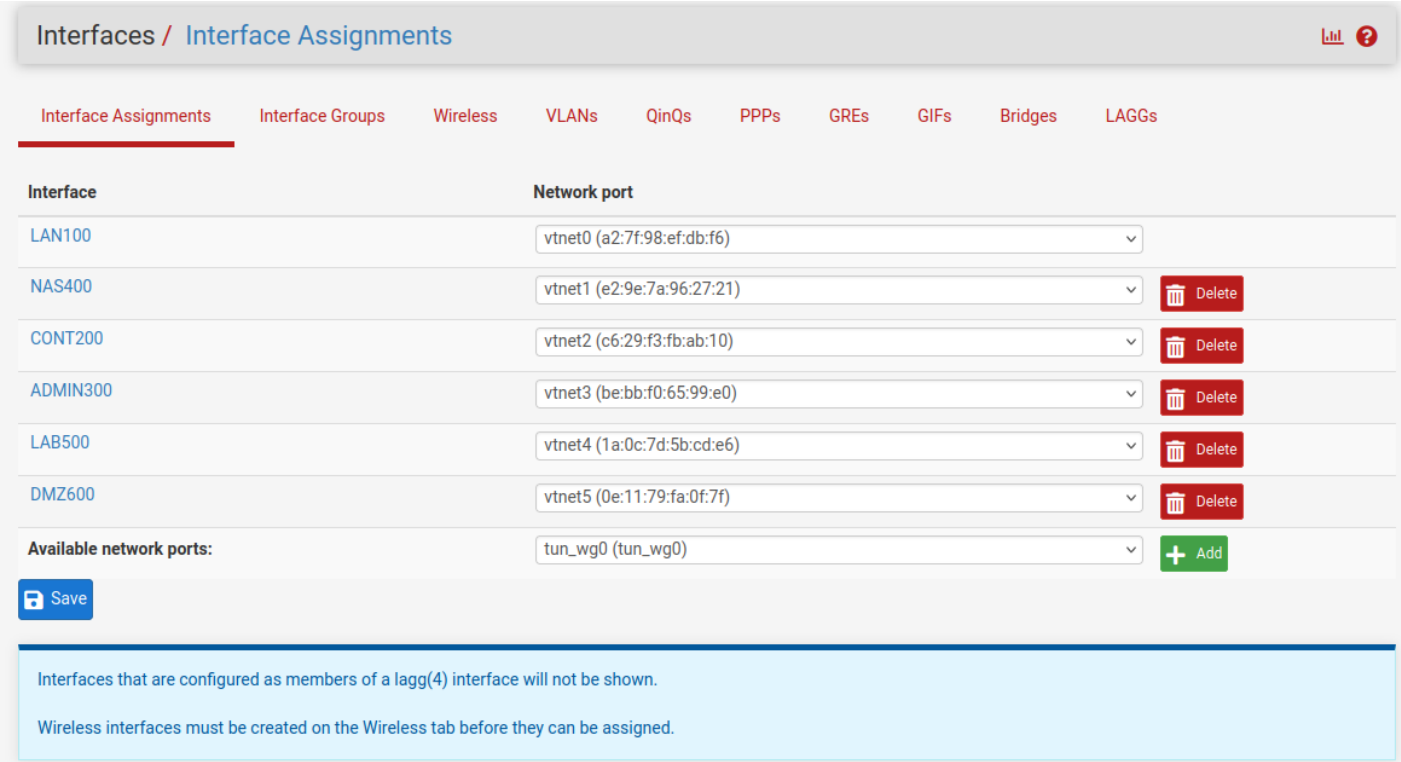
Cliquez sur **Save** puis rendez vous dans l'onglet **Settings** pour activer le service Wireguard et cliquez sur **Save** :



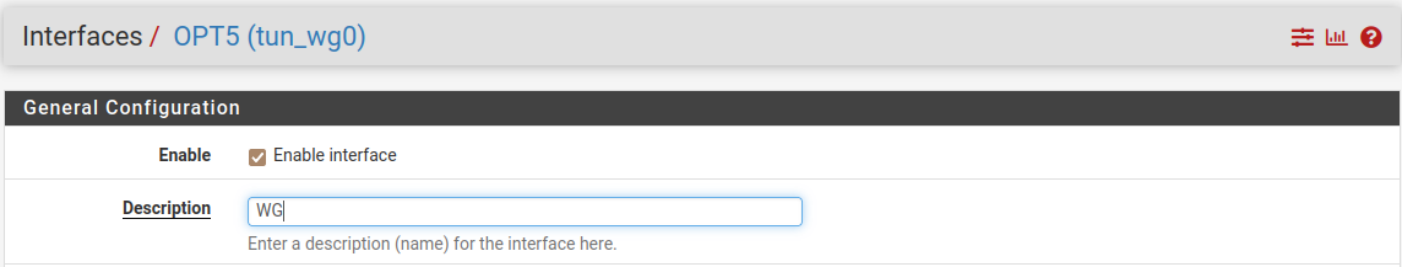
Cliquez sur **Apply Changes** :



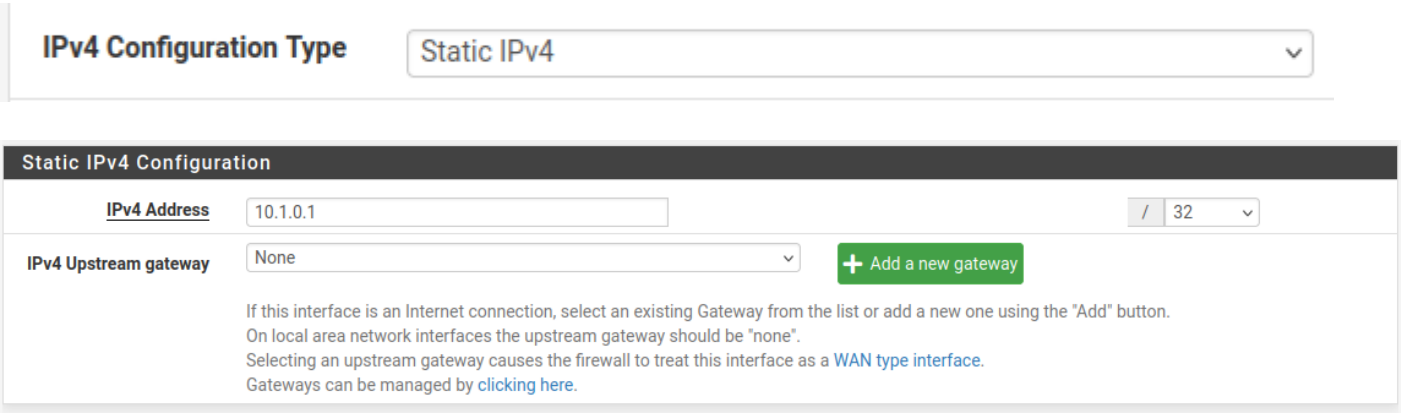
Après, allez sur **Interfaces > Assignements**, sélectionnez l'interface du tunnel et cliquez sur **Add** :



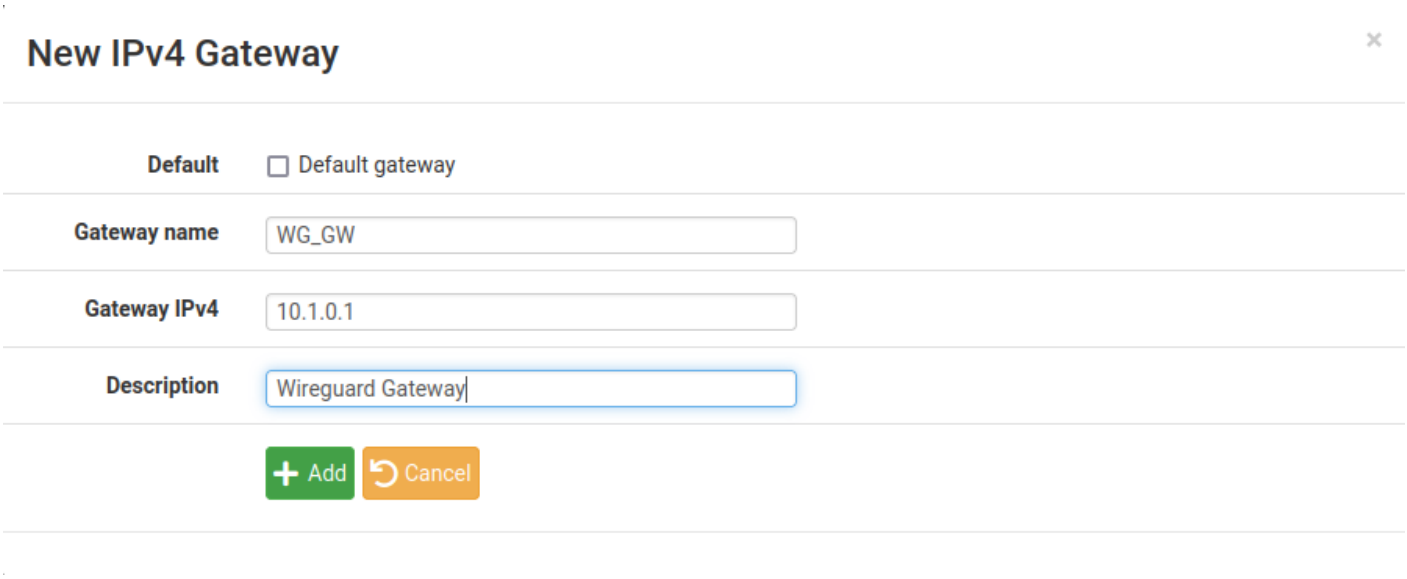
Cliquez sur le nom de la nouvelle interface créée pour accéder à sa configuration puis activez l'interface et modifiez son nom :



En **IPv4 Configuration Type** sélectionnez **Static IPv4** puis dans Static IPv4 Configuration renseignez l'adresse du routeur sur le réseau VPN (définie précédemment) :

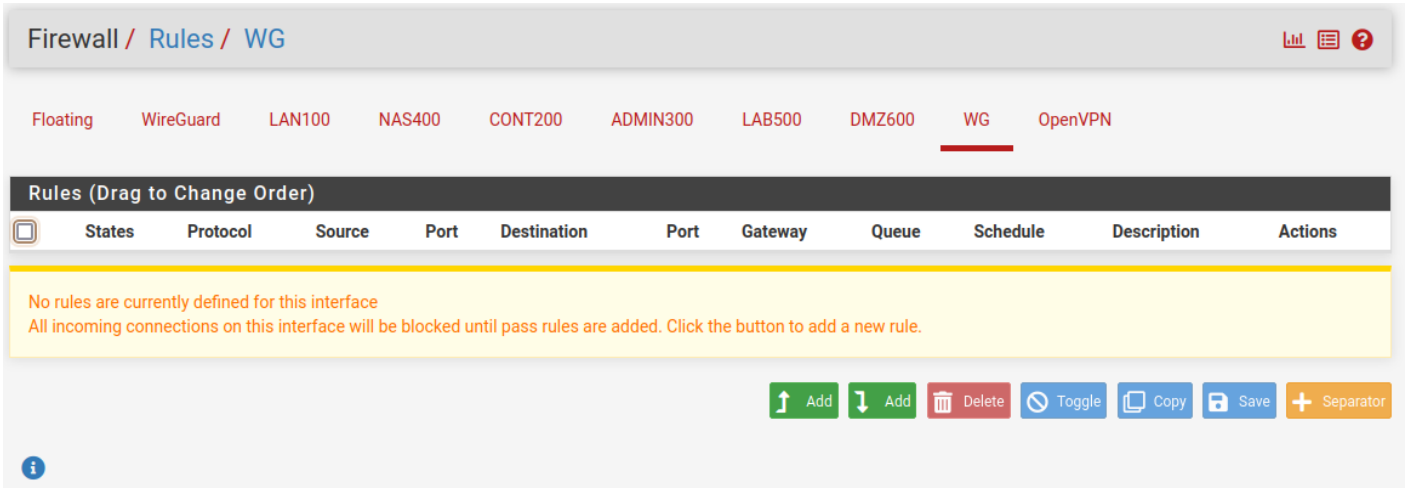


Cliquez sur **Add a new gateway** puis renseignez les informations et cliquez sur **Add** :

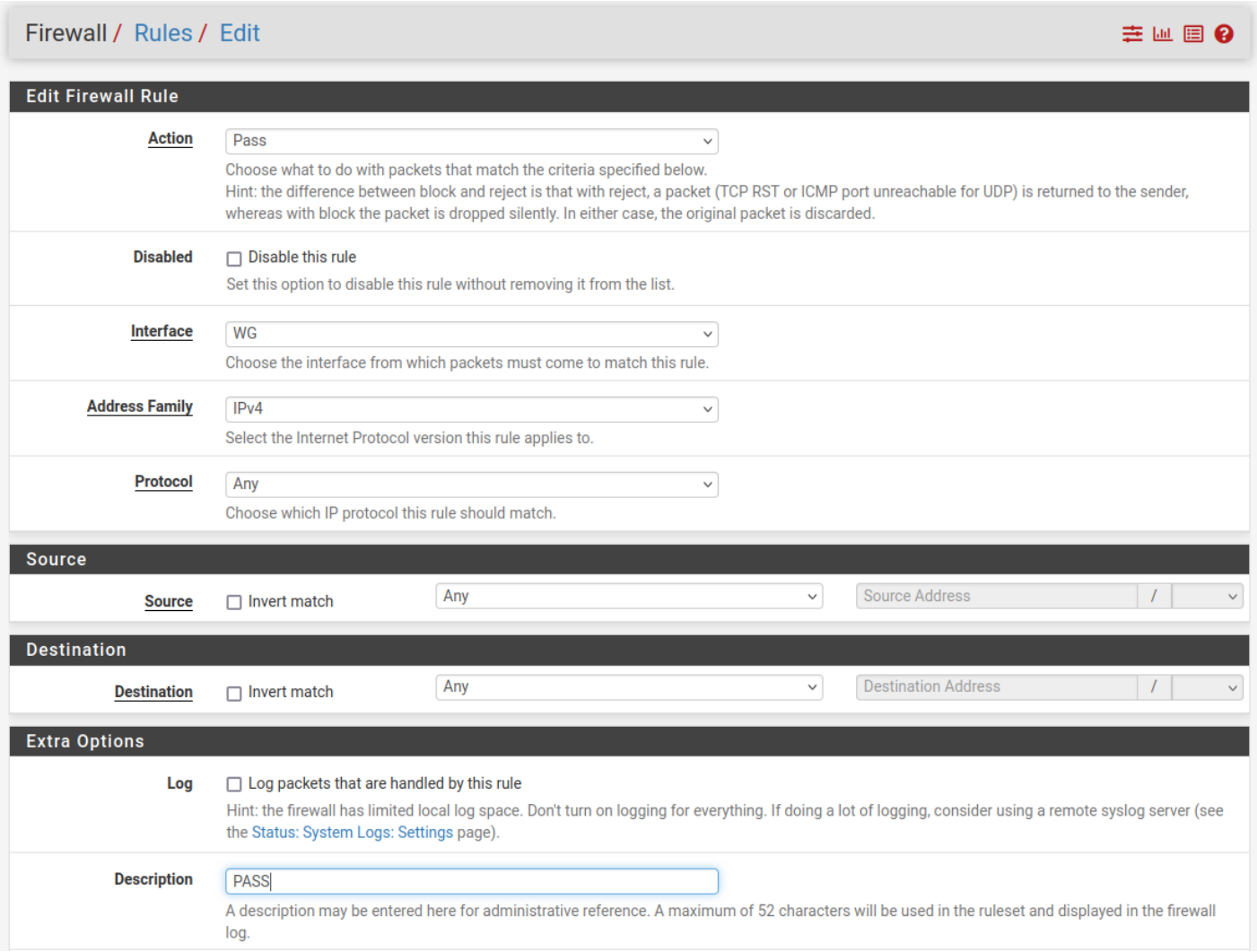


Cliquez ensuite sur **Save** et **Apply Changes**.

On doit ensuite configurer le pare-feu pour autoriser les connexions en allant dans le menu **Firewall > Rules > WG** puis **Add** :



Faite une règle pour autoriser tout le trafic ou seulement ce que vous souhaitez si vous souhaitez affiner vos règles et cliquez sur **Save** et **Apply Changes** :



> Vous devez aussi créer une règle sur votre **WAN** pour autoriser le flux **UDP/51820** vers votre pare-feu.

La dernière étape consiste à créer le fichier de configuration du client VPN :

```
[Interface]
PrivateKey = <PEER_PRIV_KEY>
Address = 10.1.0.2/24

[Peer]
PublicKey = <SRV_PUB_KEY>
AllowedIPs = 10.1.0.0/24, 192.168.5.0/24
Endpoint = <SRV_PUBLIC_IP>:51820
```

Revision #6
Created 28 May 2024 07:25:42 by Elieroc
Updated 28 May 2024 09:05:58 by Elieroc