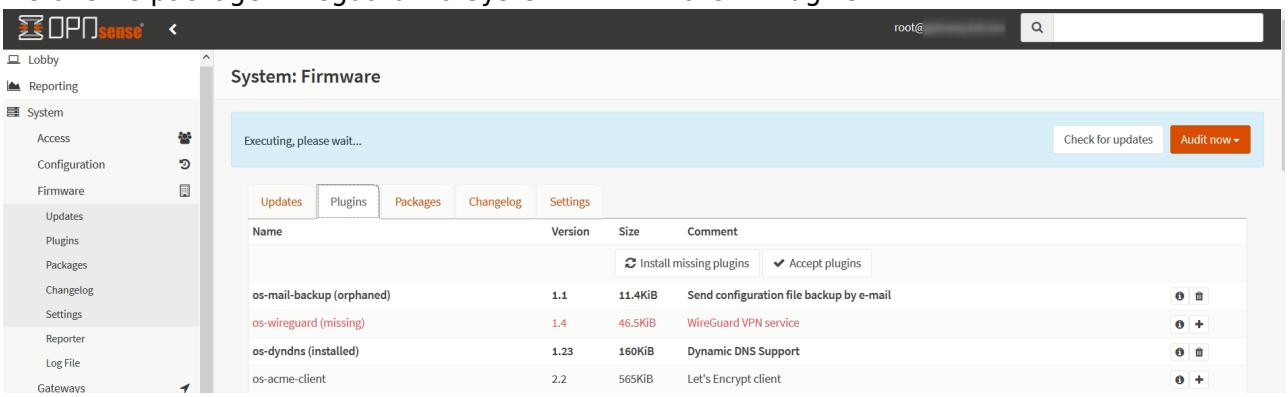
OPNSense : Wireguard VPN

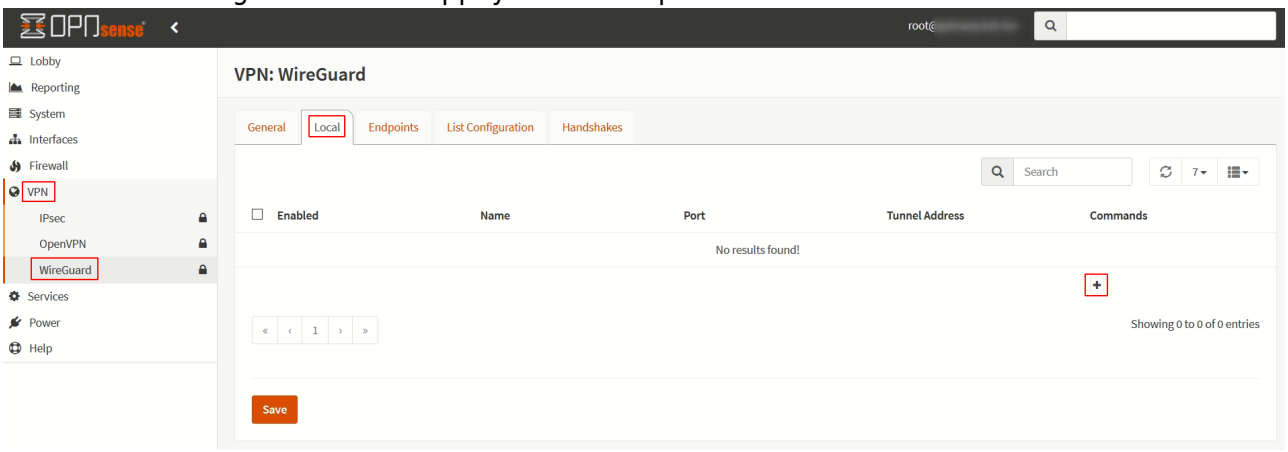
Côté OPNSENSE

Configuration du VPN

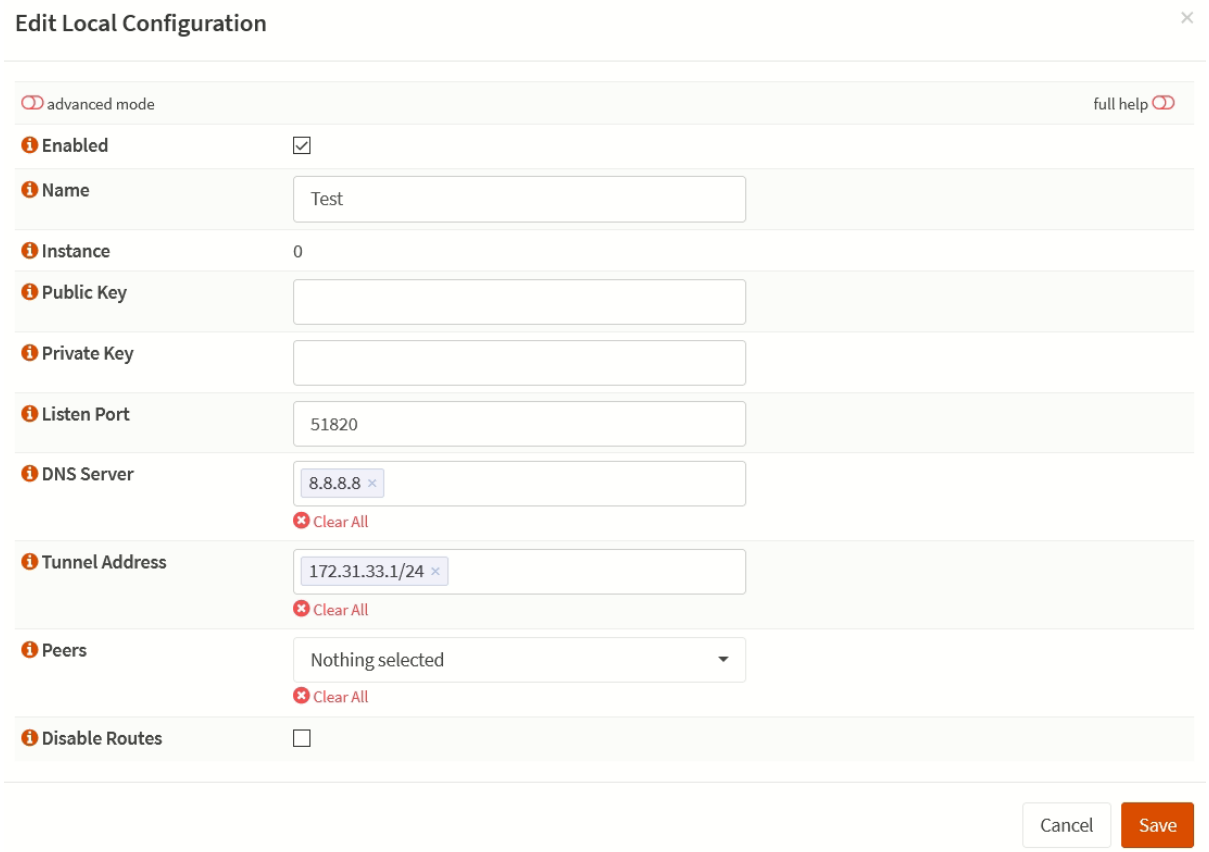
1. Installer le package Wireguard via System → Firmware → Plugins



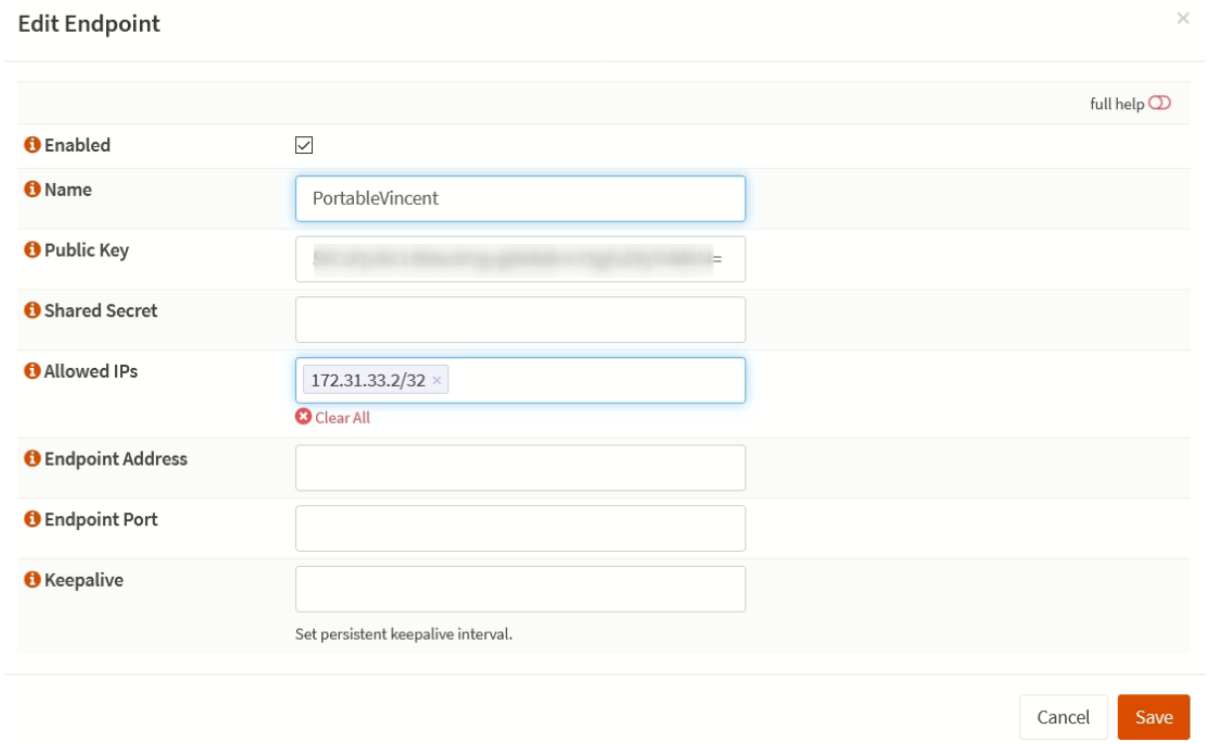
2. Faire F5 dans le navigateur pour faire apparaître le nouveau menu VPN Wireguard
3. Dans VPN → Wireguard → Local appuyez sur le + pour créer une nouvelle entité



4. Créer la configuration de la sorte:
    1. Name: Nom de la connexion
    2. Public Key & Private Key: peuvent être laissés vides, ils seront remplis après avoir pressé Save
    3. DNS Server: Indiquer le serveur DNS que vous souhaitez utilisez
    4. Tunnel address: Définir un subnet qui autorise la communication entre l'entité et le Peer. De préférénce un CDIR 24
    5. Peer: On devra retourner et choisir le Peer autorisé une fois créé

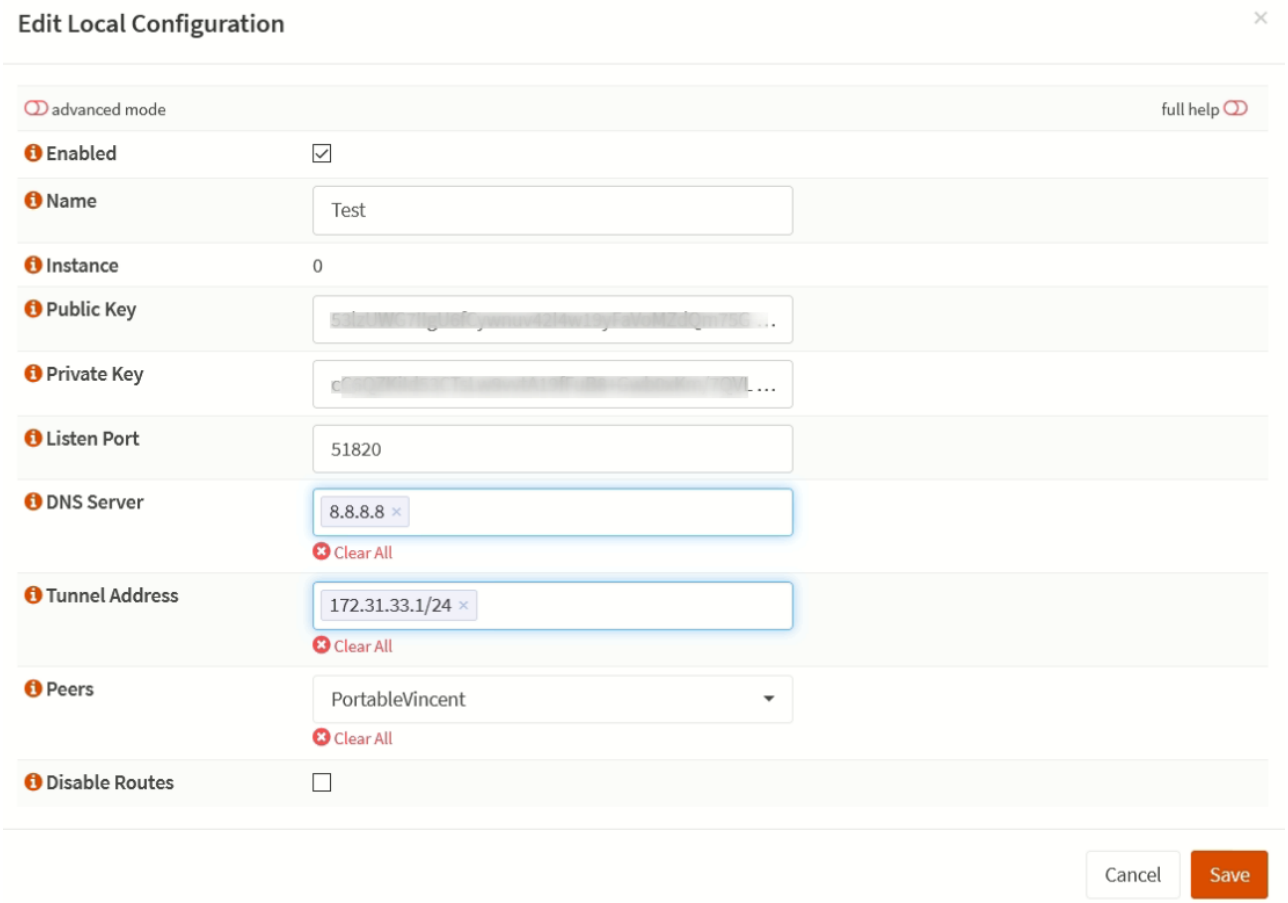


5. Dans VPN → Wireguard → Endpoints appuyez sur le + pour créer une nouvelle Peer
6. Créer la configuration de la sorte:
    1. Name: Donner un nom
    2. Public Key: doit être la clée publique générée par le client
    3. Shared Secret: optionnel, permet de mettre un mot de passe sur la connexion
    4. Allowed IP, on prend une adresse dans le Tunnel Address, en CDIR 32
    5. Enpoint Address & Endpoint Port: si il s'agit d'une configuration en RoadWarrior, ces deux champs peuvent rester vide

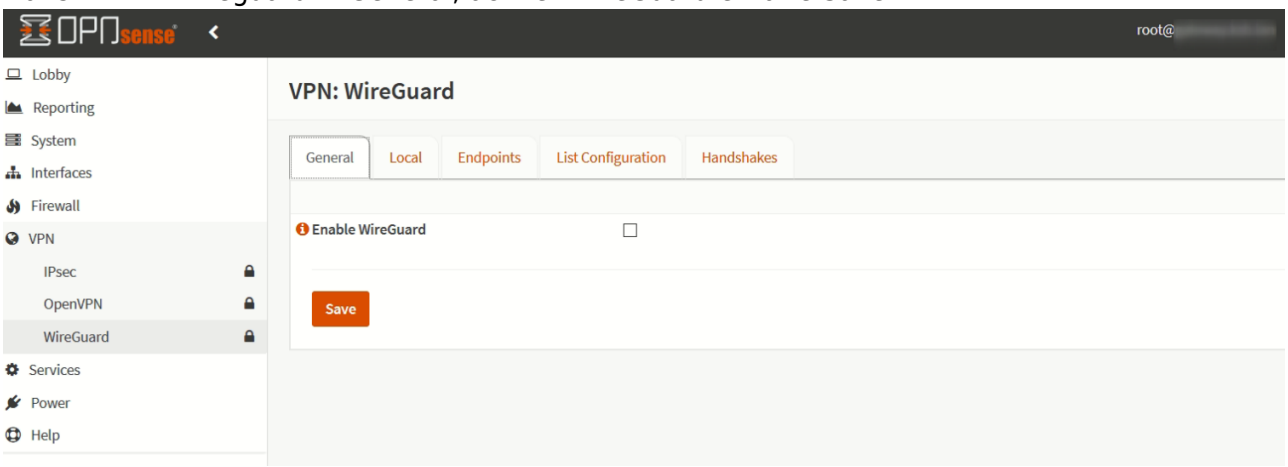


7. Retourner dans VPN → Wireguard → Local et éditer l'entité créée pour sélectionner le Peer

distant.

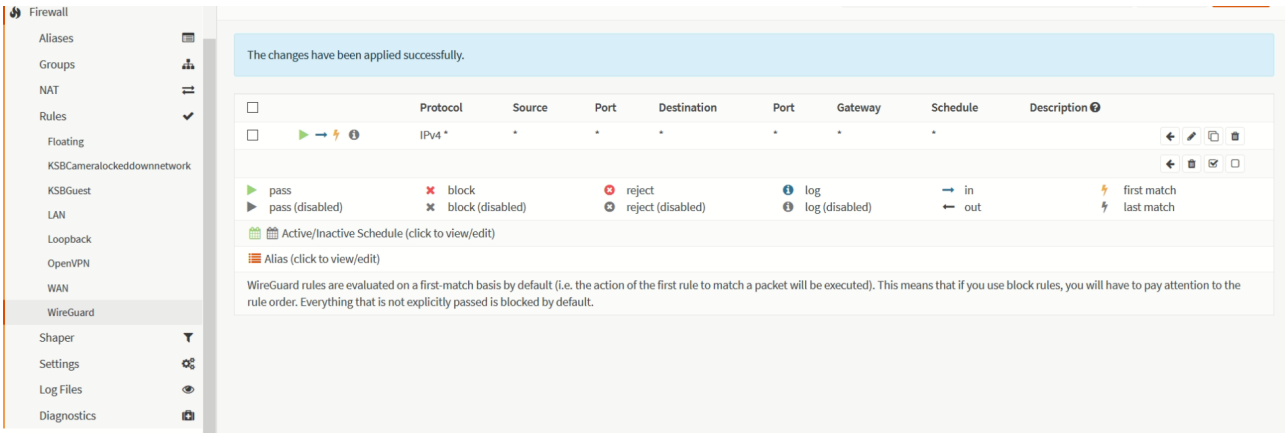


8. Dans VPN → Wireguard → General, activer WireGuard et faire Save



Règles Firewall

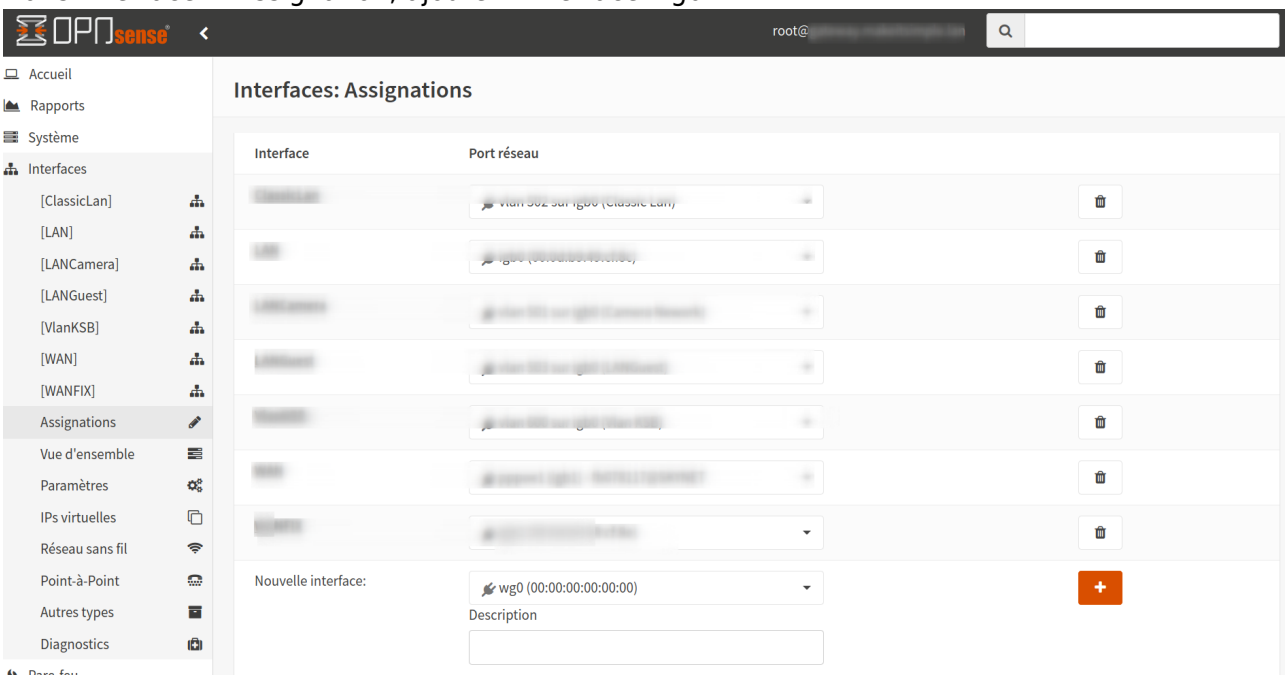
1. Prévoir une règle dans Firewall → Rules → WireGuard pour autoriser le trafic désiré. Un Accept All est envisageable pour un test.



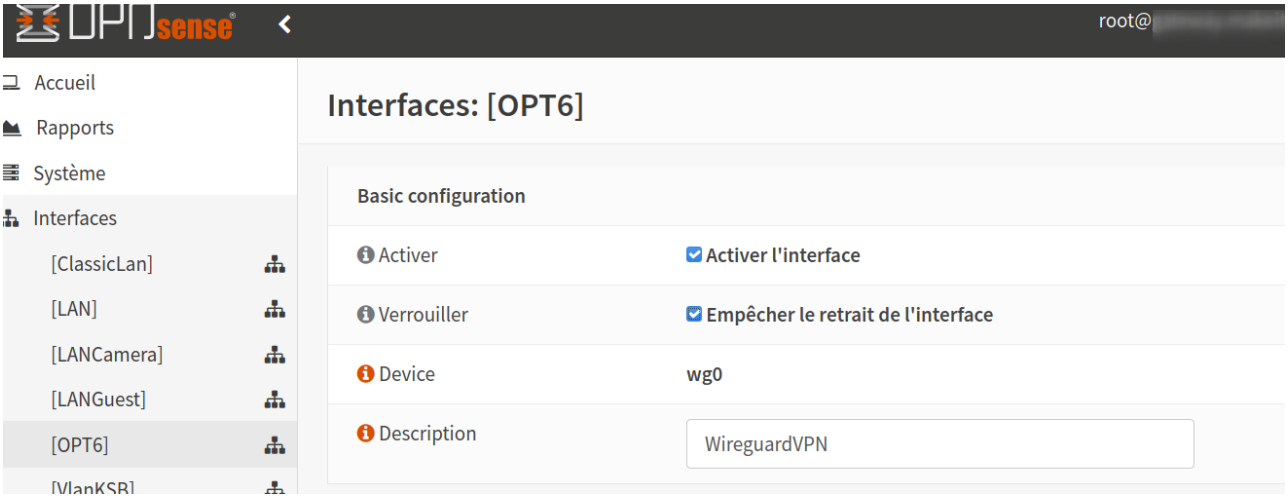
2. Dans Firewall → Rules → Wan: créer une règle qui accepte le port UDP 51820 sur ce firewall

Autoriser le trafic Internet pour les clients Wireguard

1. Dans Interface → Assignation, ajouter l'interface wg0



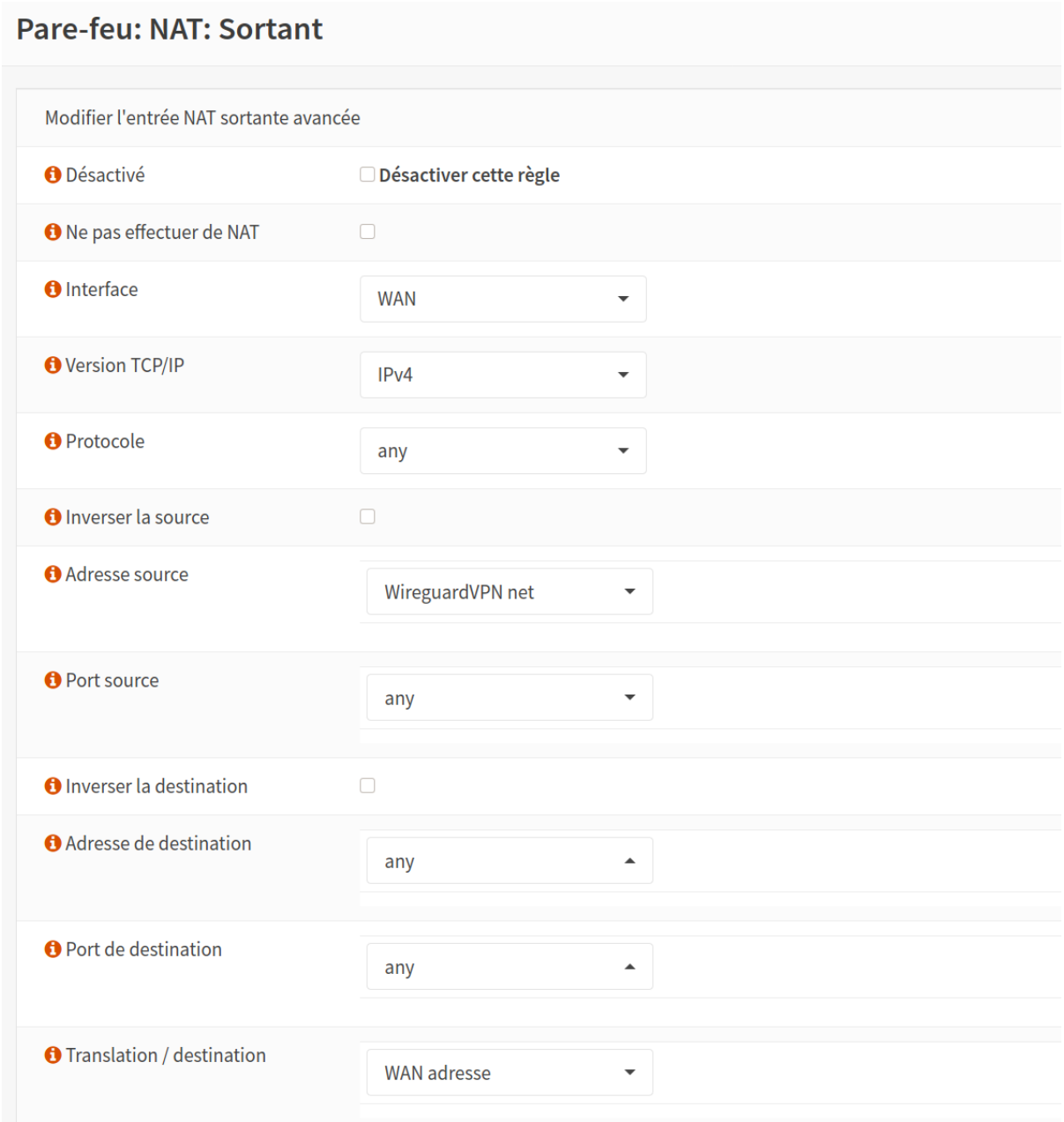
2. Aller dans l'interface fraichement créée, activez la, empêcher le retrait et donner un nom plus facile à retenir



3. Aller ensuite dans Firewall → NAT → Sortant et mettre le mode sur Hybride

puis Appliquer les changements

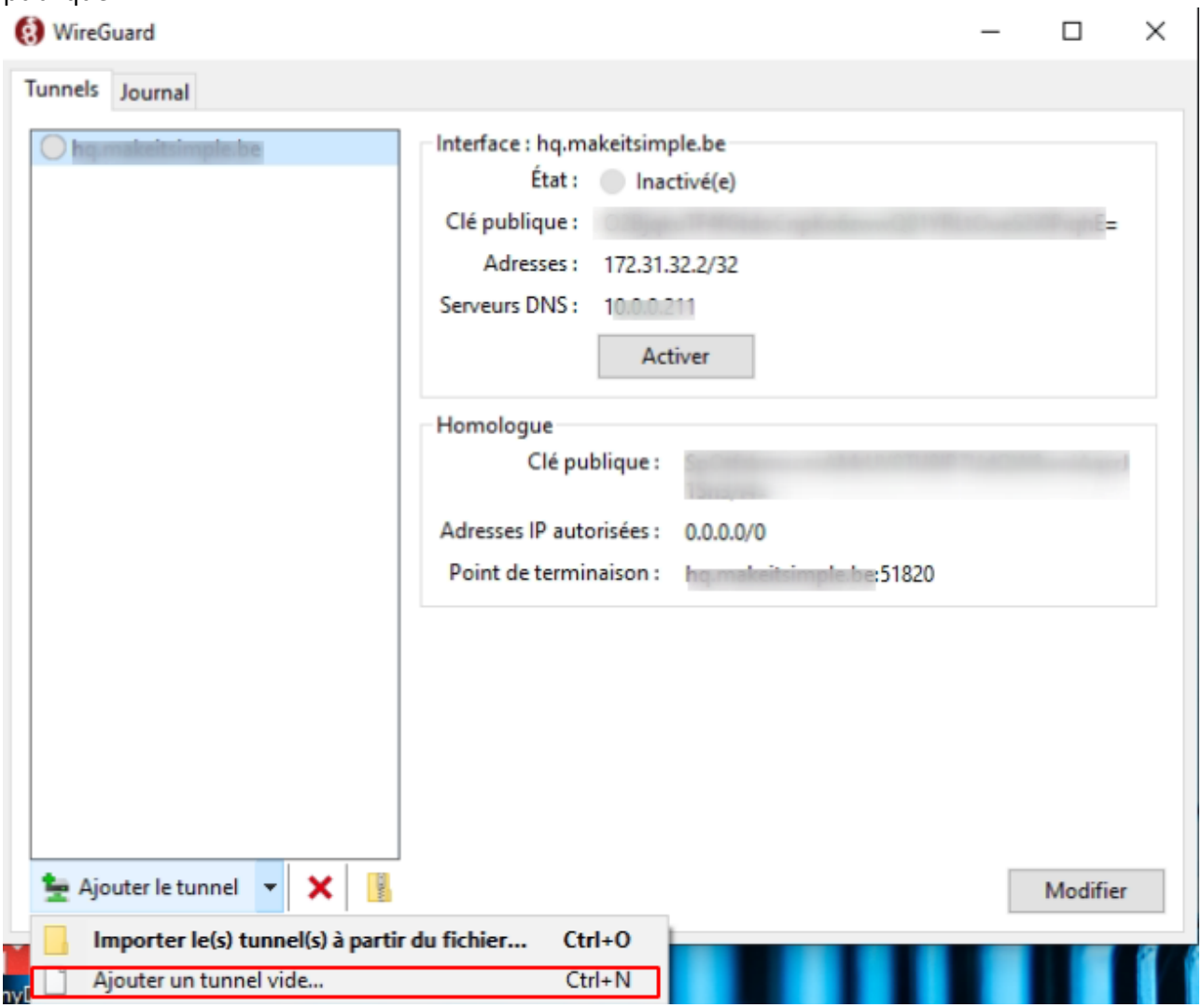
4. Toujours dans Firewall → NAT → Sortant, ajouter une règle fixe avec les propriétés suivantes:
    1. Interface WAN
    2. Source address “votre interface wireguard NET”
    3. Translation / destination: Wan Addresse



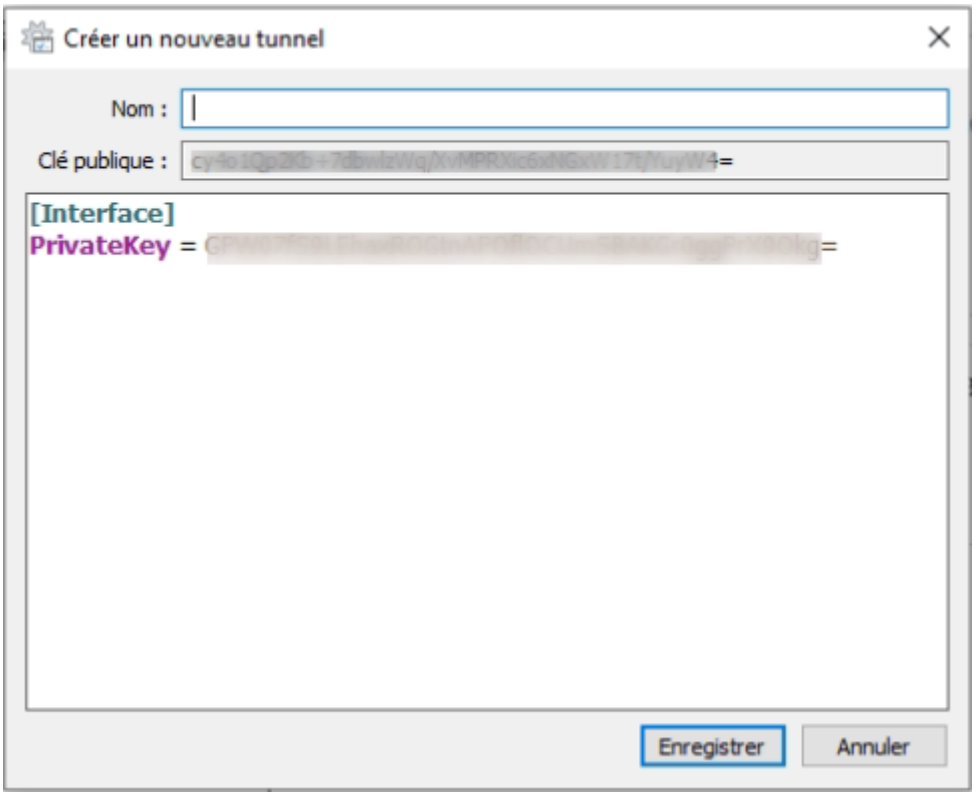
Côté client

Configuration d'un client Windows en mode RoadWarrior

1. Dans le client Windows, créer un nouveau tunnel vide. Il créera directement une clé privée et publique



2. Récupérer la clé publique pour la configuration du Peer/Endpoint dans OpenVPN



3. Ajouter les éléments suivant après le privatekey

```
Address = 172.31.33.2/32
DNS = 10.0.0.211

[Peer]
PublicKey = LA_CLE_PUBLIQUE_DU_SERVEUR_OPNSENSE
AllowedIPs = 0.0.0.0/0
Endpoint = LADRESSE_DU_SERVEUR_OPNSENSE:51820
```

Sources

- https://docs.opnsense.org/manual/how-tos/wireguard-client.html