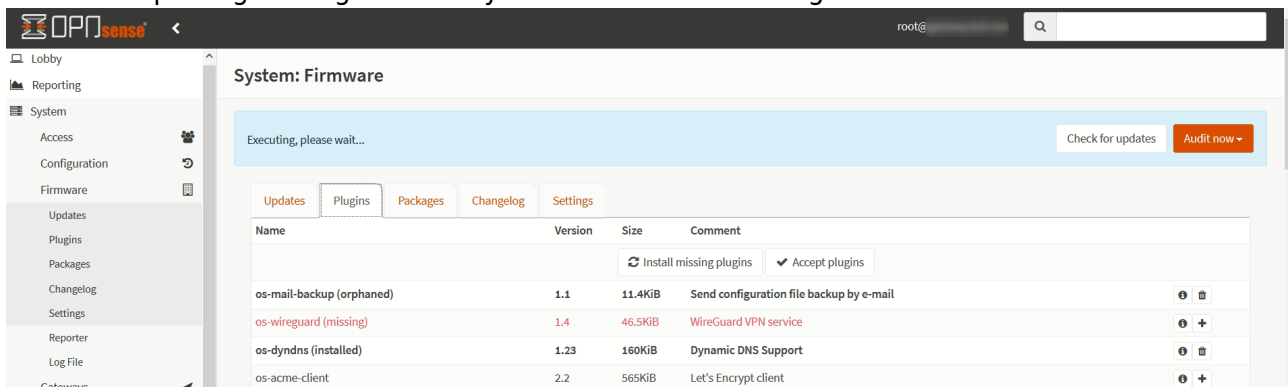


OPNSense : Wireguard VPN

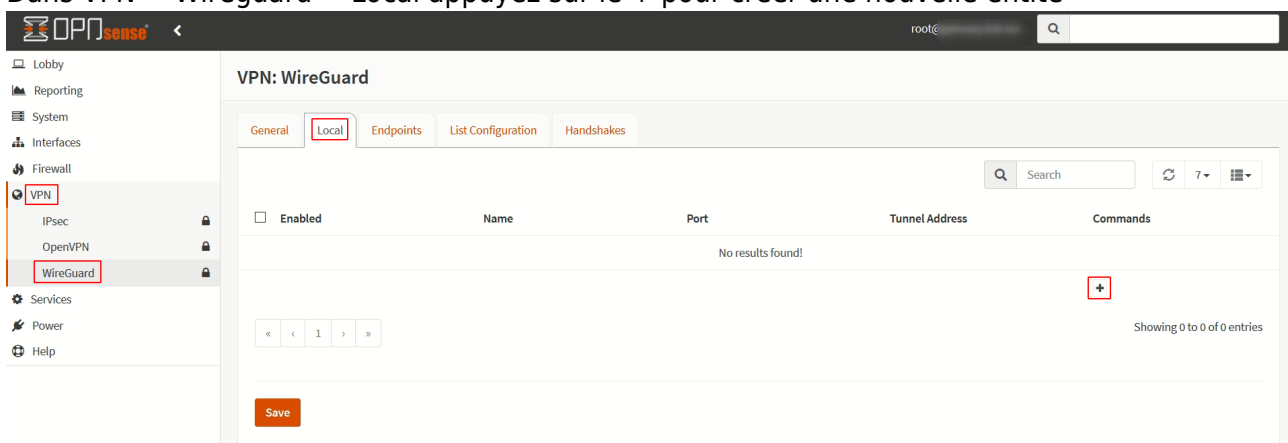
Côté OPNSENSE

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 utiliser
 4. Tunnel address: Définir un subnet qui autorise la communication entre l'entité et le Peer. De préférence un CDIR 24
 5. Peer: On devra retourner et choisir le Peer autorisé une fois créé

Edit Local Configuration ✕

advanced mode full help 

Enabled

Name

Instance 0

Public Key

Private Key

Listen Port

DNS Server ✕
✕ Clear All

Tunnel Address ✕
✕ Clear All

Peers ▼
✕ Clear All

Disable Routes


Cancel Save

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 clé 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 CIDR 32
5. Enpoint Address & Enpoint Port: si il s'agit d'une configuration en RoadWarrior, ces deux champs peuvent rester vide

Edit Endpoint ✕

advanced mode full help 

Enabled

Name

Public Key

Shared Secret

Allowed IPs ✕
✕ Clear All

Endpoint Address

Endpoint Port

Keepalive
Set persistent keepalive interval.

Cancel Save

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

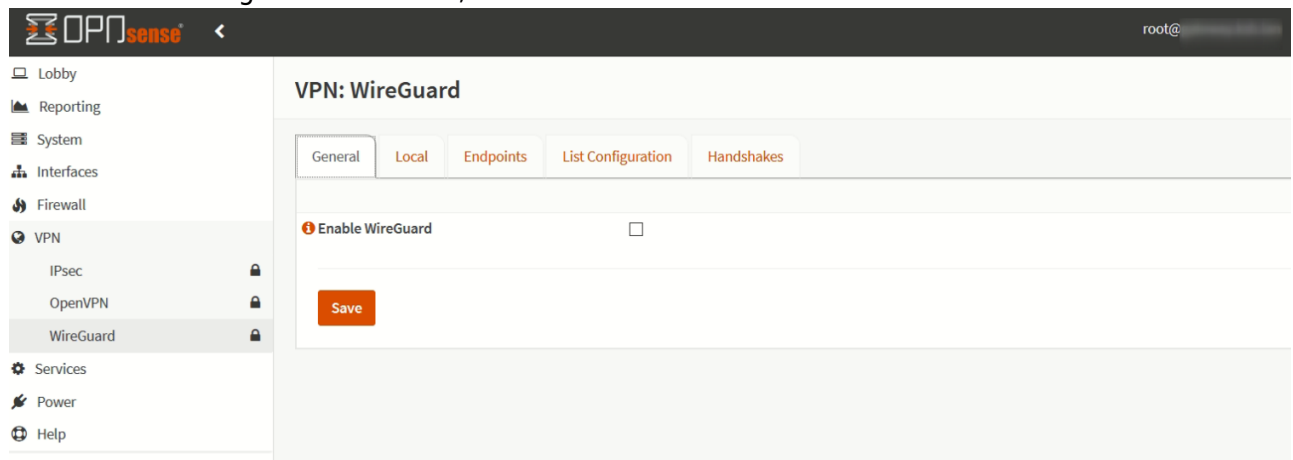
distant.

Edit Local Configuration

advanced mode full help

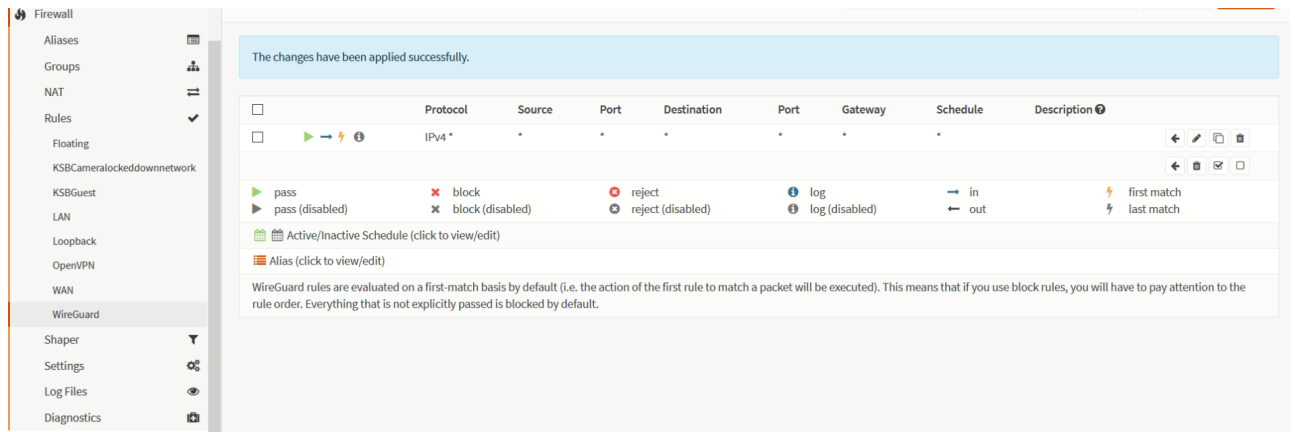
Enabled	<input checked="" type="checkbox"/>
Name	<input type="text" value="Test"/>
Instance	0
Public Key	<input type="text" value="-----BEGIN PUBLIC KEY-----"/>
Private Key	<input type="text" value="-----BEGIN PRIVATE KEY-----"/>
Listen Port	<input type="text" value="51820"/>
DNS Server	<input type="text" value="8.8.8.8"/> Clear All
Tunnel Address	<input type="text" value="172.31.33.1/24"/> Clear All
Peers	<input type="text" value="PortableVincent"/> Clear All
Disable Routes	<input type="checkbox"/>

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



Règles Firewall

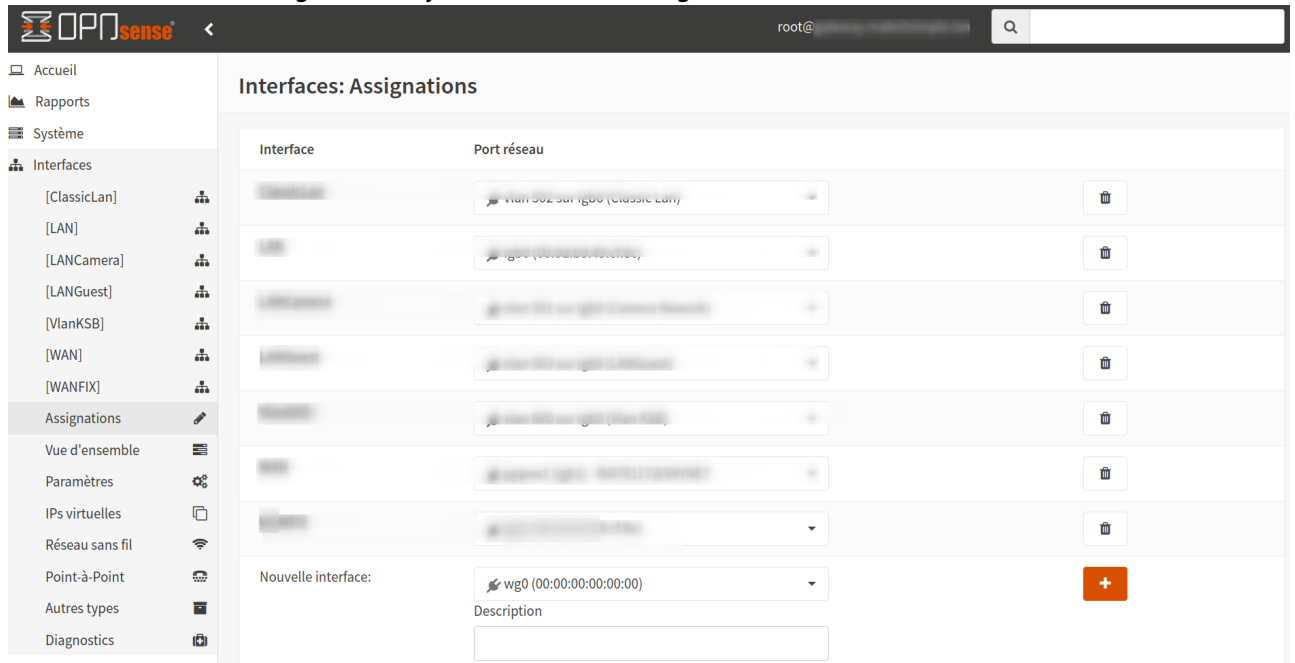
1. Prévoir une règle dans Firewall → Rules → WireGuard pour autoriser le trafic désiré. Un Accept All est envisageable pour un test.



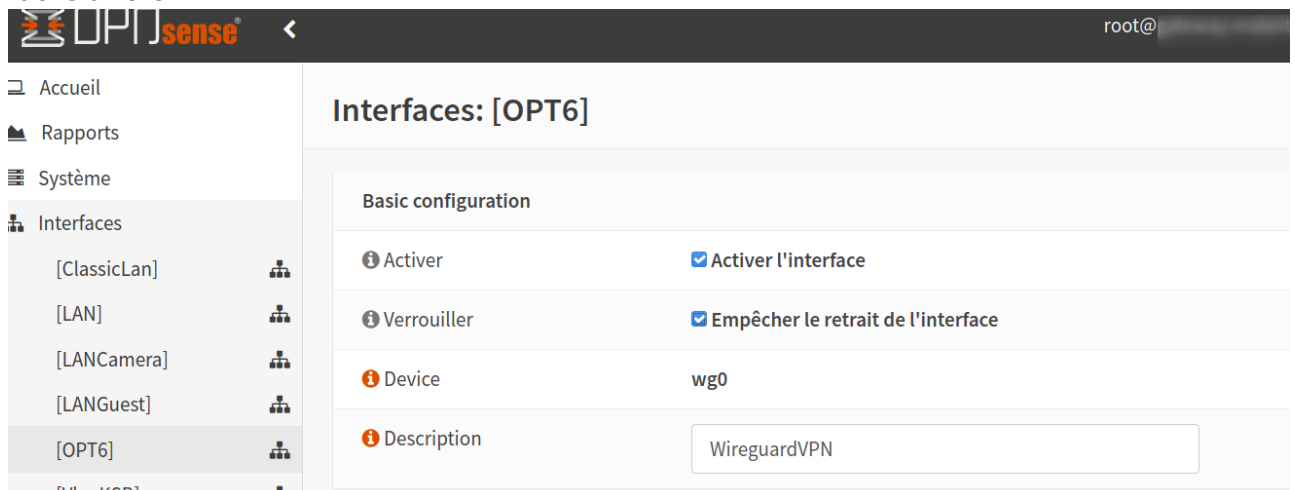
2. Dans Firewall → Rules → Wan: créer une règle qui accepte le port UDP 51820 sur ce firewall

Autoriser le trafic Internet pour les clients Wireguard

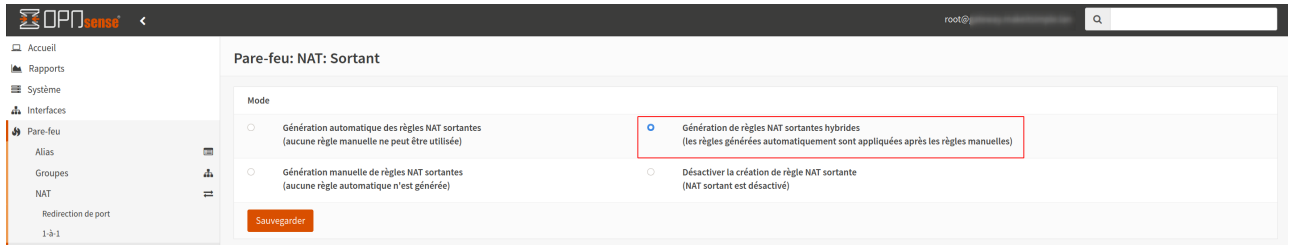
1. Dans Interface → Assignation, ajouter l'interface wg0



2. Aller dans l'interface fraîchement 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 Adresse

Pare-feu: NAT: Sortant

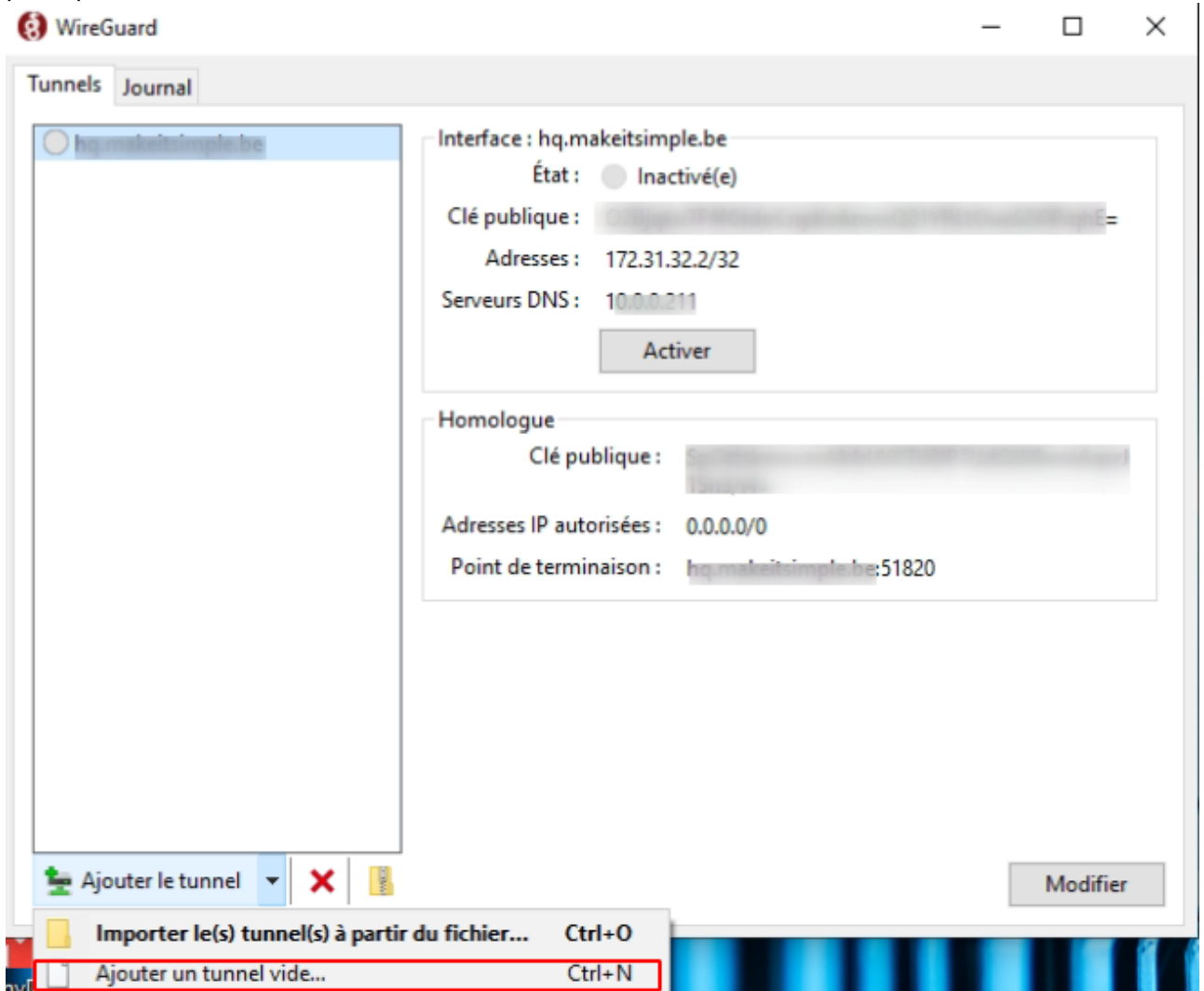
Modifier l'entrée NAT sortante avancée

<input checked="" type="checkbox"/> Désactivé	<input type="checkbox"/> Désactiver cette règle
<input checked="" type="checkbox"/> Ne pas effectuer de NAT	<input type="checkbox"/>
<input checked="" type="checkbox"/> Interface	WAN
<input checked="" type="checkbox"/> Version TCP/IP	IPv4
<input checked="" type="checkbox"/> Protocole	any
<input checked="" type="checkbox"/> Inverser la source	<input type="checkbox"/>
<input checked="" type="checkbox"/> Adresse source	WireguardVPN net
<input checked="" type="checkbox"/> Port source	any
<input checked="" type="checkbox"/> Inverser la destination	<input type="checkbox"/>
<input checked="" type="checkbox"/> Adresse de destination	any
<input checked="" type="checkbox"/> Port de destination	any
<input checked="" type="checkbox"/> Translation / destination	WAN adresse

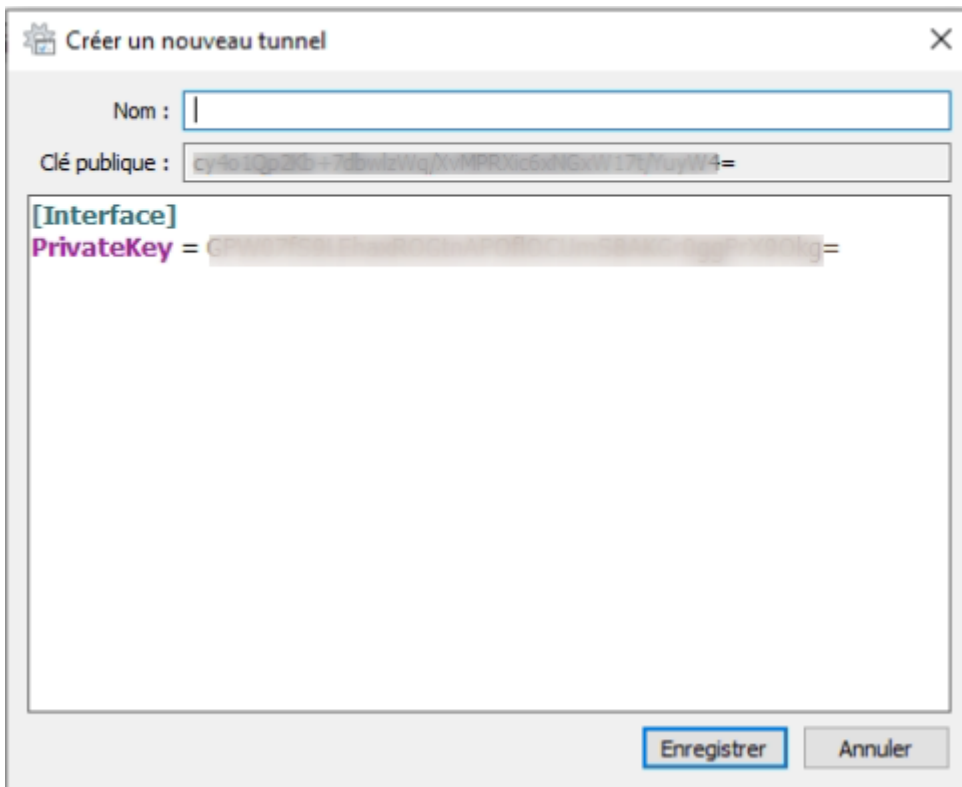
Côté client

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>

From: <https://wiki.makeitsimple.be/> - makeITsimple wiki

Permanent link: <https://wiki.makeitsimple.be/doku.php?id=reseau:opnsense:wireguard&rev=1610643799>

Last update: 2021/06/20 09:42

