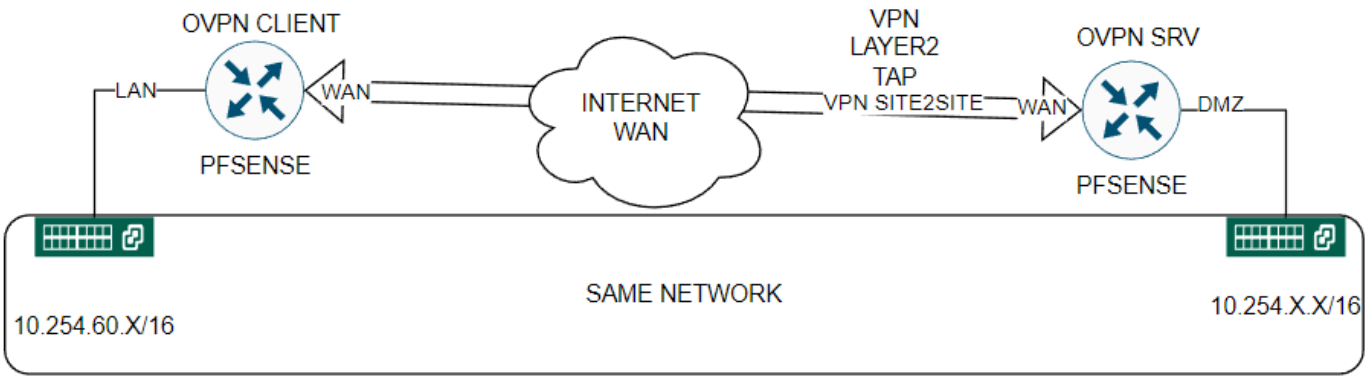
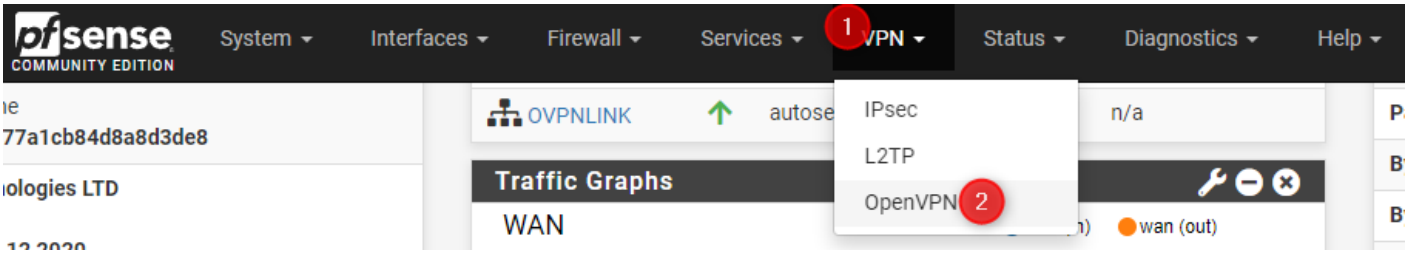
pfSense VPN site to site avec OPENVPN en L2 TAP en Shared KEY

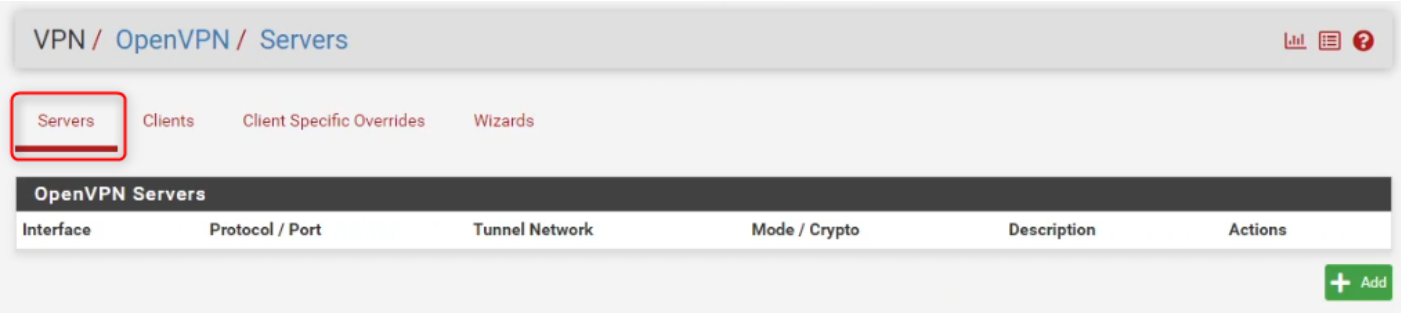


PARTIE SERVEUR

Mise en place du serveur VPN sur pfSense



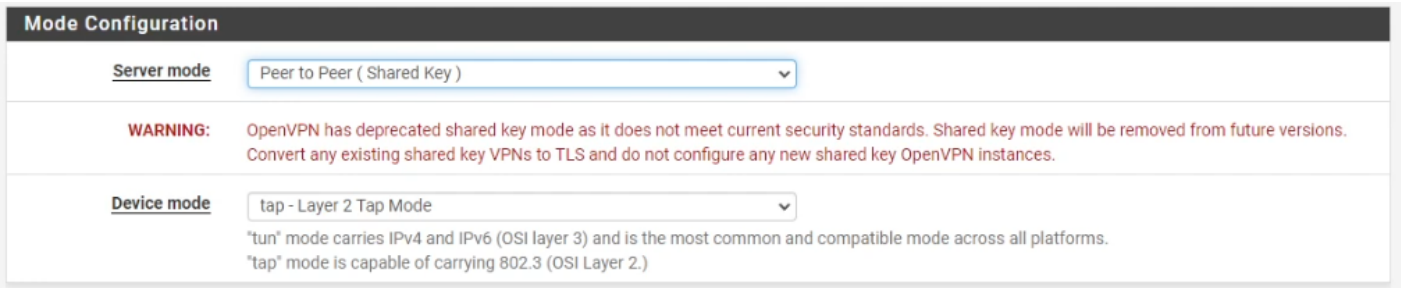
Configuration du openVPN "Server":



Sélectionnez "tap - Layer 2 Tap Mode" dans le "Mode Configuration"

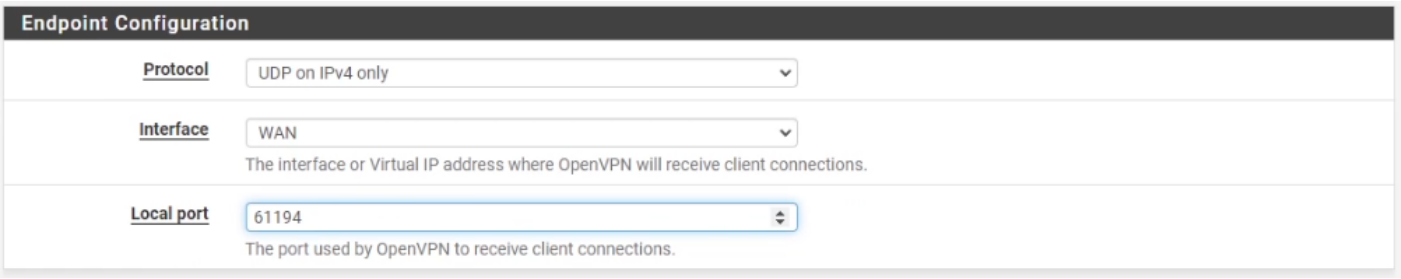
Modifier le "Server mode" en "Peer to Peer (Shared Key)"

(attention cette configuration ne sera plus supportée sur les futures versions il est recommandé un certificat)



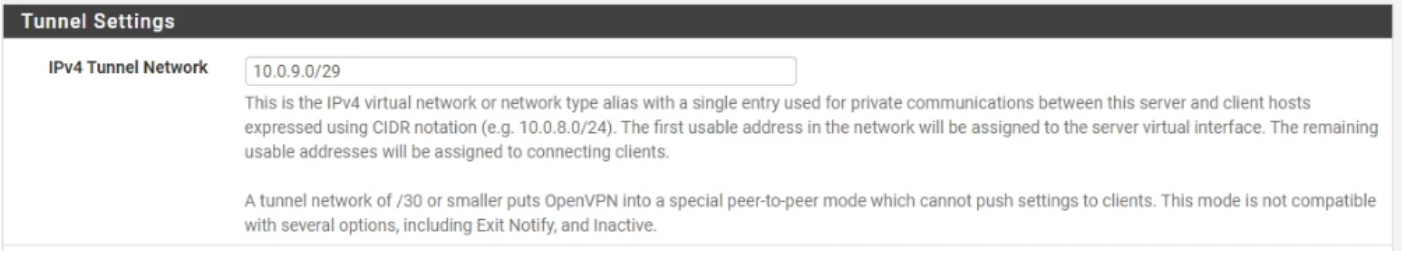
Configuration du port utilisé pour le VPN dans "Endpoint Configuration"

(Il est recommandé de modifier le port par défaut)

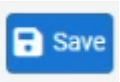


Configuration "IPv4 Tunnel Network" du "Tunnel Settings"

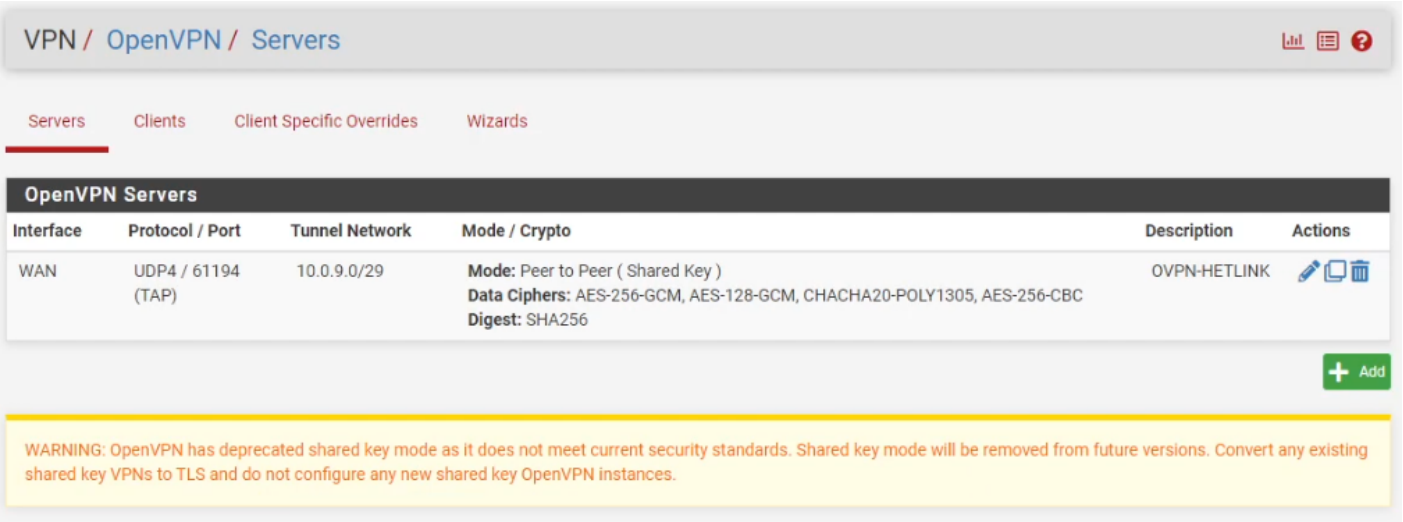
(ce réseau va être utilisé uniquement pour openVPN et n'aura pas d'impact sur le réseau)



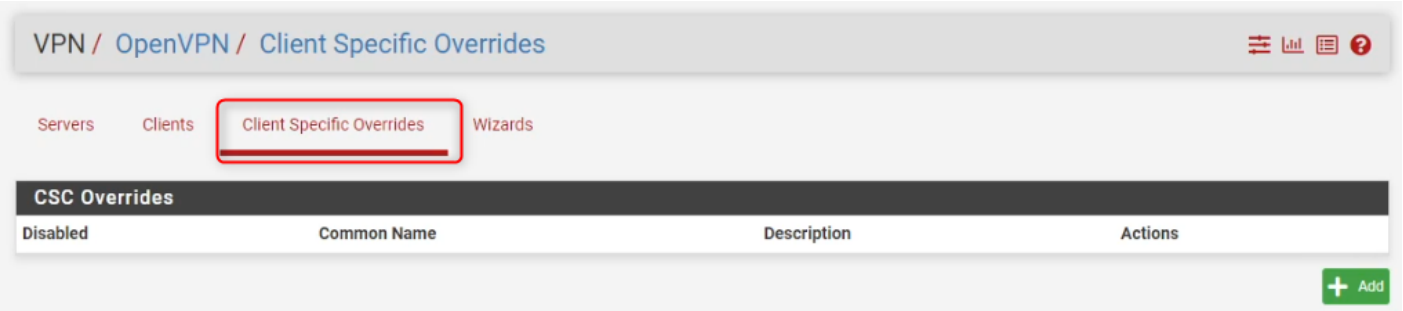
Pouvez sauvegarder la configuration



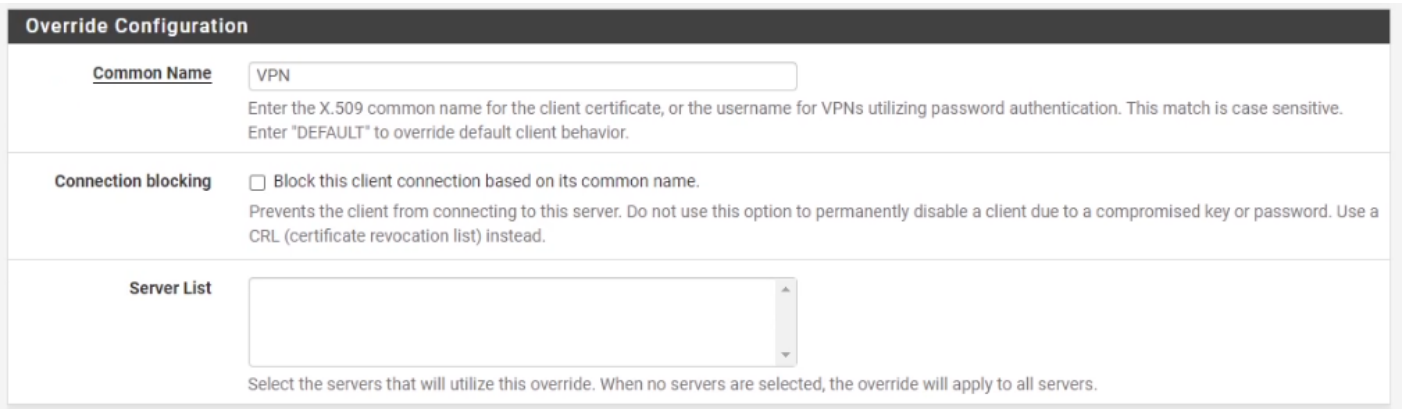
Une fois sauvegardée ça nous donne :



Configuration du openVPN "Client Specific Overrides":



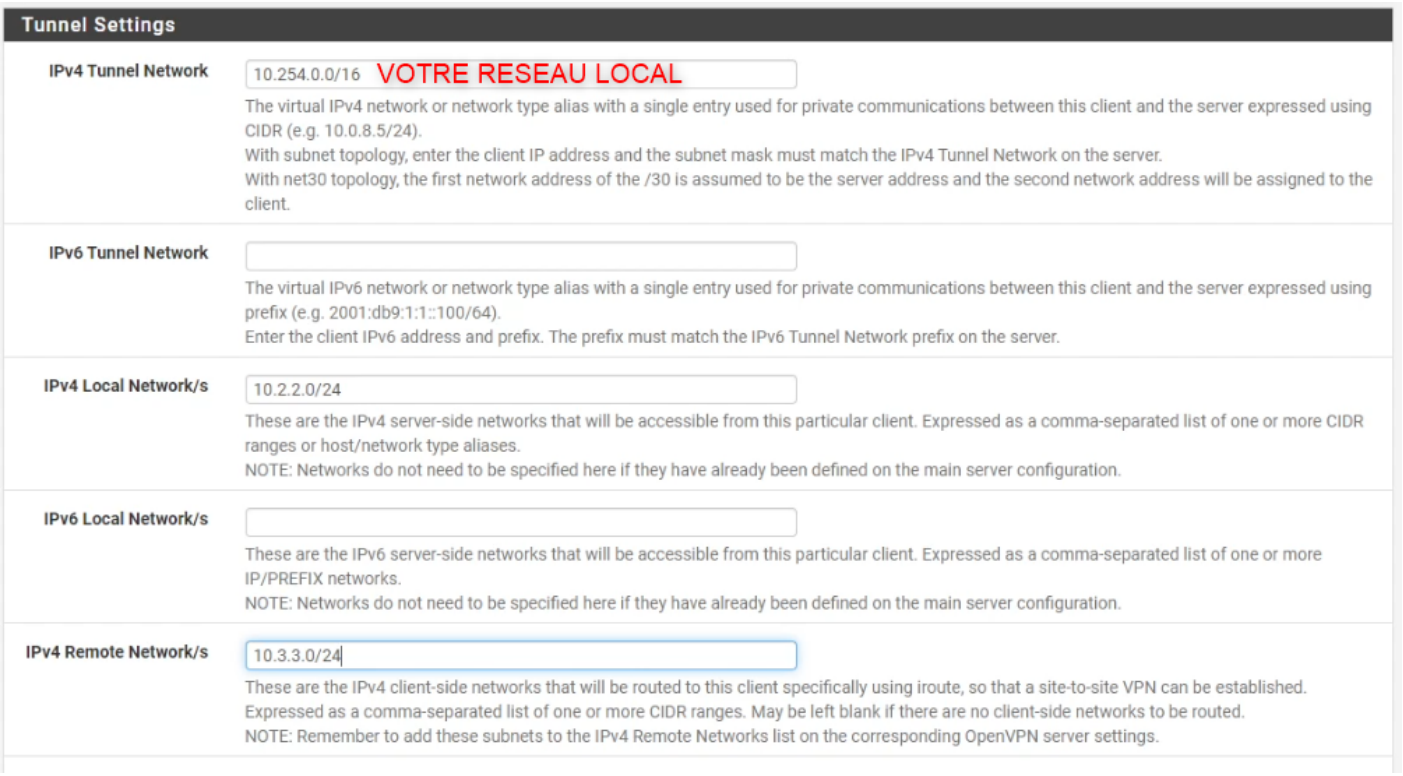
Donner un nom "VPN" dans "Commun Name" dans "Override Configuration"



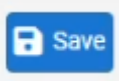
Configuration "IPv4 Tunnel Network" du "Tunnel Settings"

Pour "IPv4 Tunnel Network" mettez l'adresse IP de votre réseau local qui sera lié à votre VPN

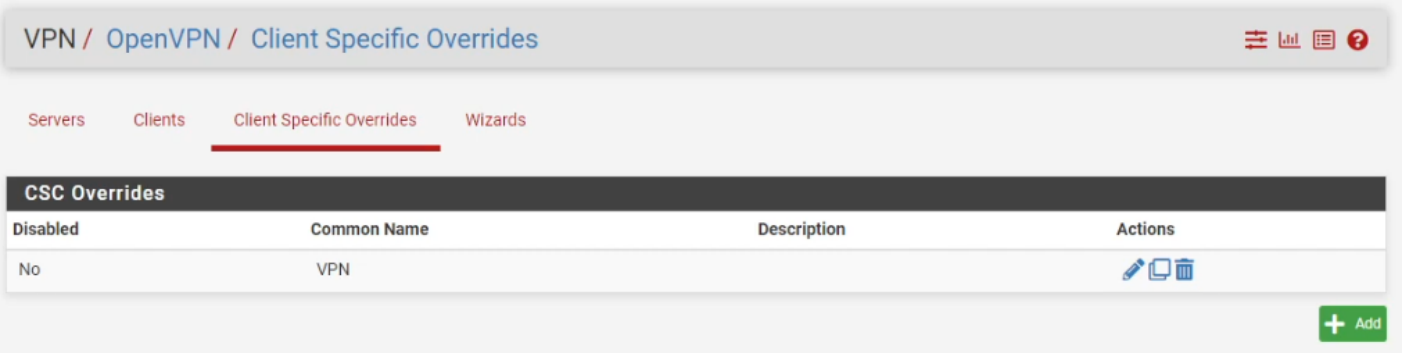
(pour le reste vous pouvez le laisser comme dans le tutoriel ça n'aura pas d'impact sur le réseau)



Pouvez sauvegarder la configuration

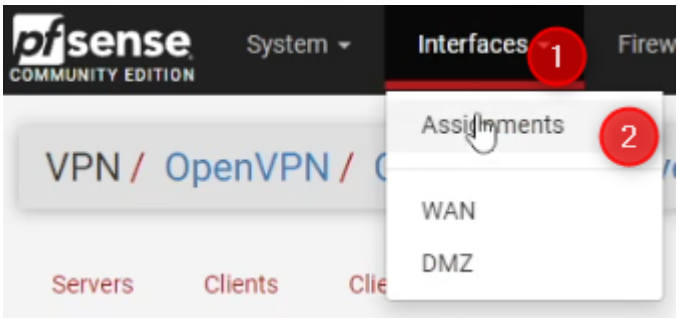


Une fois sauvegardée ça nous donne :

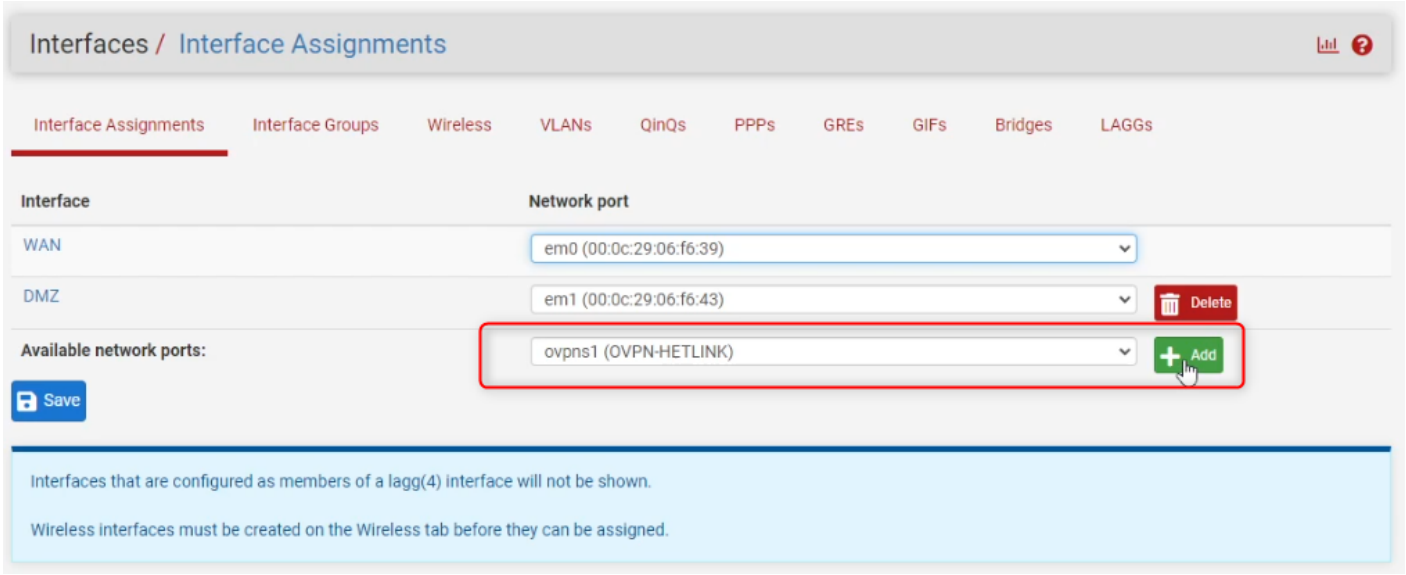


Configurations des interfaces réseau

Allez dans "Interfaces" et ensuite dans "Assignments"

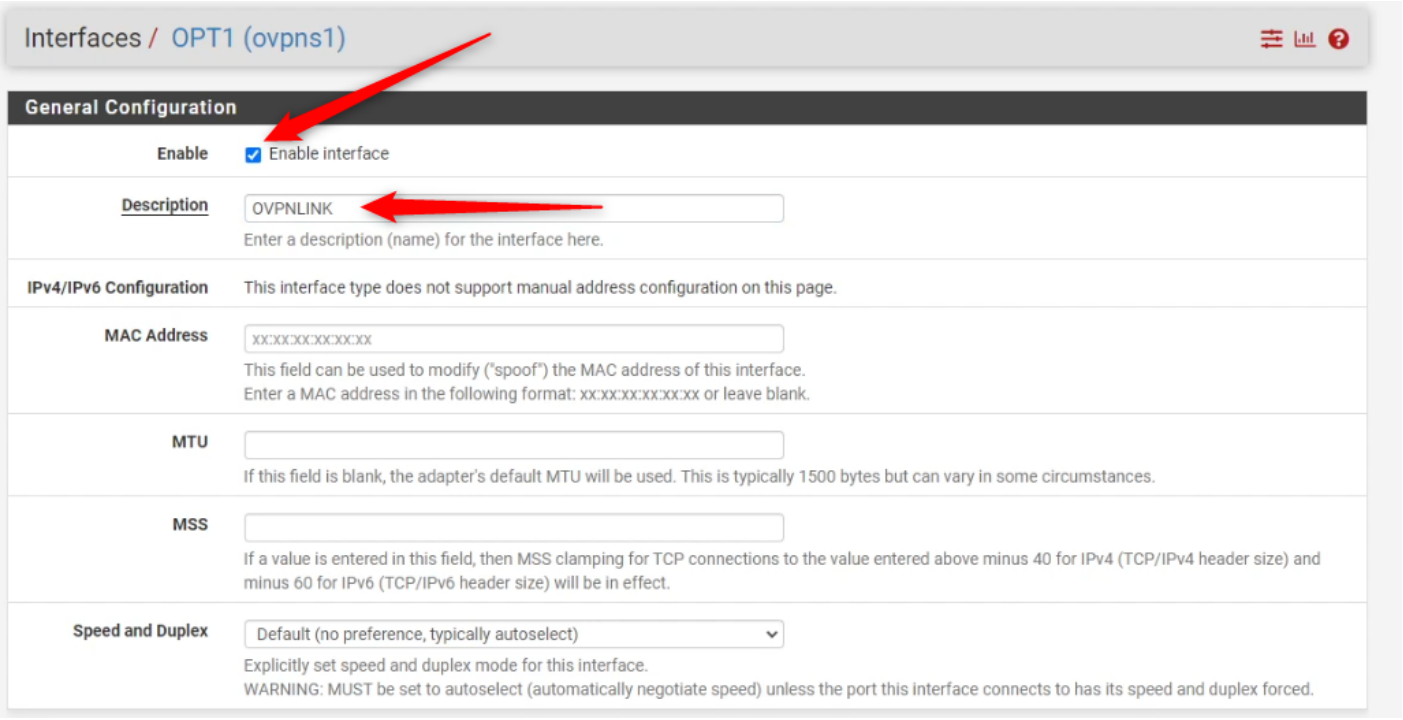


Ajouter la nouvelle interface disponible liée au VPN "ovpns1"

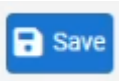


Aller sur la nouvelle interface "OPT1"

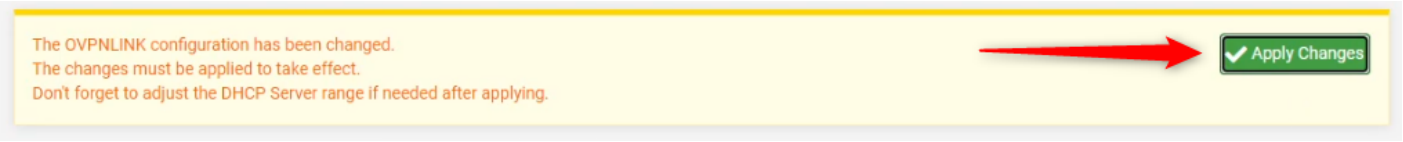
Activer l'interface via "Enable interface" et ajouter une description (le nom)

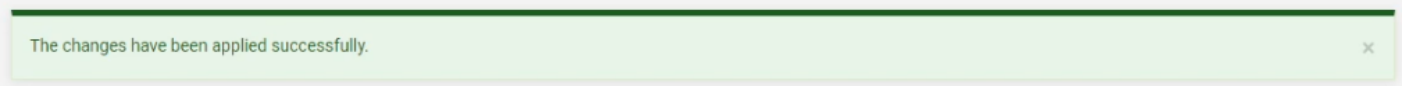


Pouvez sauvegarder la configuration

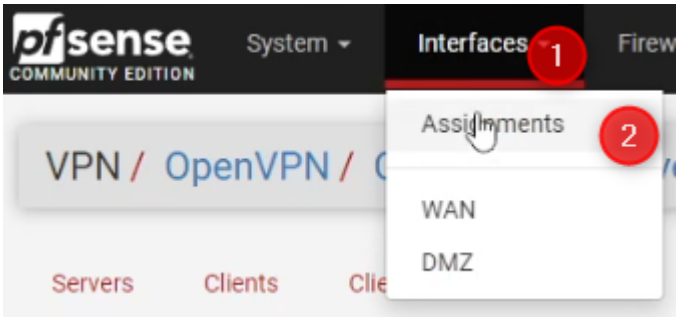


Appliquer les changements

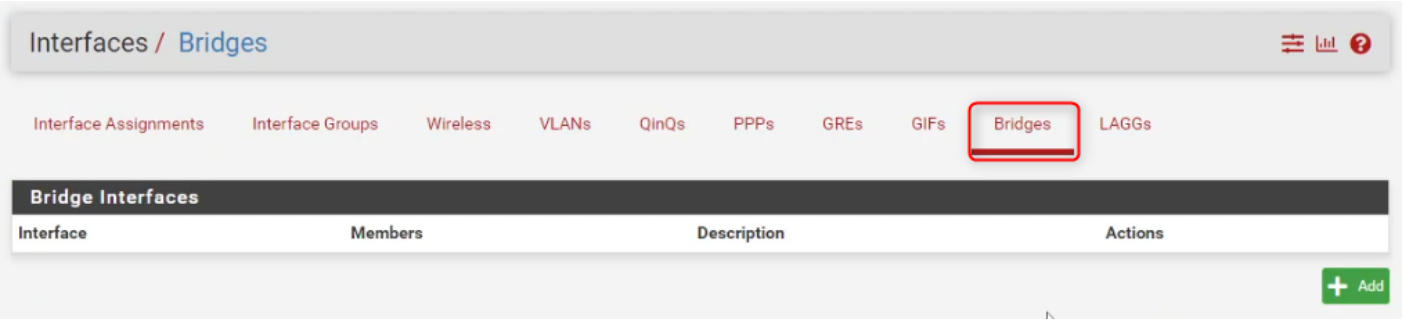




Retourner dans "Interfaces" et ensuite dans "Assignments"

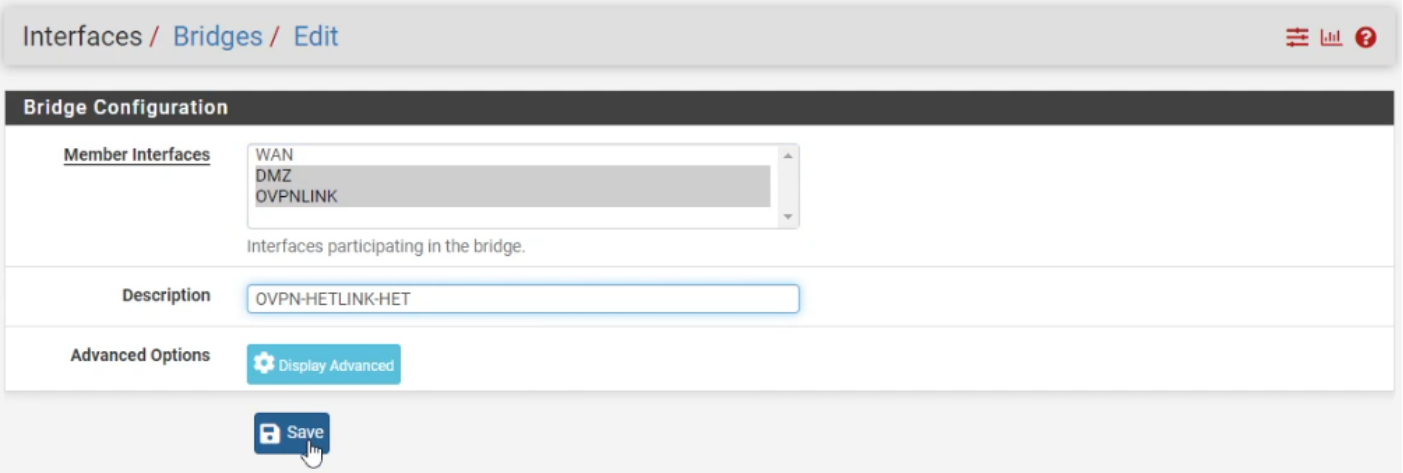


Allez dans la partie "Bridges"

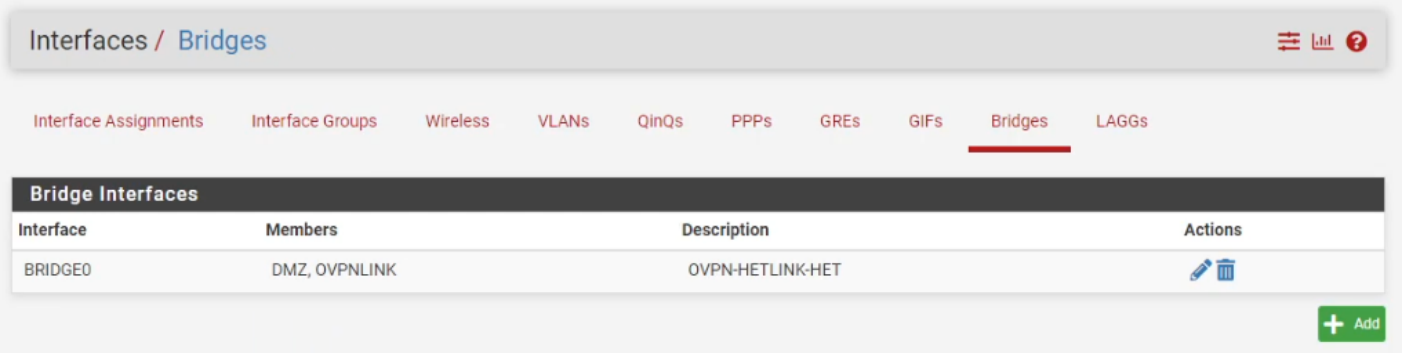


Créer un "Bridges" entre l'interface du réseau local et l'interface du VPN

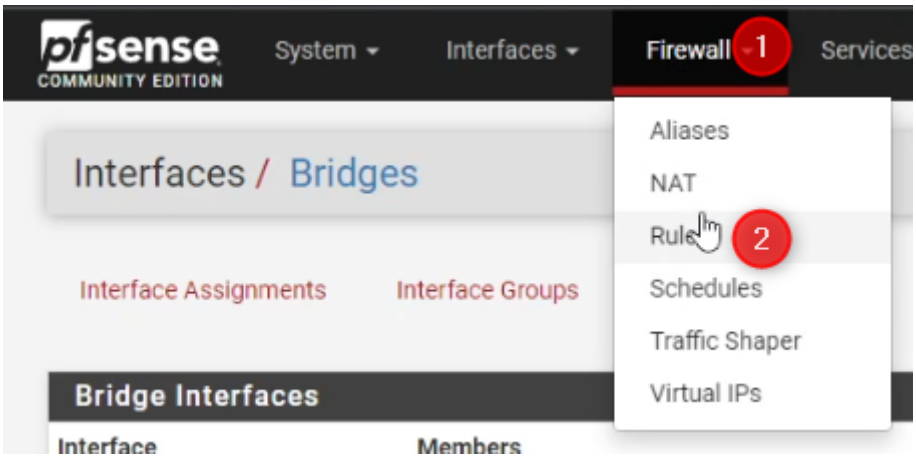
(pour cela vous avez juste à sélectionner les deux interfaces réseaux)



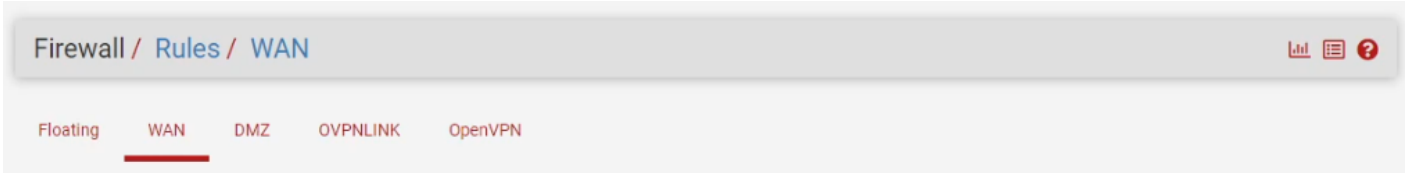
Ce qui nous donne cela:



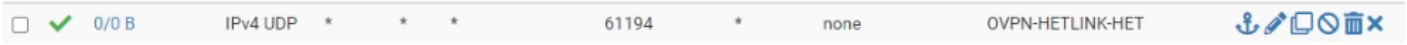
Configuration des règles de "Firewall" dans "Firewall" et ensuite dans "Rules"



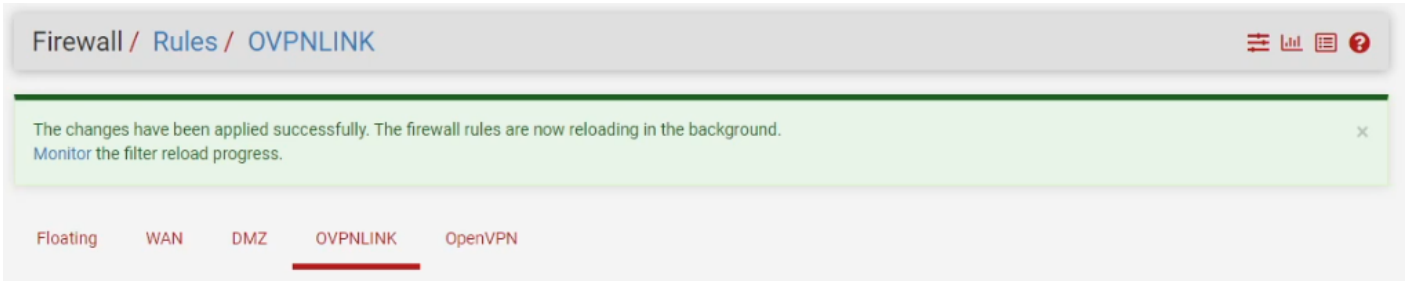
WAN:



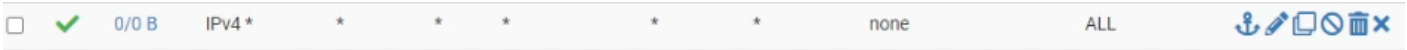
Ajout de la règle pour faire passer le trafic du VPN sur Internet (WAN)



OVPNLINK:

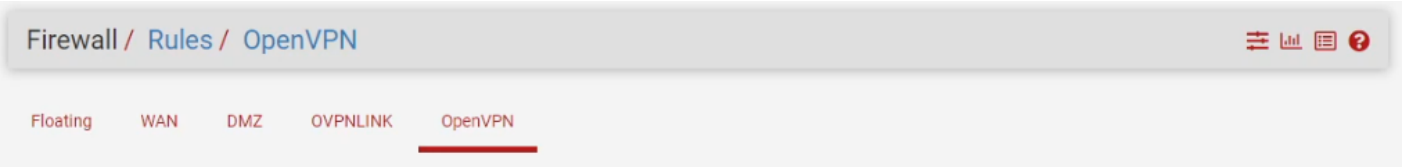


Ajout de la règle pour faire passer le trafic entre le VPN et le réseau



Ajout de la règle pour bloquer le trafic du DHCP sur le réseau via le VPN

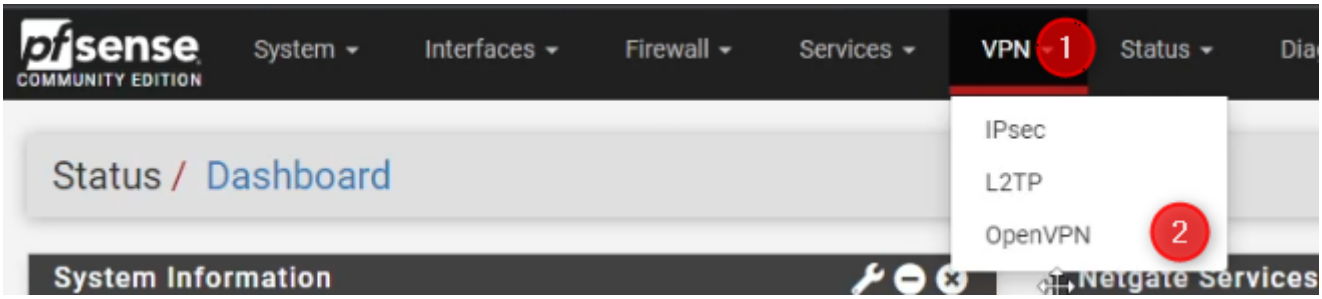
OpenVPN:



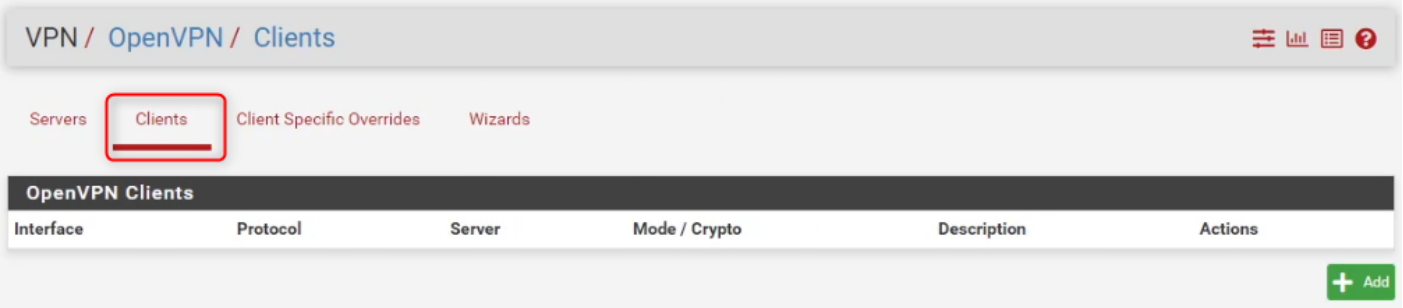
Ajout de la règle pour faire passer le trafic entre le VPN et le réseau

PARTIE CLIENT

Mise en place du client VPN sur pfSense



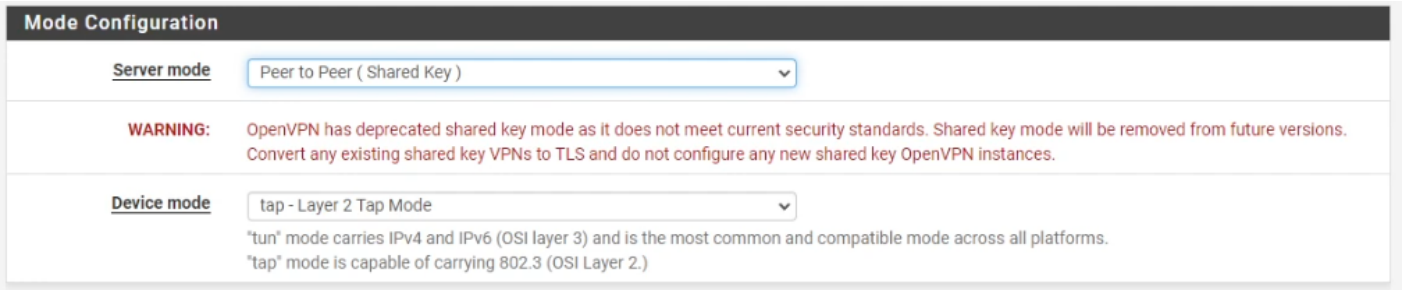
Configuration du openVPN "Clients":



Sélectionnez "tap - Layer 2 Tap Mode" dans le "Mode Configuration"

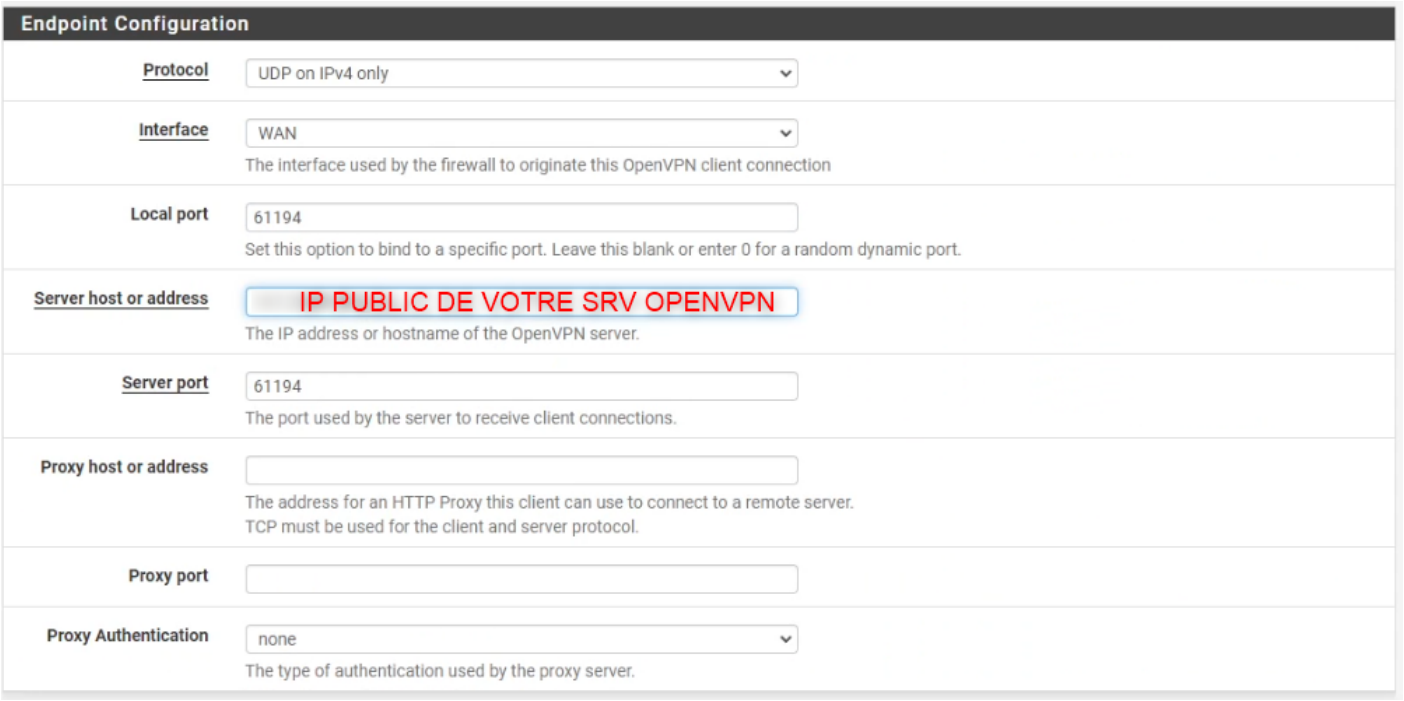
Modifier le "Server mode" en "Peer to Peer (Shared Key)"

(attention cette configuration ne sera plus supportée sur les futures versions il est recommandé un certificat)



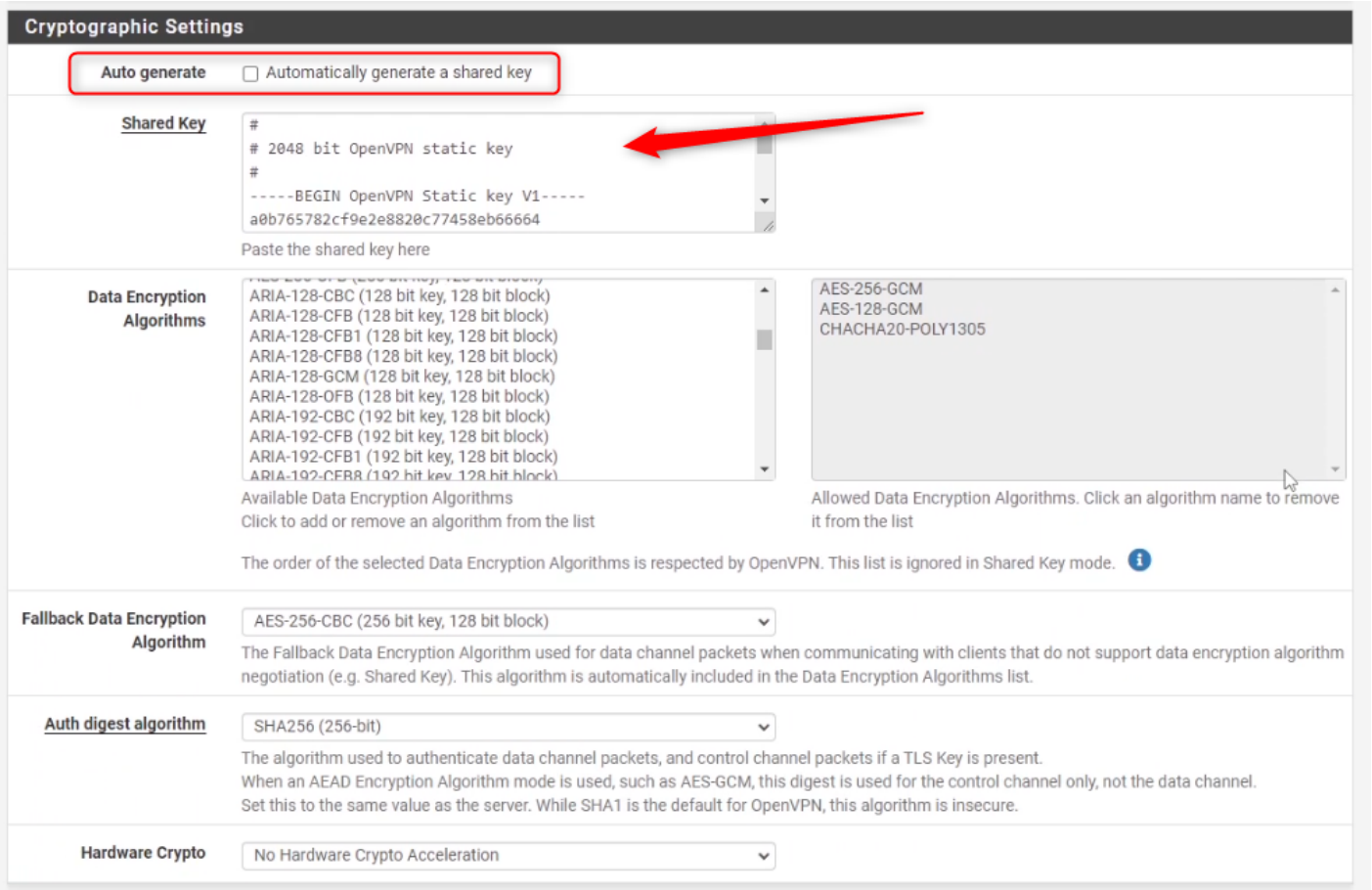
Configuration du port utilisé pour le VPN dans "Endpoint Configuration" et dans "Server host or address" mettait l'adresse IP de votre serveur openVPN.

(l'adresse IP public de votre routeur pfSense configurait auparavant)



Ajouter la clé pré partagée qui a été générée sur le serveur openVPN

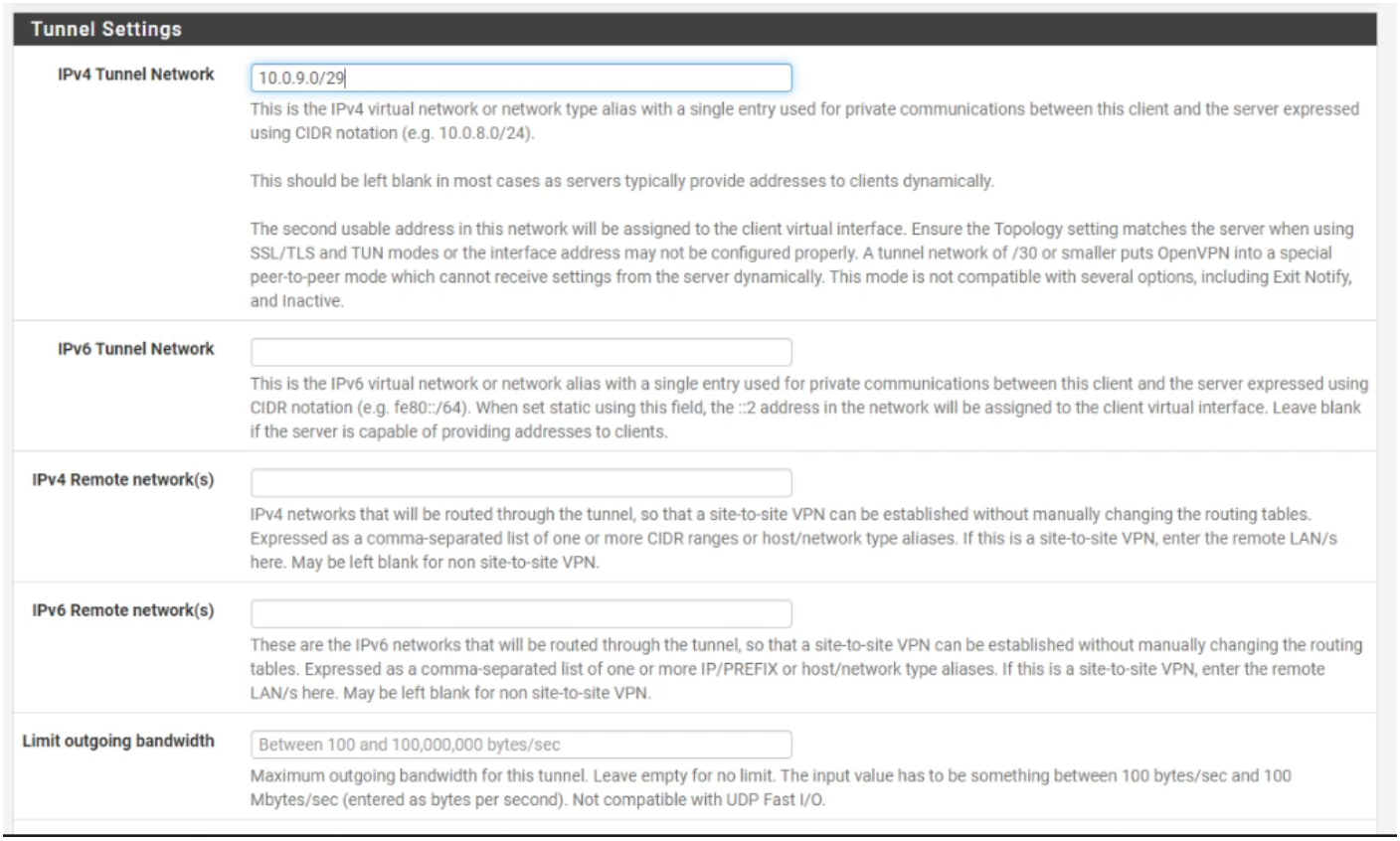
Mettez la dans "Cryptographic Settings" en suite "Shared Key"



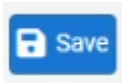
Configuration "IPv4 Tunnel Network" du "Tunnel Settings"

Pour "IPv4 Tunnel Network" mettez l'adresse IP de votre réseau local qui sera lié à votre VPN

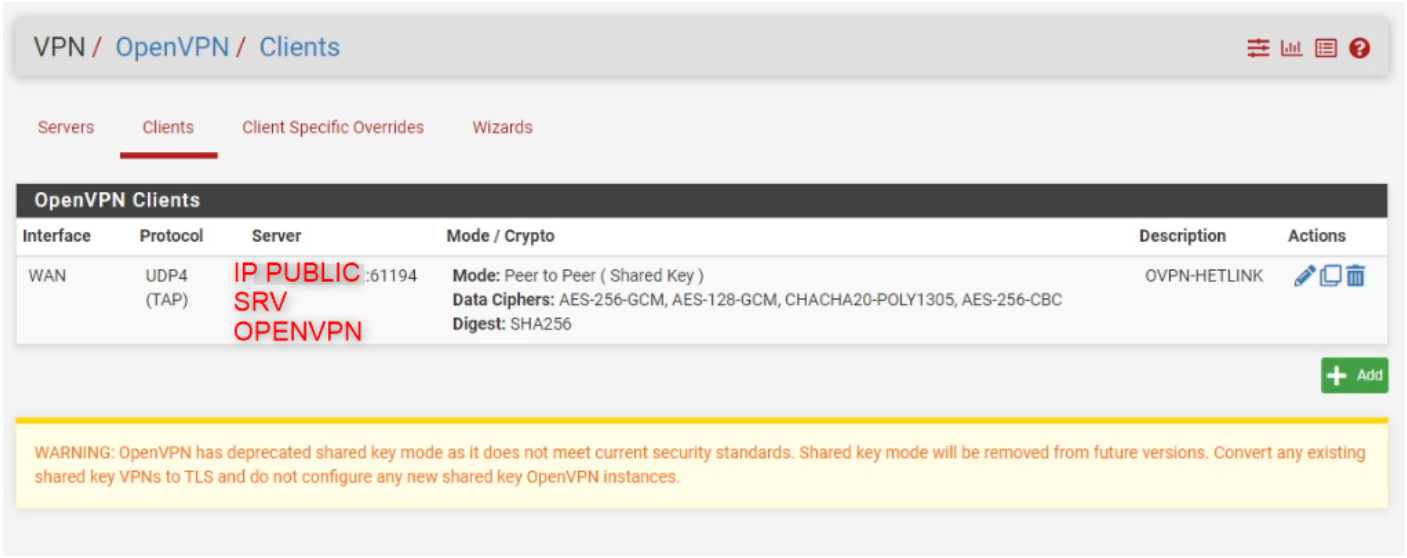
(pour le reste vous pouvez le laisser comme dans le tutoriel ça n'aura pas d'impact sur le réseau)



Pouvez sauvegarder la configuration

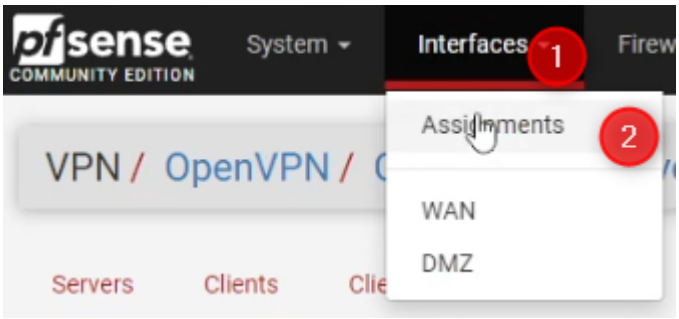


Une fois sauvegardée ça nous donne :

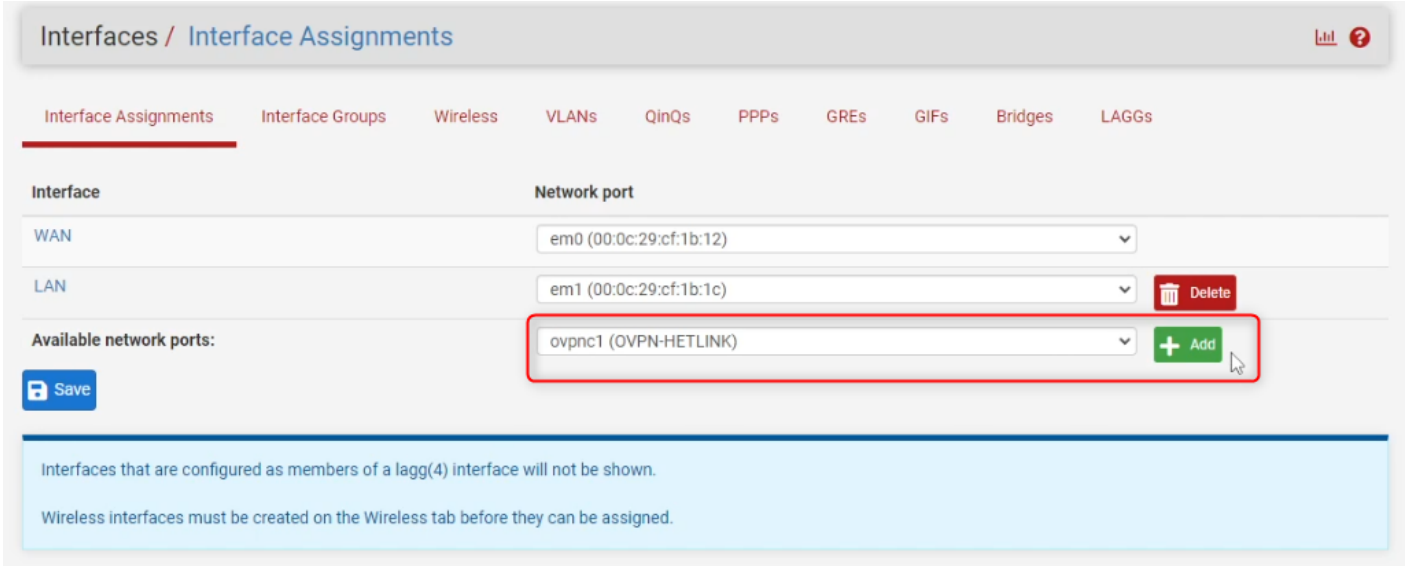


Configurations des interfaces réseau

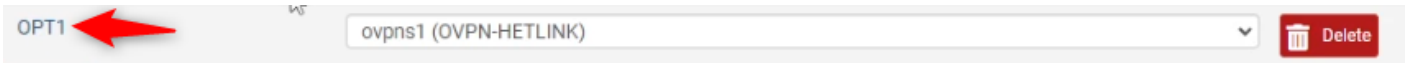
Allez dans "Interfaces" et ensuite dans "Assignments"



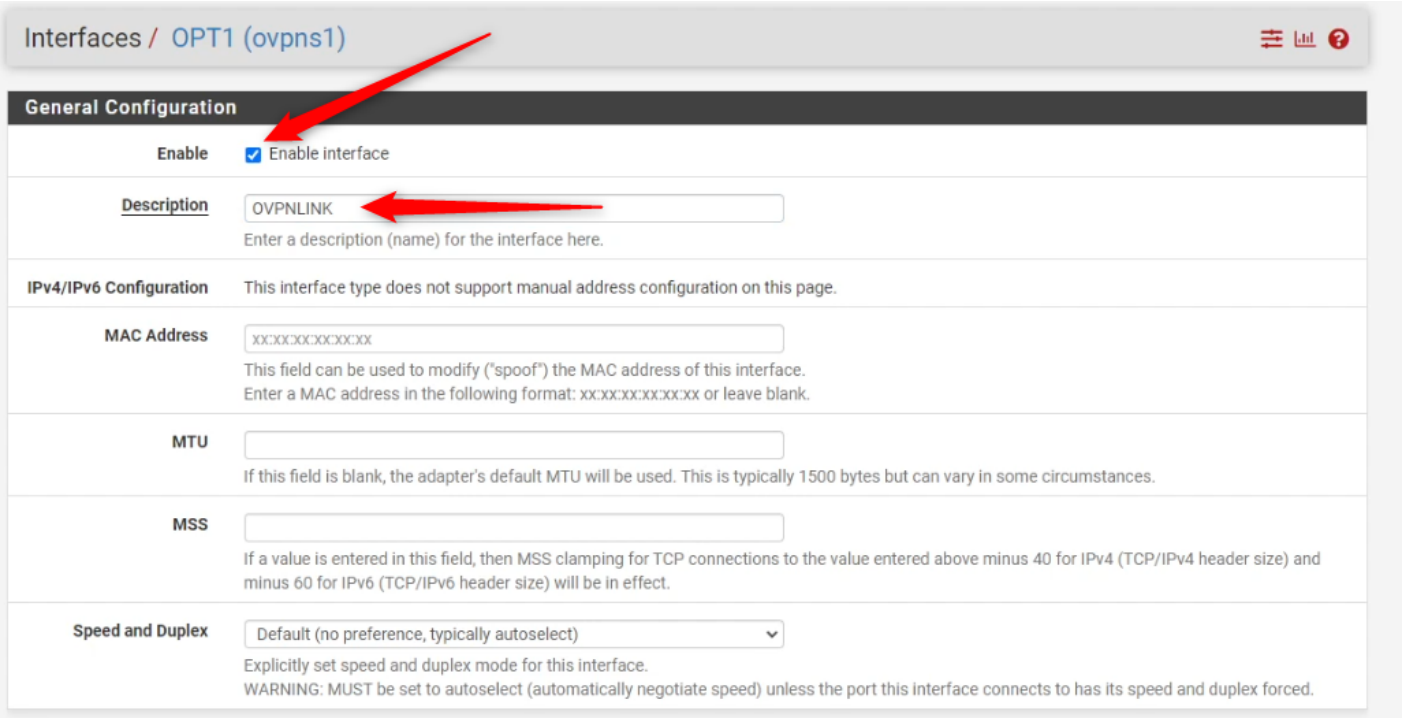
Ajouter la nouvelle interface disponible liée au VPN "ovpns1"



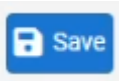
Aller sur la nouvelle interface "OPT1"



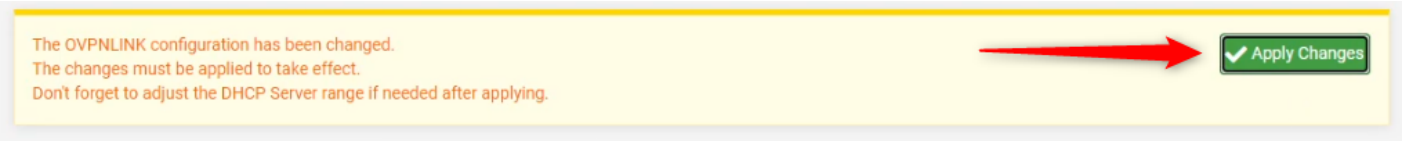
Activer l'interface via "Enable interface" et ajouter une description (le nom)

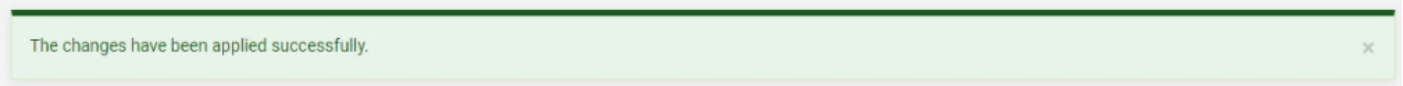


Pouvez sauvegarder la configuration

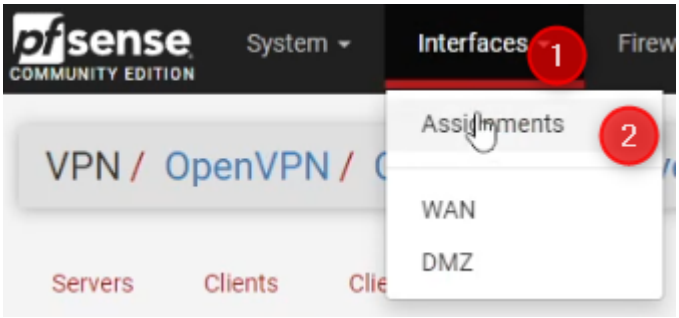


Appliquer les changements

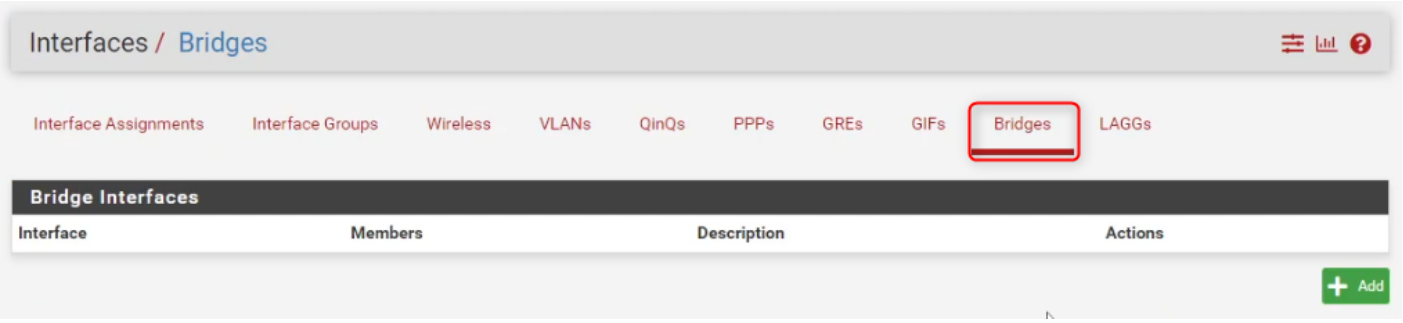




Retourner dans "Interfaces" et ensuite dans "Assignments"

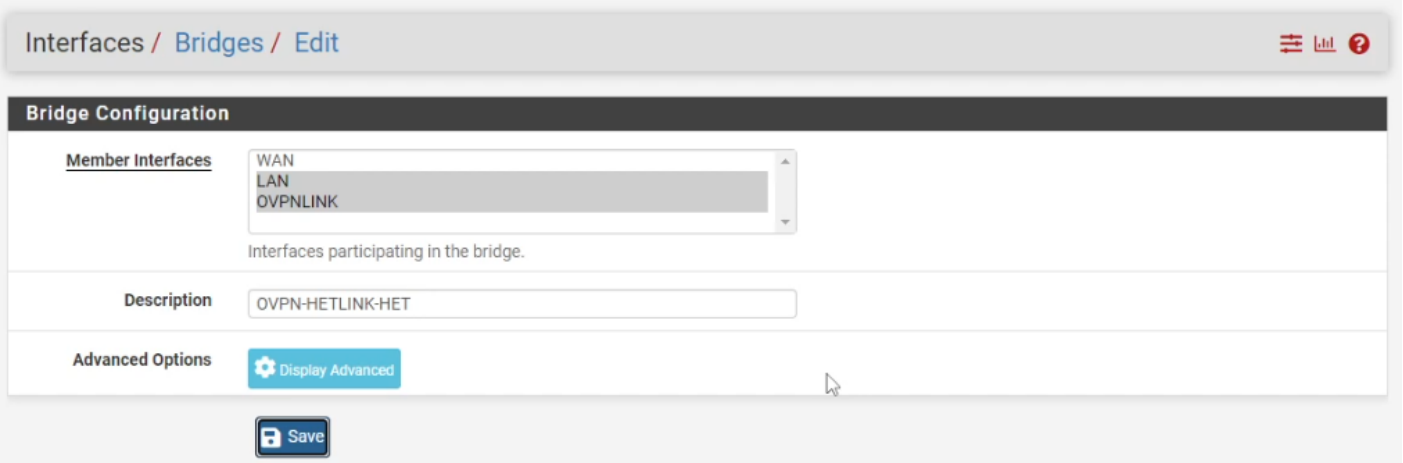


Allez dans la partie "Bridges"

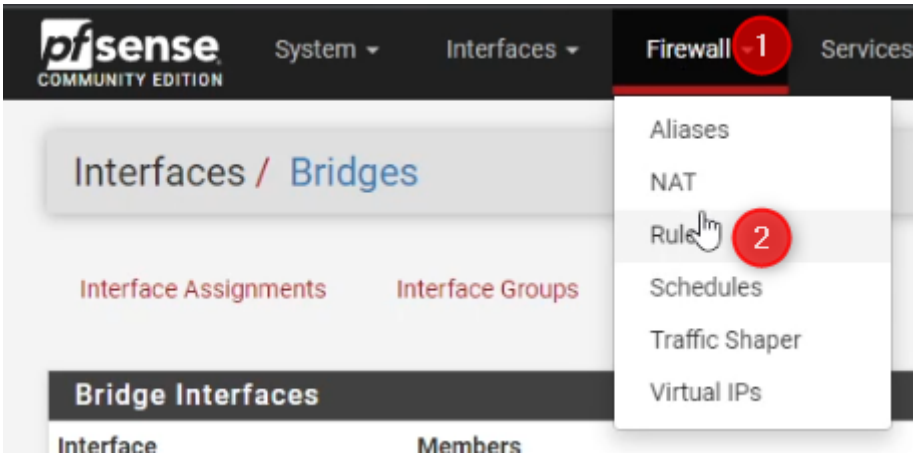


Créer un "Bridges" entre l'interface du réseau local et l'interface du VPN

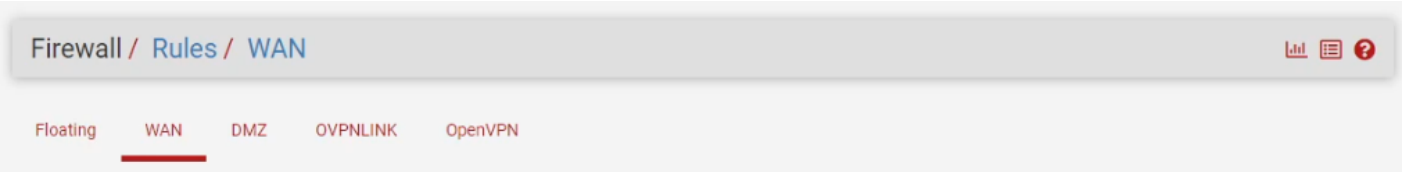
(pour cela vous avez juste à sélectionner les deux interfaces réseaux)



Configuration des règles de "Firewall" dans "Firewall" et ensuite dans "Rules"



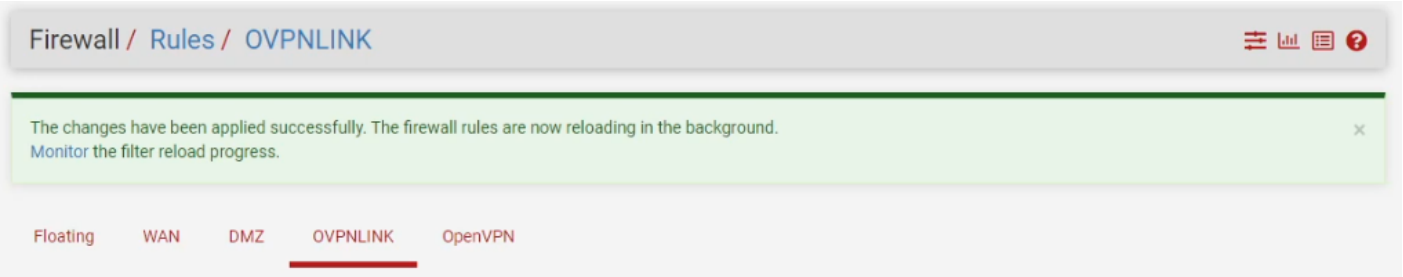
WAN:



Ajout de la règle pour faire passer le trafic du VPN sur Internet (WAN)

☐	✓	0/0 B	IPv4 UDP	*	*	*	61194	*	none	OVPN-HETLINK

OVPNLINK:



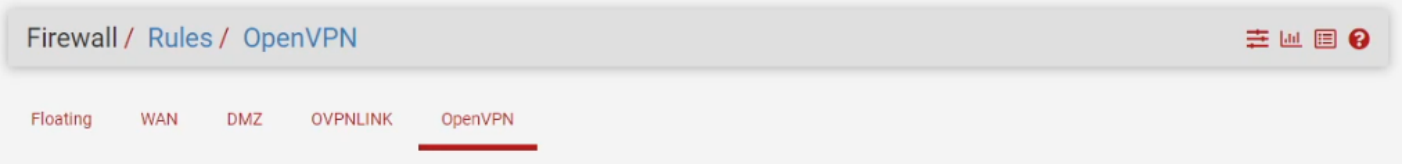
Ajout de la règle pour faire passer le trafic entre le VPN et le réseau

☐	✓	0/0 B	IPv4 *	*	*	*	*	*	none	ALL

Ajout de la règle pour bloquer le trafic du DHCP sur le réseau via le VPN

☐	✗	0/0 B	IPv4 UDP	*	*	*	67 - 68	*	none	DHCP

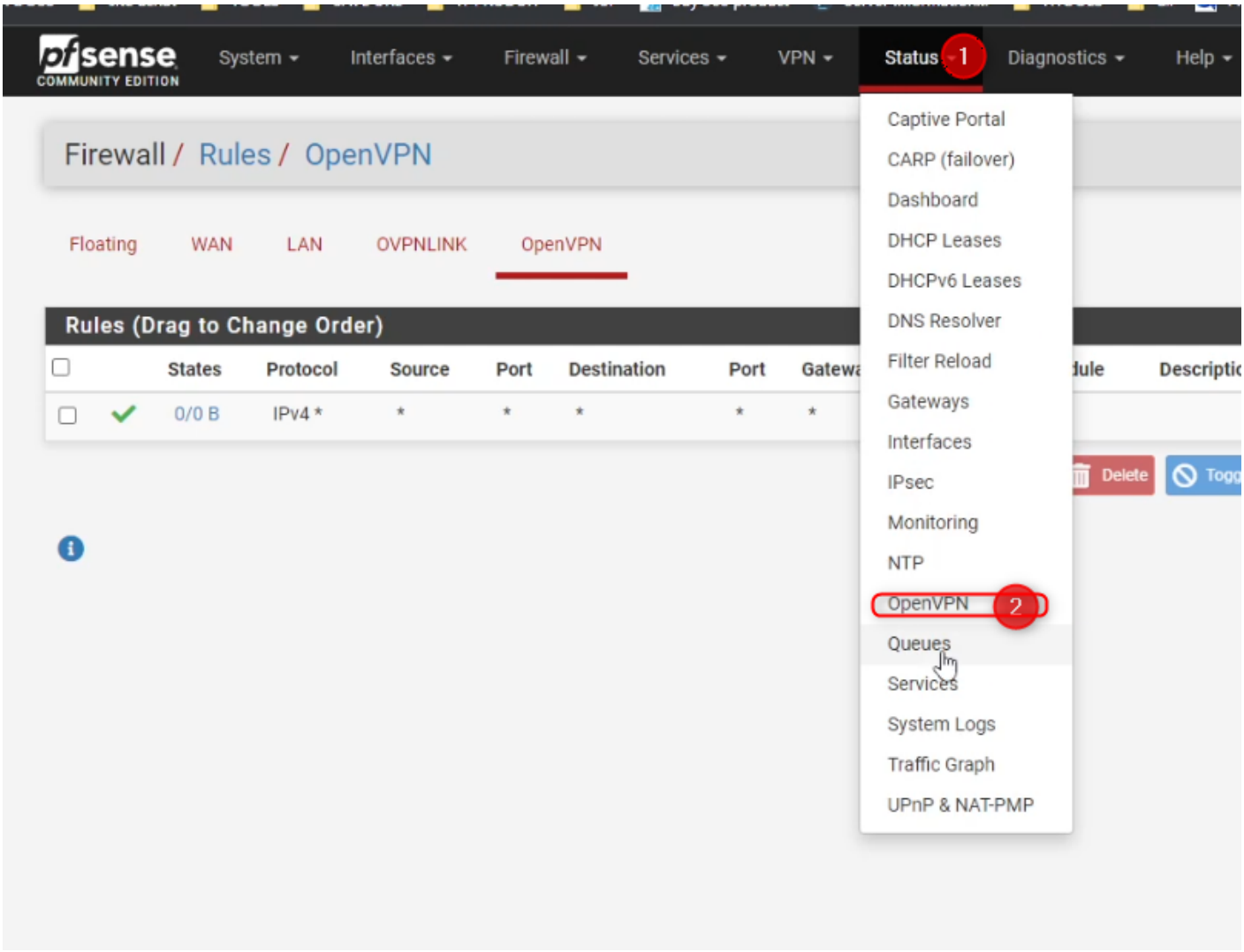
OpenVPN:



Ajout de la règle pour faire passer le trafic entre le VPN et le réseau

☐	✓	0/0 B	IPv4 *	*	*	*	*	*	none	ALL

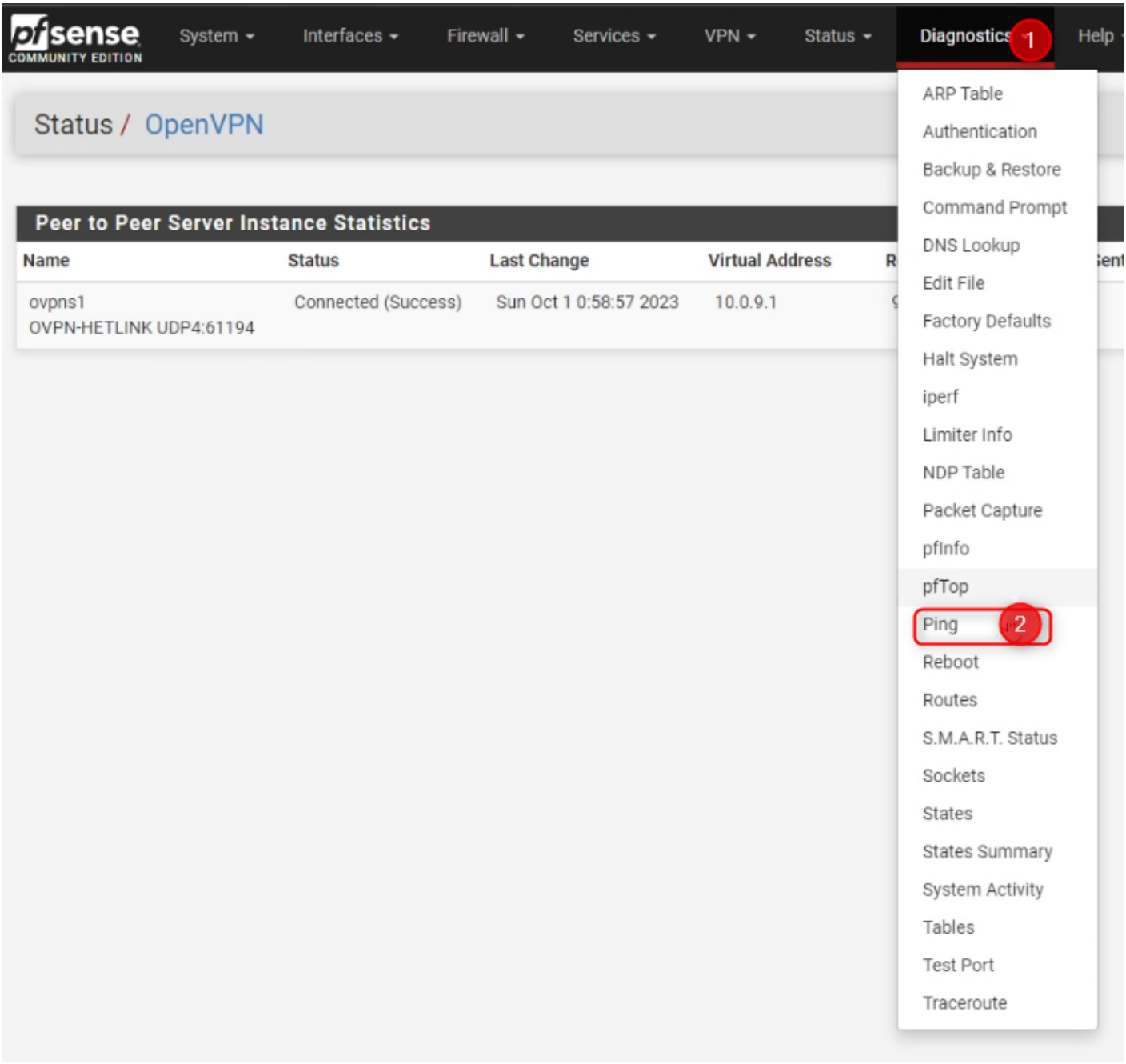
Contrôle de la connexion du VPN entre les deux routeurs

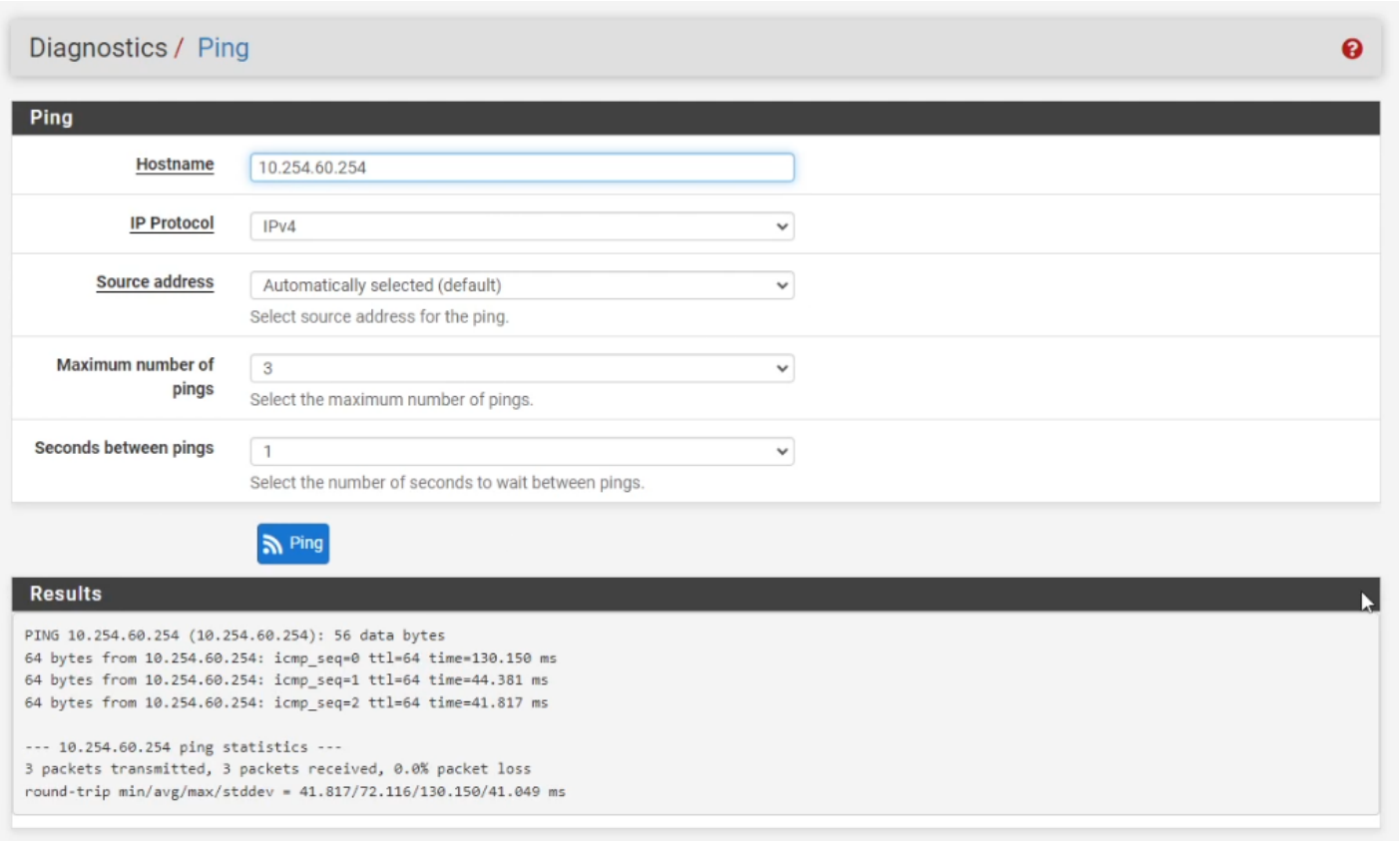


DEPUIS LE SERVEUR

DEPUIS LE CLIENT

Pour continuer le test nous pouvons effectuer un "ping" entre les deux sites





Revision #3
Created 8 October 2023 15:49:32 by Admin
Updated 8 October 2023 17:58:00 by Admin