Le choix du Firewall

Jusqu'ici j'utilisai plus souvent IPFire que je trouvais simple et efficace – interface ROUGE, VERTE, ORANGE c'est clair. Il est aussi très pratique pour le mode proxy web.

Mais PFSense a des avantages que n'a pas Ipfire, en particulier le client VPN !

Du coup, j'utilise les 2 en parallèle, une seule machine passe par PFSense pour son tunnel, les autres utilisateurs sortent par le proxy.

Installation de PFsense

C'est l'objet d'un autre tuto – cependant vous trouverez sur beaucoup de sites le mode d'emploi.

C'est très simple : mettez l'image Iso- suivez l'installation…c'est quasiment pareil que sur Ipfire

Au reboot vous devrez choisir entre les cartes virtuelles, celle qui va sur la WAN et celle qui va sur le LAN-WAN, LAN c'est plus pro que RED, Green..

Après l'administration se fait depuis le réseau Lan via l'interface web.

Client VPN vers un serveur dédié ou un VPS

Sur le serveur

- Installer le serveur OpenVPN (apt-get)
- Créer le certificat et les clés CA (autorité de certification)
- Créer le certificat et la clé authentifiant le serveur
- Créer un client, son certificat et sa clé
- Créer une route

https://openclassrooms.com/courses/protegez-l-ensemble-de-vos-communications-sur-internet-1/tp-mettez-en-place-votre-propre-serveur-openvpn-sous-linux

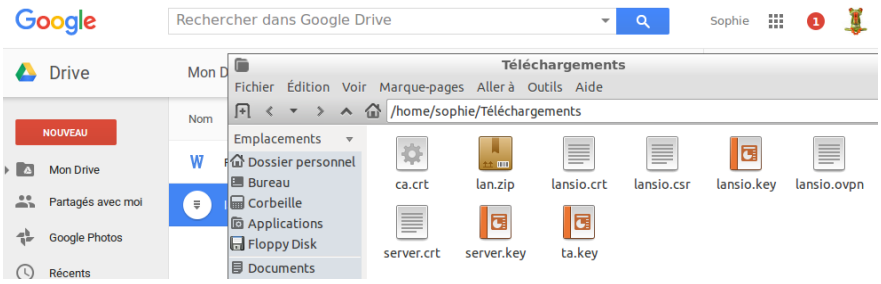
ou

https://technique.arscenic.org/reseau/openvpn-a-virtual-private-network/article/installation-et-configuration-d

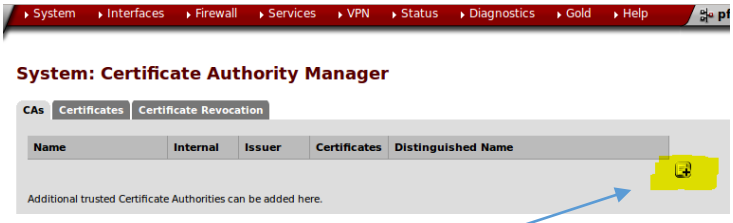
- Pour récupérer des certificats (dossier créé sur le serveur) sous Windows utilisez WinSCP.

Sur PFSense en tant que client

- Au préalable importer les certificats



- Menu « System » de PfSense , CertManager

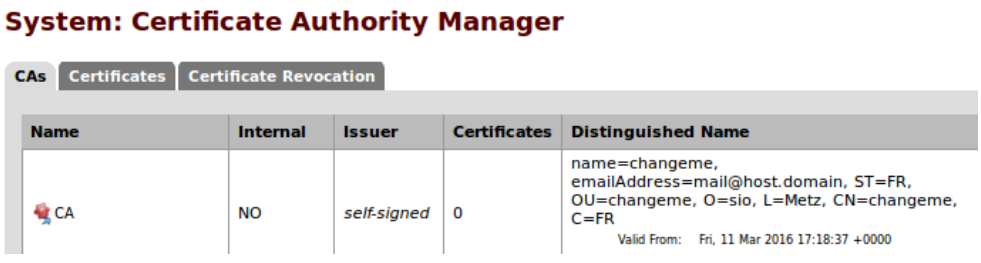


Il faut déjà importer le certificat de l'autorité de certification, en fait le certificat qui vous a permis d'auto-signer les autres certificats.

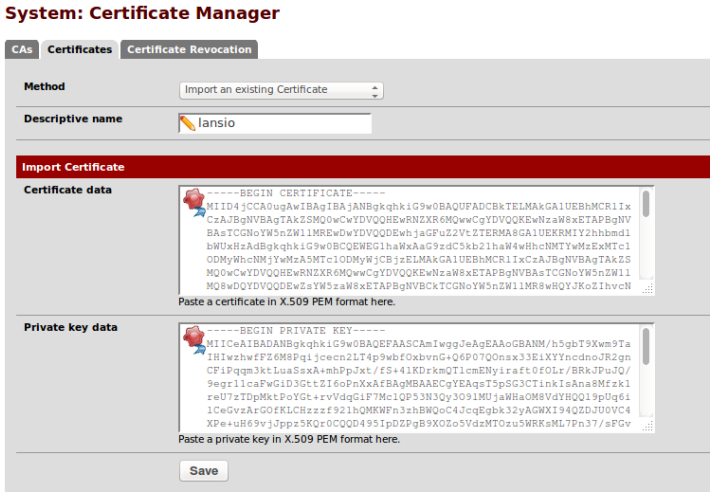
Cliquer sur Ajouter

- Avec un éditeur de texte
- (Bouton droit sur le fichier .crt , ouvrir avec : choisir (ou trouver l'application notepad.exe sous Windows)
- Copier-coller l'ensemble des caractères.

Sauvegarder et vous obtenez un certificat :



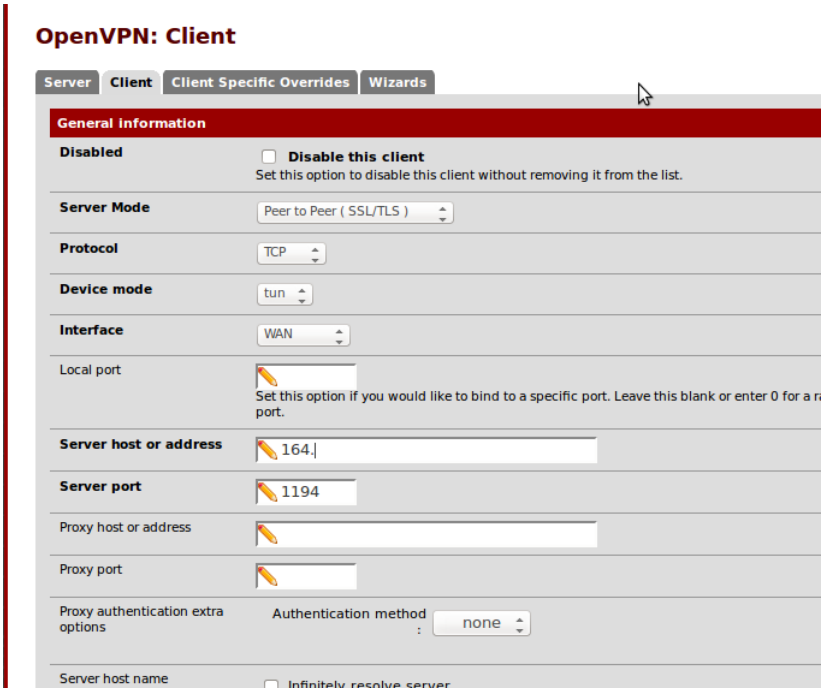
Il faut maintenant importer le certificat client



Création du client OpenVPN

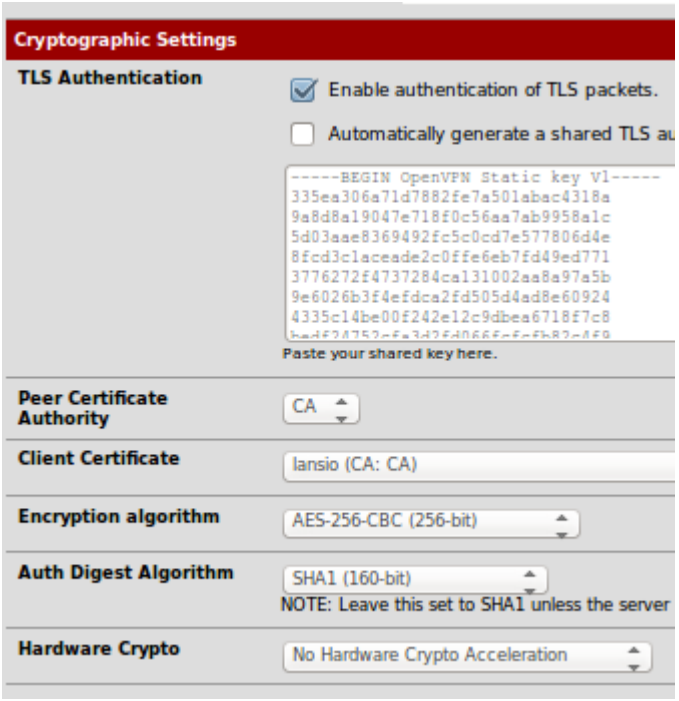
Il faut aller ensuite dans le menu « VPN », OpenVPN

Dans l'onglet Client, sélectionner ajouter 

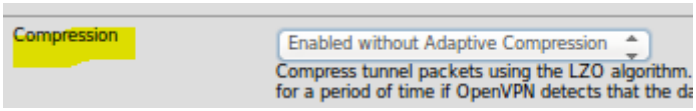


Dans « Crytpo Settings » vous retrouver les certificats importer précédemment.

Attention à décocher Automatically generate …et copier la clé dans la case.



Ensuite attention à la compression



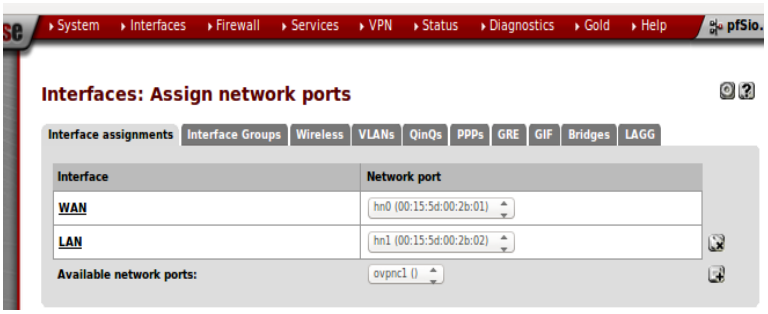
Dans les « Tunnels settings » Ip v4 tunnels, entrez l'adressage paramétré via le serveur (souvent en 10.0.8.0/24 ou 10.8.0.0./24)

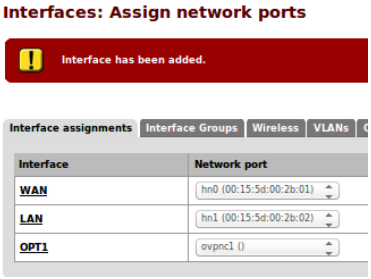
C'est dans cet adressage que la carte virtuelle créée pour le tunnel va être.

Redirection du trafic

Assigner l'interface du tunnel

Il faut maintenant assigner la connexion openVPN à une carte pour pouvoir rediriger le trafiic vers le VPN.



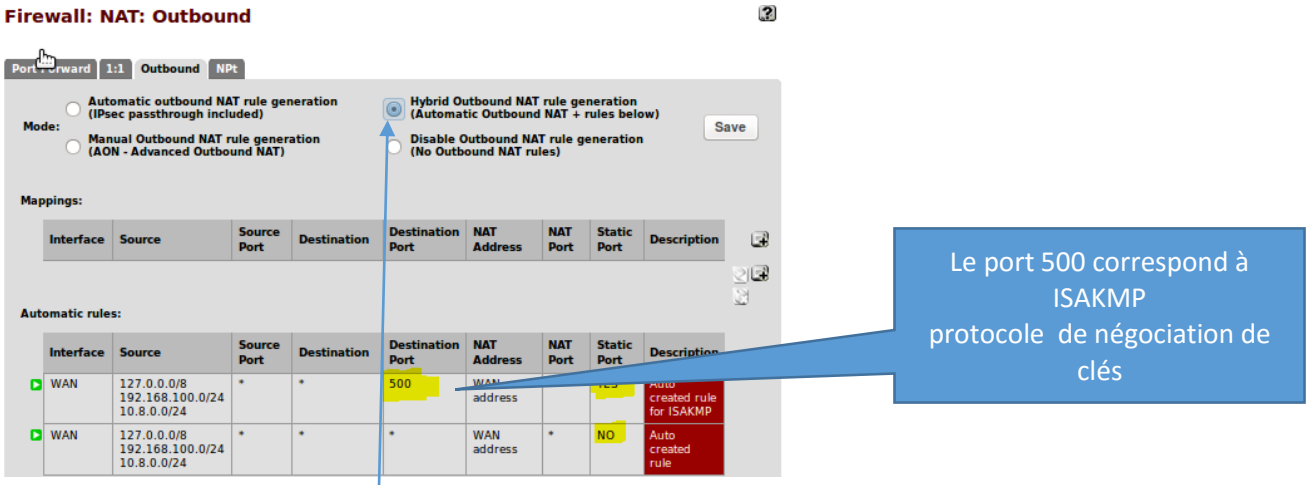


Créer la redirection

Dans le menu Firewall, NAT

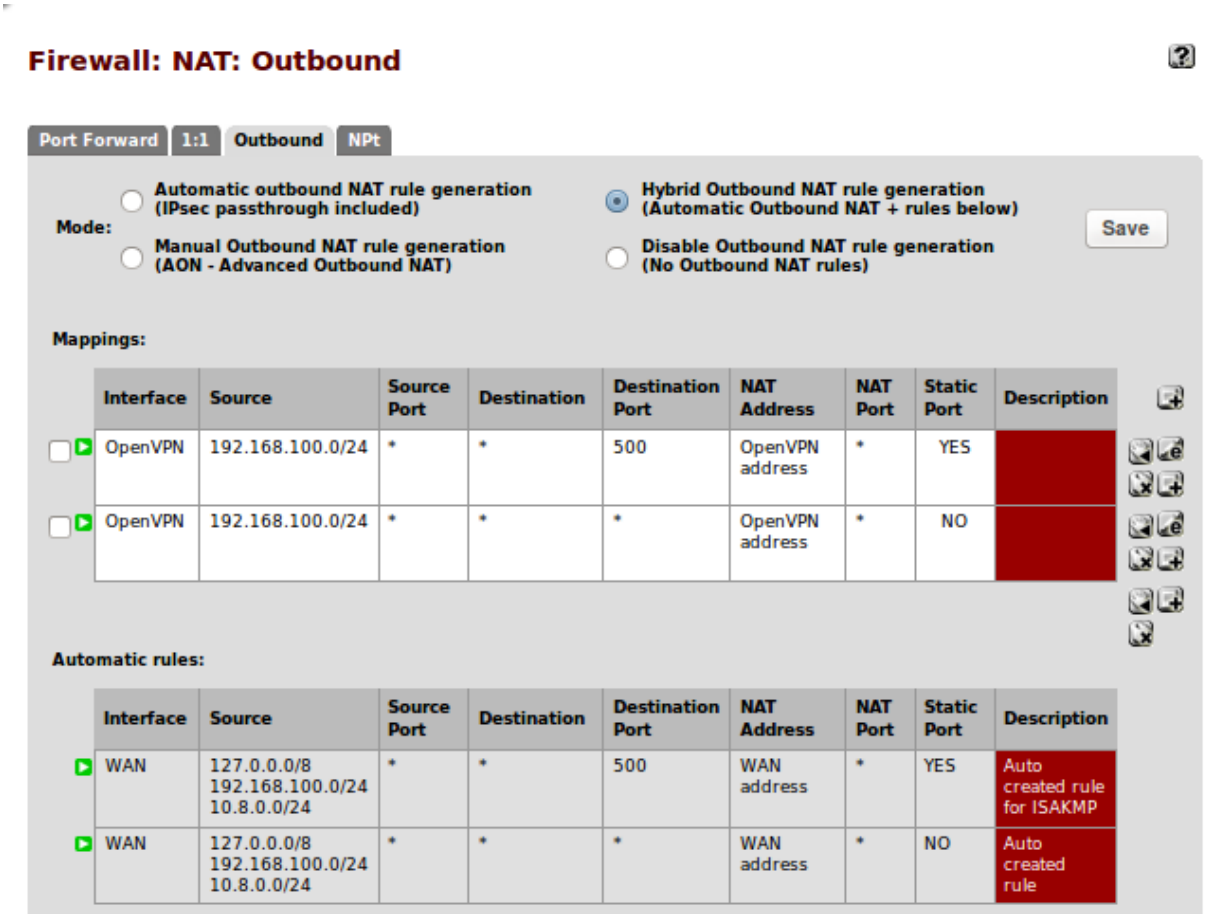
Aller dans l'onglet Outbound

Par défaut il existe ces règles



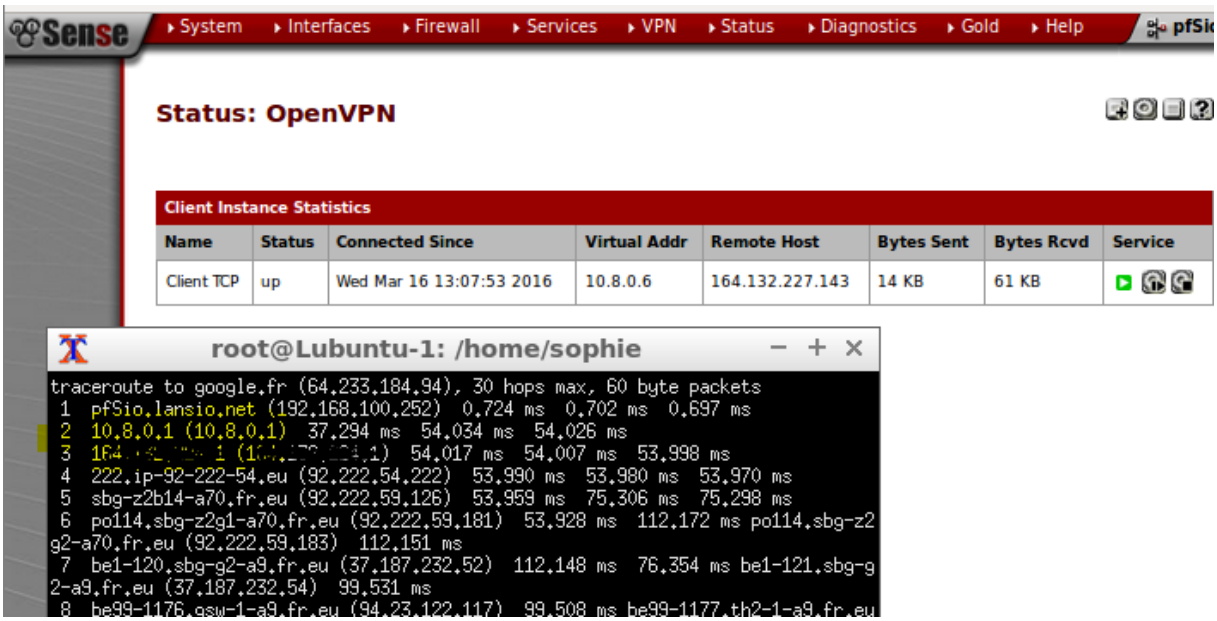
Il faut créer 2 nouvelles règles, pour cela cliquer d'abord sur Hybrid

Ces règles sont la copie des 2 existantes mais pour l'interface du tunnel :



Redémarrer le service openvpn

Puis effectuer un tracert (ou traceroute sous linux) pour vérifier que vous passez bien dans le tunnel



Voilà le tunnel est ouvert et il est possible maintenant de naviguer librement sur le web.

FIN