

## 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/protégez-l-ensemble-de-vos-communications-sur-internet-1/tp-mettez-en-place-votre-propre-serveur-openvpn-sous-linux>

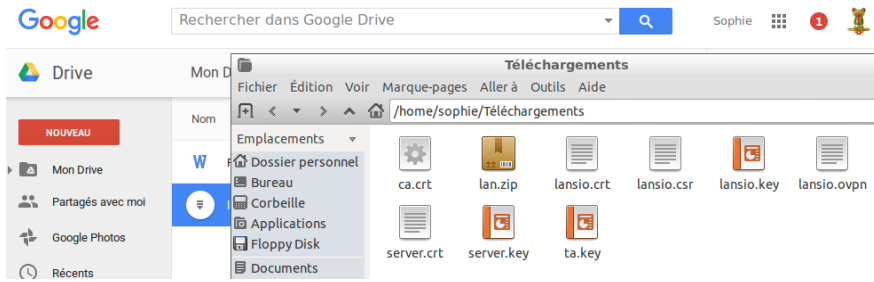
ou

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

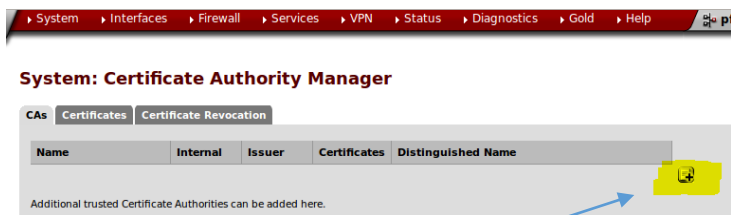
- Pour récupérer des certificats (dossier créé sur le serveur) sous Windows utilisez WinSCP.

### 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 :

### System: Certificate Authority Manager

Name	Internal	Issuer	Certificates	Distinguished Name
CA	NO	self-signed	0	name=changeme, emailAddress=mail@host.domain, ST=FR, OU=changeme, O=sio, L=Metz, CN=changeme, C=FR Valid From: Fri, 11 Mar 2016 17:18:37 +0000

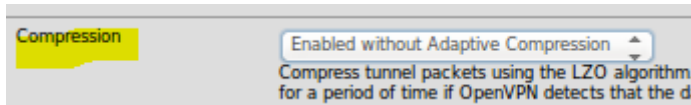


Dans « Crypto Settings » vous retrouver les certificats importer précédemment.

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



Ensuite attention à la compression



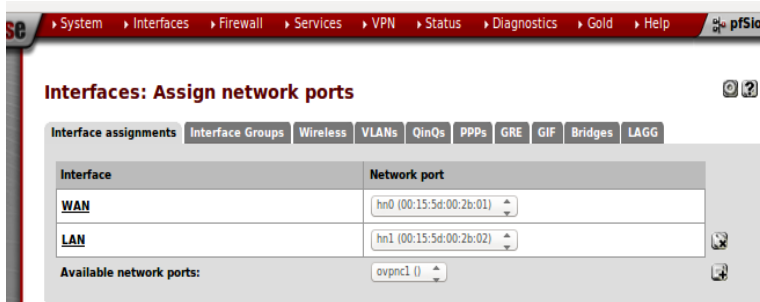
Dans les « Tunnels settings » Ip v4 tunnels, entrez l'adressage paramétré via le serveur (souvent en 10.0.8.0/24 ou 10.8.0.0./24)

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

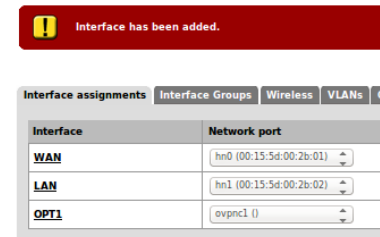
## Redirection du trafic

Assigner l'interface du tunnel

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



## Interfaces: Assign network ports



Créer la redirection

Dans le menu Firewall, NAT

Aller dans l'onglet Outbound

Par défaut il existe ces règles

### Firewall: NAT: Outbound

Mode:

- Automatic outbound NAT rule generation (IPsec passthrough included)
- Hybrid Outbound NAT rule generation (Automatic Outbound NAT + rules below)
- Manual Outbound NAT rule generation (AON - Advanced Outbound NAT)
- Disable Outbound NAT rule generation (No Outbound NAT rules)

Mappings:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
WAN	127.0.0.0/8 192.168.100.0/24 10.8.0.0/24	*	*	500	WAN address	*	YES	Auto created rule for ISAKMP
WAN	127.0.0.0/8 192.168.100.0/24 10.8.0.0/24	*	*	*	WAN address	*	NO	Auto created rule

Automatic rules:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
WAN	127.0.0.0/8 192.168.100.0/24 10.8.0.0/24	*	*	500	WAN address	*	YES	Auto created rule for ISAKMP
WAN	127.0.0.0/8 192.168.100.0/24 10.8.0.0/24	*	*	*	WAN address	*	NO	Auto created rule

Le port 500 correspond à ISAKMP protocole de négociation de clés

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 :

### Firewall: NAT: Outbound

Mode:

- Automatic outbound NAT rule generation (IPsec passthrough included)
- Hybrid Outbound NAT rule generation (Automatic Outbound NAT + rules below)
- Manual Outbound NAT rule generation (AON - Advanced Outbound NAT)
- Disable Outbound NAT rule generation (No Outbound NAT rules)

Mappings:

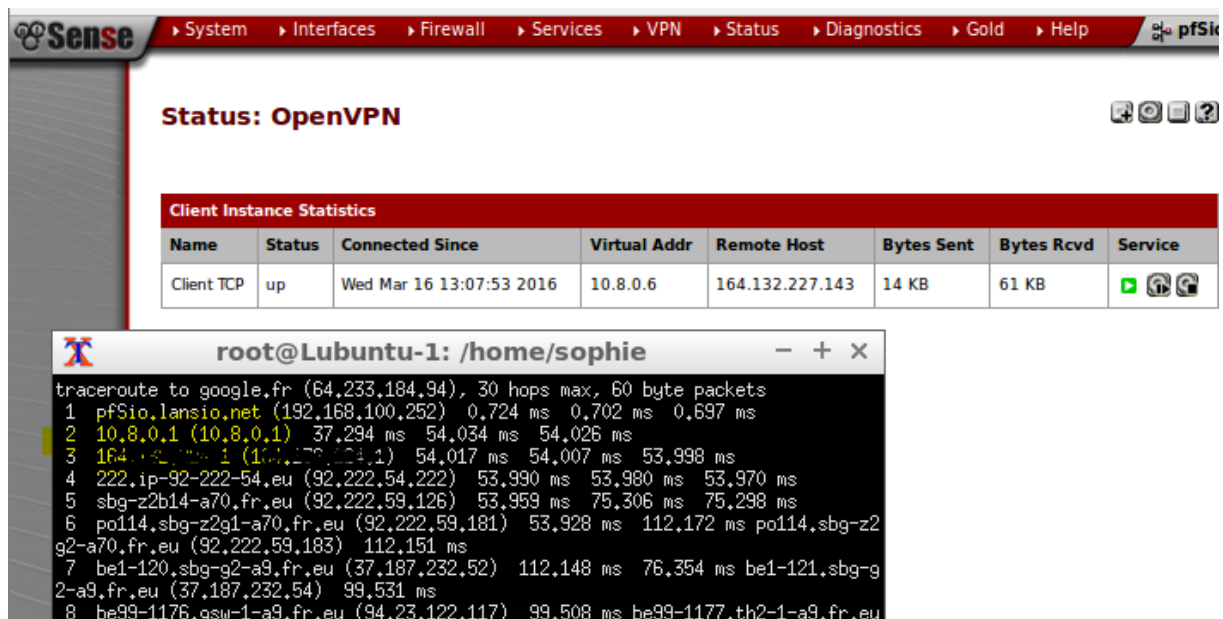
Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
OpenVPN	192.168.100.0/24	*	*	500	OpenVPN address	*	YES	
OpenVPN	192.168.100.0/24	*	*	*	OpenVPN address	*	NO	

Automatic rules:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
WAN	127.0.0.0/8 192.168.100.0/24 10.8.0.0/24	*	*	500	WAN address	*	YES	Auto created rule for ISAKMP
WAN	127.0.0.0/8 192.168.100.0/24 10.8.0.0/24	*	*	*	WAN address	*	NO	Auto created rule

Redémarrer le service openvpn

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



The screenshot shows the pfSense web interface with the 'Status: OpenVPN' page. Below the status, there is a 'Client Instance Statistics' table. In the foreground, a terminal window shows the output of a traceroute command.

Name	Status	Connected Since	Virtual Addr	Remote Host	Bytes Sent	Bytes Rcvd	Service
Client TCP	up	Wed Mar 16 13:07:53 2016	10.8.0.6	164.132.227.143	14 KB	61 KB	

```
root@Lubuntu-1: /home/sophie
traceroute to google.fr (64.233.184.94), 30 hops max, 60 byte packets
 1  pfSio.lansio.net (192.168.100.252)  0.724 ms  0.702 ms  0.697 ms
 2  10.8.0.1 (10.8.0.1)  37.294 ms  54.034 ms  54.026 ms
 3  164.132.227.1 (164.132.227.1)  54.017 ms  54.007 ms  53.998 ms
 4  222.ip-92-222-54.eu (92.222.54.222)  53.990 ms  53.980 ms  53.970 ms
 5  sbg-z2b14-a70.fr.eu (92.222.59.126)  53.959 ms  75.306 ms  75.298 ms
 6  po114.sbg-z2g1-a70.fr.eu (92.222.59.181)  53.928 ms  112.172 ms  po114.sbg-z2
g2-a70.fr.eu (92.222.59.183)  112.151 ms
 7  be1-120.sbg-g2-a9.fr.eu (37.187.232.52)  112.148 ms  76.354 ms  be1-121.sbg-g
2-a9.fr.eu (37.187.232.54)  99.531 ms
 8  be99-1176.gsw-1-a9.fr.eu (94.23.122.117)  99.508 ms  be99-1177.th2-1-a9.fr.eu
```

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

FIN