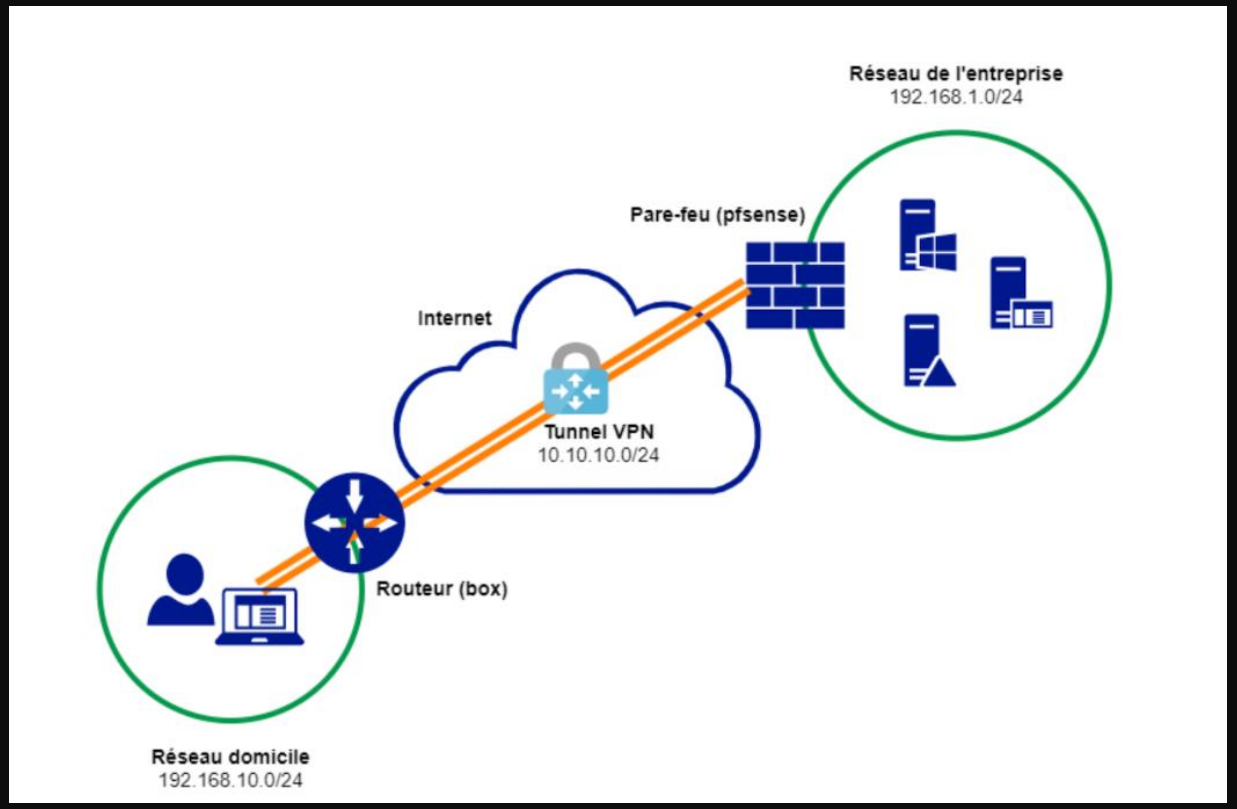
TP VPN

Mise en contexte

Je vais devoir mettre en place un VPN depuis le réseau de l'entreprise à l'aide de Pfsense afin de pouvoir permettre aux utilisateurs de se connecter au réseau depuis chez eux via OpenVPN, nous avons l'infrastructure suivante :

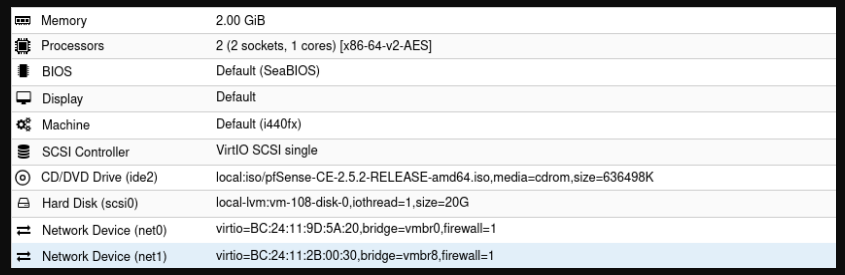


Mise en place du pfsense.

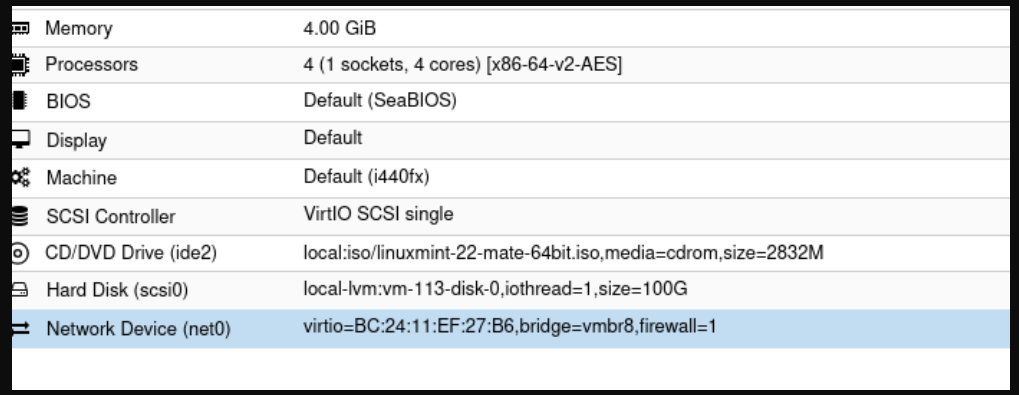
Tout d'abord il faudra mettre en place la machine pfsense, avec deux cartes réseaux, une pour le WAN (vmbr0), et une pour le LAN (vmbr8).

Ensuite pour ce qui est de l'installation de pfsense, elle a été realisée dans un tp precedent. (Cliquer ici pour le consulter).

Il faudra mettre la même carte réseau que pour le LAN sur la machine cliente afin de pouvoir le paramétrer.



Memory	2.00 GiB
Processors	2 (2 sockets, 1 cores) [x86-64-v2-AES]
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI single
CD/DVD Drive (ide2)	local:iso/pfSense-CE-2.5.2-RELEASE-amd64.iso,media=cdrom,size=636498K
Hard Disk (scsi0)	local-lvm:vm-108-disk-0,iothread=1,size=20G
Network Device (net0)	virtio=BC:24:11:9D:5A:20,bridge=vmbr0,firewall=1
Network Device (net1)	virtio=BC:24:11:2B:00:30,bridge=vmbr8,firewall=1



Memory	4.00 GiB
Processors	4 (1 sockets, 4 cores) [x86-64-v2-AES]
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI single
CD/DVD Drive (ide2)	local:iso/linuxmint-22-mate-64bit.iso,media=cdrom,size=2832M
Hard Disk (scsi0)	local-lvm:vm-113-disk-0,iothread=1,size=100G
Network Device (net0)	virtio=BC:24:11:EF:27:B6,bridge=vmbr8,firewall=1

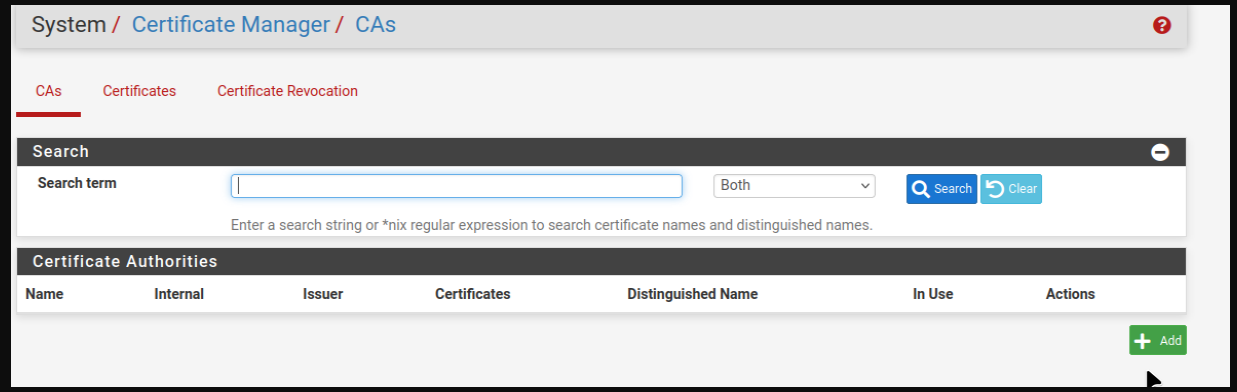
```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

KVM Guest - Netgate Device ID: 742f7e85f36e01e8befb

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)       -> vtnet0     -> v4/DHCP4: 192.168.20.90/24
LAN (lan)       -> vtnet1     -> v4: 192.168.1.1/24

0) Logout (SSH only)                  9) pfTop
1) Assign Interfaces                 10) Filter Logs
2) Set interface(s) IP address       11) Restart webConfigurator
3) Reset webConfigurator password    12) PHP shell + pfSense tools
4) Reset to factory defaults         13) Update from console
5) Reboot system                     14) Enable Secure Shell (sshd)
6) Halt system                       15) Restore recent configuration
7) Ping host                         16) Restart PHP-FPM
8) Shell
```

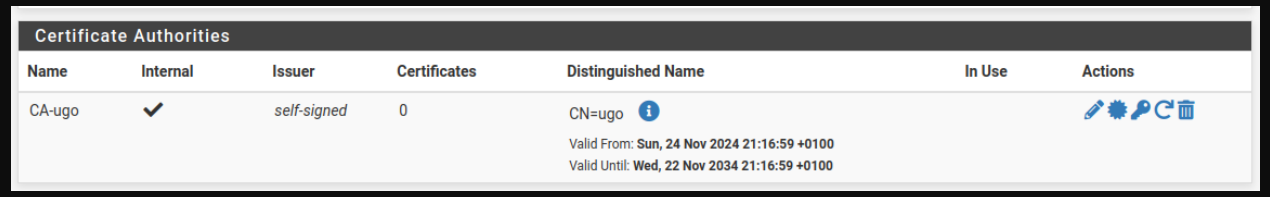
Créer une autorité de certification

Pour créer l'autorité de certification qui est nécessaire pour configurer le VPN SSL, il faudra se rendre dans system, et cert manager. Ensuite il faudra cliquer sur Add pour rentrer dans la page de configuration.

Dans Descriptive name, il faudra indiquer le nom du certificat, ici CA-UGO.

Dans Common name, il y'a le nom qui sera intégré dans les certificats qui seront générés, pour ma part j'ai mis ugo.
La modification des autres informations n'est pas obligatoire. Ensuite nous pouvons valider la configuration.





Txt

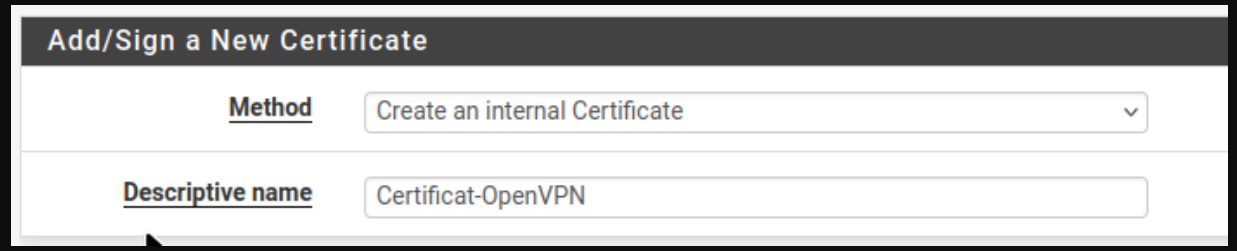
Ensuite dans certificates, nous pourrons créer un certificat pour le serveur, il faudra cliquer sur le bouton add.

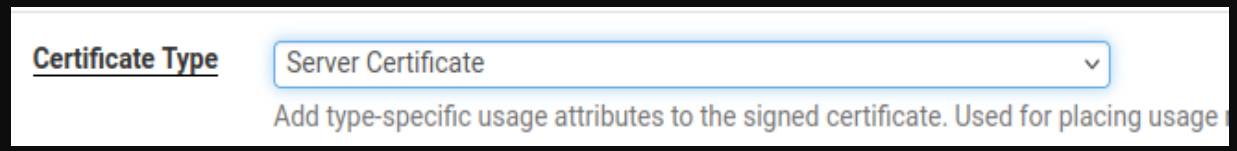
La methode a utiliser sera "create an internal certificate" et on ajoutera un nom au certificat, ici, certificat-openvpn.

Pour l'autorité de certification et le common name, je rentre les memes informations que précedemment.

Et dans le type de certificat, il faudra veiller a utiliser le certificat serveur.

Les autres paramètres ne sont pas necéssairements modifés egalement, nous pouvons donc valider avec save.





Création d'un utilisateur

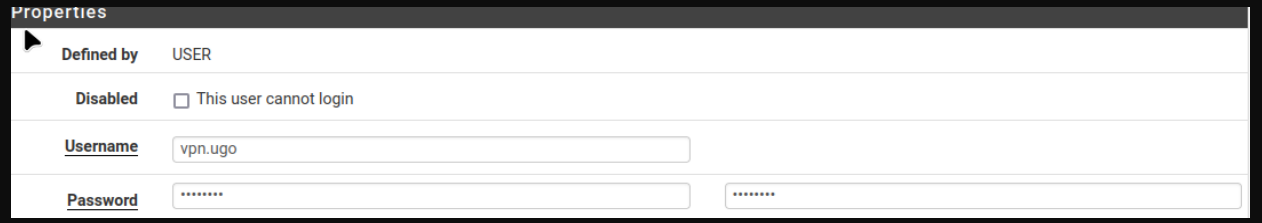
Ensuite nous allons créer un utilisateur sur pfsense dans system, user manager puis add.

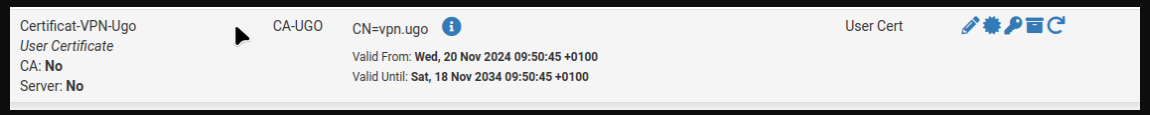
Il faudra renseigner son username, ici vpn.ugo et créer un mot de passe.

Ensuite il faudra cocher la case "click to creater a user certificate" pour pouvoir paramètrer la création du certificat utilisateur, il faudra rentrer un descriptive name et verifier que l'autorité de certificat correspond a celle créée précedemment.

Ensuite nous pouvons valider et l'utilisateur et son certificat est créé.

Dans le manager de certificat, nous pouvons constater que le certificat de type utilisateur a été créé.



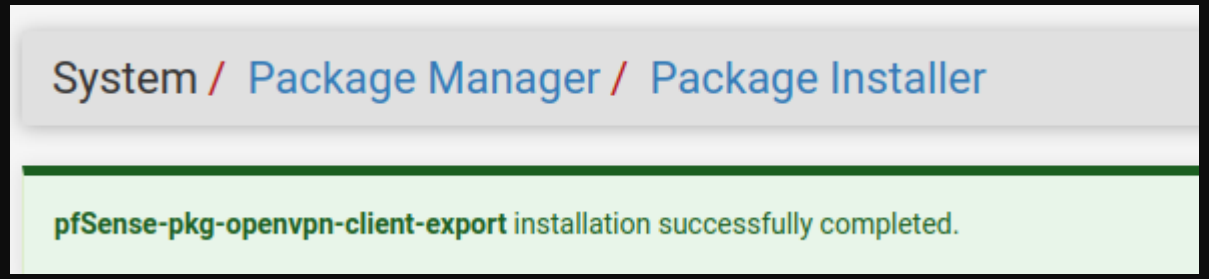


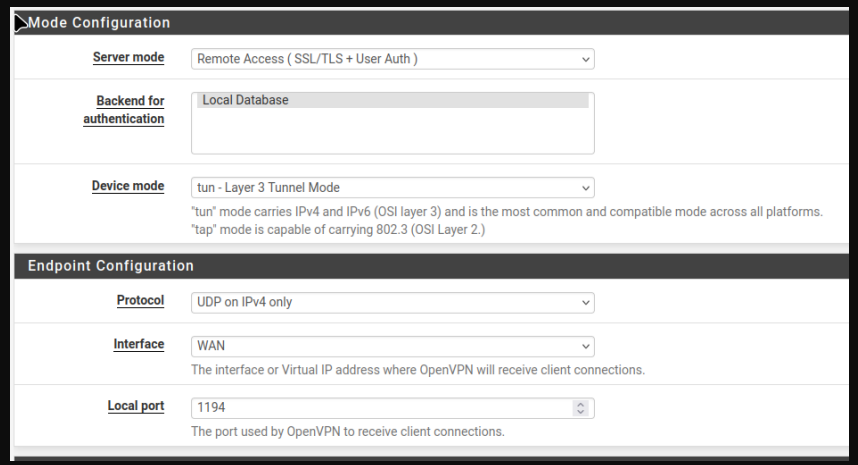
Installation du paquet OpenVPN

Afin de parametrer le VPN, il faudra installer le packet OPENvpn Servers.

Il faudra se render dans system, puis package manager puis package installer et rechercher openvpn et installer.
Ensuite, pour pouvoir le paramétrer, il faudra se rendre dans VPN, puis OpenVPN, puis servers et add.
Pour ce qui est de la configuration , on choisira le mode serveur remote access ssl/tls + user auth, le protocole sera UDP sur l'interface WAN et le port sera 1194.

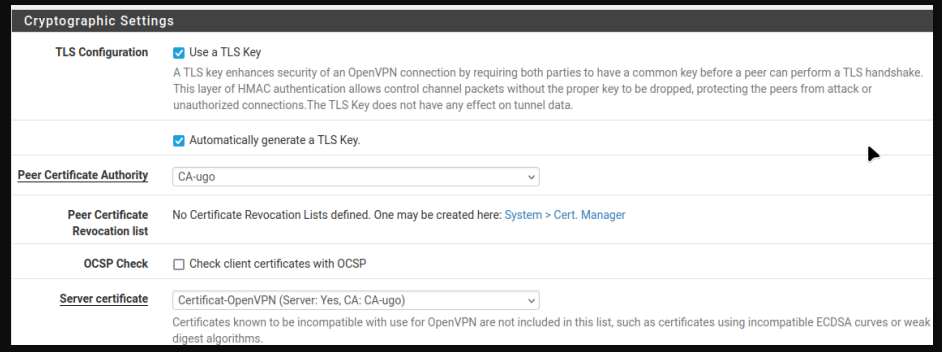
Pour ce qui est de l'encryption, utiliser AES-256-CBC sera plus sécurisé.

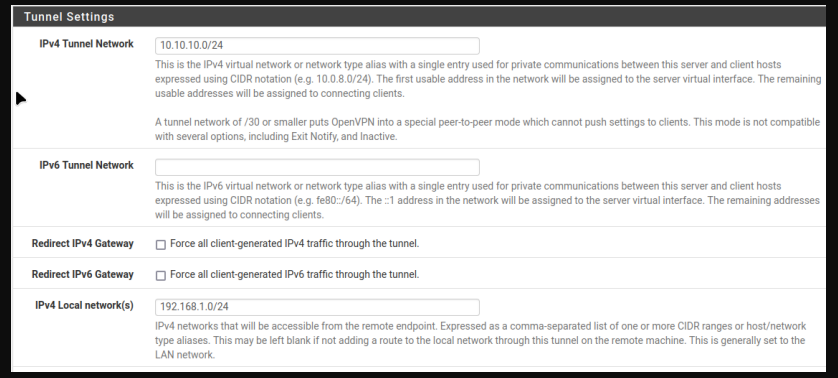


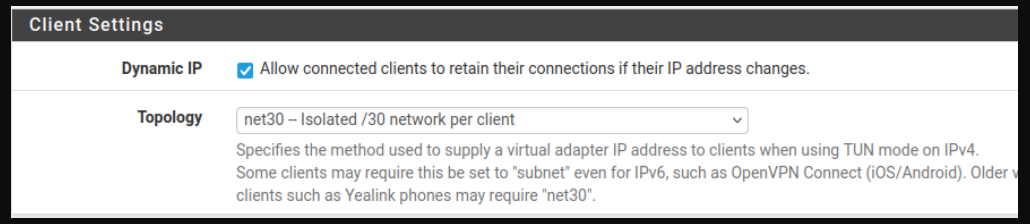


Paramètres du serveur VPN

Ensuite, il faudra renseigner le autorité de certificate, et le certificate du serveur.
Pour l'IPv4 du tunnel Network, comme vu précedemment, le réseau sera 10.10.10.0/24 et le réseau local sera 192.168.1.0/24.
Il est recommandé d'active le mode IP dynamique afin de permettre aux clients mobiles géographiquement de pouvoir se connecter.



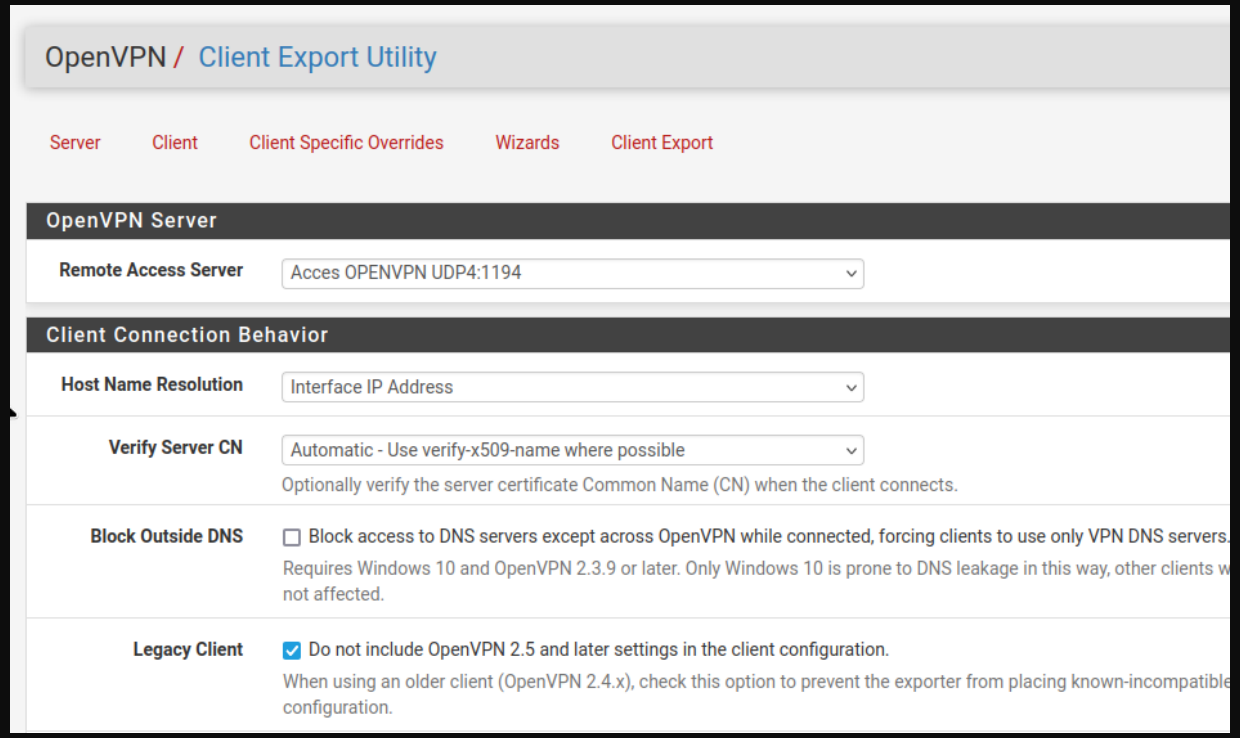


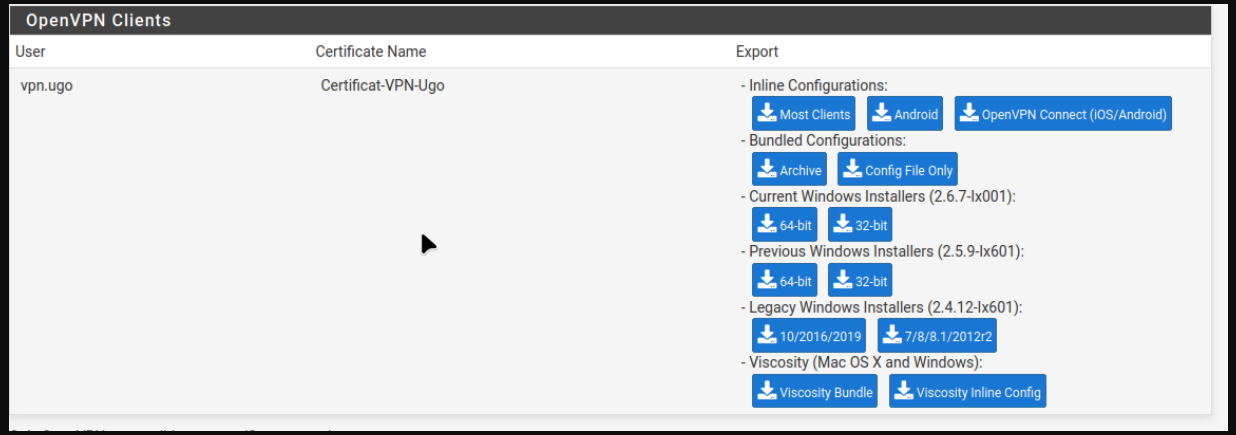


Exporter la configuration

Pour exporter la configuration VPN, il faudra se rendre dans OpenVPN, puis Client export utility et server, mettre dans le host name resolution "interface IP address et" cocher legacy client pour les clients utilisant une vieille version d'openvpn.

Ensuite il faudra télécharger la version archive de la configuration.

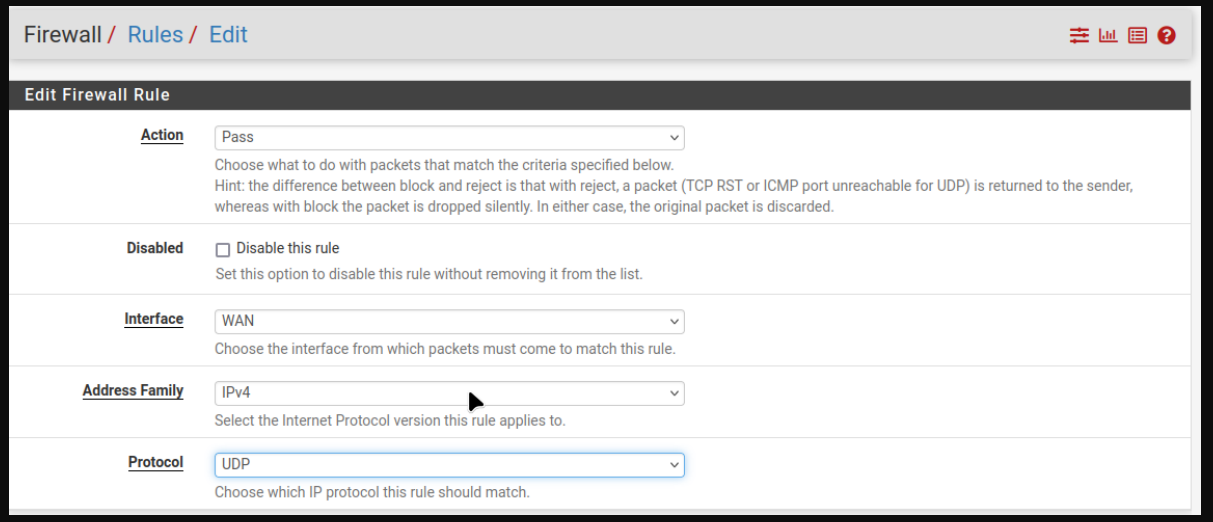


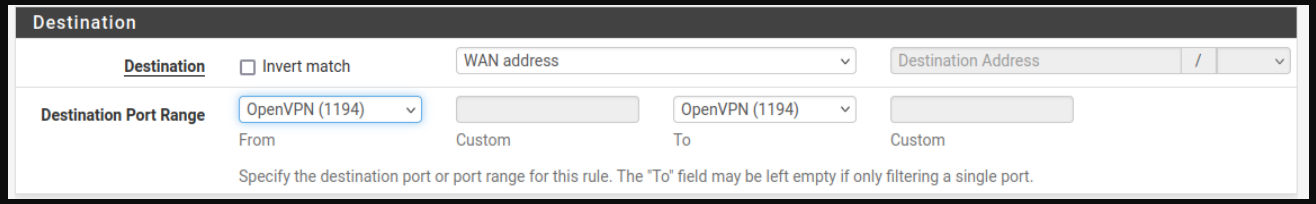


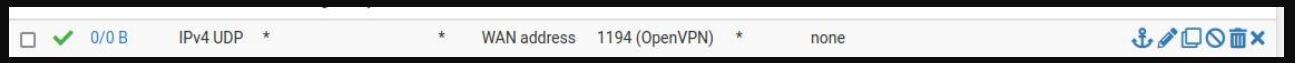
Ajout de règles du pare-feu

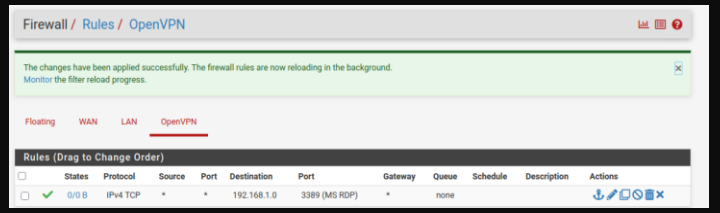
Ensuite, il faudra se rendre dans les regles du WAN, et ajouter une regle autorisant le protocole UDP pour le port 1194.

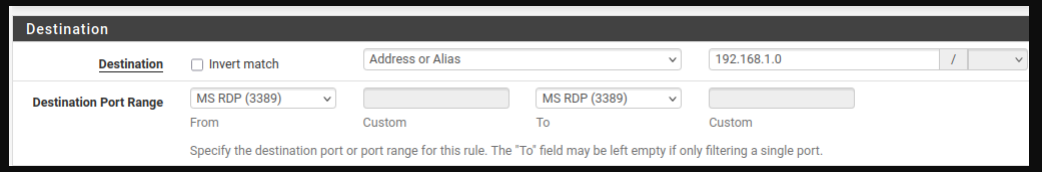
Et il faudra également rajouter une regle sur le pare-feu pour OpenVPN qui autorise les requetes a destination du port 3389 pour le réseau 192.168.1.0











Connexion avec le client

Ensuite il faudra télécharger le client OpenVPN sur la machine et télécharger le fichier de configuration exporté précedemment. Il faudra exporter ce fichier dans le dossier C:/programfiles/OpenVPN/config sur Windows.
Ensuite il faudra ouvrir OpenVPN et saisir le nom d'utilisateur et le mot de passe créé sur pfsense precedemment.