Documentation VPN Bgtw

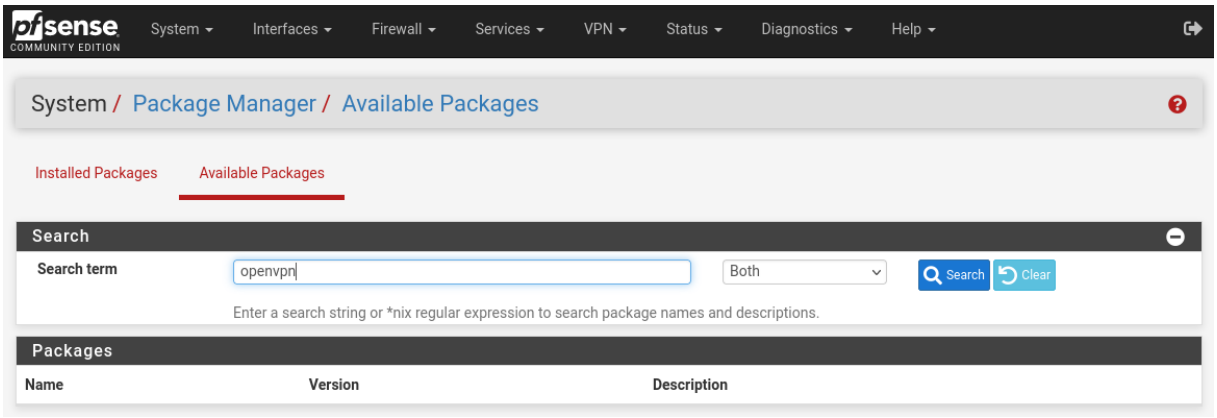
Table des matières

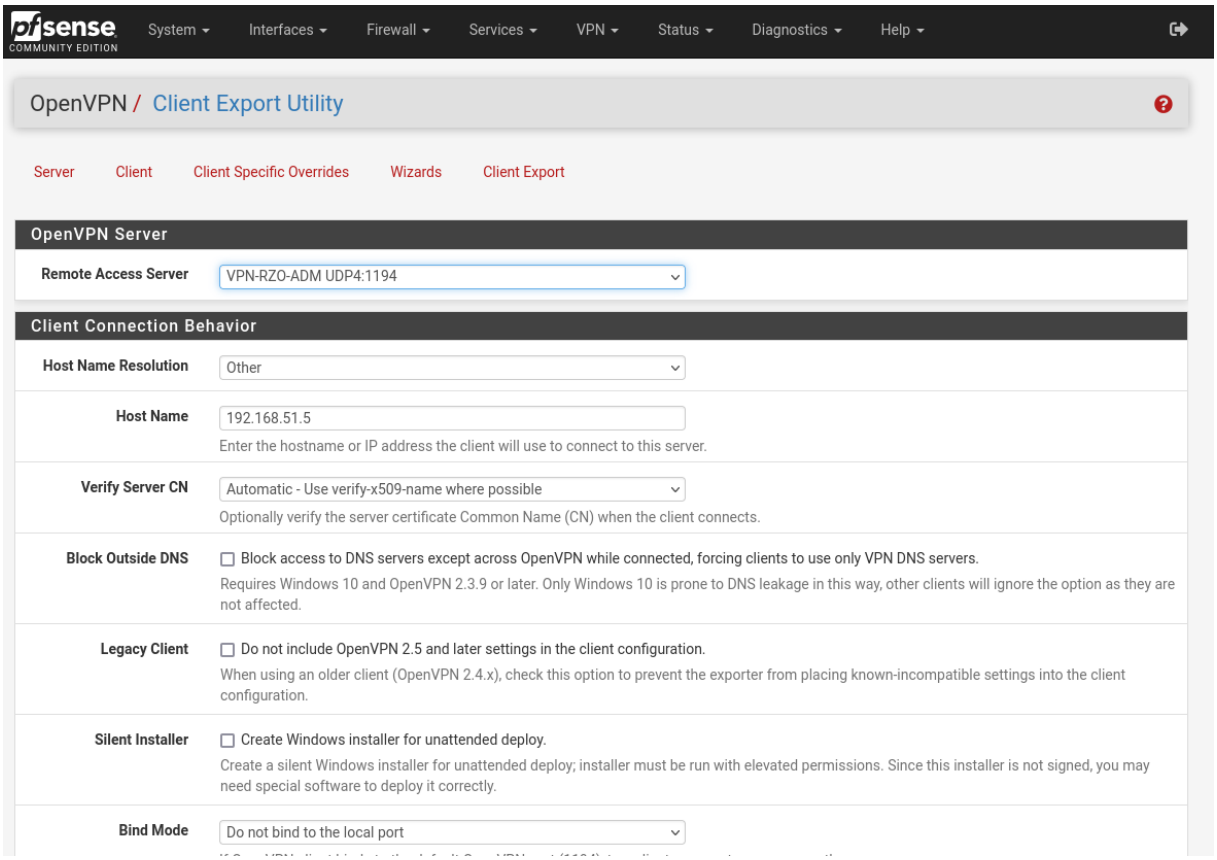
Configuration VPN pour réseau ADM

Nous devions fournir un accès aux utilisateurs du réseau ADM4 pour qu'ils puissent se connecter depuis internet au réseau interne de l'entreprise afin de pouvoir continuer à l'administrer depuis n'importe où.

Il y avait aussi le réseau DEV4 qui devait pouvoir y accéder pour pouvoir notamment continuer d'administrer le site web de l'entreprise à distance.
Pour répondre à cela, nous avons mis en place un VPN avec OpenVPN.

Avant de configurer le serveur VPN, pour se faciliter le travail, nous allons installer le package qui permet d'exporter plus facilement les clients et donc avoir une connexion directe entre le client et le serveur sans avoir à modifier quoi que ce soit sur le poste du client.





Certificate Export Options

PKCS#11 Certificate Storage
☐ Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.

Microsoft Certificate Storage
☐ Use Microsoft Certificate Storage instead of local files.

Password Protect Certificate
☐ Use a password to protect the PKCS#12 file contents or key in Viscosity bundle.

PKCS#12 Encryption
High: AES-256 + SHA256 (pfSense Software, FreeBSD, Linux, Window
Select the level of encryption to use when exporting a PKCS#12 archive. Encryption support varies by Operating System and program

Proxy Options

Use A Proxy
☐ Use proxy to communicate with the OpenVPN server.

Advanced

Additional configuration options

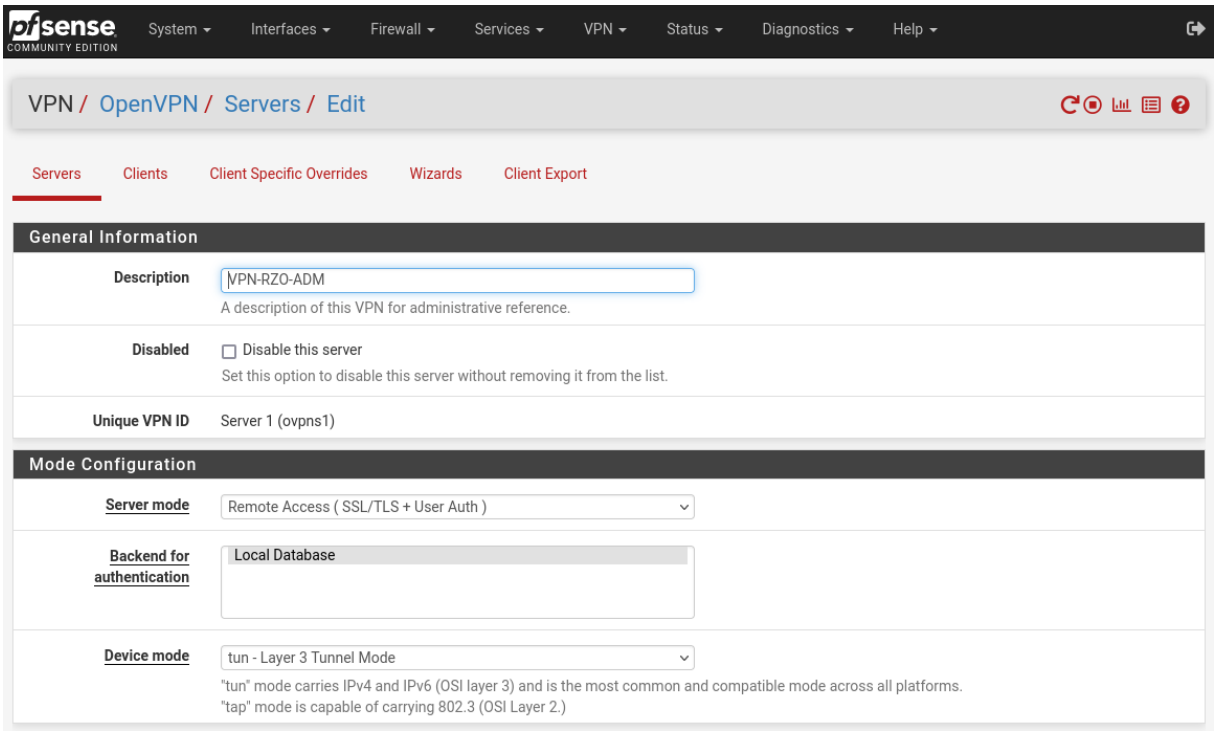
Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.

EXAMPLE: remote-random;

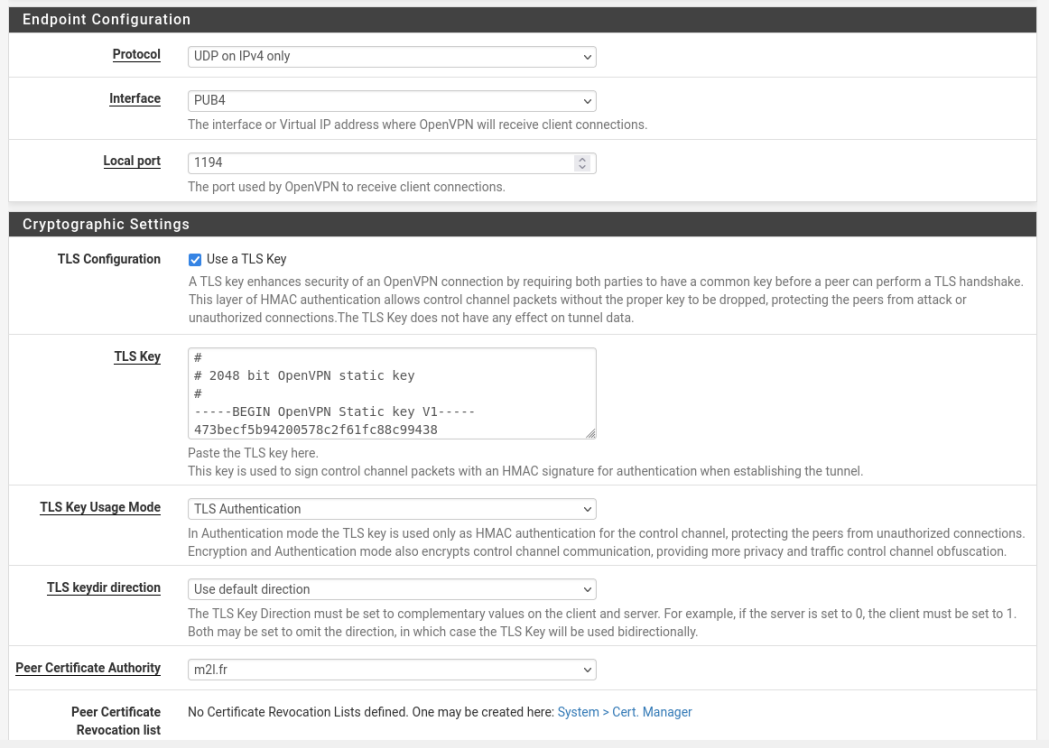
Save as default

Configuration du serveur VPN ADM4 :

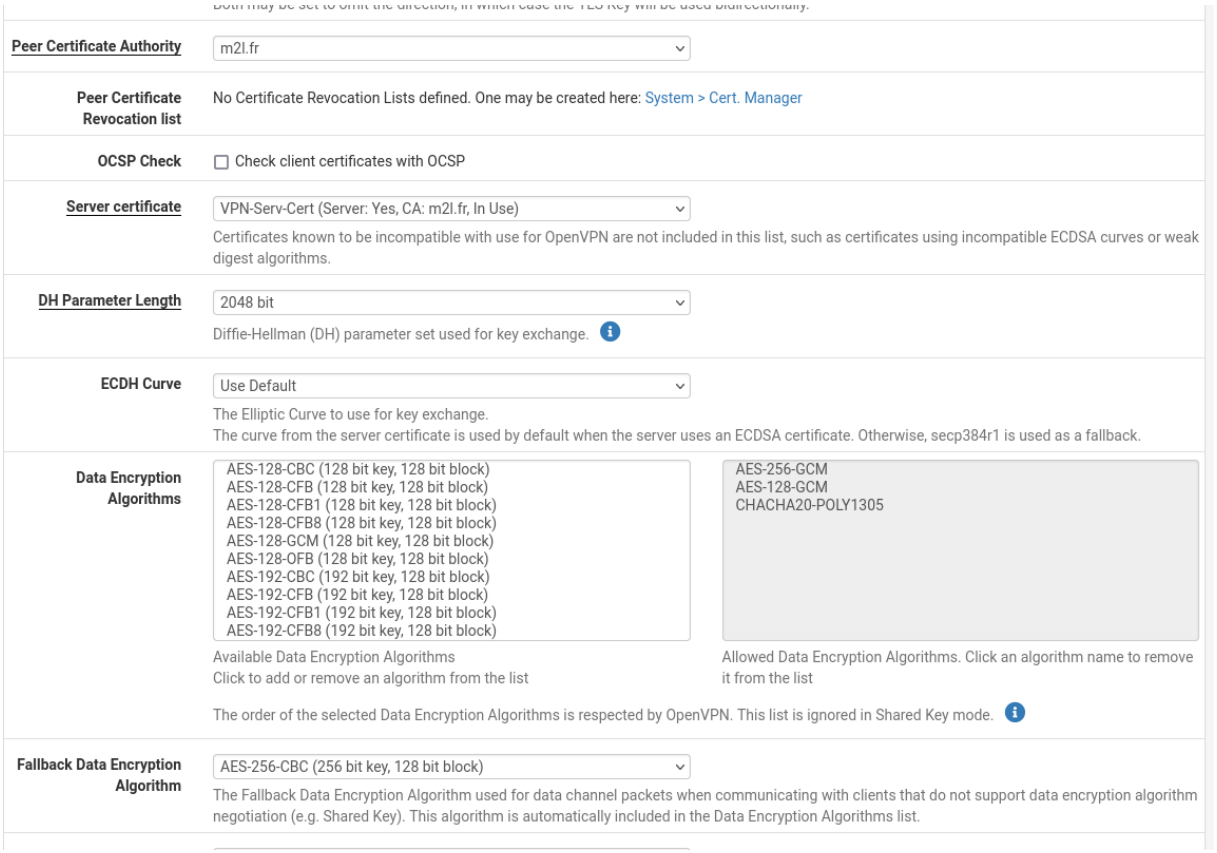
Nous allons d'abord configurer le tunnel pour les utilisateurs du réseau ADM4 :



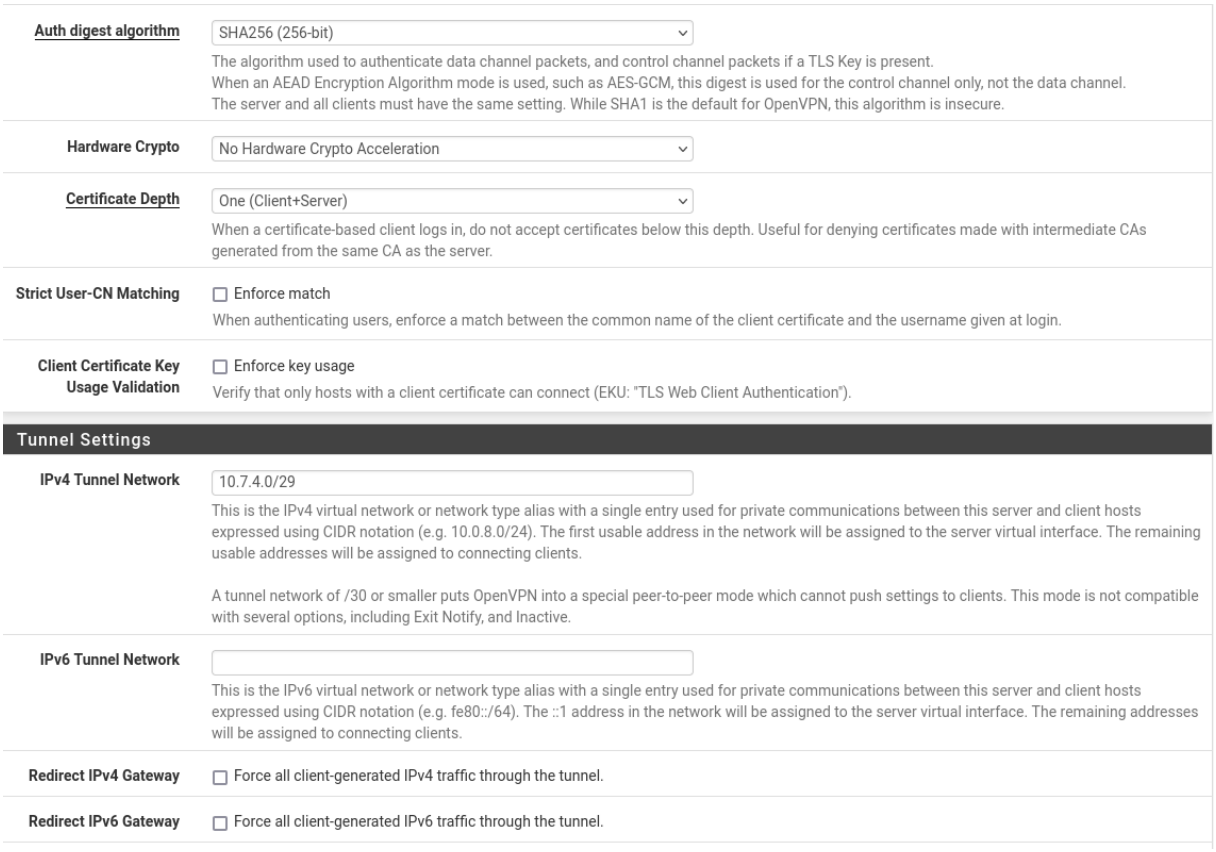
Il faut bien choisir sur quelle interface on veut que le service tourne, en l'occurrence la patte PUB4 étant celle qui est reliée au routeur Fgtw. Il faut aussi choisir le bon port.



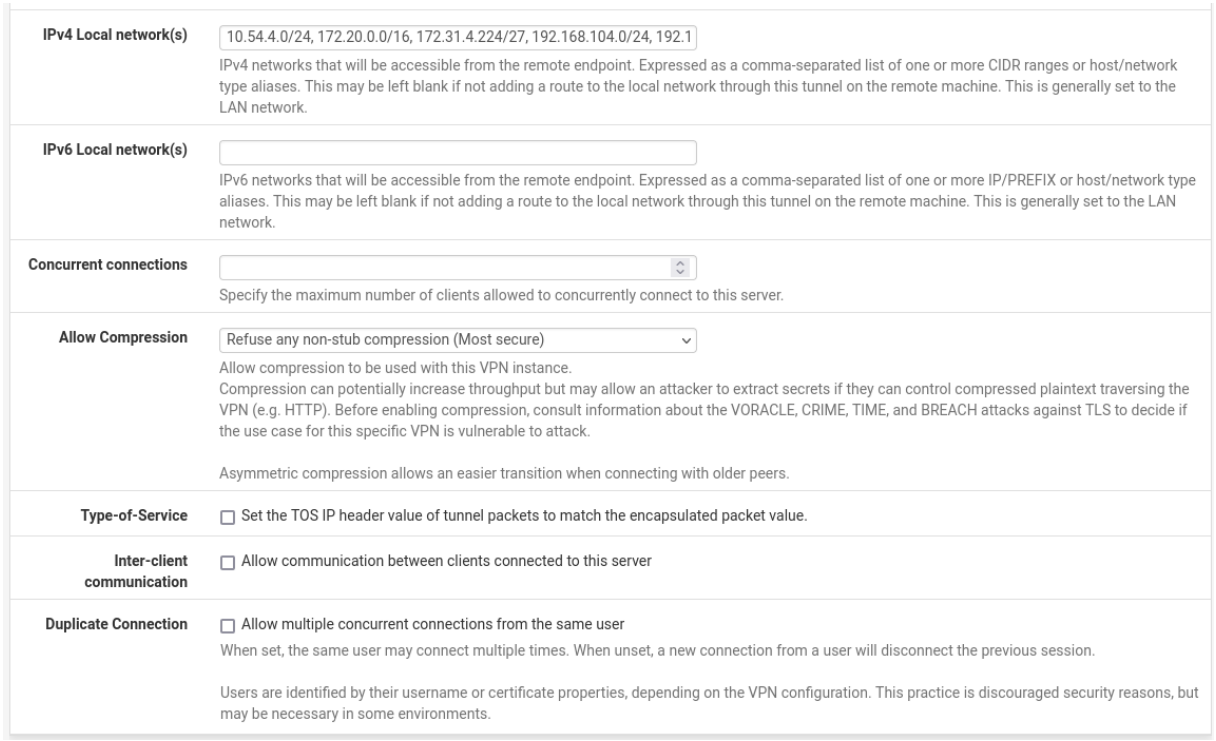
Il faut aussi choisir quel est le certificat d'autorité, nous c'est le certificat de l'entreprise du contexte. Nous devons choisir quels paramètres de chiffrement nous allons utiliser, la longueur du Diffie-Hellman etc....



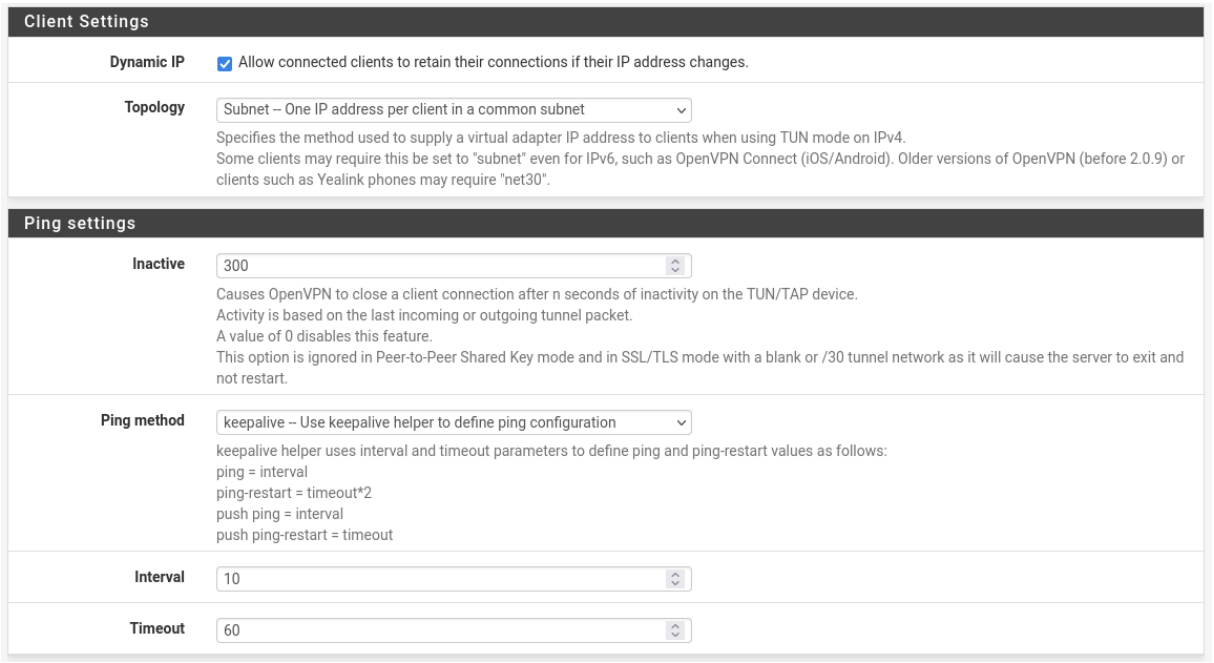
Nous allons déclarer quel sera le sous réseau utilisé par ce tunnel VPN, ici nous avons opté pour 10.7.4.0/29



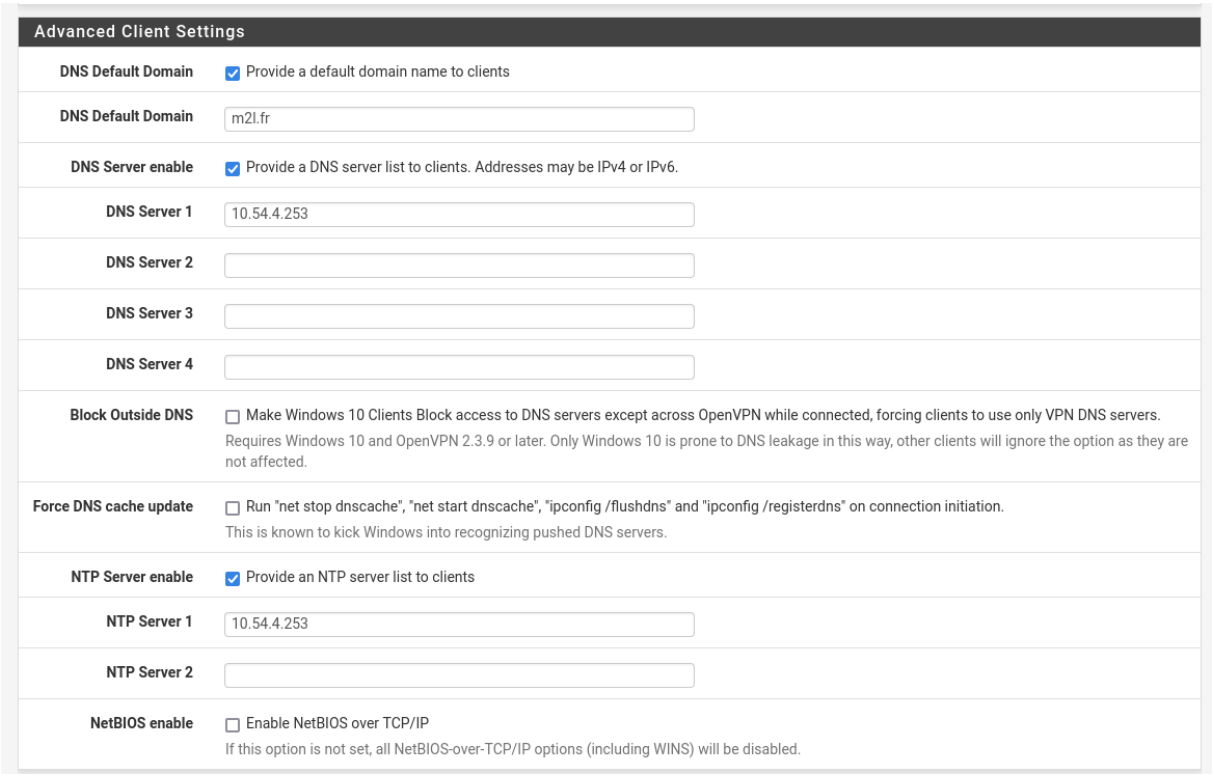
Nous allons autoriser les réseaux auxquels les utilisateurs de ADM4 peuvent acceder, étant donné que ce sont les administrateurs, ils ont le droit à tous les réseaux.

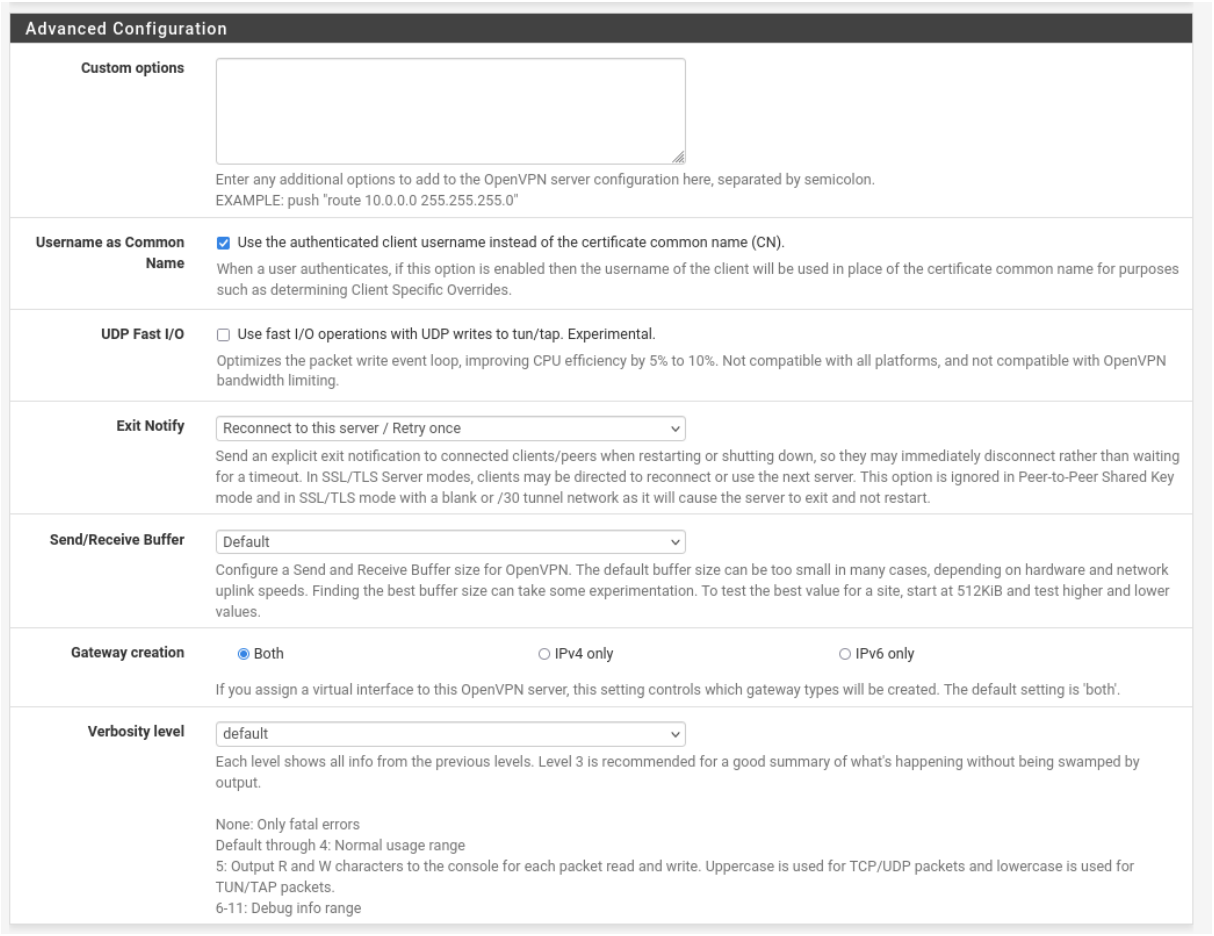


On va donner dynamiquement aux utilisateurs une configuration IP, un peu comme un DHCP.

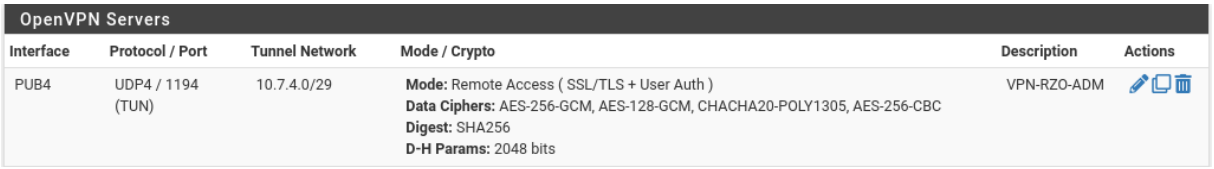


Voici la suite de la configuration IP :





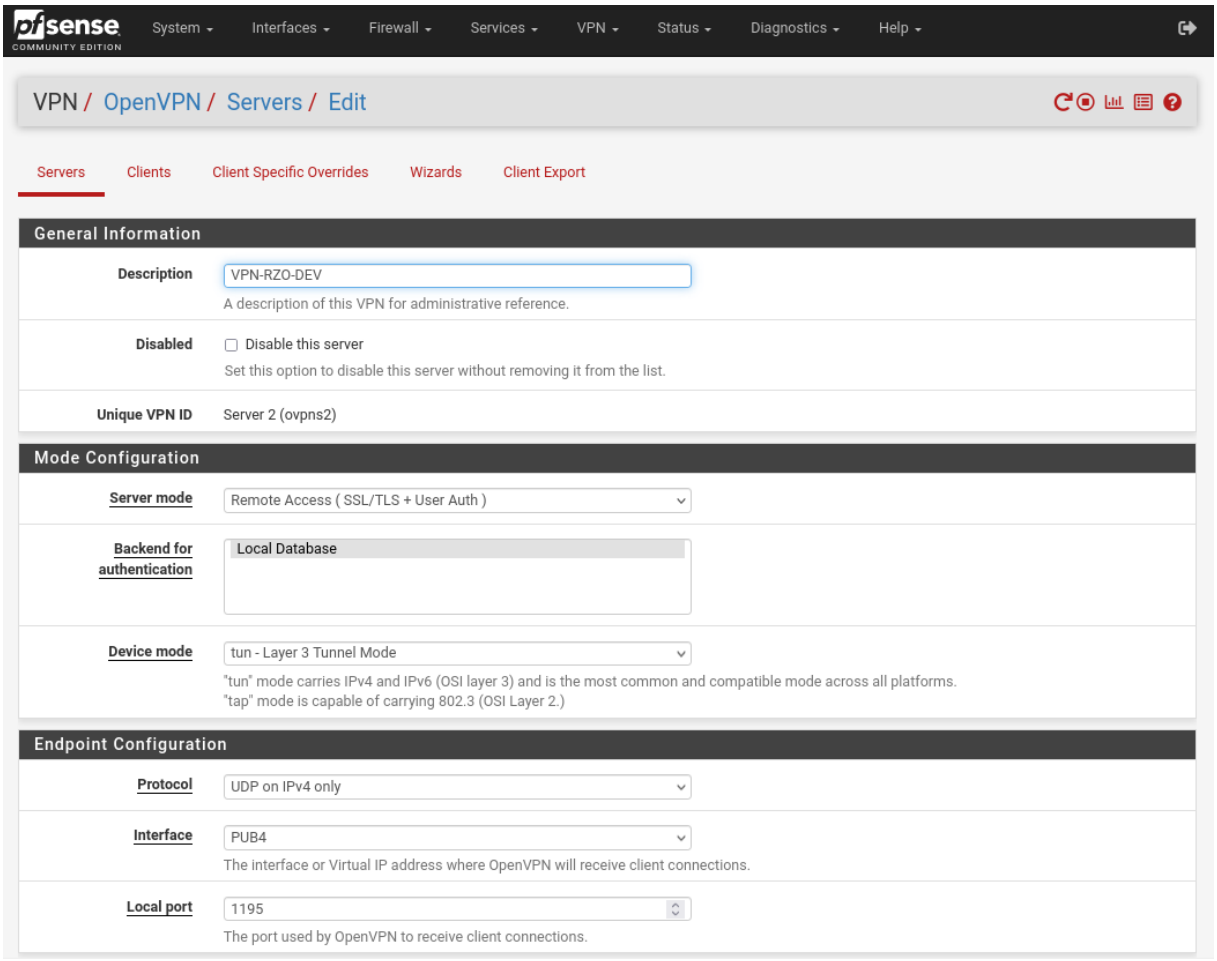
C’est la fin de la configuration du Serveur VPN ADM, il est prêt à etre utilisé.



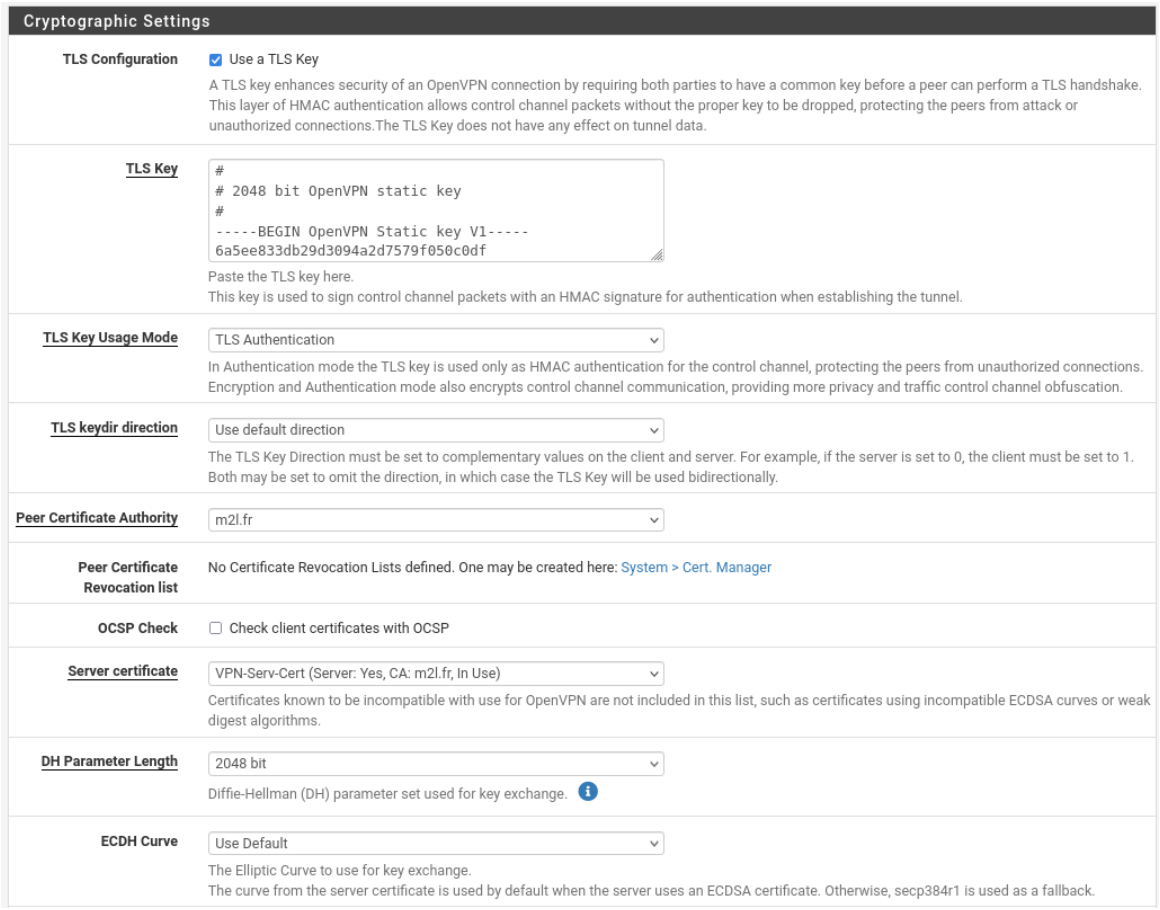
Configuration pour réseau DEV4

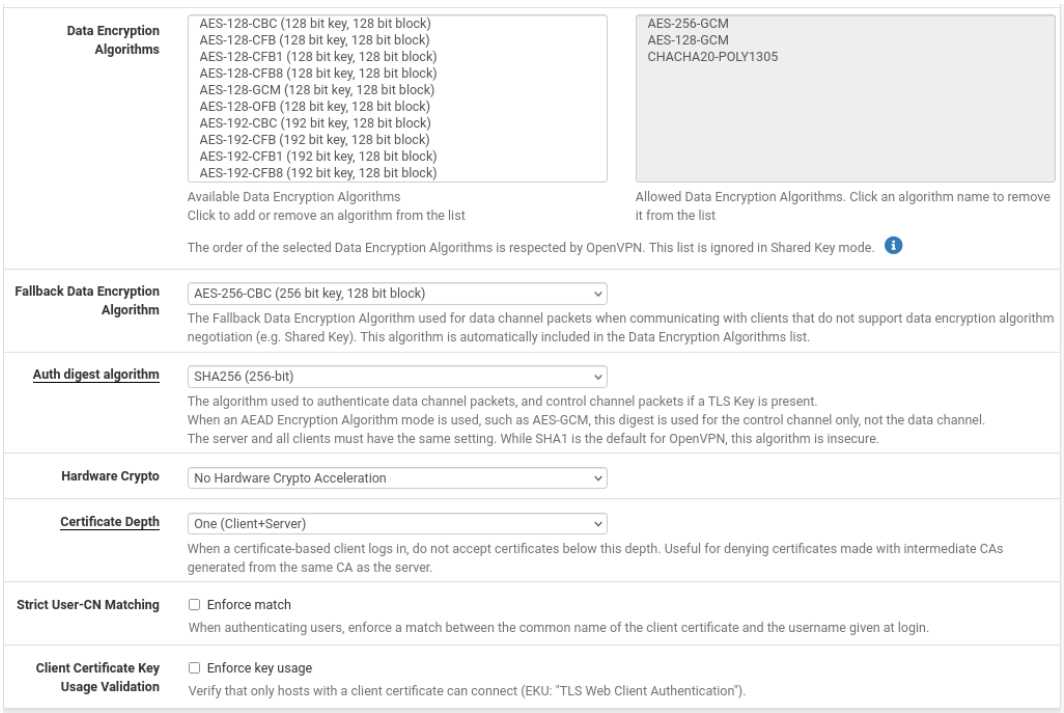
Dans cette partie je vais montrer la configuration du VPN pour DEV4 :

Ici on va changer le nom, et surtout on va changer le port sur lequel le serveur écoute parce que sur une même interface, on ne peut pas avoir deux fois le même port en écoute.

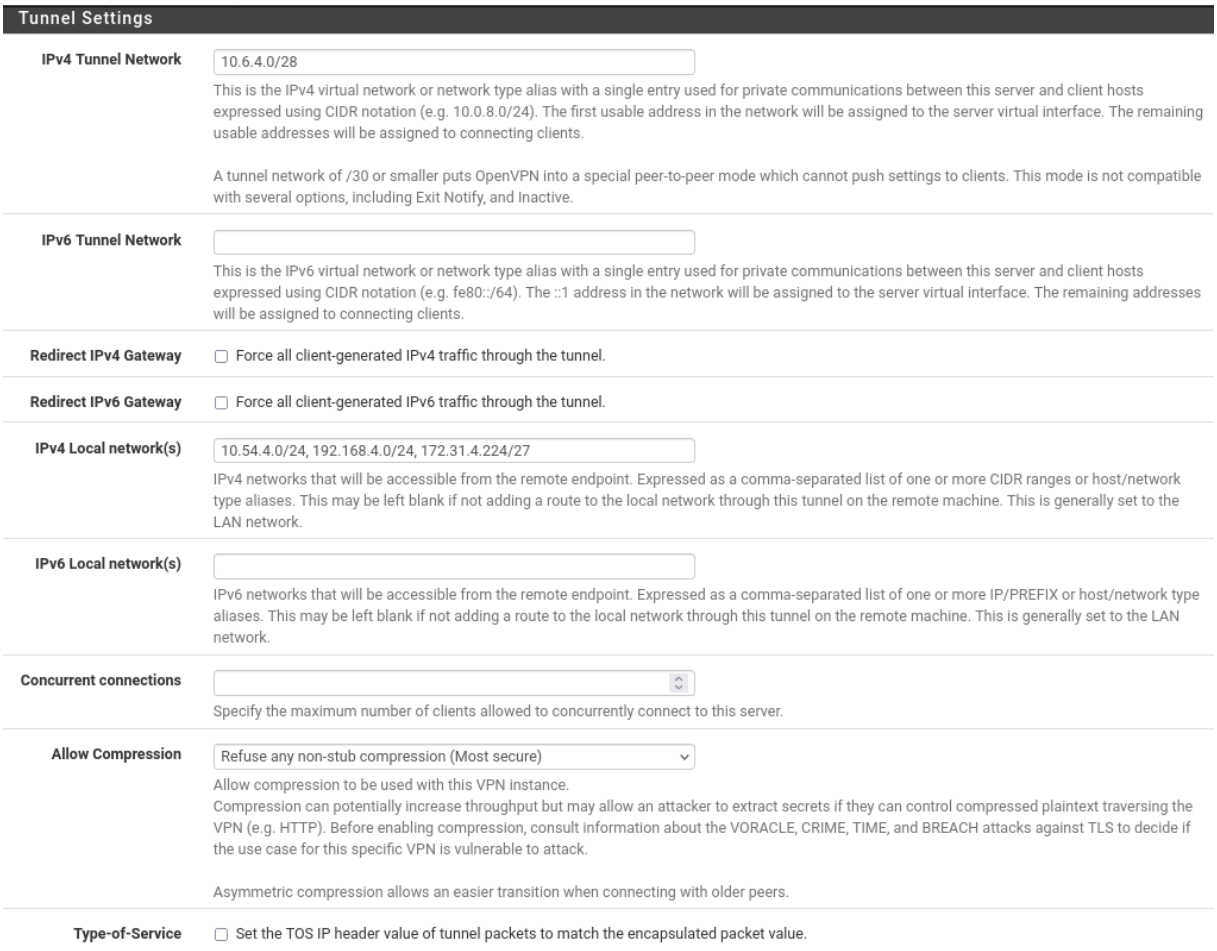


Ici on prend toujours le certificat du serveur VPN et on choisit le certificat d'autorité de l'organisme.

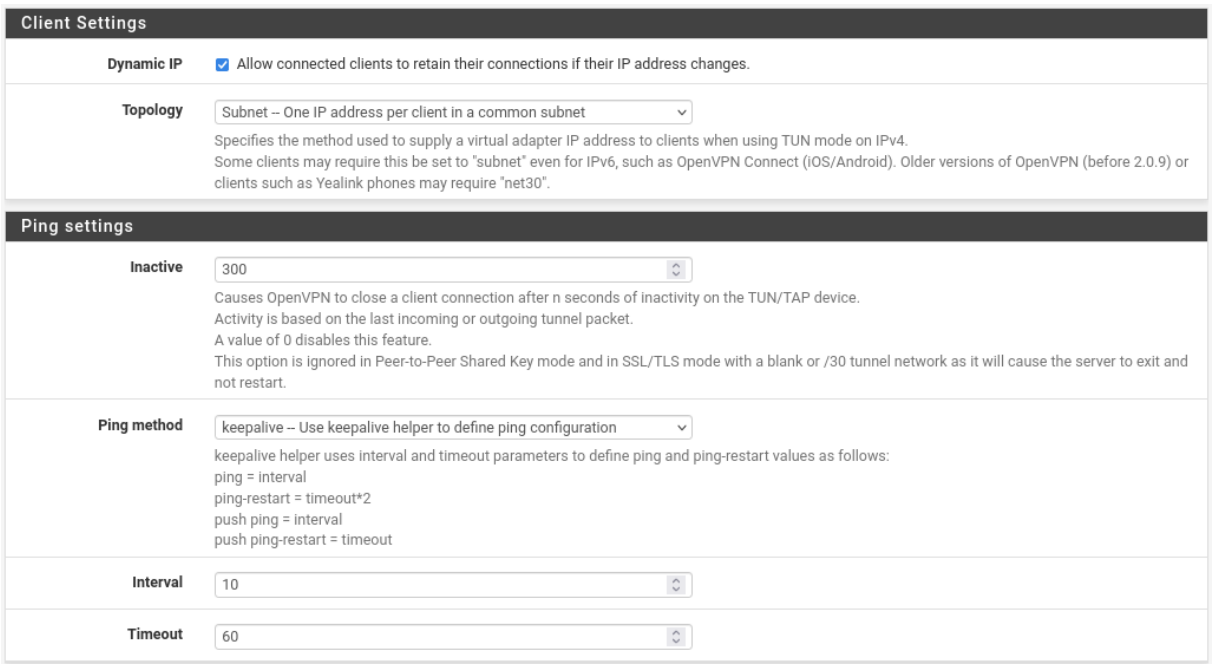




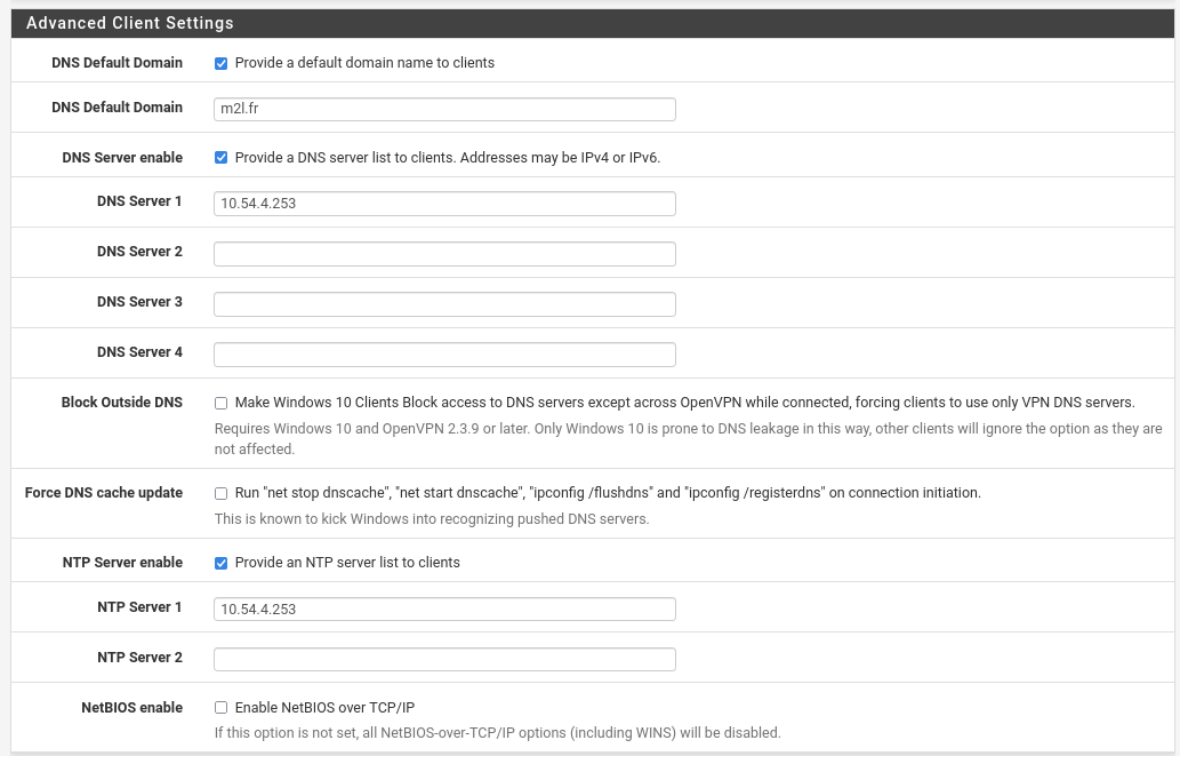
Ici, pour différencier les utilisateurs du serveur VPN ADM4 et ceux du VPN DEV4 on va mettre le réseau du tunnel en 10.6.4.0/28 et surtout on va autoriser uniquement les réseaux 10.54.4.0/24, 192.168.4.0/24 et 172.31.4.224/27 parce qu'ils ont besoin d'accéder uniquement à ces réseaux en tant que développeur.

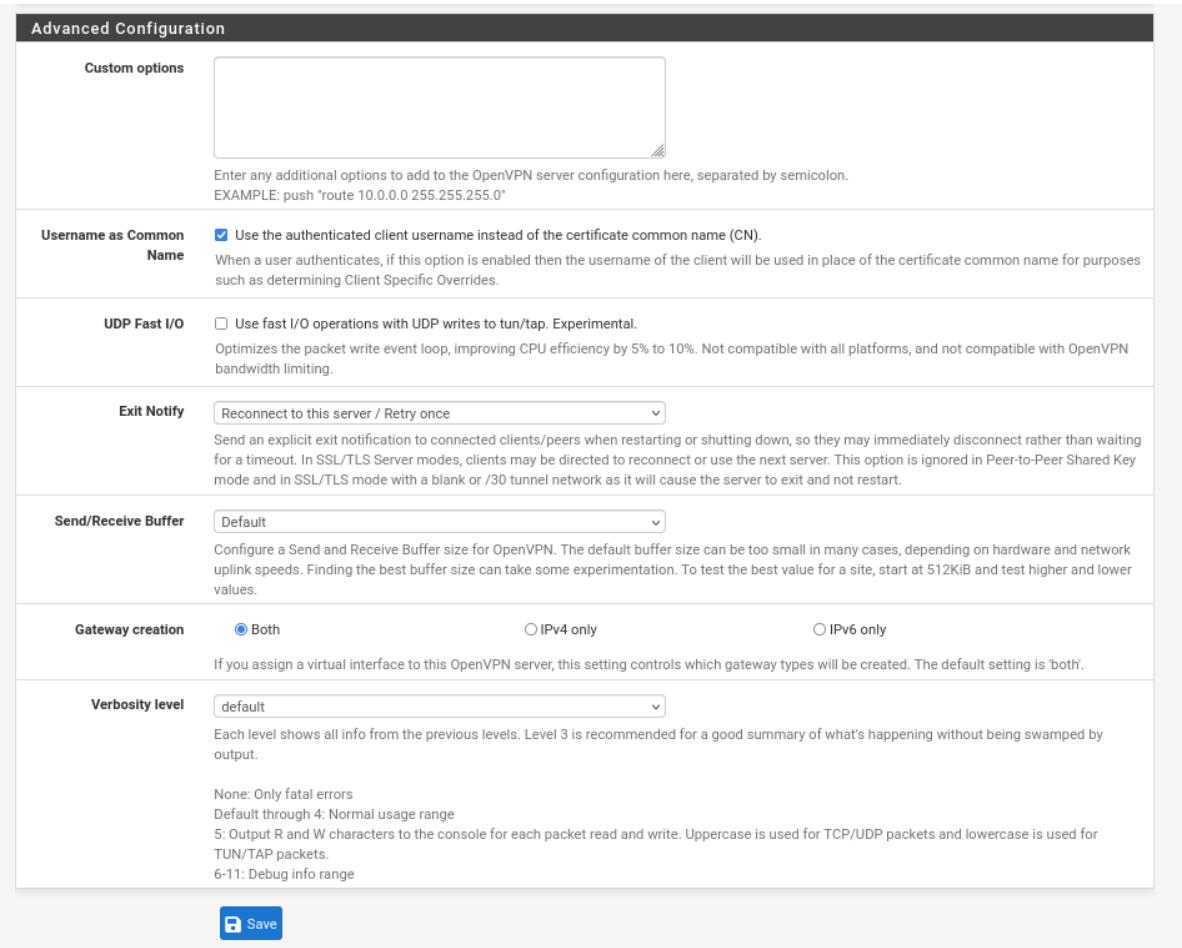


Ici on va choisir la configuration IP des utilisateurs qui utilisent le VPN.

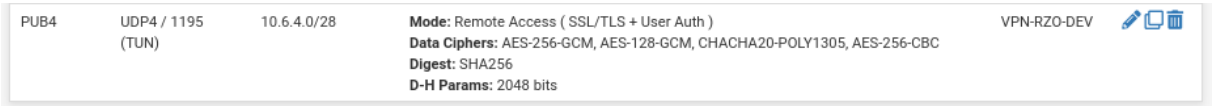


On rajoute les serveurs de temps et de noms et on peut continuer la configuration.





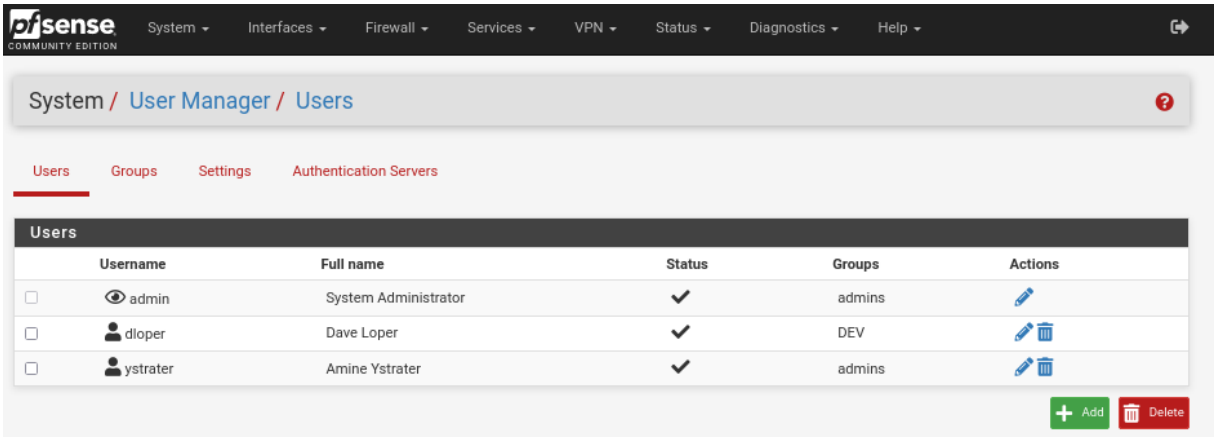
On peut voir ici que le serveur VPN DEV est créé et prêt à l'emploi.



Déclaration des utilisateurs :

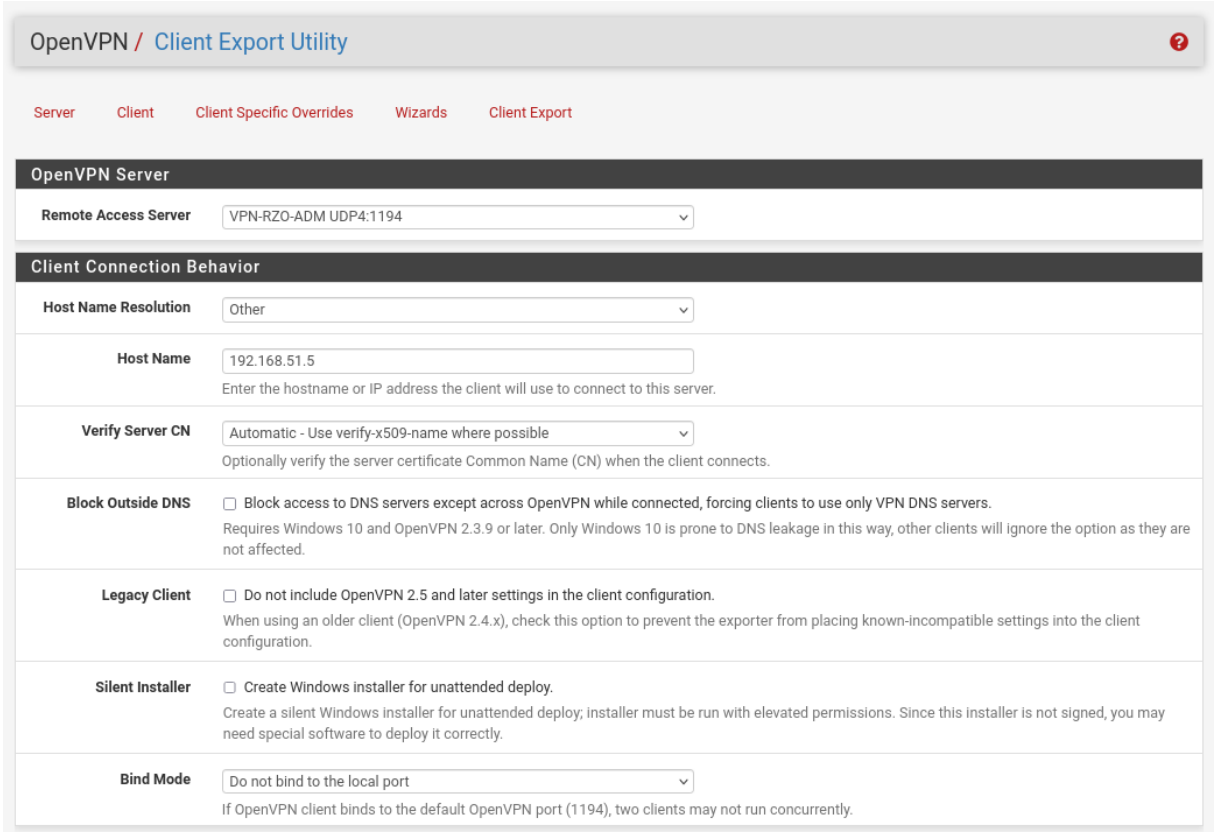
Utilisateur ADM4 :

On veut fournir la configuration pour le client afin qu'il puisse se connecter simplement en VPN, pour cela on va donc créer des utilisateurs dans le PfSense :

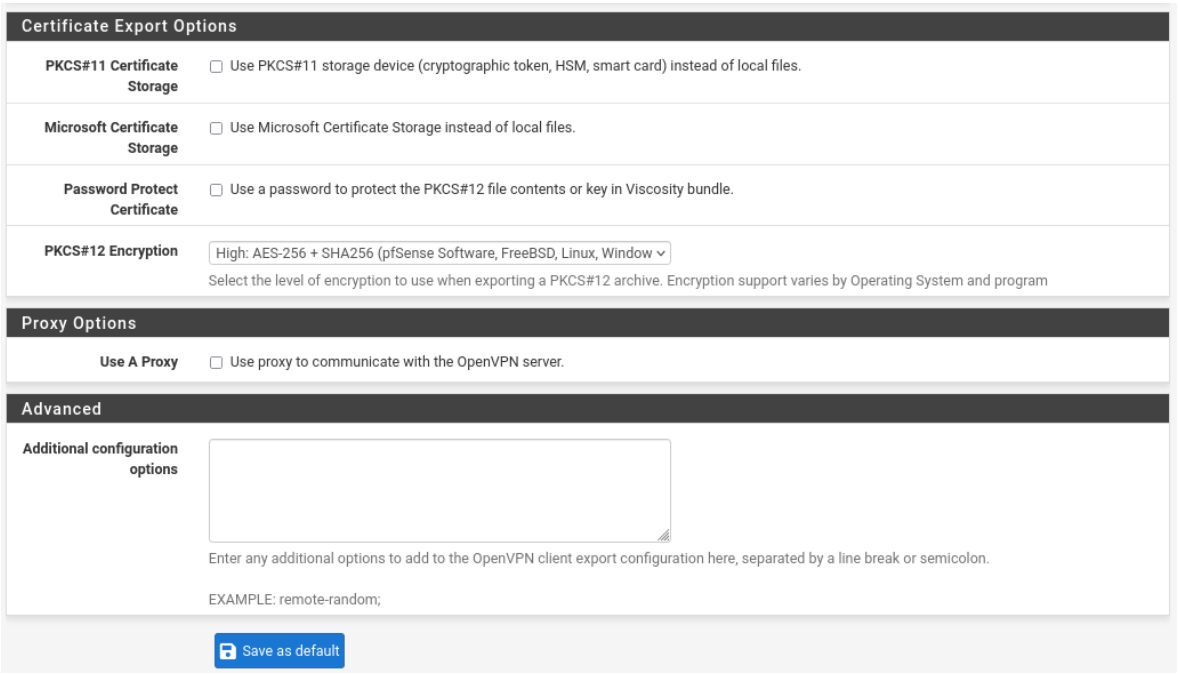


Ici on va fournir au client «ystrater » un accès au VPN pour le réseau ADM :

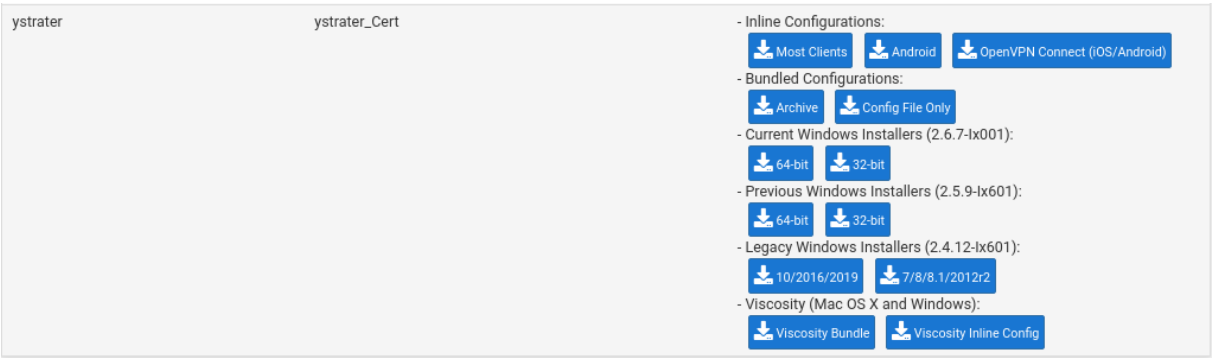
L'interface de connexion au serveur VPN est donc la patte Internet du routeur Frontal Fgtw qui possède un Nat pour rediriger le flux vers notre patte PUB4 sur lequel le serveur VPN écoute.



Nous avons besoin de toucher à rien.

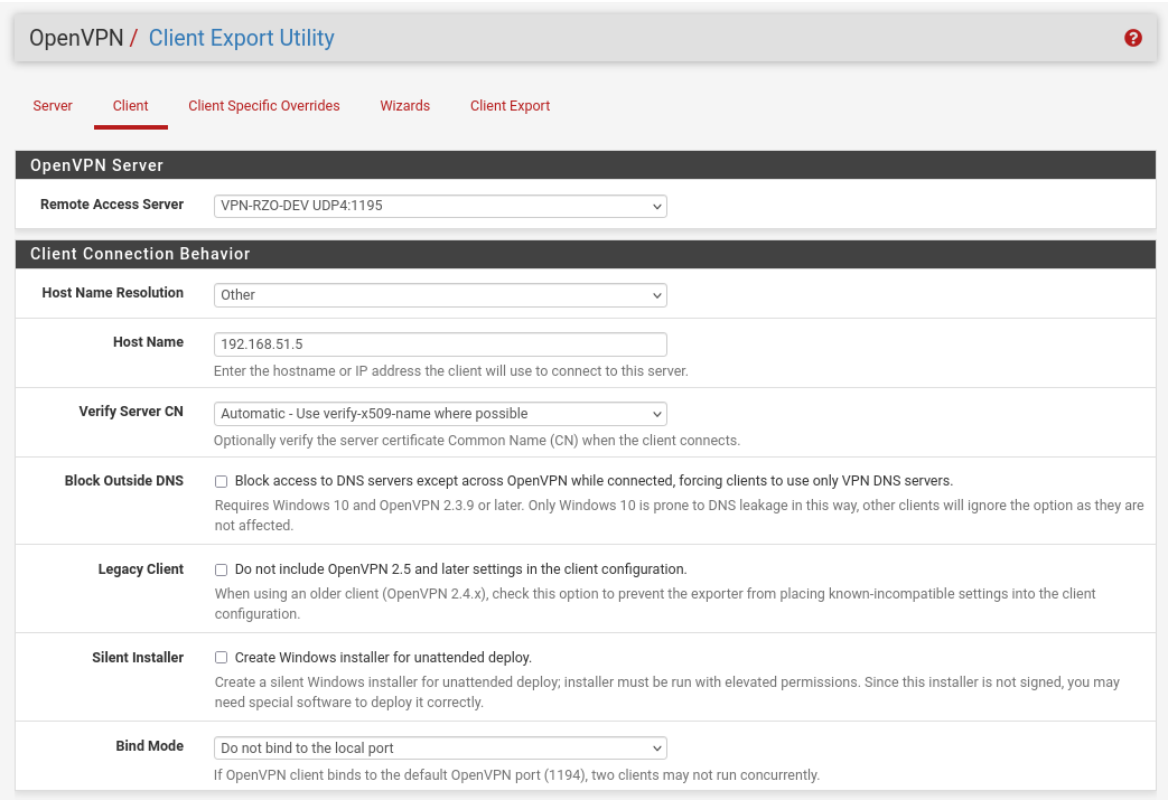


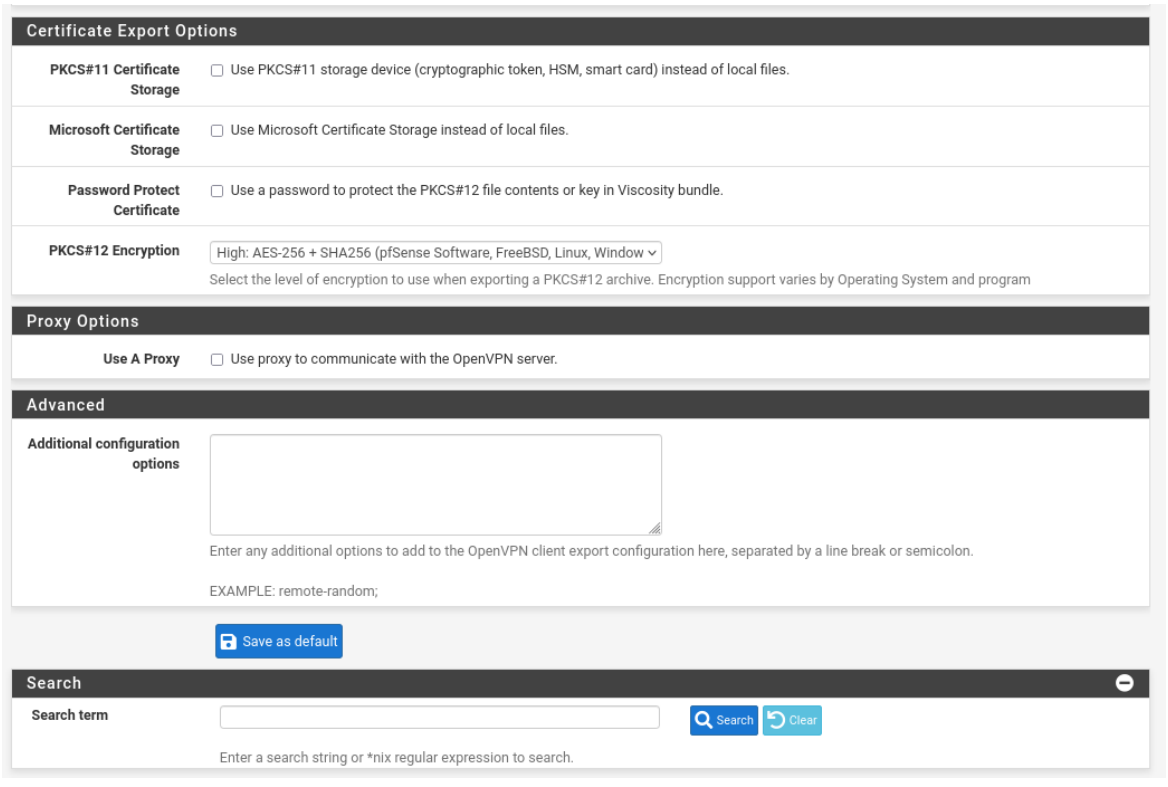
Notre utilisateur est prêt à etre exporter et qu'il pourra désormais se connecter !



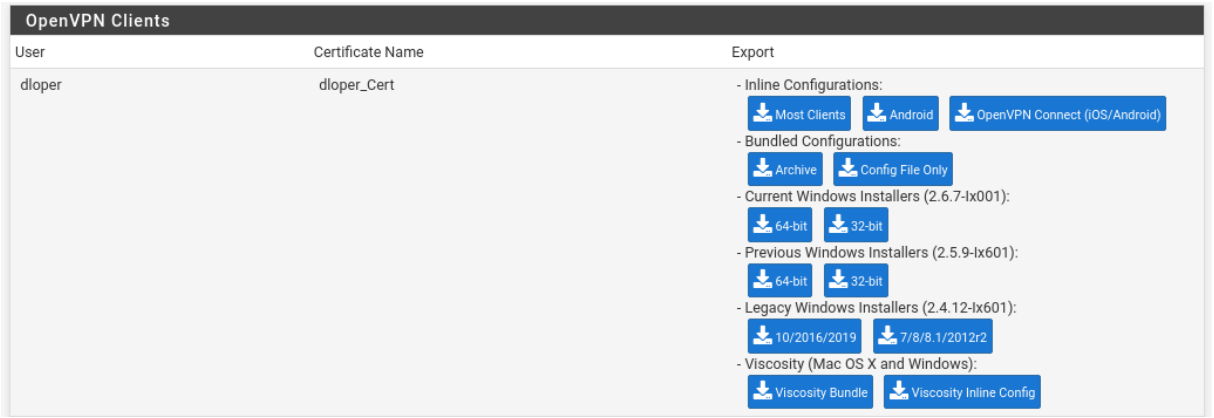
Utilisateur DEV4 :

Pour donner un accès aux utilisateurs du réseau DEV4 il faut faire attention au serveur que l'on choisit, ici on doit choisir celui qui est sur le port 1195 pour qu'il ait les caractéristiques du réseau DEV4 :

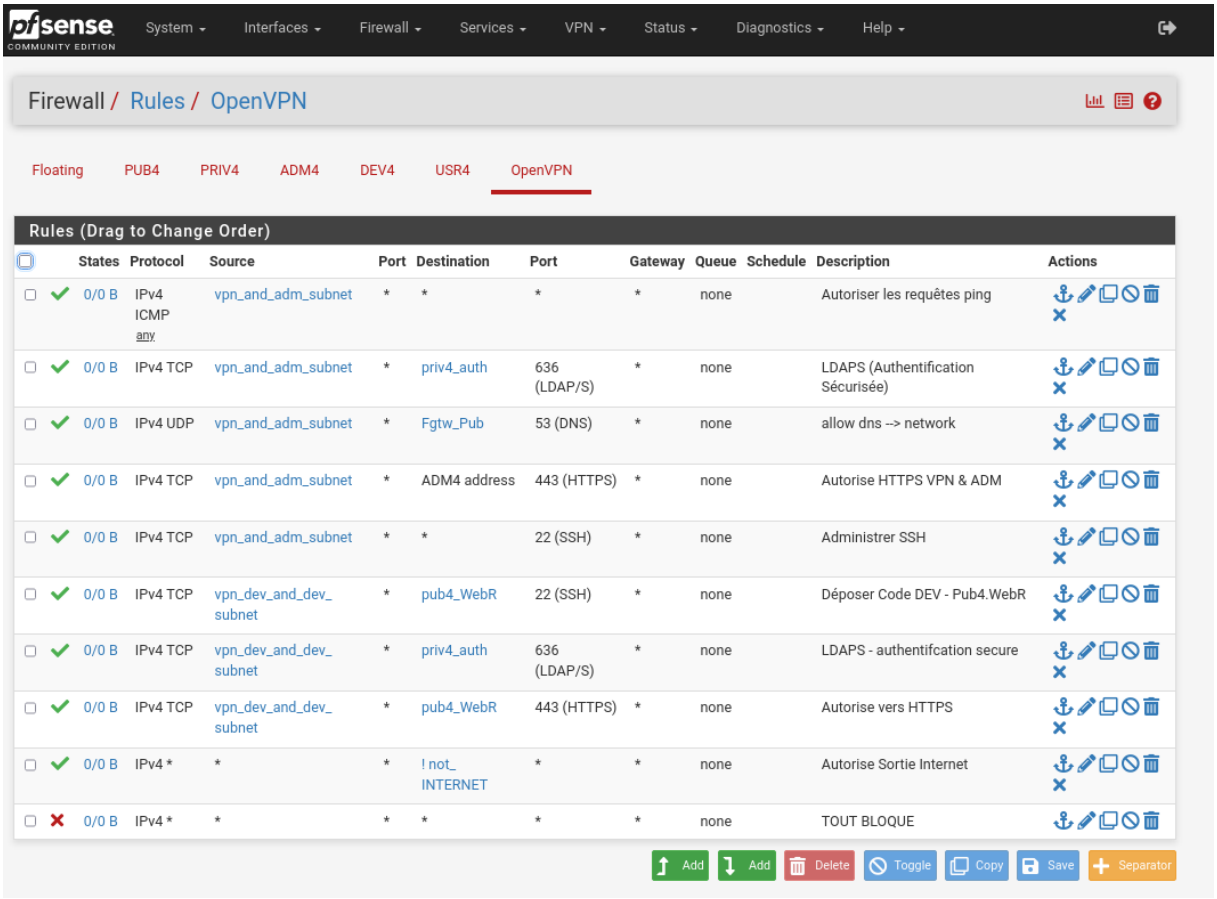




Notre utilisateur est créé et on peut l'utiliser :



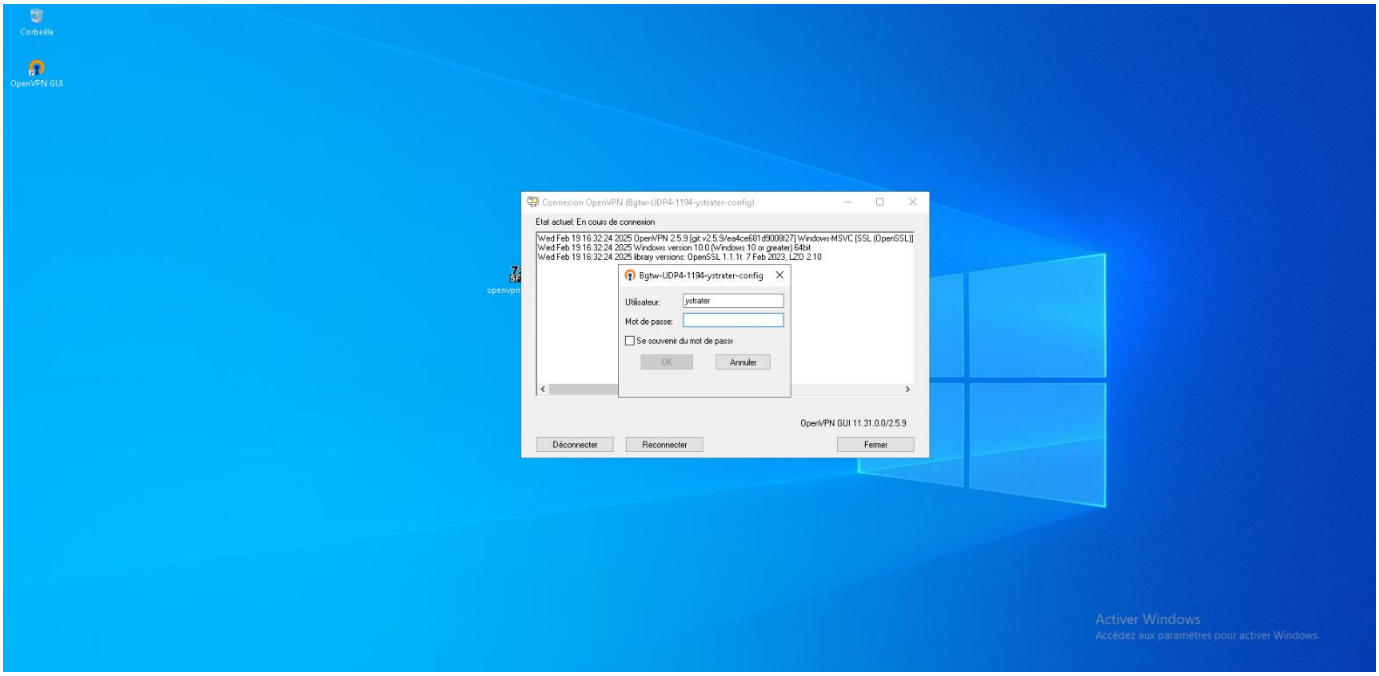
Règle de pare-feu du VPN :

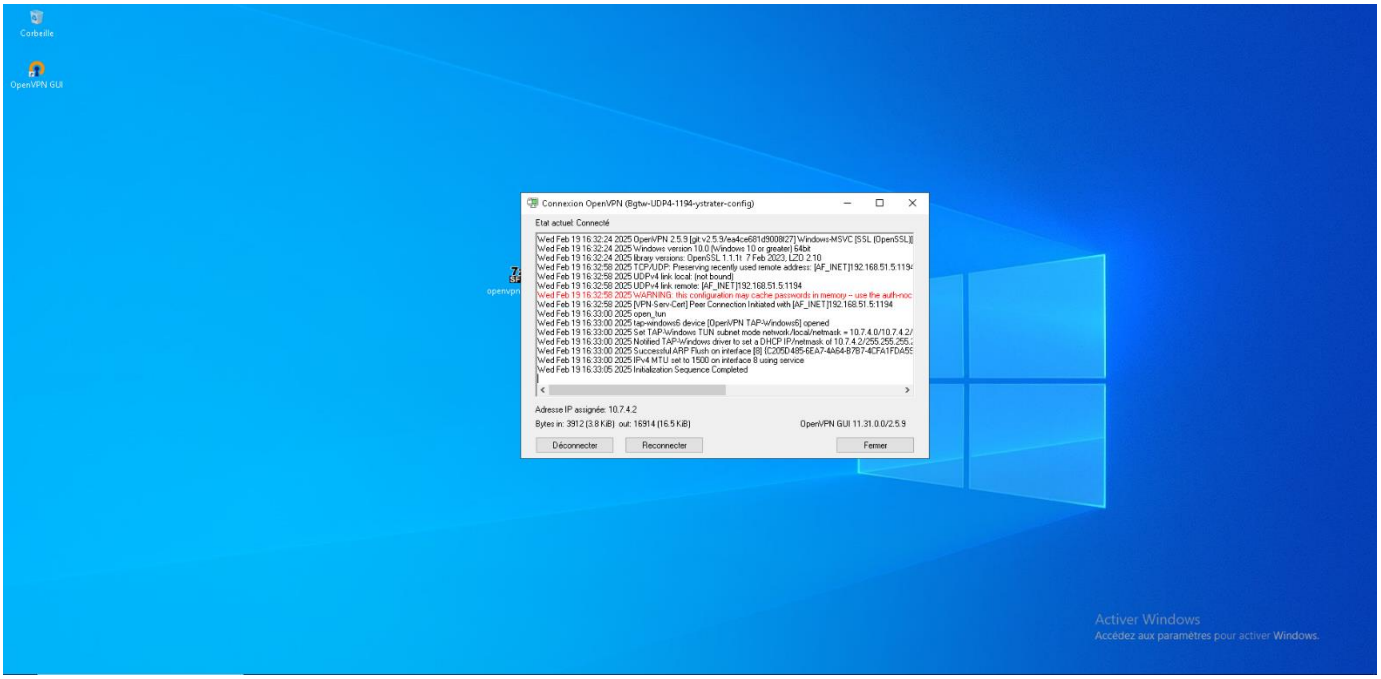


Tests VPN

Tests VPN Réseaux ADM :

On peut voir qu'on peut l'exporter et qu'il peut se connecter sur le réseau ADM :

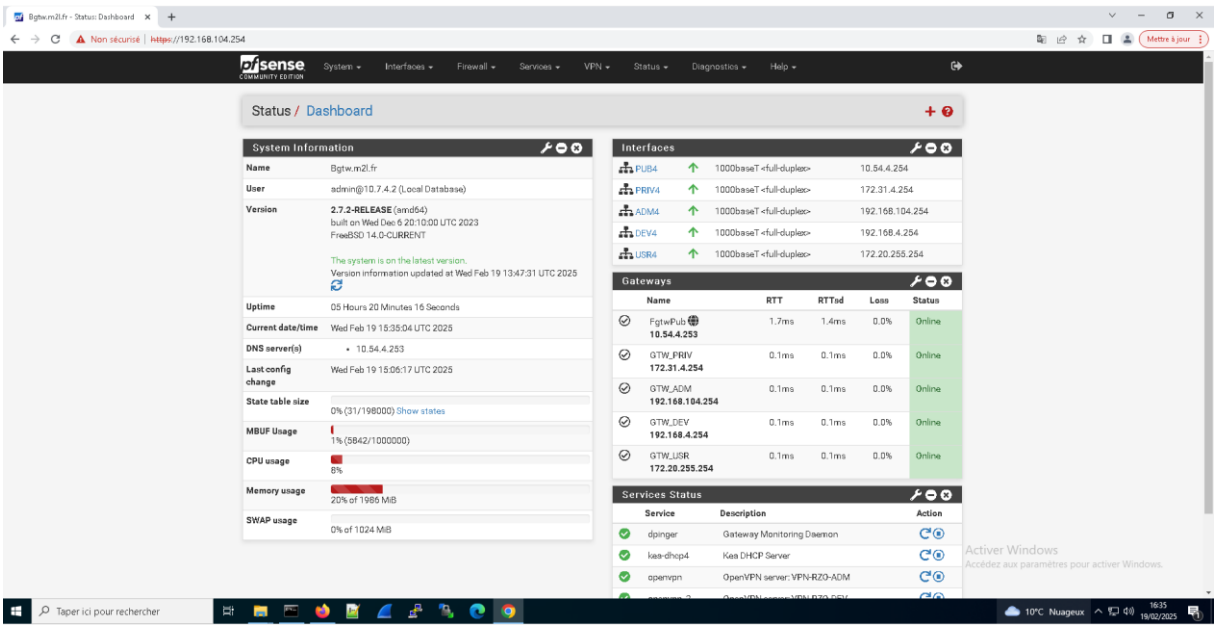




Le client à bien récupéré l'adresse IP du tunnel et donc connecté dans le réseau de l'organisme :

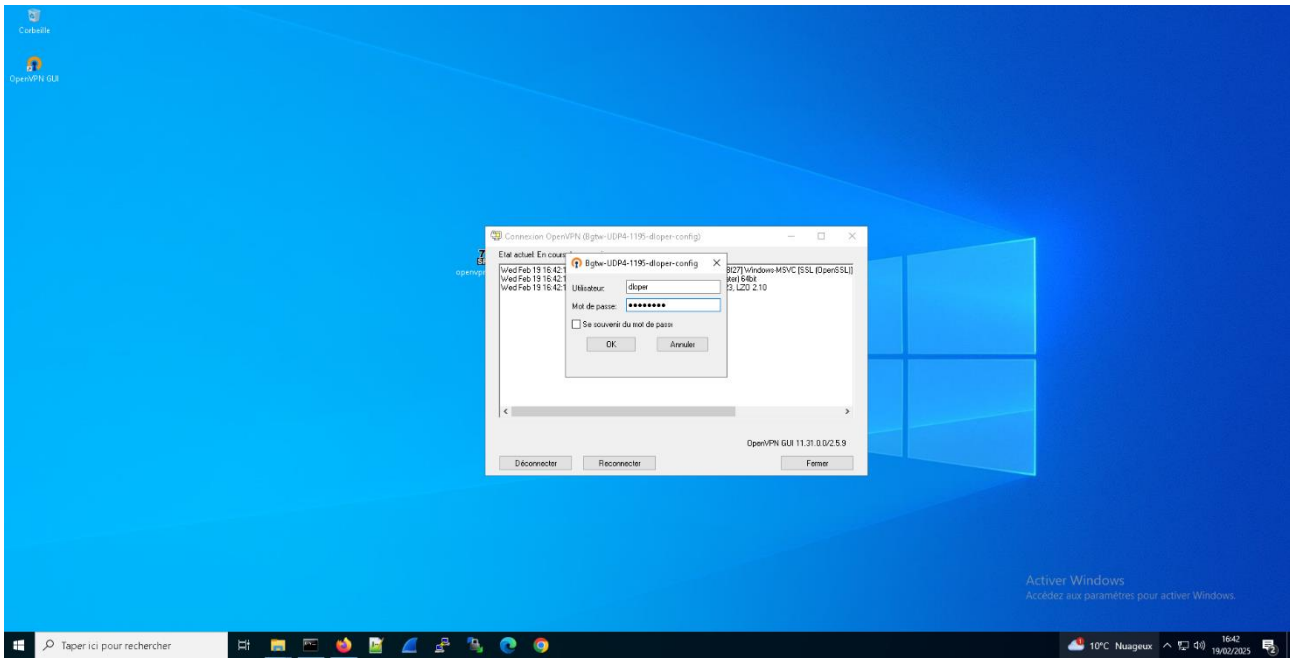
```
C:\Users\sio>ipconfig

Configuration IP de Windows


Carte inconnue OpenVPN Wintun :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte Ethernet LAN :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.55
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.1.1

Carte inconnue OpenVPN TAP-Windows6 :

   Suffixe DNS propre à la connexion. . . : m2l.fr
   Adresse IPv6 de liaison locale. . . . .: fe80::295b:8a7e:623d:253%13
   Adresse IPv4. . . . . . . . . . . . . .: 10.7.4.2
   Masque de sous-réseau. . . . . . . . . : 255.255.255.248
   Passerelle par défaut. . . . . . . . . :
```

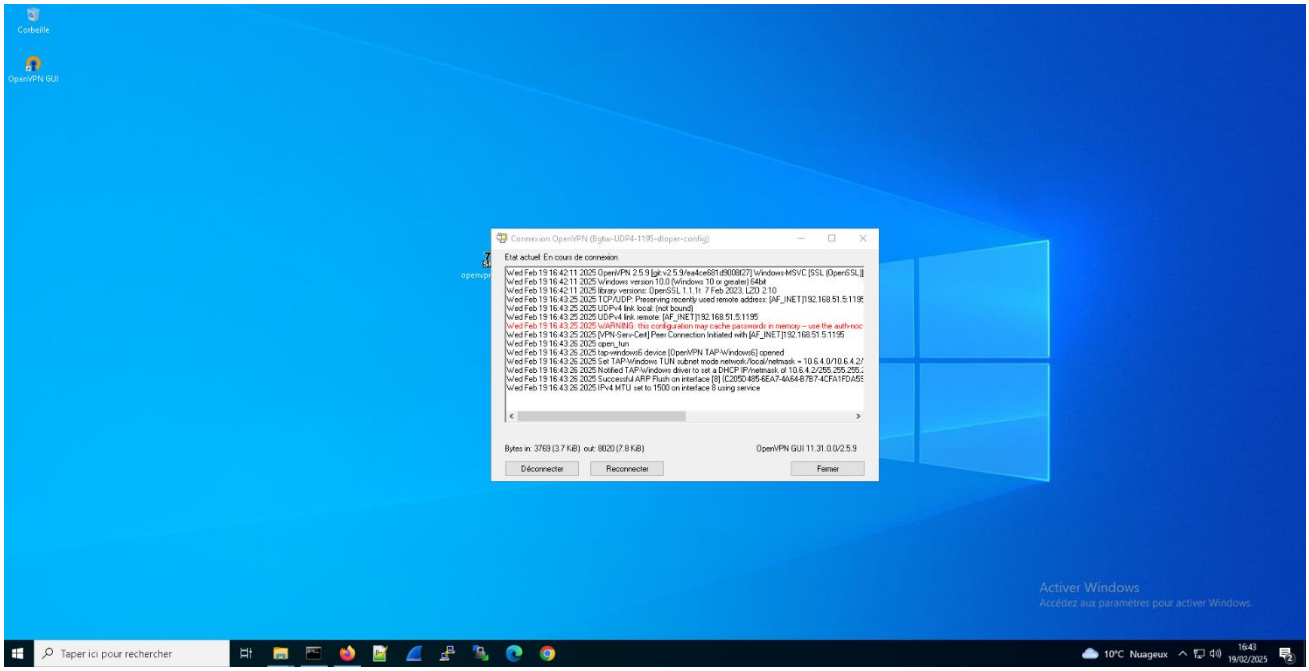
Nous sommes connecté et nous pouvons acceder à l'interface d'administration, chose qu'on ne peut pas faire en tant qu'utilisateur d'un autre réseau.



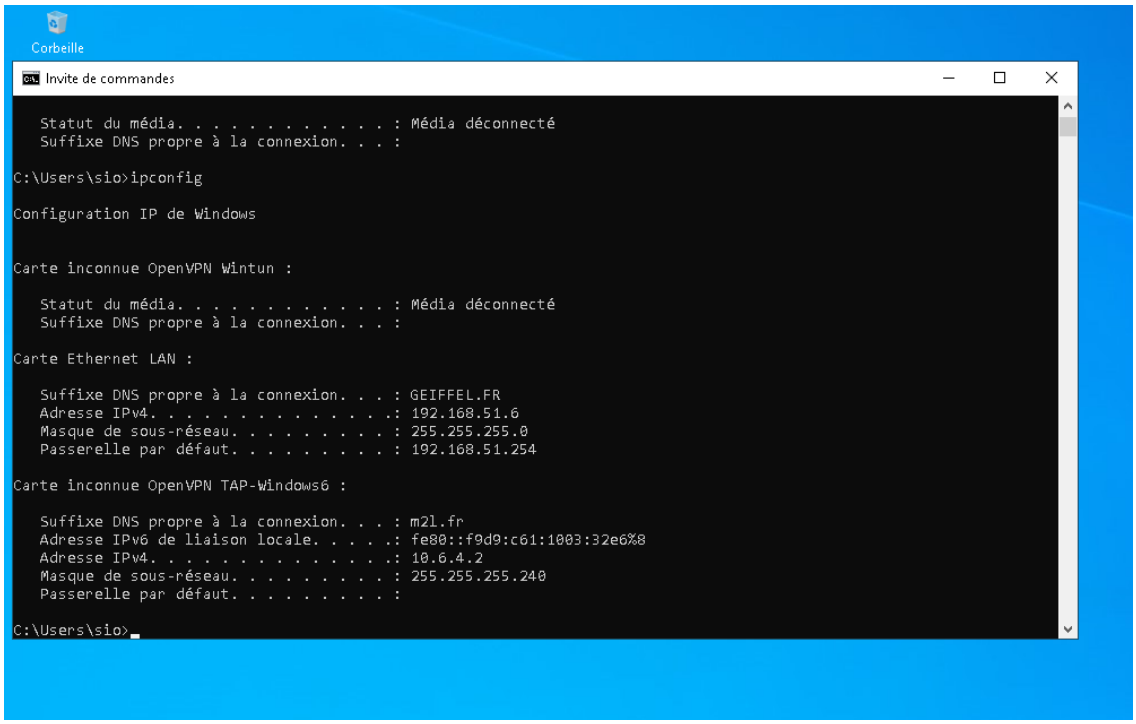
Tests VPN Réseau DEV :

On peut s’y connecter :

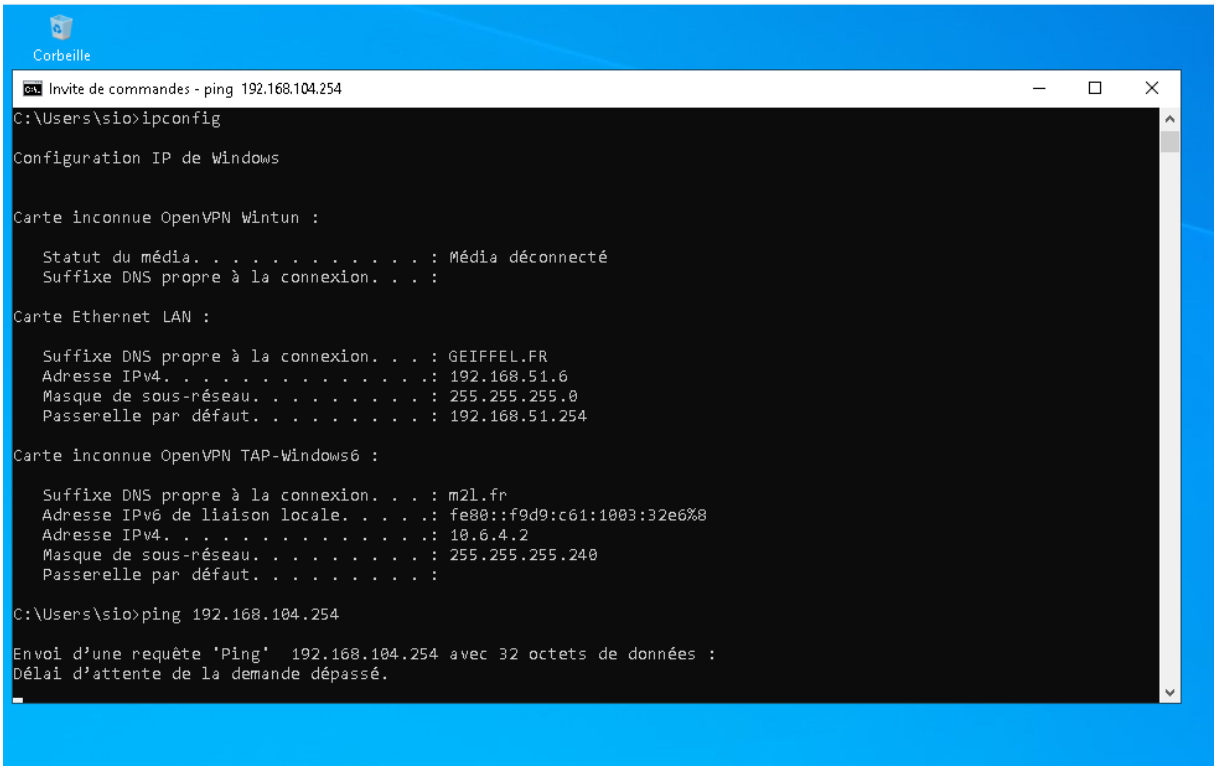




On voit bien qu'on récupère le réseau VPN du tunnel DEV4



Et qu'on ne peut pas ping l'interface d'administration :



Ni s’y connecter, preuve que nous sommes bien dans le tunnel VPN pour développeur :