OpenVPN Client-to-site avec RADIUS

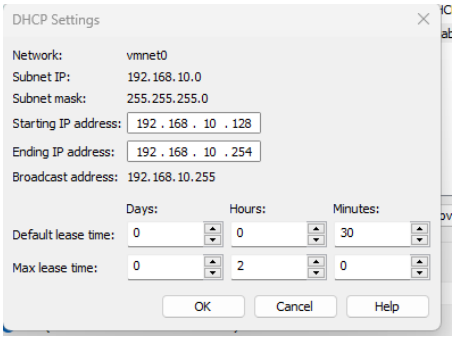
Configuration et installation d'OpenVPN pour un VPN Road Warrior client-to-site dans un domaine avec Cluster de routeurs

EHRET Louis

Table des matières

1. Configuration des postes

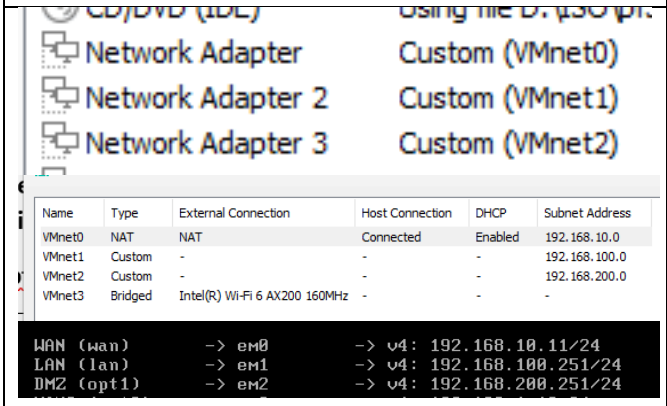
Pour ce client to site, je vais connecter le pfsense avec mon propre poste en passant par le NAT qui est en 192.168.10.X, ils vont donc être dans le même sous réseau et permettre de découvrir en premier temps le routeur depuis mon poste, et d'initialiser la connexion OpenVPN. Pour se faire, cette configuration fonctionne. J'ai donc mis que des IP fixes, et pour le NAT une IP fixe dans le sous réseau de mon NAT.



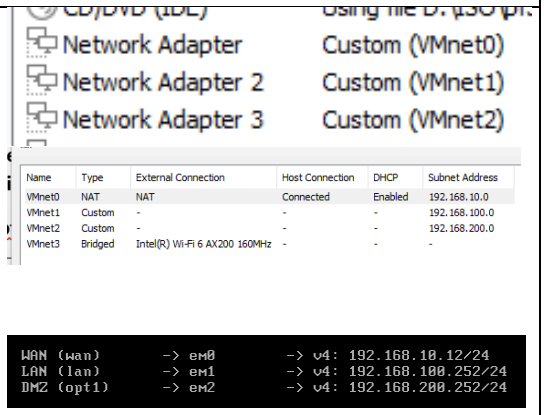
Mon NAT a récupéré cette adresse en 10.X 1

1.1 Configuration des pfsense

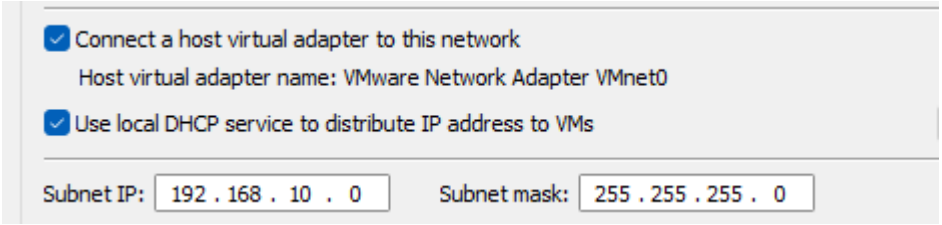
SECCIV-RTE-01



SECCIV-RTE-02

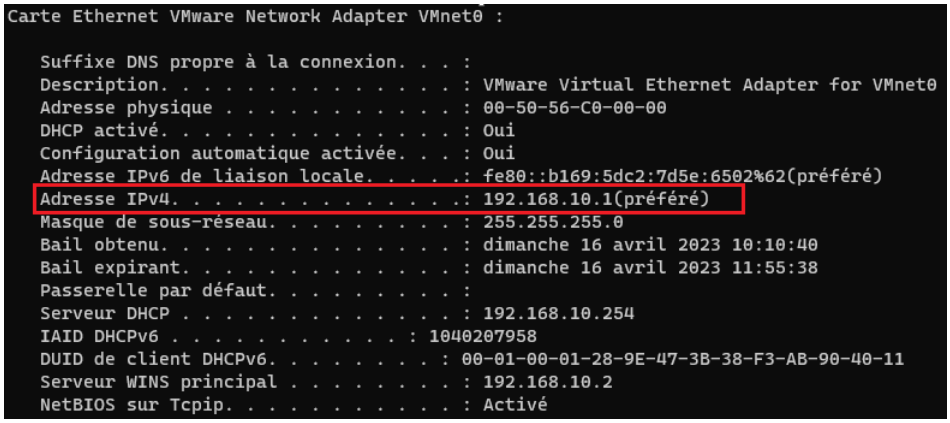


Ne pas oublier d'activer l'attribution d'une adresse IP en DHCP sur le NAT (VMNet0) pour permettre d'obtenir un sous réseau identique entre le routeur et le poste.



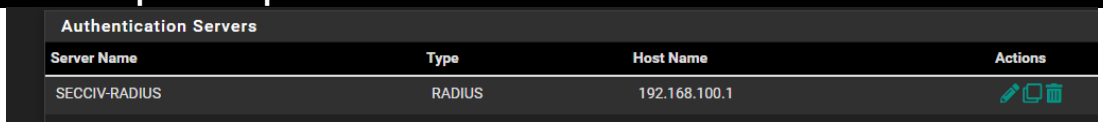
Dans la config NAT. j'ai fixé 10.X 1

1.2 Configuration de mon poste



Le poste possède la même carte VMNET0 en 192.168.10.X, pour le pont. Il faut l'adresse donnée par le poste

2. RADIUS pour OpenVPN

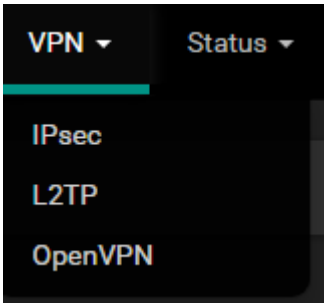


Nous allons passer à la configuration du VPN Client to site avec OpenVPN. Comme nous l'avons configuré avant, nous avons déjà notre authentification RADIUS de fonctionnel et nous l'utiliserons pour authentifier les utilisateurs distants avec pour plus de simplicité et de protection, la configuration est trouvable sur le site internet « https://louis-ehret.Info dans les projets -> afficher plus.

3. Configuration du serveur OpenVPN

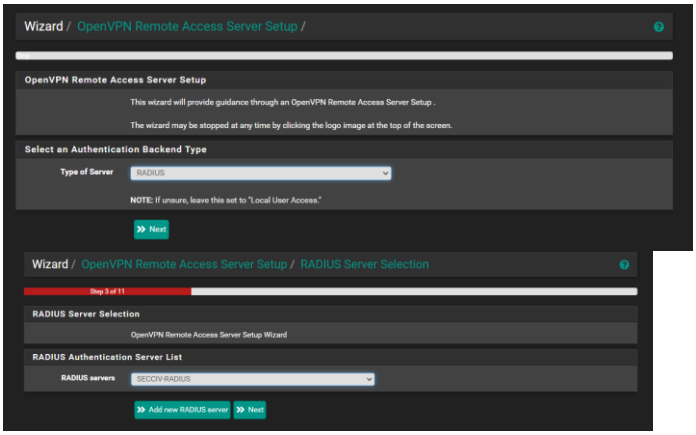
Désormais, nous allons configurer notre OpenVPN pour nous permettre d'exporter la configuration, et d'effectuer les derniers paramétrages pour l'accès à distance.

Se rendre dans VPN -> OpenVPN



Puis dans « Wizards ».

Là, nous pouvons mentionner qu'on souhaite utiliser RADIUS comme serveur d'authentification. On peut faire Next.

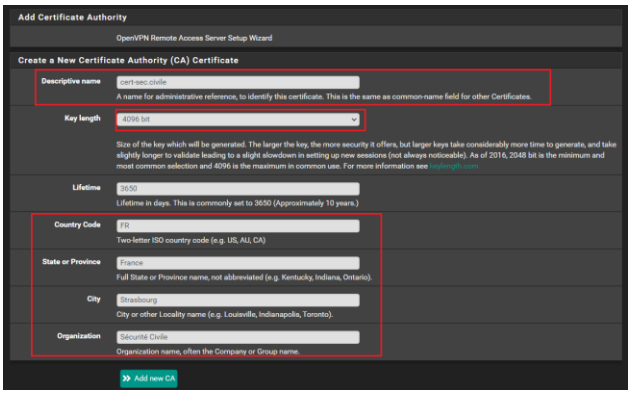


Il nous demande lequel on souhaite utiliser, et on va utiliser celui que nous avons configuré. Mais nous aurions pu très bien en ajouter un autre.

On peut faire Next.

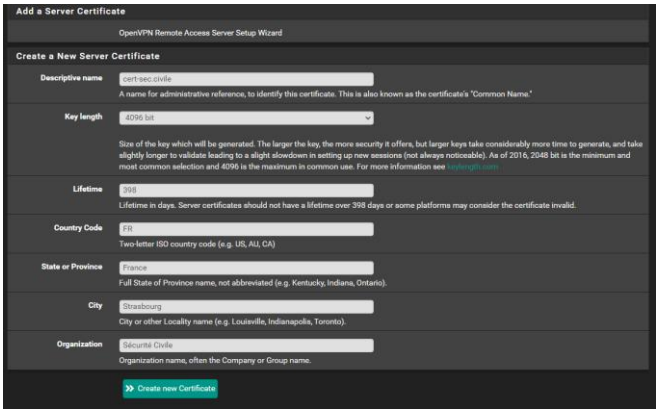
Pour le certificat d'autorité, on va donc en créer un, indiquer

On peut faire Next.



De même pour le certificat du serveur, on va en créer un.

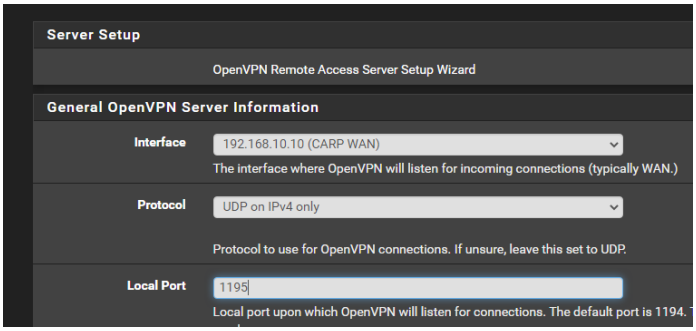
On peut faire Next.



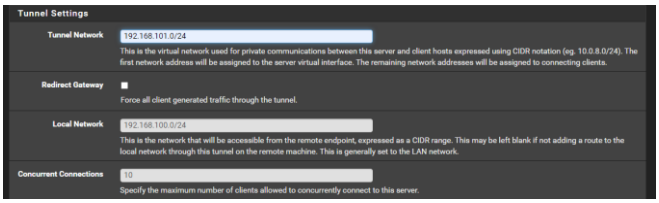
Dans « General OpenVPN Server Information », renseigner notre CARP WAN pour bien signifier que c'est les 2 routeurs ensemble qui sont concernés.

Le port ici que nous utilisons est le 1195, le TCP UDP.

Plus bas, nous avons le tunnel.

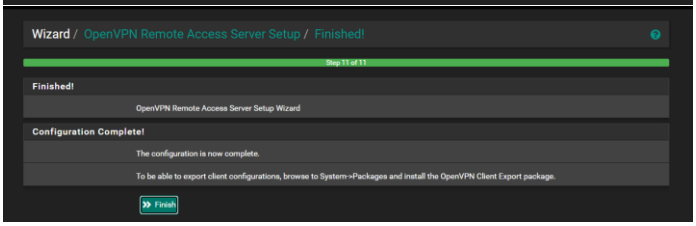


On renseigne pour le tunnel l'IP 192.168.101.0, et qui force la redirection du tunnel, et 192.168.100.0 pour le local network car c'est le réseau de notre LAN

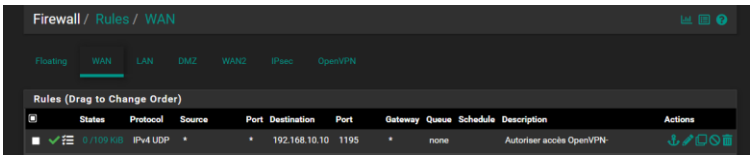


On installe aussi les règles d'OpenVPN au sein du pare-feu que nous verrons après.

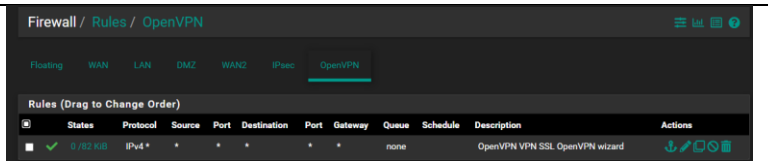
Notre configuration est terminée, mais nous avons encore quelques choses à modifier.



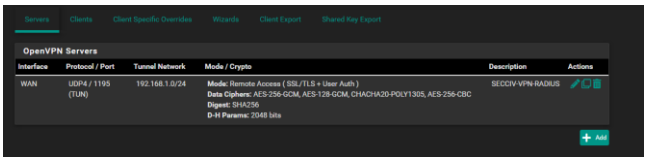
Une règle pour le WAN a bien été attribué. C'est celle que nous avons ajouté avant avec « Firewall Rule » qui nous permet de n'importe quelle source, de se connecter à 192.168.10.10 via OpenVPN uniquement.



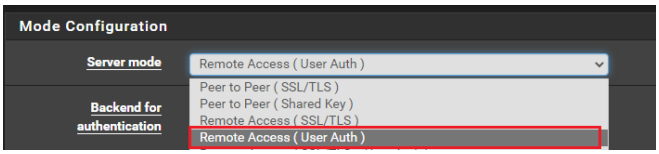
Pareil pour la catégorie OpenVPN, une règle autorisant tout vers tout à été ajoutée.



Nous allons néanmoins encore le modifier et cliquer sur le petit stylo à droite.

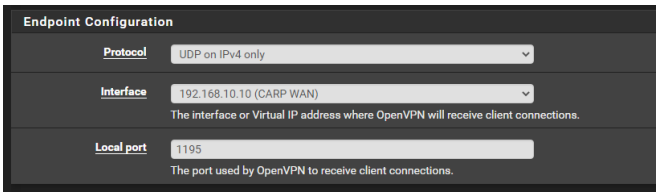


Dans la catégorie « Mode Configuration », indiquer remote access (User Auth), et non SSL/TLS + User Auth par exemple).

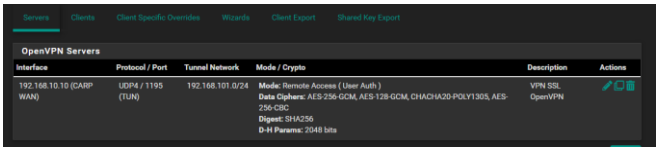


Vous allez pouvoir avoir accès à l'export du client et à l'installation automatique d'OpenVPN que l'on verra après.

Bien vérifier que le CARP est là et le bon port.



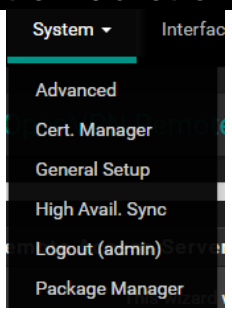
Notre serveur OpenVPN est opérationnel et près à être testé



4. Installation de l'exportation du client

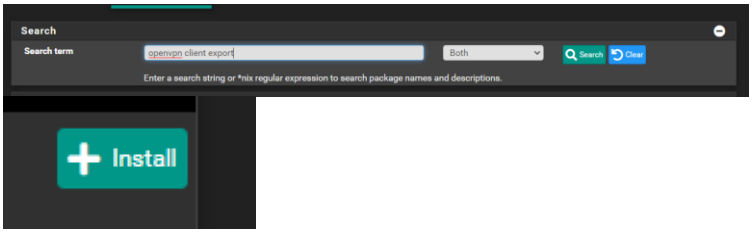
Pour pouvoir exporter notre VPN, il faut que nous allions télécharger le packet.

Pour se faire, se rendre dans System -> Package Manager

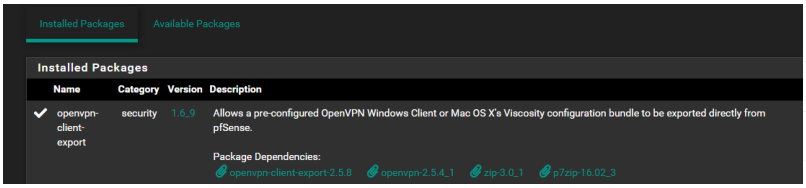


Taper « openvpn client export »

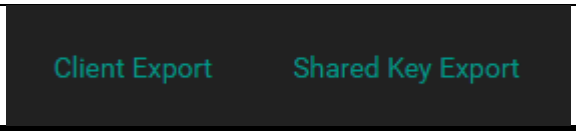
Faire installer.



Et quand on retourne dans « Packager Manager, on voit bien que le packet a été installé.

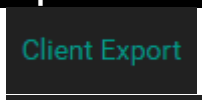


Nous avons 2 nouvelles catégories qui nous serviront plus tard.

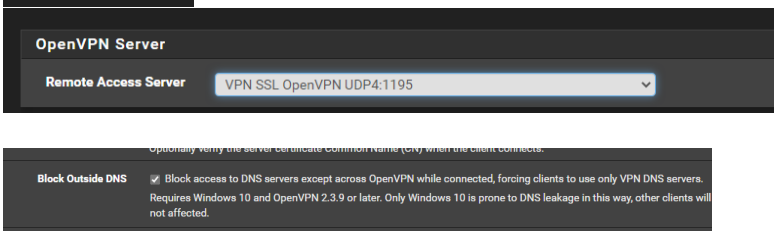


5. Configuration de l'export pour le client

Désormais, nous allons pouvoir exporter en cliquant sur « Client Export ».

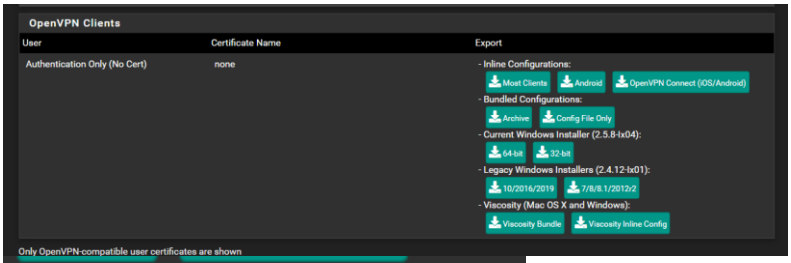


La première partie de la page doit afficher ceci, et nous expliquer qui est le serveur d'accès distant. Ici, notre RADIUS, via TCP UDP du port 1195.

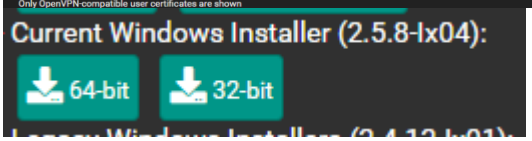


Si on poursuit les modifications, on a la possibilité de bloquer les DNS de l'extérieur, c'est ce que nous allons faire.

Plus bas encore, nous avons les clients OpenVPN. Il faut désormais télécharger OpenVPN client sur mon poste pour tester si tout fonctionne.



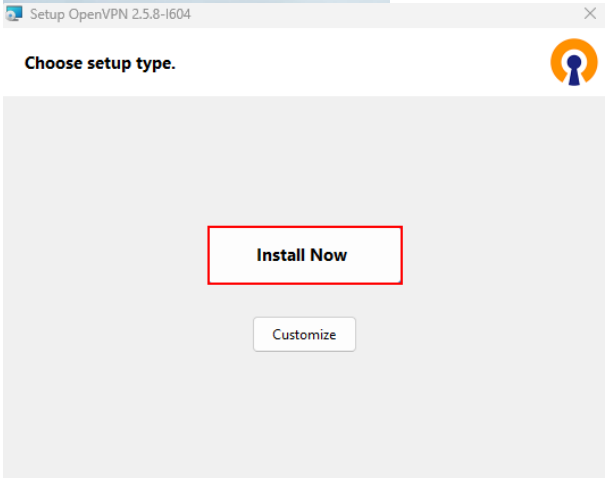
Pour se faire, télécharger le package « Current Windows Installer ».



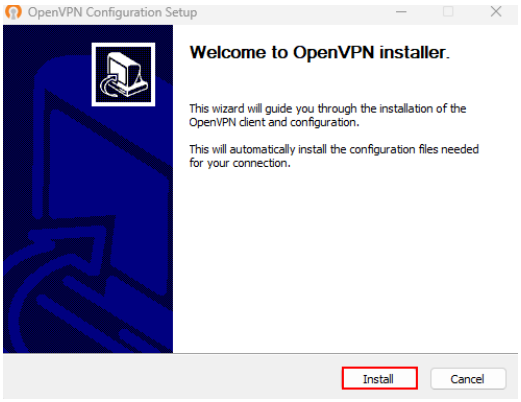
6. Installation d'OpenVPN sur le poste client

Une fois copié, le mettre sur le bureau de l'ordinateur hôte, par exemple. Retournons sur mon pc pour commencer l'installation

Cliquez sur **Install now** pour installer le client OpenVPN.

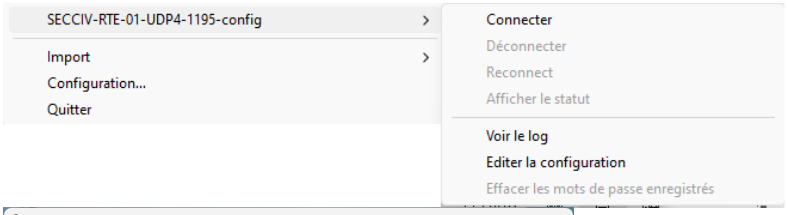


Une autre fenêtre qui concerne la configuration du client OpenVPN apparaitra, cliquez sur **Install** et suivez la configuration.



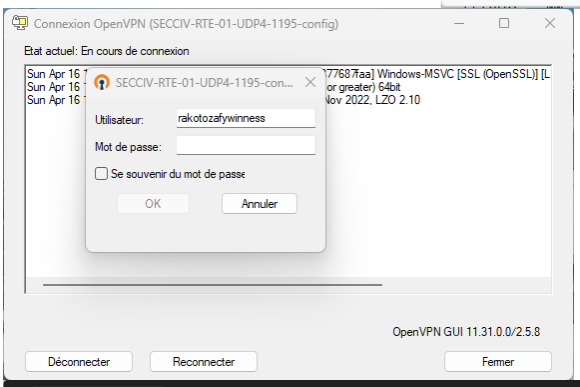
Le client OpenVPN installé, procédez au test de connexion sur le tunnel VPN, étant donné que toute la configuration que nous avons effectué a été intégré à l'installation.

Effectuer un clic droit, puis sélectionner la configuration, elle doit porter les mêmes informations que notre configuration avec UDP4, le routeur, et le port 1195.

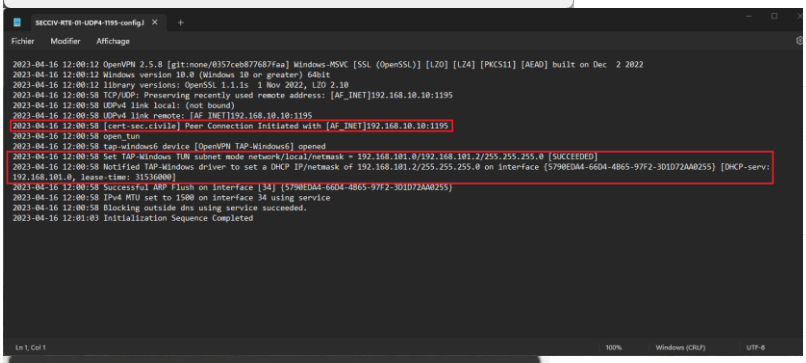


Il nous suffit de renseigner des identifiants d'utilisateur de l'AD dans OpenVPN pour permettre d'établir la connexion.

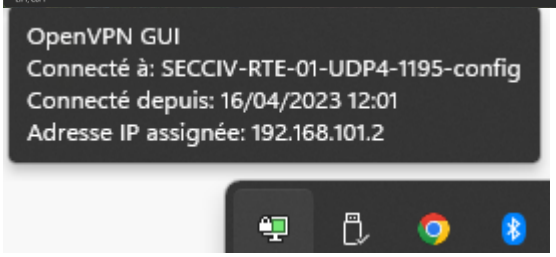
Rappel : Nous n'utilisons pas de certificat utilisateur, mais RADIUS comme serveur d'authentification. C'est donc pfsense qui a interrogé le serveur pour vérifier si les informations fournies pour la connexion étaient en corrélation avec les informations de l'annuaire Windows.



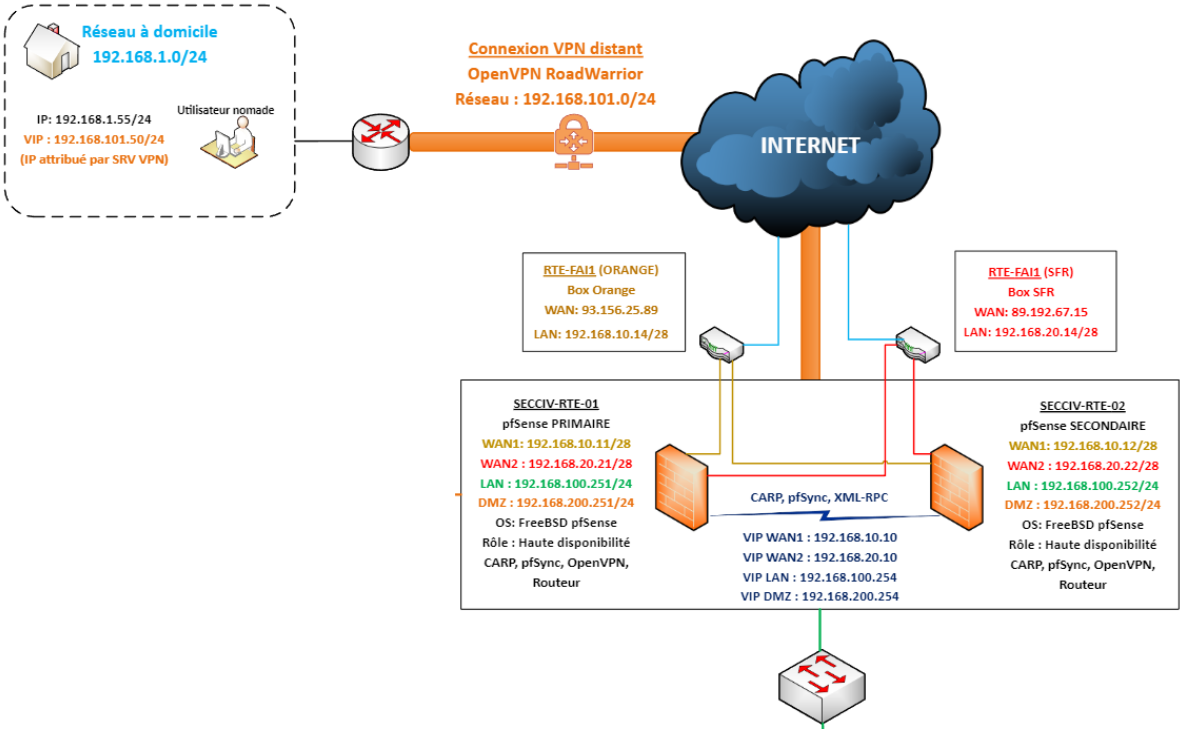
Les logs nous indiquent bien que la connexion a été établie.



On a obtenu une adresse IP 192.168.101.2, et je suis bien connecté à mon routeur via le tunnel.



Notre Client-to-site est opérationnel et fonctionnel.


Réseau à domicile
192.168.1.0/24
IP: 192.168.1.55/24
VIP : 192.168.101.50/24
(IP attribué par SRV VPN)
Utilisateur nomade
Connexion VPN distant
OpenVPN RoadWarrior
Réseau : 192.168.101.0/24
INTERNET
RTE-FAI1 (ORANGE)
Box Orange
WAN: 93.156.25.89
LAN: 192.168.10.14/28
RTE-FAI1 (SFR)
Box SFR
WAN: 89.192.67.15
LAN: 192.168.20.14/28
SECCIV-RTE-01
pfSense PRIMAIRE
WAN1: 192.168.10.11/28
WAN2 : 192.168.20.21/28
LAN : 192.168.100.251/24
DMZ : 192.168.200.251/24
OS: FreeBSD pfSense
Rôle : Haute disponibilité
CARP, pfSync, OpenVPN,
Routeur
CARP, pfSync, XML-RPC
VIP WAN1 : 192.168.10.10
VIP WAN2 : 192.168.20.10
VIP LAN : 192.168.100.254
VIP DMZ : 192.168.200.254
SECCIV-RTE-02
pfSense SECONDAIRE
WAN1: 192.168.10.12/28
WAN2 : 192.168.20.22/28
LAN : 192.168.100.252/24
DMZ : 192.168.200.252/24
OS: FreeBSD pfSense
Rôle : Haute disponibilité
CARP, pfSync, OpenVPN,
Routeur