



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

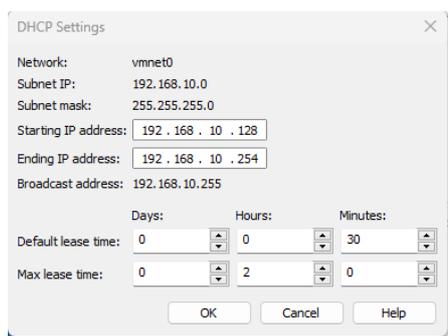
EHRET Louis

Table des matières

1. Configuration des postes.....	2
1.1 Configuration des pfsense	2
1.2 Configuration de mon poste.....	2
2. RADIUS pour OpenVPN.....	3
3. Configuration du serveur OpenVPN.....	3
4. Installation de l'exportation du client	5
5. Configuration de l'export pour le client.....	6
6. Installation d'OpenVPN sur le poste client.....	6

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

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	NAT	NAT	Connected	Enabled	192.168.10.0
VMnet1	Custom	-	-	-	192.168.100.0
VMnet2	Custom	-	-	-	192.168.200.0
VMnet3	Bridged	Intel(R) Wi-Fi 6 AX200 160MHz	-	-	-

```

WAN (wan) -> em0 -> v4: 192.168.10.11/24
LAN (lan) -> em1 -> v4: 192.168.100.251/24
DMZ (opt1) -> em2 -> v4: 192.168.200.251/24
                    
```

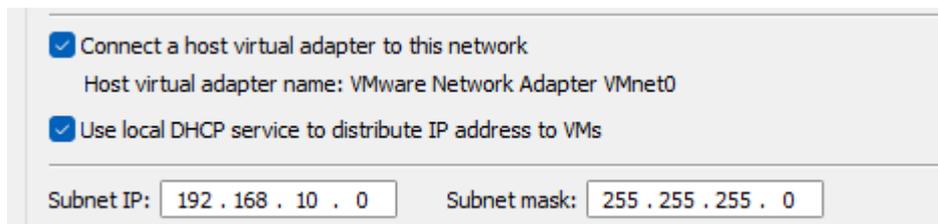
SECCIV-RTE-02

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	NAT	NAT	Connected	Enabled	192.168.10.0
VMnet1	Custom	-	-	-	192.168.100.0
VMnet2	Custom	-	-	-	192.168.200.0
VMnet3	Bridged	Intel(R) Wi-Fi 6 AX200 160MHz	-	-	-

```

WAN (wan) -> em0 -> v4: 192.168.10.12/24
LAN (lan) -> em1 -> v4: 192.168.100.252/24
DMZ (opt1) -> em2 -> v4: 192.168.200.252/24
                    
```

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

```

Carte Ethernet VMware Network Adapter VMnet0 :
Suffixe DNS propre à la connexion. . . . . :
Description. . . . . : VMware Virtual Ethernet Adapter for VMnet0
Adresse physique . . . . . : 00-50-56-C0-00-00
DHCP activé. . . . . : Oui
Configuration automatique activée. . . . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::b169:5dc2:7d5e:6502%62(préféré)
Adresse IPv4. . . . . : 192.168.10.1(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : dimanche 16 avril 2023 10:10:40
Bail expirant. . . . . : dimanche 16 avril 2023 11:55:38
Passerelle par défaut. . . . . :
Serveur DHCP . . . . . : 192.168.10.254
IAID DHCPv6 . . . . . : 1040207958
DUID de client DHCPv6. . . . . : 00-01-00-01-28-9E-47-3B-38-F3-AB-90-40-11
Serveur WINS principal . . . . . : 192.168.10.2
NetBIOS sur Tcpip. . . . . : Activé
                    
```

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

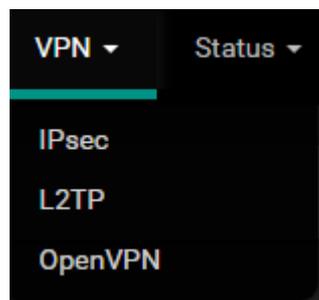
Authentication Servers			
Server Name	Type	Host Name	Actions
SECCIV-RADIUS	RADIUS	192.168.100.1	  

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.

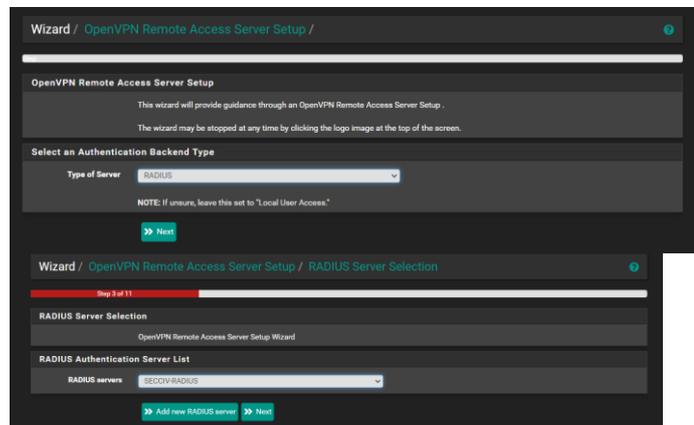
Se rendre dans VPN -> OpenVPN



Puis dans « Wizards ».

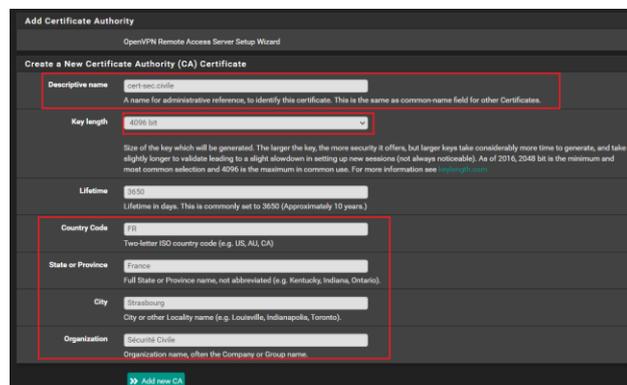


Là, nous pouvons mentionner qu'on souhaite utiliser RADIUS comme serveur d'authentification. On peut faire Next.



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.

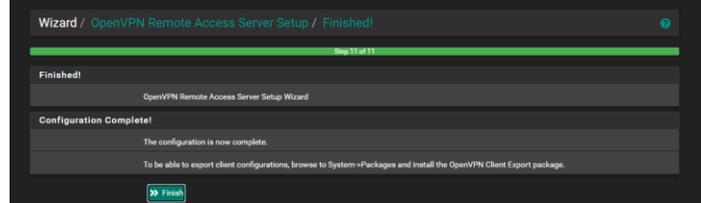
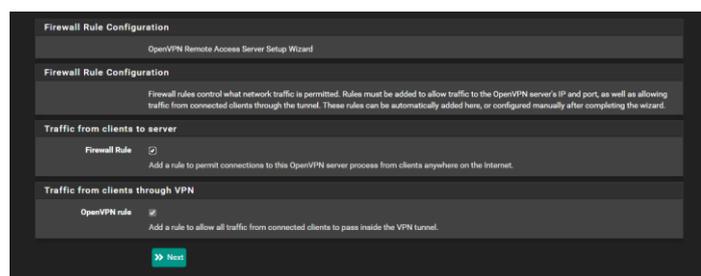
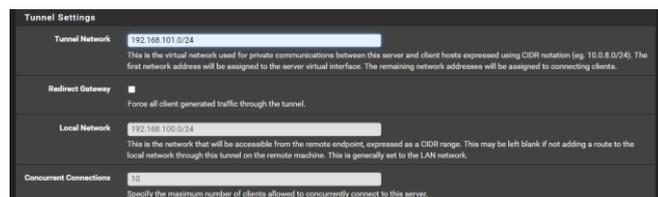
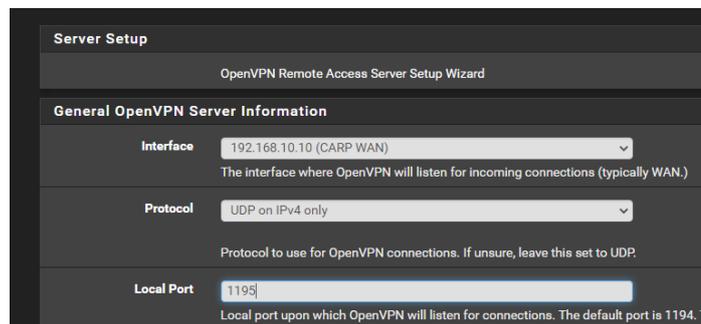
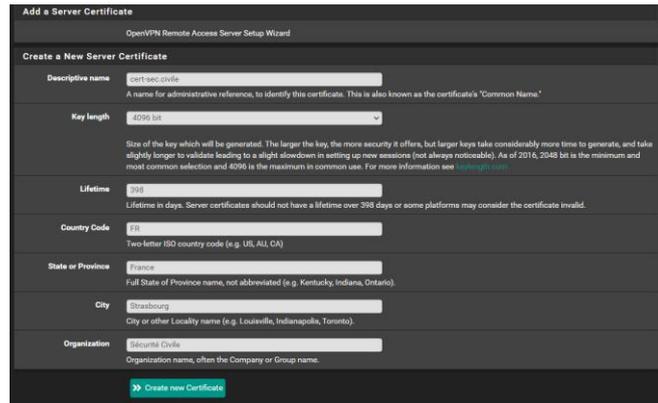
Plus bas, nous avons le tunnel.

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

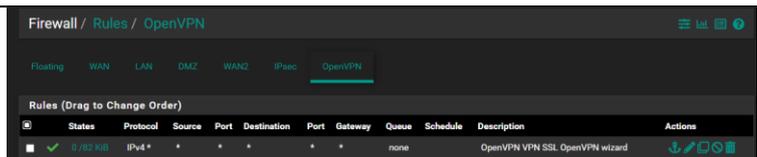
On installe aussi les règles d'OpenVPN au sein du pare-feu que nous verrons après.

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

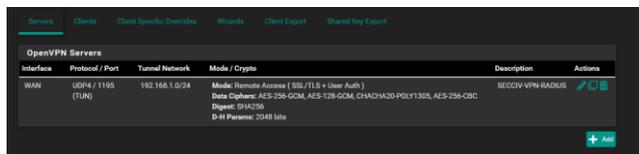
Une règle pour le WAN a bien été attribué. C'est celle que nous avons ajouté avant avec « Firewall Rule » qui nous permet de n'importe quelle source, de se connecter à 192.168.10.10 via OpenVPN uniquement.



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.



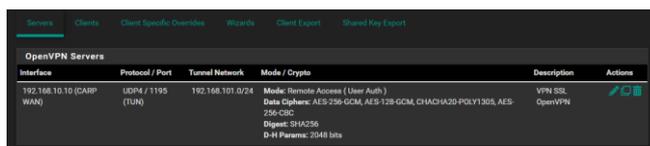
Dans la catégorie « Mode Configuration », indiquer remote access (User Auth), et non SSL/TLS + User Auth par exemple).



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



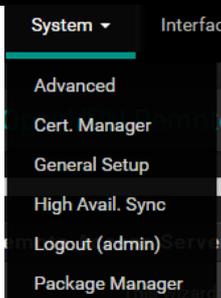
Bien vérifier que le CARP est là et le bon port.



Notre serveur OpenVPN est opérationnel et près à être testé

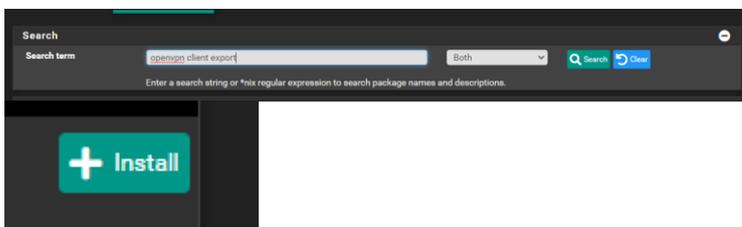
4. Installation de l'exportation du client

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



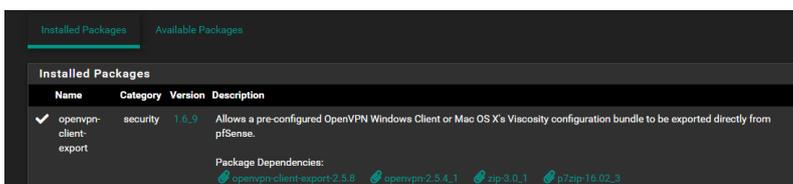
Pour se faire, se rendre dans System -> Package Manager

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.

Client Export

Shared Key Export

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 ».

Client Export

OpenVPN Server

Remote Access Server VPN SSL OpenVPN UDP4:1195

Optionally verify the server certificate Common Name (CN) when the client connects.

Block Outside DNS

Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will not be affected.

OpenVPN Clients

User	Certificate Name	Export
Authentication Only (No Cert)	none	<ul style="list-style-type: none"> - Inline Configurations: <ul style="list-style-type: none"> Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: <ul style="list-style-type: none"> Archive Config File Only - Current Windows Installer (2.5.8-1x04): <ul style="list-style-type: none"> 64-bit 32-bit - Legacy Windows Installers (2.4.12-1x01): <ul style="list-style-type: none"> 10/2016/2019 7/8/8.1/2012/2 - Viscosity (Mac OS X and Windows): <ul style="list-style-type: none"> Viscosity Bundle Viscosity Inline Config

Only OpenVPN-compatible user certificates are shown

Current Windows Installer (2.5.8-1x04):

64-bit 32-bit

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.

7z
SFX
openvpn-SECCIV
-RTE-01-UDP4-11
95-Install-2.5.8-16
04-amd64.exe

Setup OpenVPN 2.5.8-1604

Choose setup type.

Install Now

Customize

Une autre fenêtre qui concerne la configuration du client OpenVPN apparaîtra, 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.

The image displays a series of screenshots documenting the OpenVPN client installation and connection process on a Windows system.

- OpenVPN Configuration Setup:** The initial installation wizard window, where the 'Install' button is highlighted in red.
- Configuration Context Menu:** A right-click menu for the configuration profile 'SECCIV-RTE-01-UDP4-1195-config', with 'Connecter' (Connect) highlighted.
- Connexion OpenVPN:** A dialog box for entering credentials. The user 'rakotozafywinness' is entered, and the password field is visible.
- OpenVPN GUI:** The main interface showing the connection status. A summary box indicates: 'Connecté à: SECCIV-RTE-01-UDP4-1195-config', 'Connecté depuis: 16/04/2023 12:01', and 'Adresse IP assignée: 192.168.101.2'.
- Terminal Logs:** A terminal window showing the underlying network and OpenVPN processes, with a red box highlighting the successful IP assignment: 'Successful TAP-Windows driver to set a DHCP IP/netmask of 192.168.101.2/255.255.255.0 on interface [796E064-6004-4865-97F2-301D72A0255] [DHCP-Serv: 192.168.101.6, lease-time: 31536000]'.

Notre Client-to-site est opérationnel et fonctionnel.

