12/12/2023

Procédure OpenVPN

Sommaire

Table des matières

Table des illustrations

1- Introduction

Cette procédure explique comment paramétrer un VPN OPEN SSL.

Un portail VPN SSL permet d'établir une connexion à la fois vers des sites web distants. Ainsi, les utilisateurs distants accèdent à la passerelle avec leur navigateur web après avoir été authentifiés par une méthode prise en charge par la passerelle. L'accès se fait via une page web qui fait office de portail vers d'autres services.

1.1– Schéma

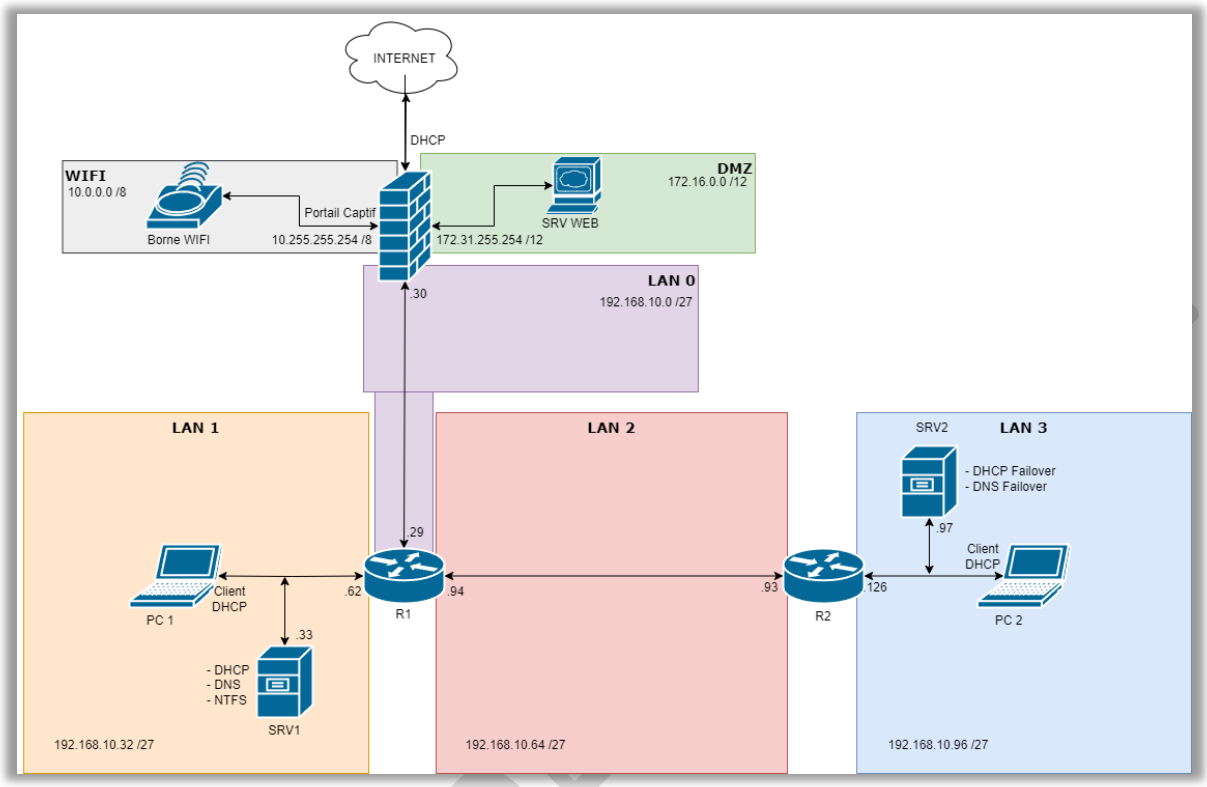
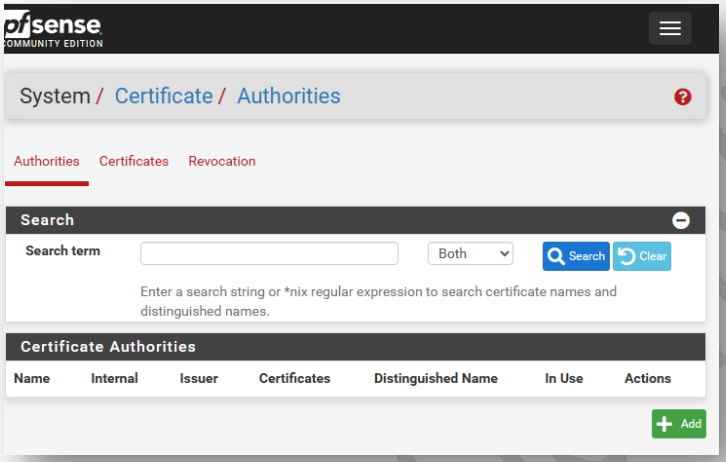


Figure 1 - Schéma réseau avant VPN

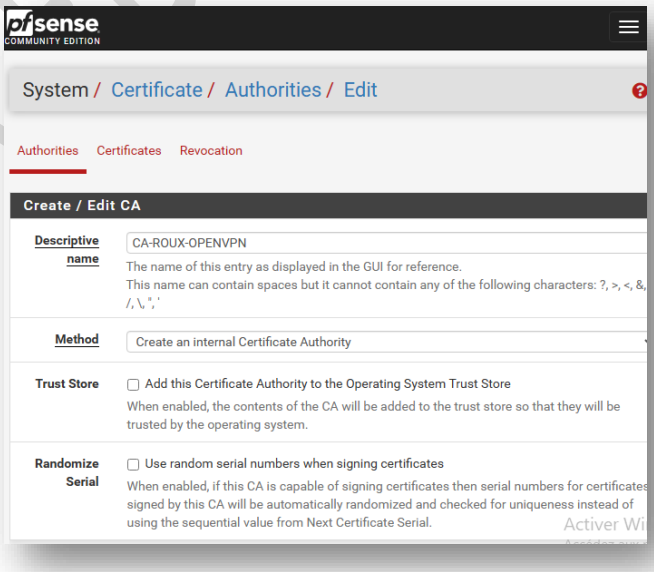
2- Créer l'autorité de certification

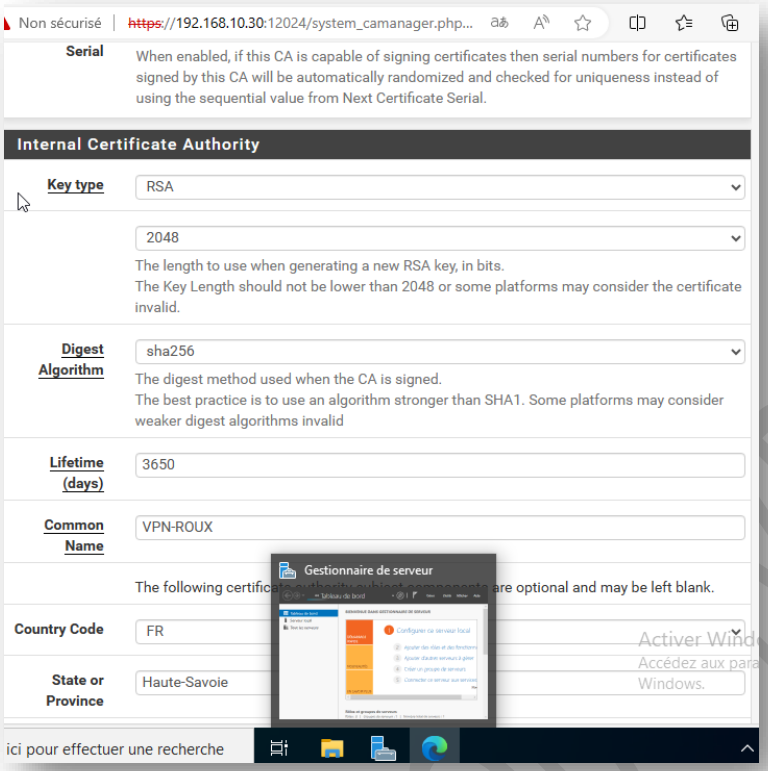
1. Pour créer l'autorité de certification sur pfSense (si vous n'en avez pas déjà une), vous devez accéder au menu : **System > Cert. Manager**
   Dans l'onglet "**CAs**", cliquez sur le bouton "**Add**".



Donnez un nom à l'autorité de certification, par exemple "**CA-ITCONNECT-OPENVPN**", ce nom sera visible seulement dans Pfsense. Choisissez la méthode "**Create an internal Certificate Authority**".

Concernant le nom qui sera **affiché dans les certificats, il s'agit du champ "Common Name"**, j'indique "it-connect" pour ma part. Remplissez les autres valeurs : la région, la ville, etc... et cliquez sur "**Save**" pour créer la CA.



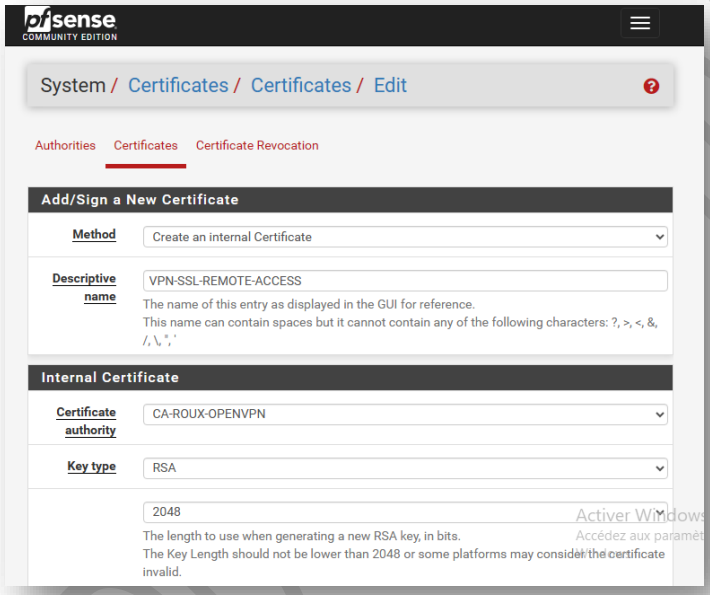


3. Créer le certificat serveur

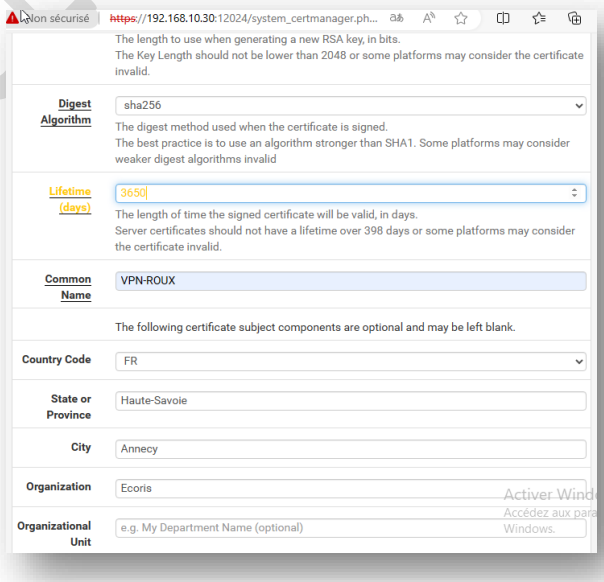
Nous devons créer un certificat de type "Server" en nous basant sur notre nouvelle autorité de certification. Toujours dans "**Certificate Manager**", cette fois-ci dans l'onglet "**Certificates**", cliquez sur le bouton "**Add/Sign**".

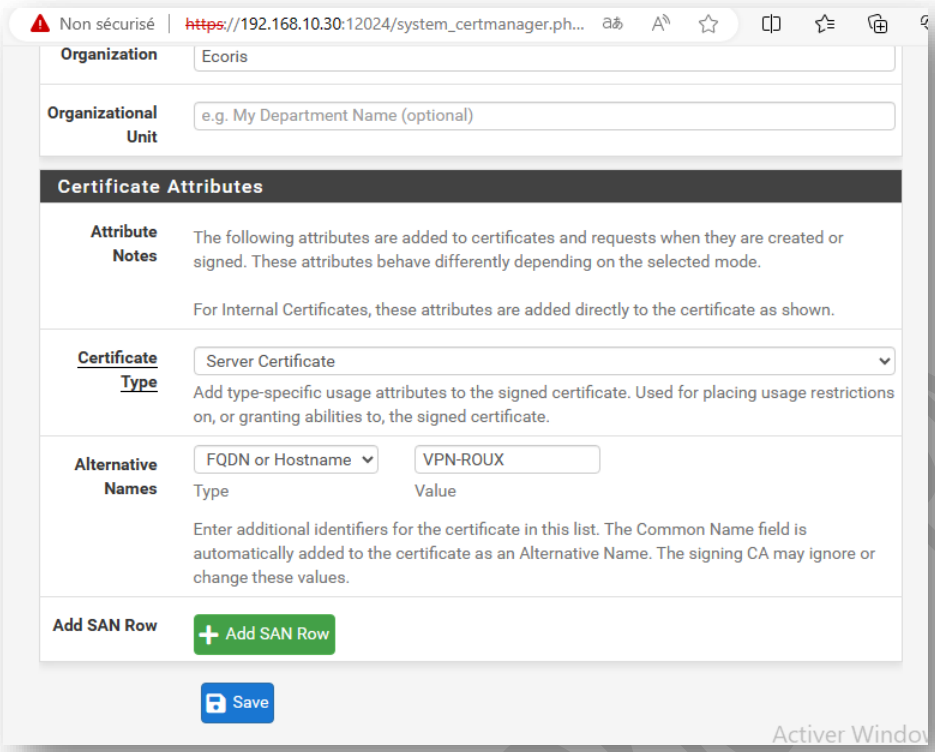
1. Choisissez la méthode "Create an Internal Certificate" puisqu'il s'agit d'une création, donnez-lui un nom (VPN-SSL-REMOTE-ACCESS) et sélectionnez l'autorité de certification au niveau du paramètre "Certificate authority".

Par défaut, la validité du certificat est fixée à 3650 jours soit 10 ans. Le "Common Name" correspond là aussi au nom intégré dans le certificat, si vous souhaitez établir une connexion VPN basée sur un nom de domaine, il est préférable d'indiquer cette valeur ici.



2. Choisissez bien le **type de certificat (Certificate Type)** suivant : **Server Certificate**.



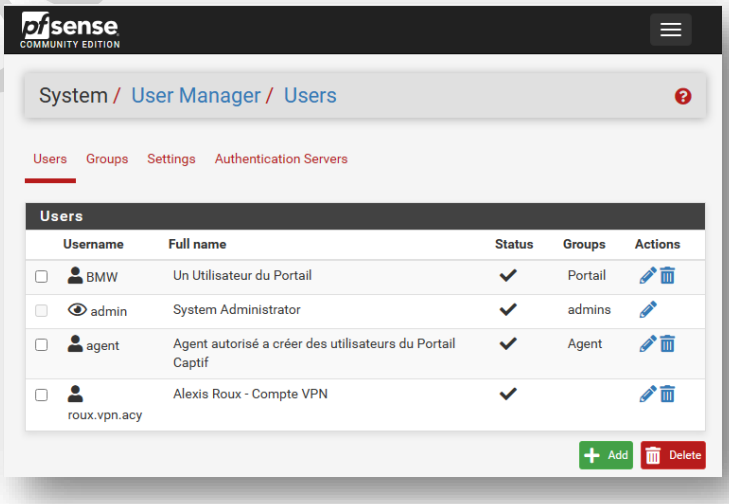


3. Après avoir cliqué sur "**Save**" pour **valider la création du certificat**, il apparaît dans la liste des certificats du Pare-feu.

4. Créer les utilisateurs locaux

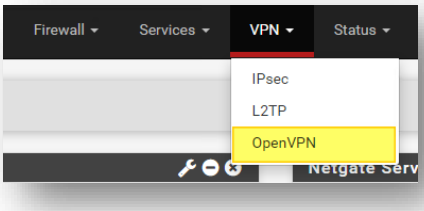
Comme je le disais en introduction, nous allons utiliser une base de compte interne au Pare-feu dans cet exemple. Je vais donc **créer un utilisateur ainsi qu'un certificat de type "User" pour l'authentification VPN.**

Pour créer l'utilisateur, il faut indiquer un identifiant, un mot de passe... Ainsi que cocher l'option "**Click to create a user certificate**" : cela va ajouter le formulaire de création du certificat juste en dessous. Pour créer le certificat, on se base sur notre autorité de certification.

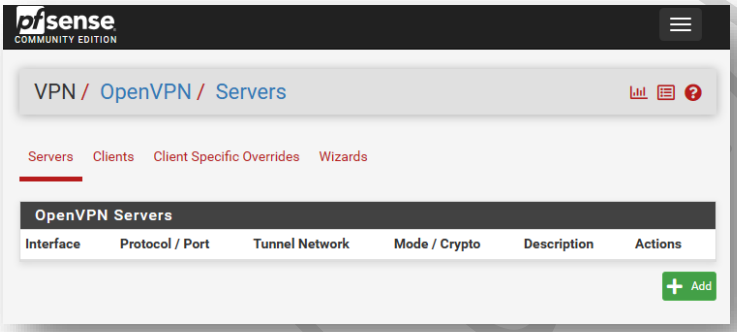


5. Configurer le serveur OpenVPN.

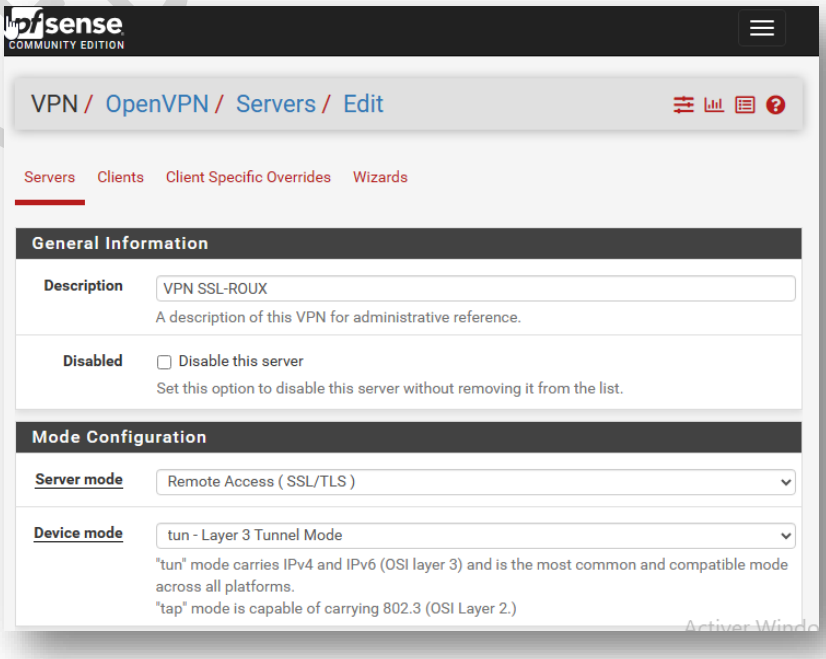
1. **Maintenant que la partie certificat est opérationnelle et que nous disposons d'un compte utilisateur, on peut s'attaquer à la configuration du VPN.**
2. **Cliquez sur le menu "**VPN**" puis "**OpenVPN**".**

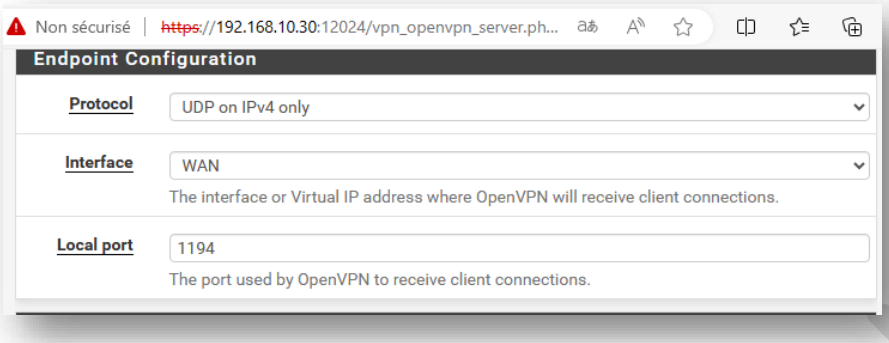


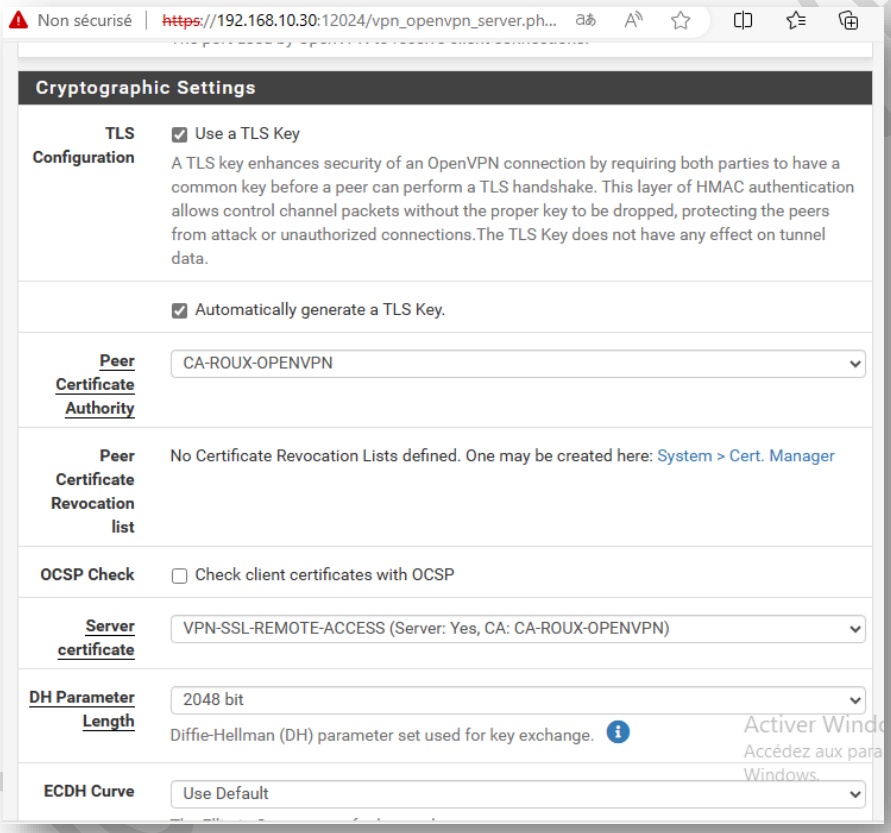
3. **Dans l'onglet "**Servers**", cliquez sur "**Add**" pour créer une nouvelle configuration**.

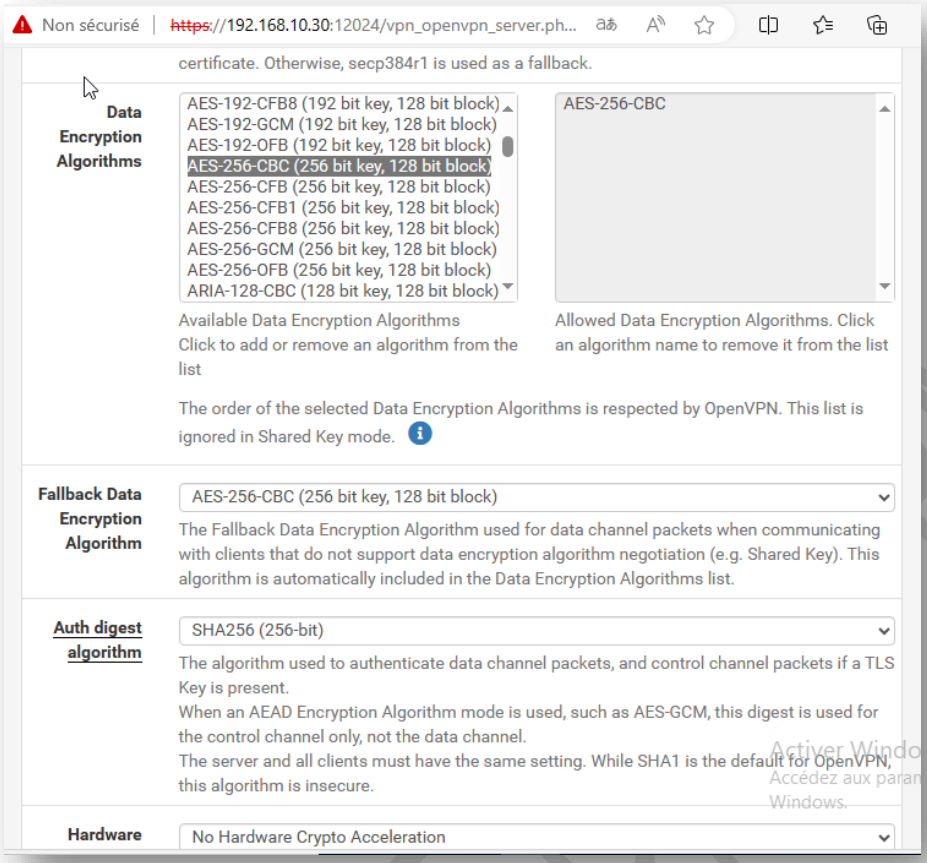


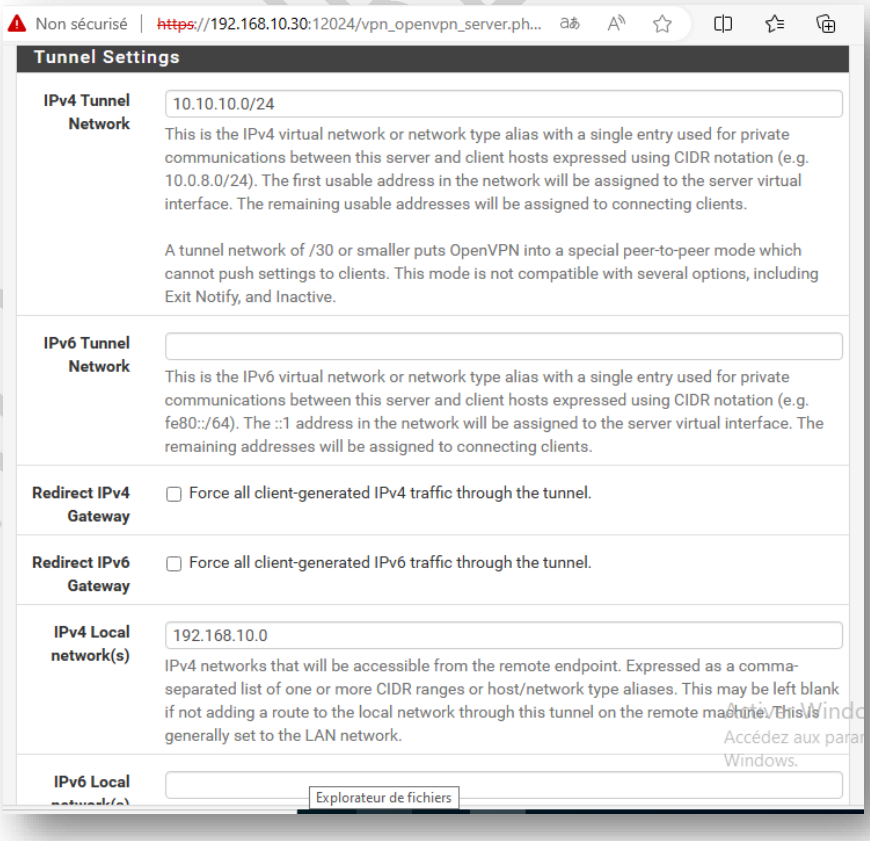
4. La première chose à faire, c'est de choisir le "**Server Mode**" suivant : **Remote Access (SSL/TLS + User Auth)**. Pour le VPN, le protocole s'appuie sur de l'UDP, avec **le port 1194 par défaut : je vous recommande d'utiliser un port différent.** Pour l'interface, nous allons conserver "WAN" puisque c'est bien par cette interface que l'on va se connecter en accès distant.

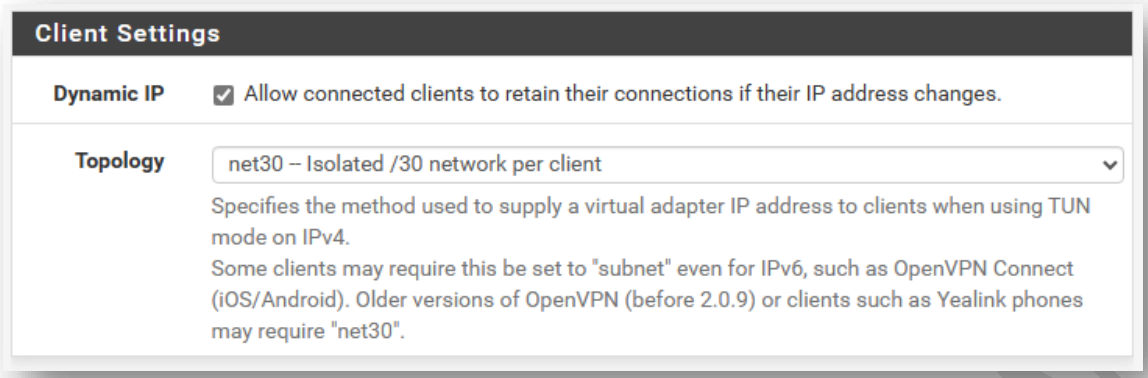


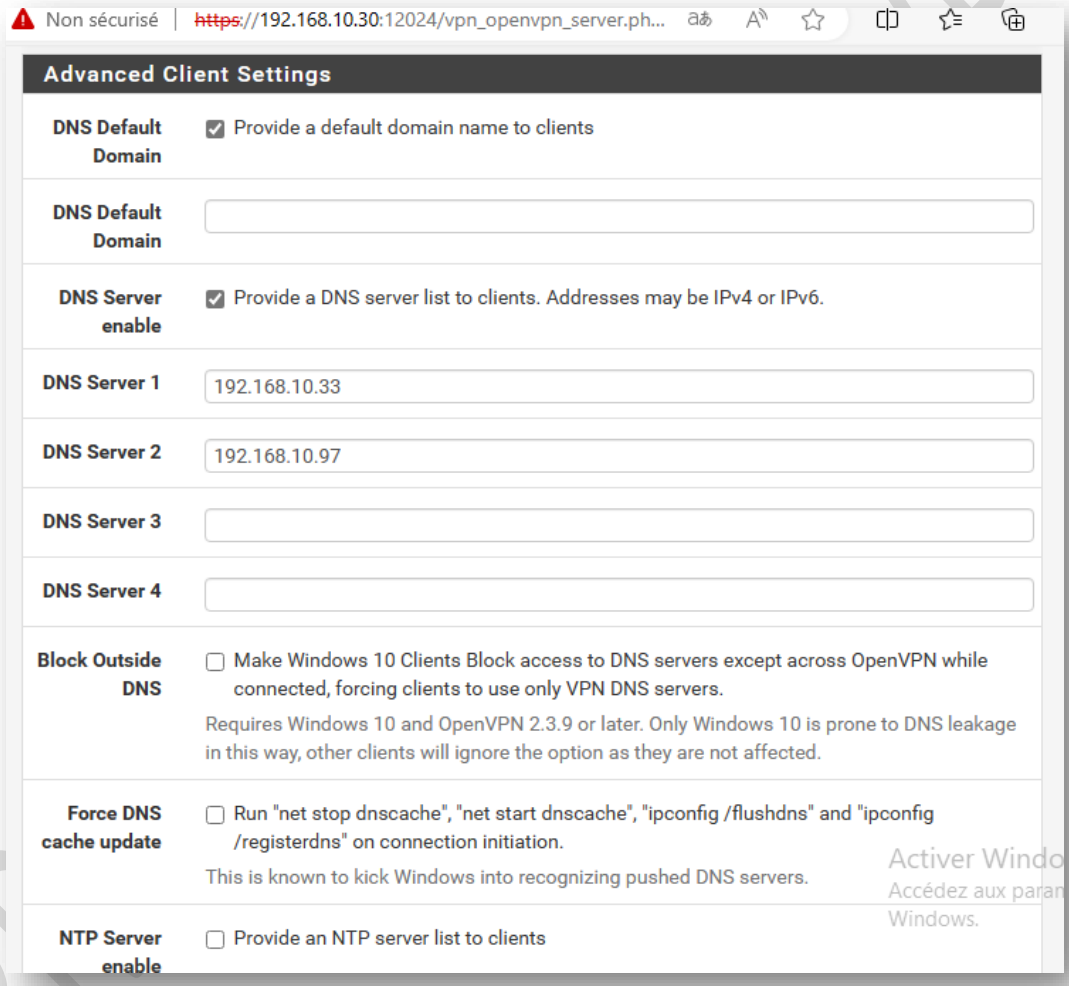


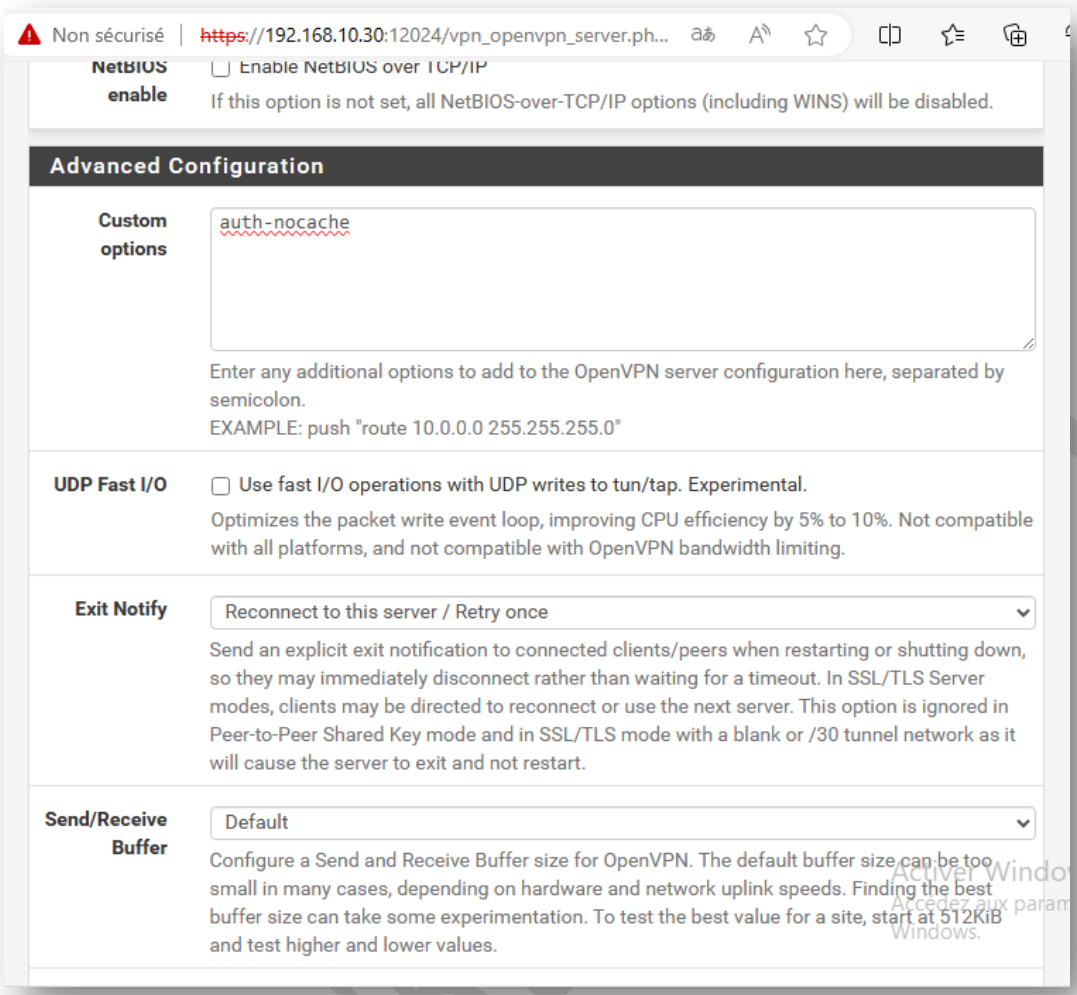



Non sécurisé | https://192.168.10.30:12024/vpn_openvpn_server.ph...
certificate. Otherwise, secp384r1 is used as a fallback.
Data Encryption Algorithms
AES-192-CFB8 (192 bit key, 128 bit block)
AES-192-GCM (192 bit key, 128 bit block)
AES-192-OFB (192 bit key, 128 bit block)
AES-256-CBC (256 bit key, 128 bit block)
AES-256-CFB (256 bit key, 128 bit block)
AES-256-CFB1 (256 bit key, 128 bit block)
AES-256-CFB8 (256 bit key, 128 bit block)
AES-256-GCM (256 bit key, 128 bit block)
AES-256-OFB (256 bit key, 128 bit block)
ARIA-128-CBC (128 bit key, 128 bit block)
AES-256-CBC
Available Data Encryption Algorithms
Click to add or remove an algorithm from the list
Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list
The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode.
Fallback Data Encryption Algorithm
AES-256-CBC (256 bit key, 128 bit block)
The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.
Auth digest algorithm
SHA256 (256-bit)
The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.
Hardware
No Hardware Crypto Acceleration


Non sécurisé | https://192.168.10.30:12024/vpn_openvpn_server.ph...
Tunnel Settings
IPv4 Tunnel Network
10.10.10.0/24
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.
A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.
IPv6 Tunnel Network
This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
Redirect IPv4 Gateway
Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway
Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)
192.168.10.0
IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
IPv6 Local
Explorateur de fichiers


Client Settings
Dynamic IP
Allow connected clients to retain their connections if their IP address changes.
Topology
net30 – Isolated /30 network per client
Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4.
Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".


Non sécurisé
https://192.168.10.30:12024/vpn_openvpn_server.ph...
Advanced Client Settings
DNS Default Domain
Provide a default domain name to clients
DNS Default Domain
DNS Server enable
Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1
192.168.10.33
DNS Server 2
192.168.10.97
DNS Server 3
DNS Server 4
Block Outside DNS
Make Windows 10 Clients 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 ignore the option as they are not affected.
Force DNS cache update
Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation.
This is known to kick Windows into recognizing pushed DNS servers.
NTP Server enable
Provide an NTP server list to clients



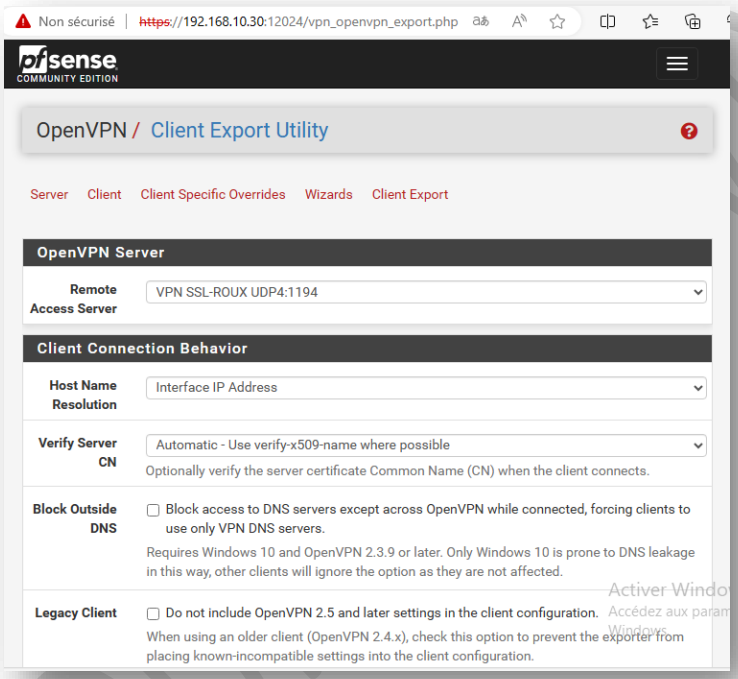
Validez la configuration... Votre configuration VPN est prête !

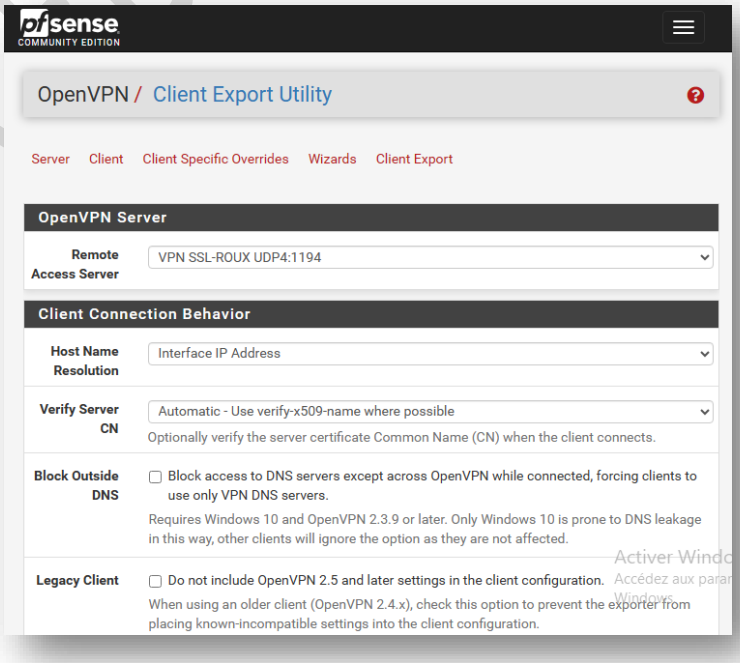
6. Exporter la configuration OpenVPN.

1. Pour télécharger la configuration au format ".ovpn", il est nécessaire d'installer un paquet supplémentaire sur notre pare-feu. Rendez-vous dans le menu suivant : System > Package Manager > Available Packages.

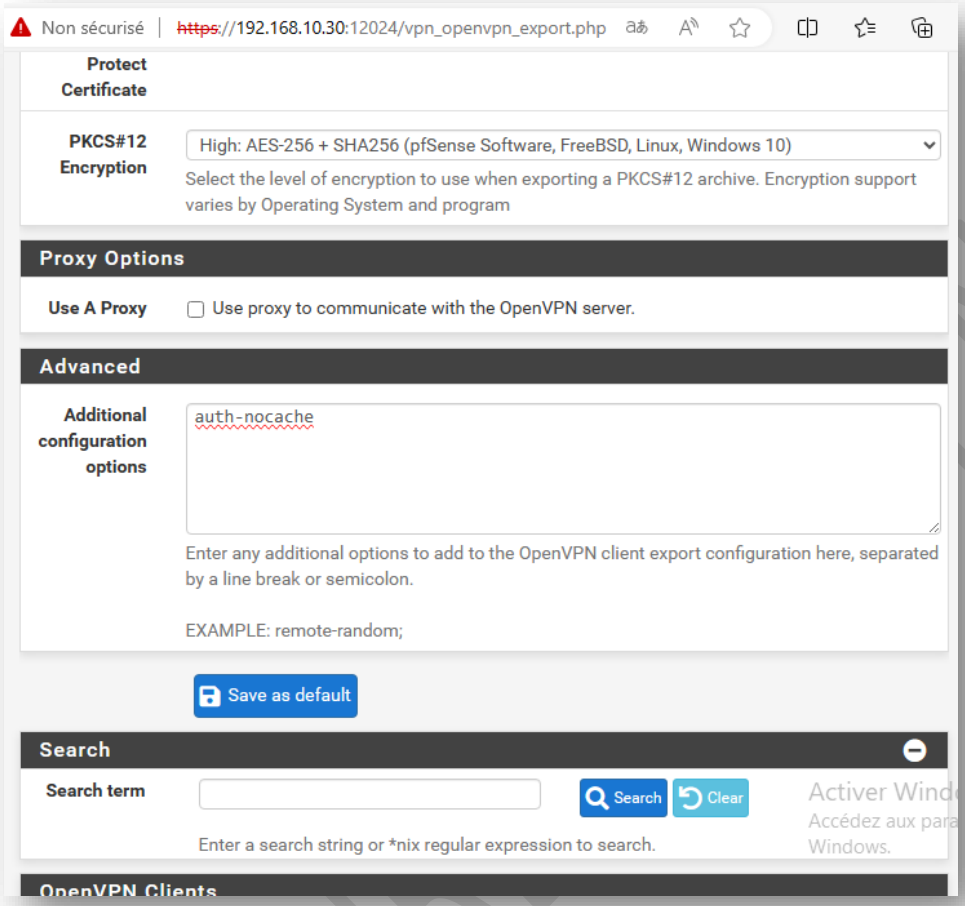
2. Recherchez "openvpn" et installez le paquet : openvpn-client-export. Lorsque c'est fait, retournez dans le menu "OpenVPN" puis dans l'onglet "Client Export".

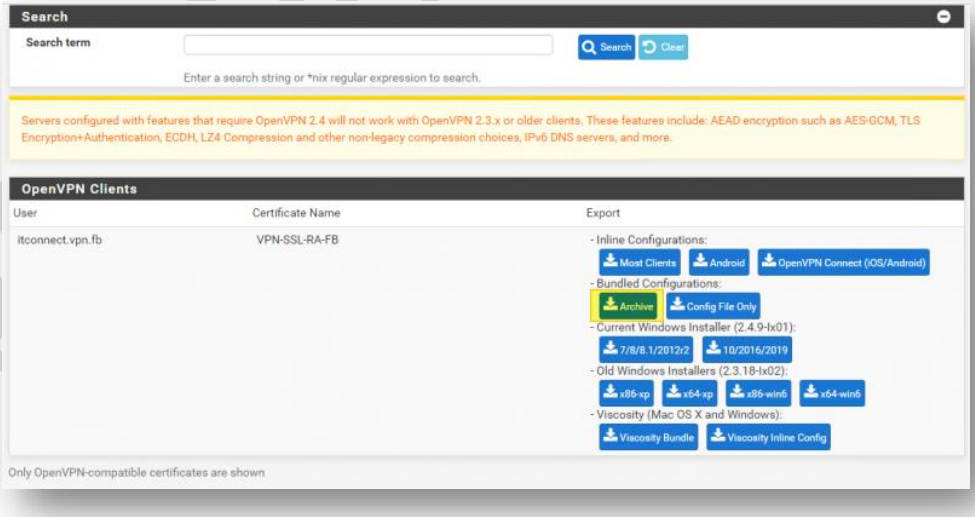
3. Si vous souhaitez utiliser l'adresse IP publique pour vous connecter, utilisez l'option "Interface IP Address" pour l'option "Host Name Resolution". Il y a d'autres options possibles, notamment par nom de domaine.





4. Les autres options peuvent être laissées par défaut... Il y a seulement notre option "**auth-nocache**" à reporter dans la section des options additionnelles.





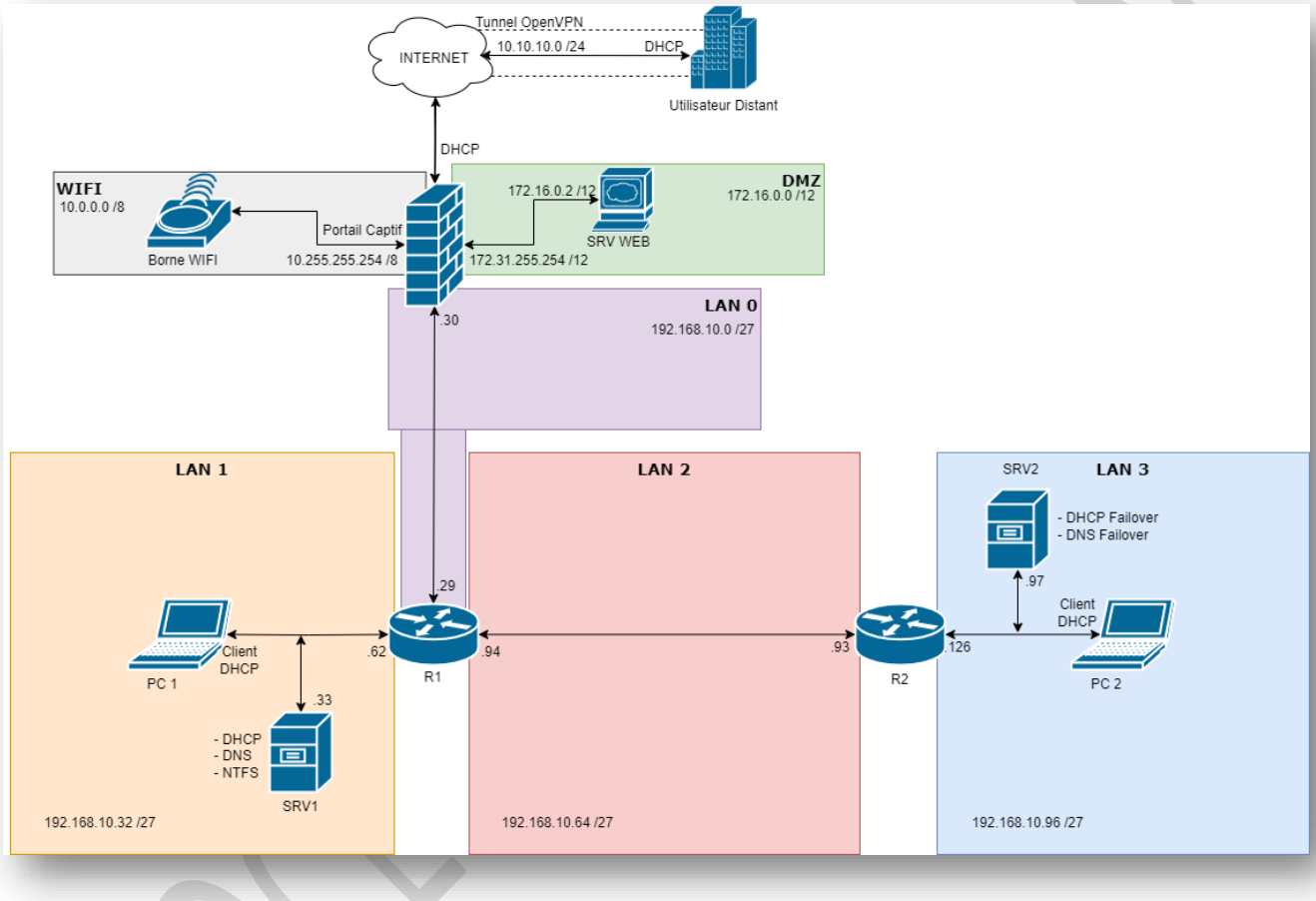


Figure 2 - Schéma réseau après VPN