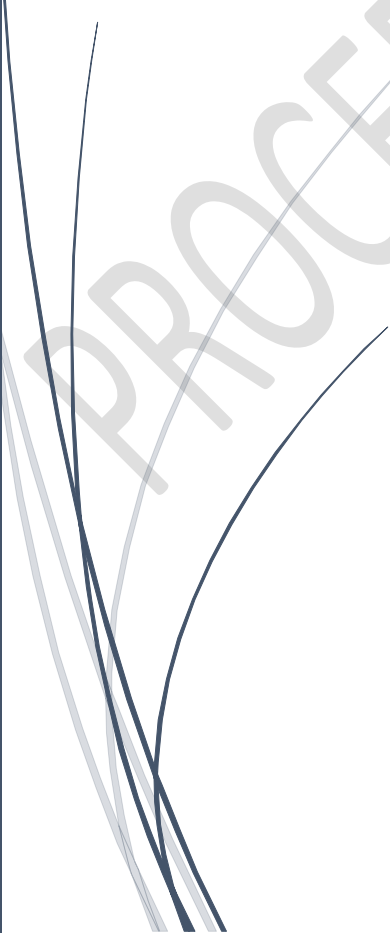
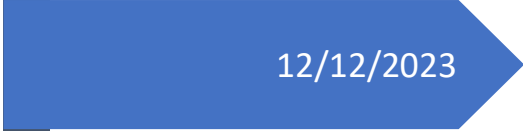


12/12/2023

# Procédure OpenVPN

PROCEDURE OpenVPN



Sommaire

## Table des matières

---

Table des illustrations .....	1
1- Introduction .....	2
1.1- Schéma.....	3
2- Créer l'autorité de certification .....	4
3. Créer le certificat serveur .....	6
4. Créer les utilisateurs locaux .....	7
5. Configurer le serveur OpenVPN.....	8
6. Exporter la configuration OpenVPN.....	13

## Table des illustrations

---

Figure 1 - Schéma réseau .....	3
--------------------------------	---

## 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.

PROCEDURE OpenVPN

## 1.1– Schéma

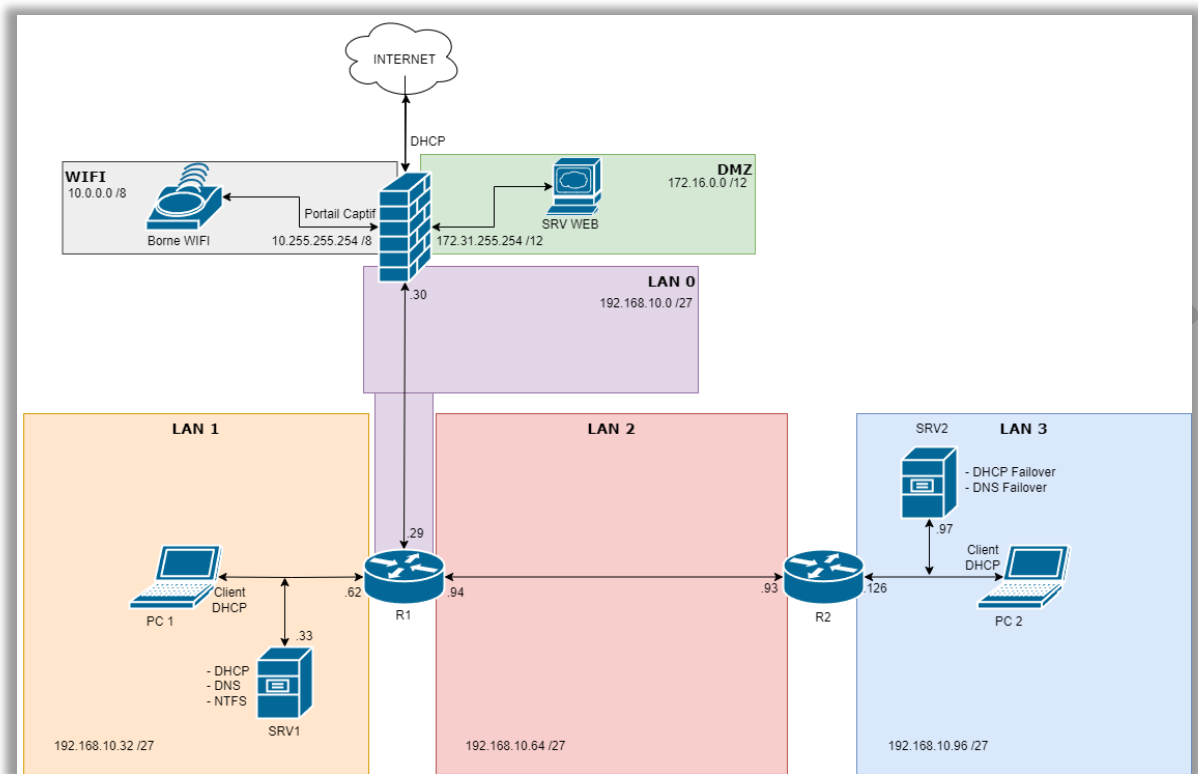
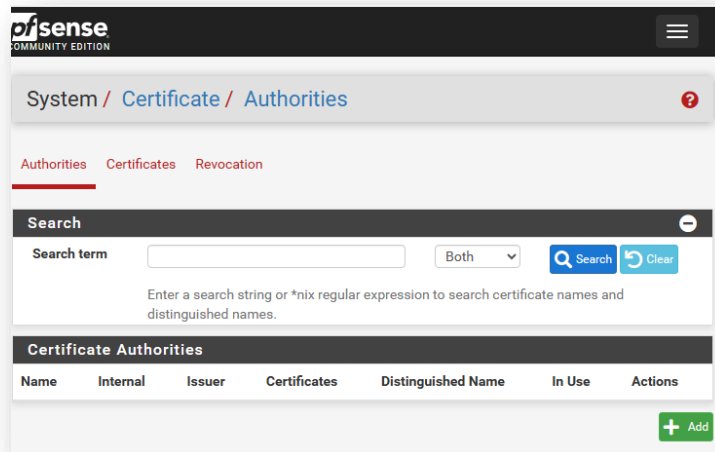


Figure 1 - Schéma réseau avant VPN

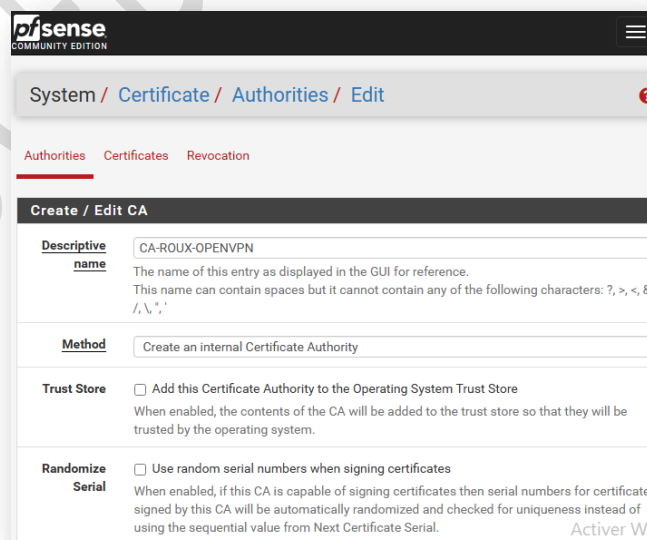
## 2- Créer l'autorité de certification

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.



Non sécurisé | [https://192.168.10.30:12024/system\\_camanager.php...](https://192.168.10.30:12024/system_camanager.php...)

**Serial**  
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

**Internal Certificate Authority**

**Key type** RSA

2048  
The length to use when generating a new RSA key, in bits.  
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

**Digest Algorithm** sha256  
The digest method used when the CA is signed.  
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

**Lifetime (days)** 3650

**Common Name** VPN-ROUX

The following certificate fields are optional and may be left blank.

**Country Code** FR

**State or Province** Haute-Savoie

ici pour effectuer une recherche

Gestionnaire de serveur  
Configurer ce serveur local  
Ajouter des sites et des fichiers  
Ajouter des sites de services  
Configurer ce serveur aux services

Activer Windows  
Accédez aux paramètres Windows.

### 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.

System / Certificates / Certificates / Edit

Authorities Certificates Certificate Revocation

**Add/Sign a New Certificate**

**Method** Create an internal Certificate

**Descriptive name** VPN-SSL-REMOTE-ACCESS  
The name of this entry as displayed in the GUI for reference.  
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, \*, '.

**Internal Certificate**

**Certificate authority** CA-ROUX-OPENVPN

**Key type** RSA

2048  
The length to use when generating a new RSA key, in bits.  
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

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

Non sécurisé https://192.168.10.30:12024/system\_certmanager.ph...

The length to use when generating a new RSA key, in bits.  
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

**Digest Algorithm** sha256  
The digest method used when the certificate is signed.  
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.

**Lifetime (days)** 3650  
The length of time the signed certificate will be valid, in days.  
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

**Common Name** VPN-ROUX

The following certificate subject components are optional and may be left blank.

**Country Code** FR

**State or Province** Haute-Savoie

**City** Annecy

**Organization** Ecoris

**Organizational Unit** e.g. My Department Name (optional)

Non sécurisé | [https://192.168.10.30:12024/system\\_certmanager.ph...](https://192.168.10.30:12024/system_certmanager.ph...)

**Organization**

**Organizational Unit**

**Certificate Attributes**

**Attribute Notes** The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.  
For Internal Certificates, these attributes are added directly to the certificate as shown.

**Certificate Type**

**Alternative Names**    
Type Value

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

**Add SAN Row**

- 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.

pfSense COMMUNITY EDITION

System / User Manager / Users

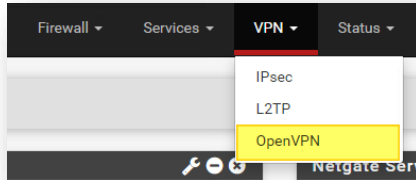
Users Groups Settings Authentication Servers

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	BMW	Un Utilisateur du Portail	✓	Portail	<input type="button" value="edit"/> <input type="button" value="delete"/>
<input type="checkbox"/>	admin	System Administrator	✓	admins	<input type="button" value="edit"/>
<input type="checkbox"/>	agent	Agent autorisé à créer des utilisateurs du Portail Captif	✓	Agent	<input type="button" value="edit"/> <input type="button" value="delete"/>
<input type="checkbox"/>	roux.vpn.acy	Alexis Roux - Compte VPN	✓		<input type="button" value="edit"/> <input type="button" value="delete"/>

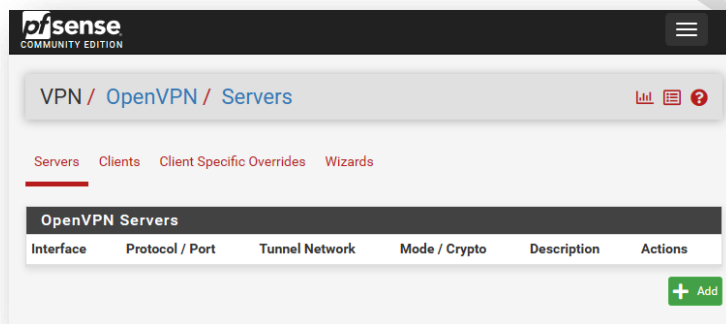


## 5. Configurer le serveur OpenVPN.

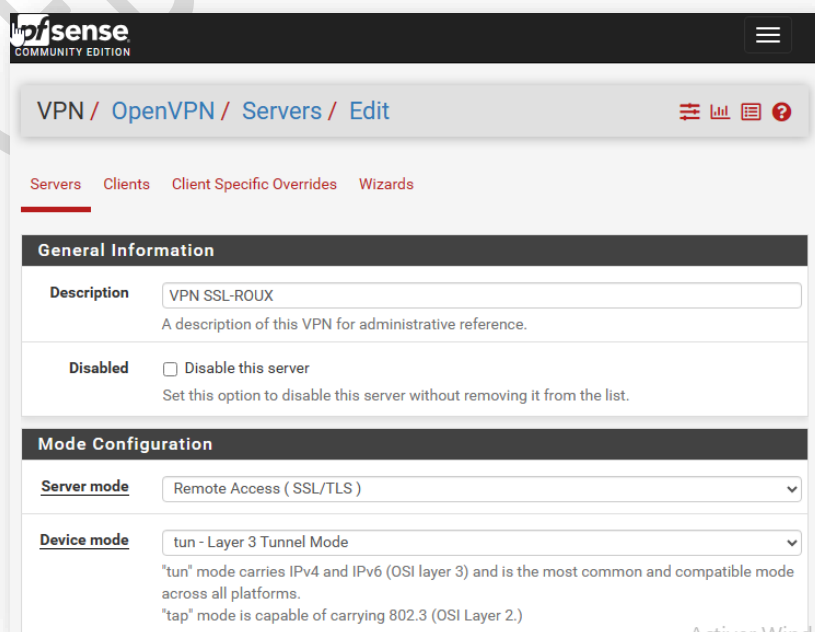
1. Maintenant que la partie certificat est opérationnelle et que nous disposons d'un compte utilisateur, on peut s'attaquer à la configuration du VPN.
2. Cliquez sur le menu "VPN" puis "OpenVPN".



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...](https://192.168.10.30:12024/vpn_openvpn_server.ph...)

### Endpoint Configuration

**Protocol**

**Interface**   
The interface or Virtual IP address where OpenVPN will receive client connections.

**Local port**   
The port used by OpenVPN to receive client connections.

Non sécurisé | [https://192.168.10.30:12024/vpn\\_openvpn\\_server.ph...](https://192.168.10.30:12024/vpn_openvpn_server.ph...)

### Cryptographic Settings

**TLS Configuration**  Use a TLS Key  
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

Automatically generate a TLS Key.

**Peer Certificate Authority**

**Peer Certificate Revocation list** No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

**OCSP Check**  Check client certificates with OCSP

**Server certificate**

**DH Parameter Length**   
Diffie-Hellman (DH) parameter set used for key exchange. ⓘ

**ECDH Curve**

Non sécurisé | [https://192.168.10.30:12024/vpn\\_openvpn\\_server.ph...](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)

Available Data Encryption Algorithms  
Click to add or remove an algorithm 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...](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 network(s)**

Explorateur de fichiers

### Client Settings

**Dynamic IP**  Allow connected clients to retain their connections if their IP address changes.

**Topology**

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...](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**

**DNS Server 2**

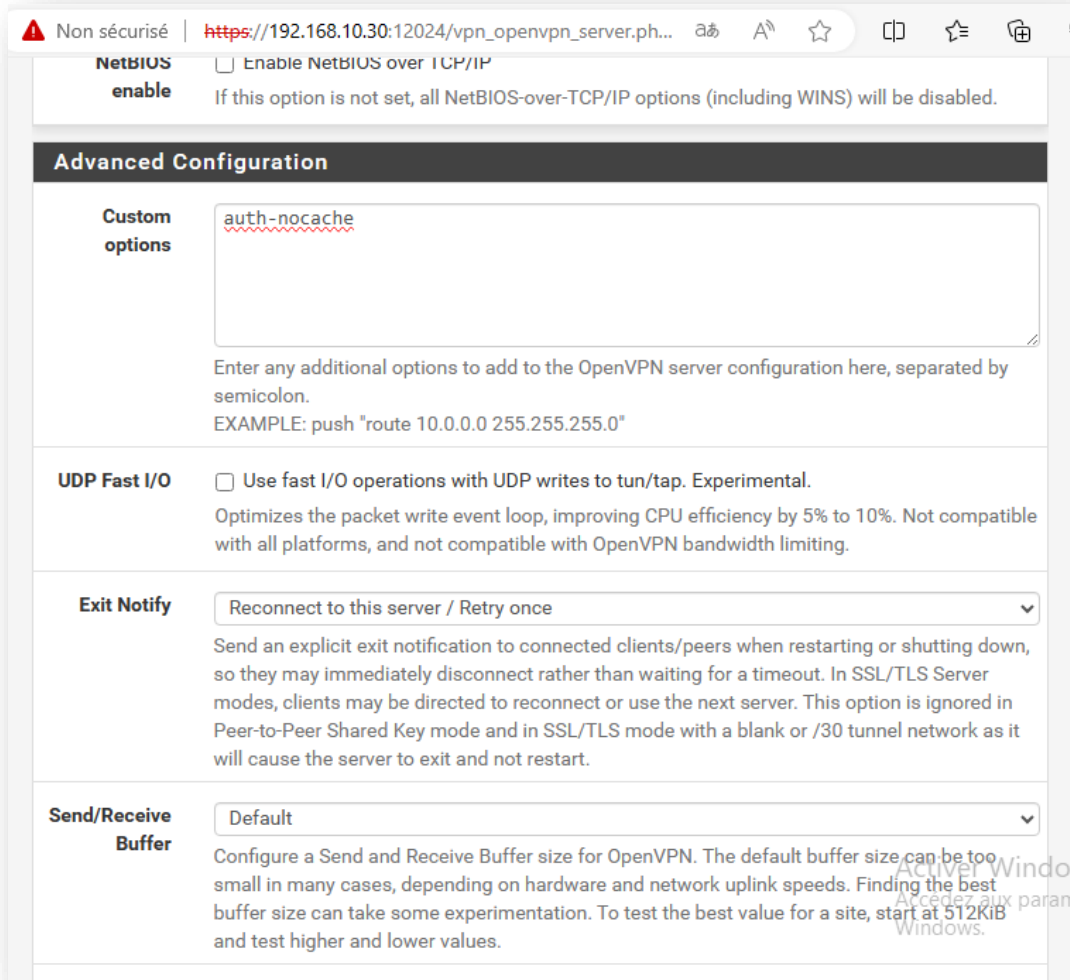
**DNS Server 3**

**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.

Non sécurisé | [https://192.168.10.30:12024/vpn\\_openvpn\\_export.php](https://192.168.10.30:12024/vpn_openvpn_export.php)

pfSense COMMUNITY EDITION

OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards Client Export

**OpenVPN Server**

Remote Access Server: VPN SSL-ROUX UDP4:1194

**Client Connection Behavior**

Host Name Resolution: Interface IP Address

Verify Server CN: Automatic - Use verify-x509-name where possible  
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 ignore the option as they are not affected.

Legacy Client:  Do not include OpenVPN 2.5 and later settings in the client configuration.  
When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.

pfSense COMMUNITY EDITION

OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards Client Export

**OpenVPN Server**

Remote Access Server: VPN SSL-ROUX UDP4:1194

**Client Connection Behavior**

Host Name Resolution: Interface IP Address

Verify Server CN: Automatic - Use verify-x509-name where possible  
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 ignore the option as they are not affected.

Legacy Client:  Do not include OpenVPN 2.5 and later settings in the client configuration.  
When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.

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.

Non sécurisé | [https://192.168.10.30:12024/vpn\\_openvpn\\_export.php](https://192.168.10.30:12024/vpn_openvpn_export.php)

### Protect Certificate

**PKCS#12 Encryption** High: AES-256 + SHA256 (pfSense Software, FreeBSD, Linux, Windows 10)  
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**  
auth-nocache

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](#)

### Search

Search term  [Search](#) [Clear](#)

Enter a search string or \*nix regular expression to search.

### OpenVPN Clients

Search  
Search term  [Search](#) [Clear](#)

Enter a search string or \*nix regular expression to search.

Servers configured with features that require OpenVPN 2.4 will not work with OpenVPN 2.3.x or older clients. These features include: AEAD encryption such as AES-GCM, TLS Encryption+Authentication, ECDH, LZ4 Compression and other non-legacy compression choices, IPv6 DNS servers, and more.

### OpenVPN Clients

User	Certificate Name	Export
itconnect.vpn.fb	VPN-SSL-RA-FB	<p>- Inline Configurations: <a href="#">Most Clients</a> <a href="#">Android</a> <a href="#">OpenVPN Connect (iOS/Android)</a></p> <p>- Bundled Configurations: <a href="#">Archive</a> <a href="#">Config File Only</a></p> <p>- Current Windows Installer (2.4.9-ix01): <a href="#">7/8/8.1/2012/2</a> <a href="#">10/2016/2019</a></p> <p>- Old Windows Installers (2.3.18-ix02): <a href="#">x86-xp</a> <a href="#">x64-xp</a> <a href="#">x86-win6</a> <a href="#">x64-win6</a></p> <p>- Viscosity (Mac OS X and Windows): <a href="#">Viscosity Bundle</a> <a href="#">Viscosity Inline Config</a></p>

Only OpenVPN-compatible certificates are shown

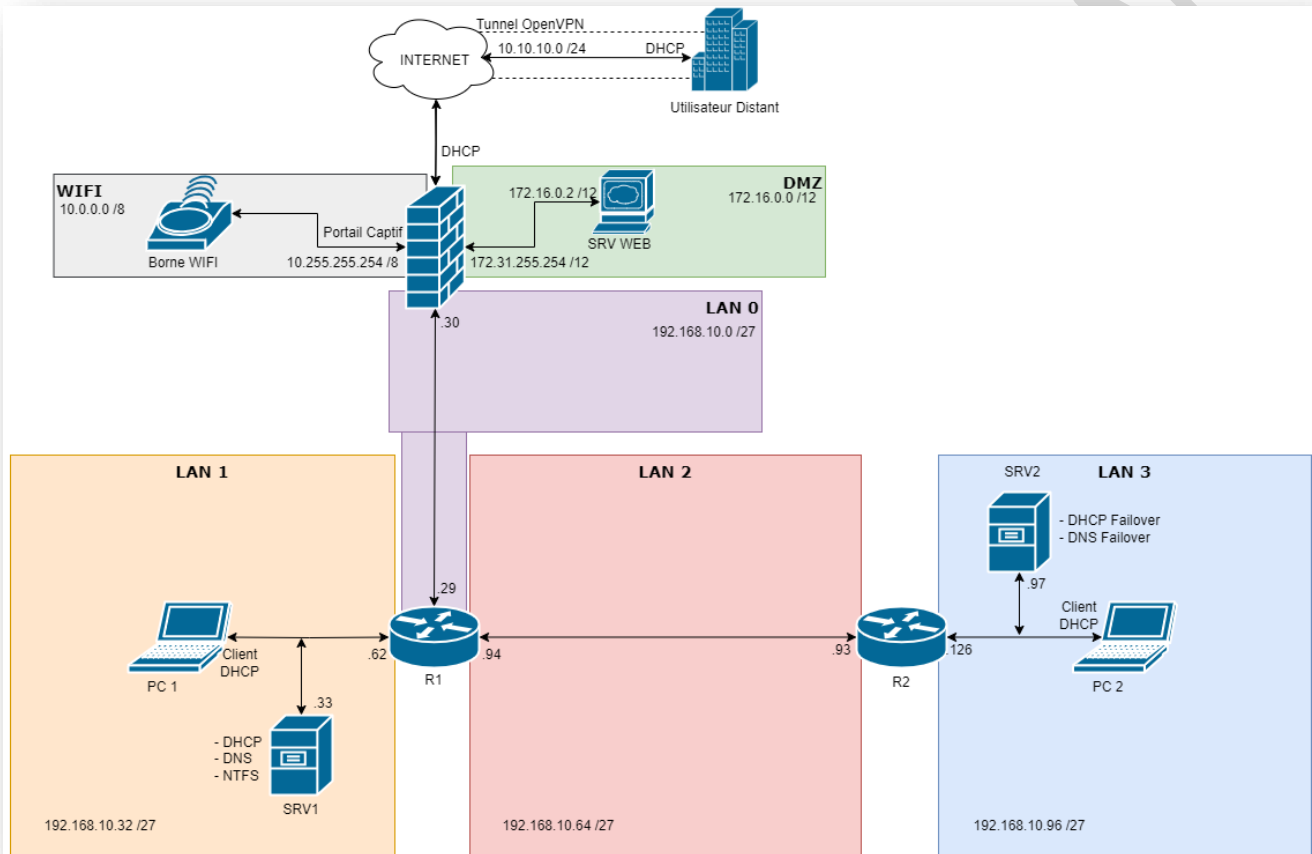


Figure 2 - Schéma réseau après VPN