



# Configuration d'OpenVPN



Matthis LAPULY  
REALISATION PERSONELLE

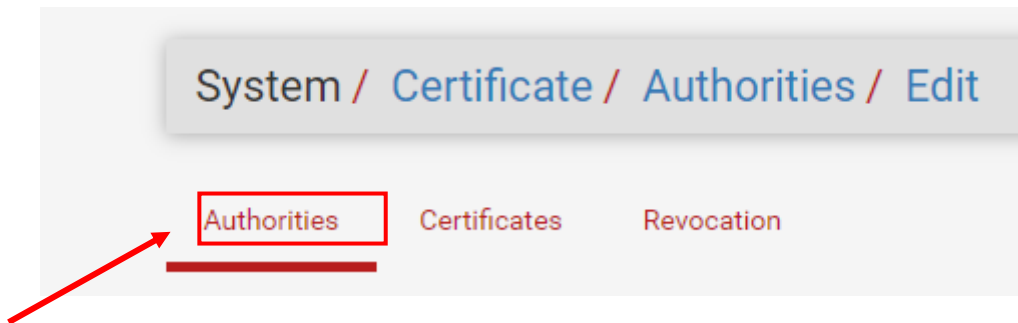
---

## I. Créations des certificats

---

**Etape 1** : On va se rendre sur l'interface Pfsense pour aller sur System < Certificates < Authorities pour ajouter une autorité

Nous devons commencer par créer une autorité de certification



## Etape 2 : Nous allons remplir les champs correspondants :

- Description Name : On nomme l'autorité de certification
- Common Name : Cela sera le nom des certificats généré par cette autorité
- Nous devons indiquer des informations concernant notre entreprise pour les champs restant

Nous laissons les autres champs par défaut

Create / Edit CA	
<b>Descriptive name</b>	CA-ASSURMER <span style="color: red;">← 1.</span>
<small>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: ?, &gt;, &lt;, &amp;, /, \, ", '.</small>	
<b>Method</b>	Create an internal Certificate Authority
<b>Trust Store</b>	<input type="checkbox"/> Add this Certificate Authority to the Operating System Trust Store <small>When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.</small>
<b>Randomize Serial</b>	<input type="checkbox"/> Use random serial numbers when signing certificates <small>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.</small>
Internal Certificate Authority	
<b>Key type</b>	RSA
	2048 <small>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.</small>
<b>Digest Algorithm</b>	sha256 <small>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</small>
<b>Lifetime (days)</b>	3650
<b>Common Name</b>	Assurmer.fr <span style="color: red;">← 2.</span>
<small>The following certificate authority subject components are optional and may be left blank.</small>	
<b>Country Code</b>	FR
<b>State or Province</b>	Île de France <span style="color: red;">← 3.</span>
<b>City</b>	Pontoise
<b>Organization</b>	Assurmer
<b>Organizational Unit</b>	e.g. My Department Name (optional)
<input type="button" value="Save"/>	

Une fois fini on va cliquer sur « Save » pour visualiser notre autorité de certification

System / Certificate / Authorities

Authorities Certificates Revocation

Search

Search term  Both Search Clear

Enter a search string or \*nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA-ASSURMER	✓	self-signed	0	ST=ile de France, O=Assumer, L=Pontoise, CN=Assumer.fr, C=FR Valid From: Sat, 14 Oct 2023 19:31:28 +0200 Valid Until: Tue, 11 Oct 2033 19:31:28 +0200		

+ Add

**Etape 3** : On va maintenant aller sur Certificate pour crée un certificat pour notre serveur

System / Certificates / Certificates / Edit

Authorities Certificates Certificate Revocation

#### Etape 4 : On va remplir les champs correspondants :

- Descriptive Name : Description de notre certificat
- Internal Certificat : Ici, nous retrouvons les informations de notre autorité de certificat créée précédemment

### Add/Sign a New Certificate

**Method** Create an internal Certificate

**Descriptive name** Certificat OpenVPN **1.**

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-ASSURMER

**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 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** Assurmer.fr

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

**Country Code** FR

**State or Province** Ile de France

**City** Pontoise

**Organization** Assurmer

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

**Certificat Type** : Nous devons mettre « Server Certificate » car cela est un certificat pour notre serveur qui va permettre d'authentifier le serveur et de déchiffrer les données

### 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** Server Certificate **2.**







Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

**Alternative Names** FQDN or Hostname

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.

## Certificat Créé

Search				
Search term		Both	Search	Clear
Enter a search string or *nix regular expression to search certificate names and distinguished names.				
Certificates				
Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (652c4112b2e84) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-652c4112b2e84		  
Certificat OpenVPN Server Certificate CA: No Server: Yes	CA- ASSURMER	ST=ile de france , O=ASSURMER, L=Pontoise, CN=Assurmer.fr, C=FR		  

**Etape 4 :** Ici, on va se rendre sur system < user manager pour crée un utilisateur pour générer un certificat de type utilisateur

System / User Manager / Users / Edit

**Users** Groups Settings Authentication Servers

**User Properties**

Defined by: USER

Disabled:  This user cannot login

Username: VPN.Assurmer.fr

Password: .....

1. (arrow pointing to Settings)

2. (arrow pointing to Username)

Nous allons penser à cocher la case « Click to create a user certificate » pour que cela générer notre certificat utilisateur qui va permettre de chiffrer les données envoyé par les utilisateurs . On pourra nommer ce certificat

Certificate  Click to create a user certificate

1. (arrow pointing to checkbox)

**Create Certificate for User**

Descriptive name: Certificat-VPN-ASSURMER

Certificate authority: CA-ASSURMER

2. (arrow pointing to dropdown)

## L'utilisateur a bien été créé

Users Groups Settings Authentication Servers

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	 VPN.Assurmer.fr		✓		 
<input type="checkbox"/>	 admin	System Administrator	✓	admins	

## Le certificat utilisateur a bien été générer









System / Certificates / Certificates ?

Authorities Certificates Certificate Revocation

**Search**

Search term  Both

Enter a search string or \*nix regular expression to search certificate names and distinguished names.

Certificates				
Name	Issuer	Distinguished Name	In Use	Actions
Certificat OpenVPN Server Certificate CA: <b>No</b> Server: <b>Yes</b>	CA-ASSURMER	ST=Ile de France , O=Assurmer, L=Pontoise, CN=Assurmer.fr, C=FR ⓘ Valid From: <b>Sat, 14 Oct 2023 19:40:29 +0200</b> Valid Until: <b>Tue, 11 Oct 2033 19:40:29 +0200</b>		   
Certificat-VPN-ASSURMER User Certificate CA: <b>No</b> Server: <b>No</b>	CA-ASSURMER	ST=Ile de France , O=Assurmer, L=Pontoise, CN=VPN.Assurmer.fr, C=FR ⓘ Valid From: <b>Sat, 14 Oct 2023 19:51:59 +0200</b> Valid Until: <b>Tue, 11 Oct 2033 19:51:59 +0200</b>	User Cert	   

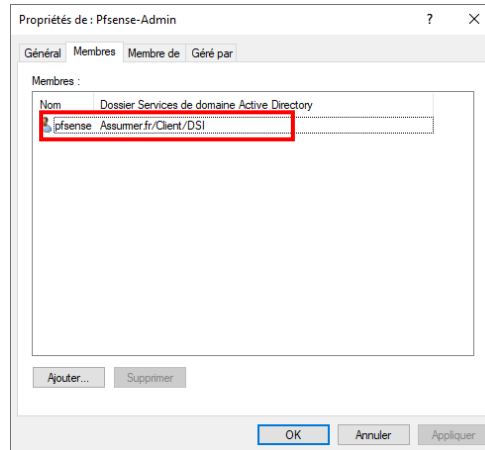
---

## II. Configuration de la liaison LDAP

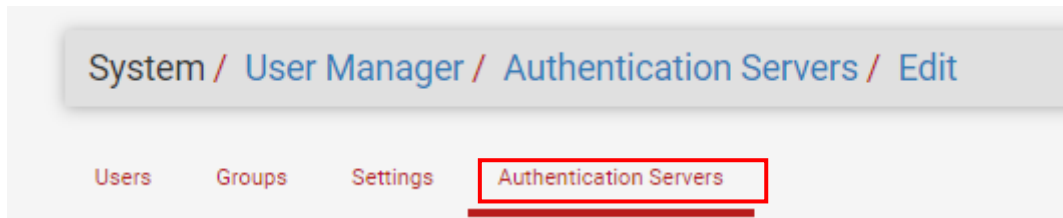
---

Etape 1 : On va créer un utilisateur « pfsense » spécialisé pour la liaison LDAP qu'on va ajouter dans un groupe AD crée spécialement pour le LDAP qu'on va appelé « pfsense-admin »

Cela va être essentiel car Pfsense va utiliser cet utilisateur pour lire notre Active directory



Etape 2 : Sur l'interface Pfsense , on va se rendre sur Authentication Servers pour crée notre liaison LDAP





### Etape 3 : Remplir les champs correspondants

#### Server Settings :

- **Descriptive Name** : On va nommer nos paramètres
- **Type** : On Sélectionne "LDAP".



The screenshot shows a 'Server Settings' form with two fields. The first field, labeled 'Descriptive name', contains the text 'LIASON LDAP'. The second field, labeled 'Type', is a dropdown menu with 'LDAP' selected. Two red arrows point to these fields: arrow '1.' points to the 'Descriptive name' field, and arrow '2.' points to the 'Type' dropdown menu.

Server Settings	
Descriptive name	LIASON LDAP
Type	LDAP

## LDAP Server Settings :

- **Bind credentials** : Nous devons ici entrer le nom d'utilisateur (sous forme de DN complet) et le mot de passe du compte AD que nous avons préparé pour la lecture des informations AD.

The screenshot shows the 'LDAP Server Settings' form with several fields highlighted in red and numbered 1 through 5. Red arrows point from text boxes on the right to these fields.

- 1.** Hostname or IP address: 172.16.20.1 (Adresse IP de notre Serveur AD)
- 2.** Port value: 389 (On choisit un transport en TCP via le port 389)
- 3.** Search scope: Entire Subtree (Base DN de notre AD)
- 4.** Base DN: DC=Assurmer,DC=fr (Base DN de notre AD)
- 5.** Bind credentials: CN=pfensesvc,OU=FINANCE,OU=Client,DC=Assurmer,DC=fr (Base DN d'un utilisateur AD et nous choisissons Microsoft AD)

Other visible fields include: Peer Certificate Authority (Global Root CA List), Protocol version (3), Server Timeout (25), Authentication containers (CN=), Extended query (unchecked), Bind anonymous (unchecked), Initial Template (Microsoft AD), User naming attribute (samAccountName), Group naming attribute (cn), and Group member attribute (memberOf).

A cette étape nous pouvons remplir le champs « **Authentification containers** » car grâce a notre user « pfense » , notre serveur pfense est capable de lire notre annuaire active directory dans son intégralité .

Dans ce champ nous allons écrire seulement « CN= » et cliquer sur « Select a container »

This close-up shows the 'Authentication containers' field with 'CN=' entered and the 'Select a container' button highlighted. Red arrows and numbers 1 and 2 point to these elements.

**1.** Authentication containers: CN=

**2.** Select a container

Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component.  
Example: CN=Users,DC=example,DC=com or OU=Staff,OU=Freelancers

Cette page va s'ouvrir dans lequel on va sélectionner toutes nos OU un par un contenant nos utilisateurs.

Cette page nous affiche toutes notre annuaire active directory grâce au nom DN d'une utilisateur AD

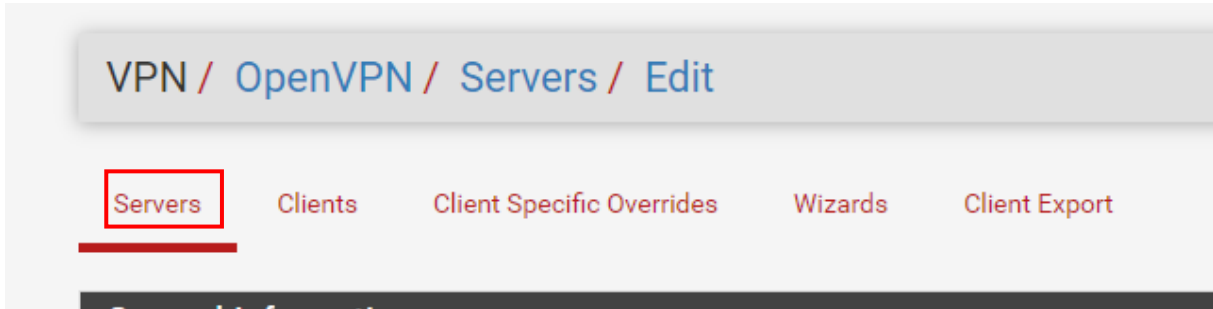
### Select LDAP containers for authentication ×

**Containers**

- OU=.,OU=MARKETING,OU=Client,DC=Assurmer,DC=fr
- OU=.,OU=Client,DC=Assurmer,DC=fr
- OU=.,DC=Assurmer,DC=fr
- OU=.,OU=SERVEUR,DC=Assurmer,DC=fr
- OU=Client,DC=Assurmer,DC=fr
- OU=Domain Controllers,DC=Assurmer,DC=fr
- OU=DSI,OU=Client,DC=Assurmer,DC=fr
- OU=FINANCE,OU=Client,DC=Assurmer,DC=fr
- OU=GROUPE,OU=Client,DC=Assurmer,DC=fr
- OU=HOST,OU=SRV,OU=SERVEUR,DC=Assurmer,DC=fr
- OU=MARKETING,OU=Client,DC=Assurmer,DC=fr
- OU=PC,DC=Assurmer,DC=fr
- OU=RDS,OU=.,DC=Assurmer,DC=fr
- OU=SERVEUR,DC=Assurmer,DC=fr
- OU=SRV,OU=SERVEUR,DC=Assurmer,DC=fr
- CN=Users,DC=Assurmer,DC=fr

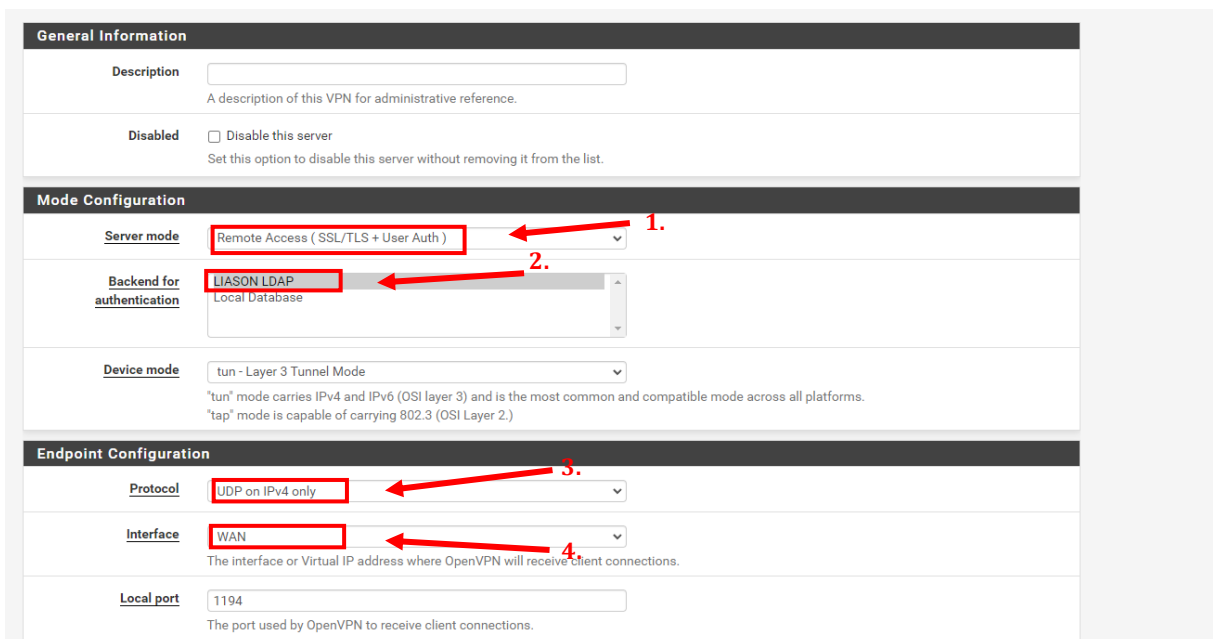
### III. Paramétrage du VPN

**Etape 1 :** Nous allons rendre sur VPN < OpenVPN < Server pour configurer notre VPN



**Etape 2 :** Remplir les champs correspondants

- **Server mode :** On sélectionne Remote Access . On va se baser sur notre certificat crée juste avant et sur une authentification par utilisateurs
- **Backend for Authentification :** On va sélectionner notre Annuaire LDAP
- **Protocol :** Pour le VPN, le protocole s'appuie sur de l'UDP, avec le port 1194 par défaut. **Nous pouvons le changer mais pour l'instant nous allons rester comme ça**
- **Interface :** Pour l'interface, nous allons conserver "WAN" puisque c'est bien par cette interface que l'on va se connecter en accès distant.

The image shows a detailed configuration form for a VPN server. It is divided into three main sections: 'General Information', 'Mode Configuration', and 'Endpoint Configuration'.  
1. In the 'Mode Configuration' section, the 'Server mode' dropdown is set to 'Remote Access ( SSL/TLS + User Auth )' and is highlighted with a red box and a red arrow labeled '1'.  
2. The 'Backend for authentication' dropdown is set to 'LIASON LDAP' and is highlighted with a red box and a red arrow labeled '2'.  
3. In the 'Endpoint Configuration' section, the 'Protocol' dropdown is set to 'UDP on IPv4 only' and is highlighted with a red box and a red arrow labeled '3'.  
4. The 'Interface' dropdown is set to 'WAN' and is highlighted with a red box and a red arrow labeled '4'.  
5. The 'Local port' text input field contains the value '1194'.

- **Peer Certificate Authority** : On retrouve notre certificat d'autorité
- **Server certificate** : On va sélectionner notre certificat serveur crée précédemment
- **Fallback Data Encryption Algorithm** : On va choisir AES-256-CBC (256 bit key , 128 bit block) .

En faisant cela , la sécurité sera renforcée, mais cela impact légèrement les performances, car le processus de chiffrement est alourdi : il sera toujours possible de modifier cette valeur.

Le reste des paramètres on va les laisser par défaut

The screenshot shows the 'Cryptographic Settings' interface. Three specific settings are highlighted with red boxes and numbered arrows:

- 1.** Points to the 'Peer Certificate Authority' dropdown menu, which is set to 'CA-ASSURMER'.
- 2.** Points to the 'Server certificate' dropdown menu, which is set to 'Certificat OpenVPN (Server: Yes, CA: CA-ASSURMER)'.
- 3.** Points to the 'Fallback Data Encryption Algorithm' dropdown menu, which is set to 'AES-256-CBC (256 bit key, 128 bit block)'.

Other visible settings include:

- TLS Configuration:** 'Use a TLS Key' is checked.
- Peer Certificate Authority:** 'CA-ASSURMER' is selected.
- OCSP Check:** 'Check client certificates with OCSP' is unchecked.
- DH Parameter Length:** '2048 bit' is selected.
- ECDH Curve:** 'Use Default' is selected.
- Data Encryption Algorithms:** A list of available algorithms is shown on the left, and a list of allowed algorithms (AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305) is shown on the right.

- **IPv4 Tunnel Network** : On va choisir une adresse du réseau VPN, c'est-à-dire que lorsqu'un client va se connecter en VPN il obtiendra une adresse IP dans ce réseau au niveau de la carte réseau locale du PC
- **IPv4 Local network** : On indique notre adresse réseau de notre LAN serveur que nous souhaitons rendre accessible via le tunnel VPN

Tunnel Settings	
IPv4 Tunnel Network	<input type="text" value="10.10.10.0/24"/> <span style="color: red;">← 1.</span> <small>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.</small>  <small>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.</small>
IPv6 Tunnel Network	<input type="text"/> <small>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.</small>
Redirect IPv4 Gateway	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)	<input type="text" value="172.16.20.0/24"/> <span style="color: red;">← 2.</span> <small>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.</small>

- **Dynamic IP** : On va cocher cette option. Cela peut être utile dans le cas où l'adresse IP publique d'un client change, il pourra maintenir sa connexion VPN. C'est surtout utile car nous avons des collaborateurs qui se connectent via une connexion 4G et en mobilité via leurs appareils nomades.
- **Topology** : On va choisir Net30-Isolated /30 network per client pour que chaque client soit isolé dans un sous-réseau (de la plage réseau VPN) afin que les clients ne puissent pas communiquer entre eux pour des réseaux de sécurité

Client Settings	
Dynamic IP	<input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes. <span style="color: red;">← 1.</span>
Topology	<input type="text" value="net30 - Isolated /30 network per client"/> <span style="color: red;">← 2.</span> <small>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".</small>

- **DNS default Domain** : On va cocher cette case et mettre le nom de notre domaine

- **DNS Server enable** : On va cocher cette case pour indiquer l'adresse IP de notre serveur DNS

**Advanced Client Settings**

DNS Default Domain	<input checked="" type="checkbox"/> Provide a default domain name to clients	← 1.
DNS Default Domain	Assumer.fr	
DNS Server enable	<input checked="" type="checkbox"/> Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.	← 2.
DNS Server 1	172.16.20.1	
DNS Server 2		
DNS Server 3		
DNS Server 4		
Block Outside DNS	<input type="checkbox"/> Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. <small>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.</small>	
Force DNS cache update	<input type="checkbox"/> Run 'net stop dnscache', 'net start dnscache', 'ipconfig /flushdns' and 'ipconfig /registerdns' on connection initiation. <small>This is known to kick Windows into recognizing pushed DNS servers.</small>	
NTP Server enable	<input type="checkbox"/> Provide an NTP server list to clients	
NetBIOS enable	<input type="checkbox"/> Enable NetBIOS over TCP/IP <small>If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.</small>	




- **Custom Options** : Nous allons rajouter l'option « auth-nocache ». Cette option offre une protection supplémentaire contre le vol des identifiants en refusant la mise en cache.

**Advanced Configuration**

Custom options

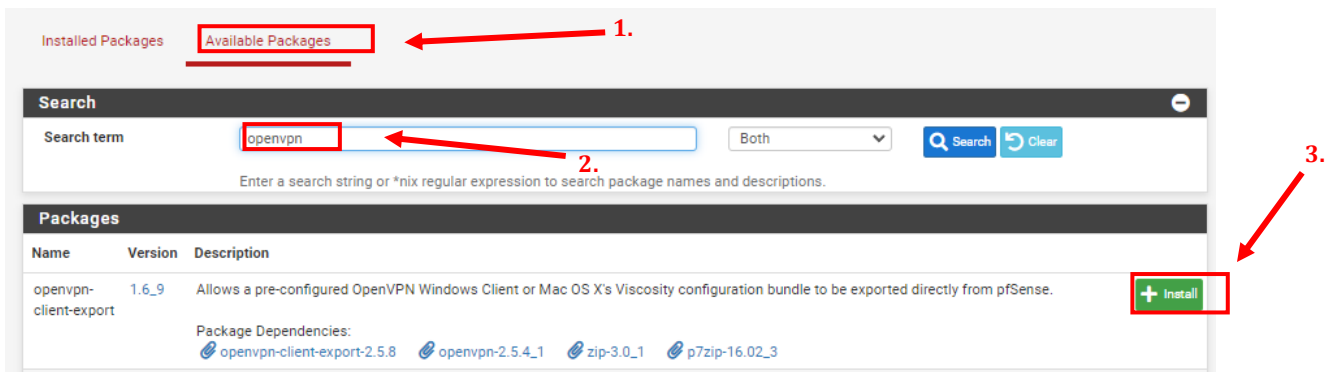
Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.  
EXAMPLE: push route 10.0.0.0 255.255.255.0"

La configuration serveur d'OpenVPN est terminé

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.10.10.0/24	<b>Mode:</b> Remote Access ( SSL/TLS + User Auth ) <b>Data Ciphers:</b> AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC <b>Digest:</b> SHA256 <b>D-H Params:</b> 2048 bits	Accès Distant OpenVpn	  

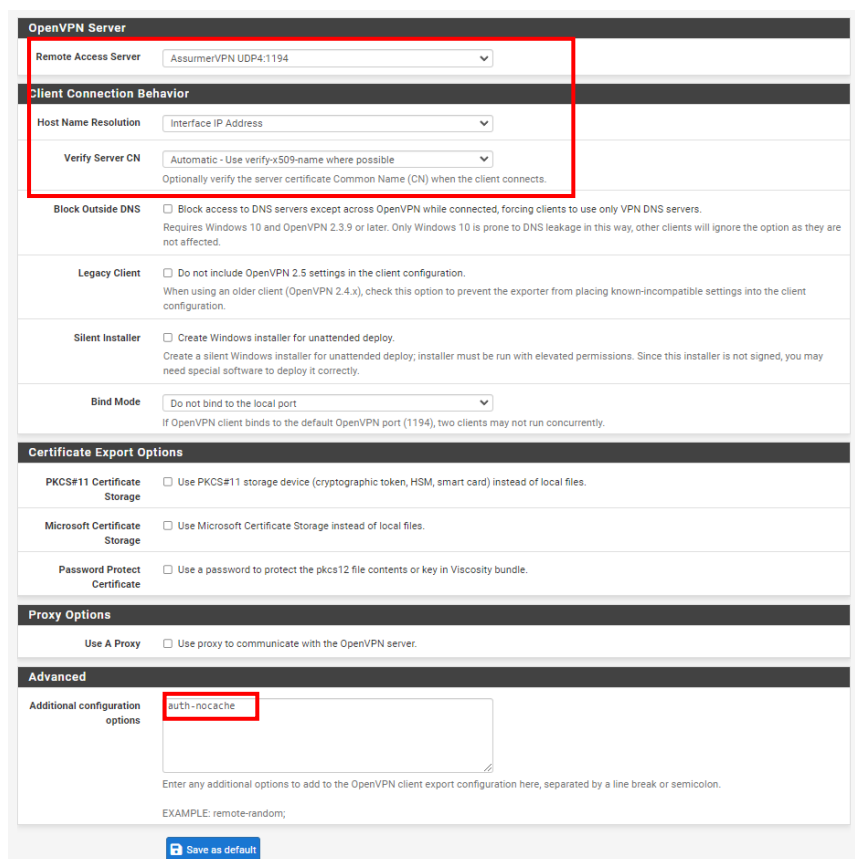
## IV. Exportation de nos configuration VPN

**Etape 1 :** On va aller dans system < package manager < Available packages pour rechercher le package OpenVpn et l'installer



Nous devons installer ce package pour pouvoir exporter les configurations faites précédemment pour les importer sur les machines clientes

**Etape 2 :** Après cela, nous nous rendons sur VPN < OpenVPN < Client Export . Nous pouvons voir les résultats de nos configurations faites juste avant



**Etape 3 :** En dessous de la part configuration, on a la possibilité de télécharger la configuration. Pour utiliser OpenVPN il faudra prendre la configuration "Bundled Configuration", au format archive pour récupérer tous les fichiers nécessaires. Il faudra aussi installer OpenVPN client sur nos pc client



OpenVPN Clients		
User	Certificate Name	Export
Certificate with External Auth	Certificat-VPN-ASSURMER	<ul style="list-style-type: none"><li>- Inline Configurations:<ul style="list-style-type: none"><li>Most Clients</li><li>Android</li><li>OpenVPN Connect (iOS/Android)</li></ul></li><li>- Bundled Configurations:<ul style="list-style-type: none"><li>Archive</li><li>Config File Only</li></ul></li><li>- Current Windows Installer (2.6.5-1x001):<ul style="list-style-type: none"><li>64-bit</li><li>32-bit</li></ul></li><li>- Previous Windows Installer (2.5.9-1x601):<ul style="list-style-type: none"><li>64-bit</li><li>32-bit</li></ul></li><li>- Legacy Windows Installers (2.4.12-1x601):<ul style="list-style-type: none"><li>10/2016/2019</li><li>7/8/8.1/2012r2</li></ul></li><li>- Viscosity (Mac OS X and Windows):<ul style="list-style-type: none"><li>Viscosity Bundle</li><li>Viscosity Inline Config</li></ul></li></ul>

---

## V. Configuration des règles de pare-feu

---

**Etape 1 :** On va se rendre sur Firewall > Rules pour créer une règle au niveau du WAN de notre pfSense. Il est nécessaire de créer une nouvelle règle pour l'interface WAN, en sélectionnant le protocole UDP.

On crée une règle pour autoriser la connexion avec le VPN. On va remplir les champs correspondants :

- Action : Pass
- Interface : WAN
- Protocol : UDP
- Source : On laisse en Any pour les réseaux externes
- Destination : On met WAN adresse et on indique le port de notre VPN choisi précédemment

**Edit Firewall Rule**

**Action**    
 Choose what to do with packets that match the criteria specified below.   
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**  Disable this rule   
 Set this option to disable this rule without removing it from the list.

**Interface**    
 Choose the interface from which packets must come to match this rule.

**Address Family**    
 Select the Internet Protocol version this rule applies to.

**Protocol**    
 Choose which IP protocol this rule should match.

**Source**

**Source**  Invert match   /    
 [Display Advanced](#)   
 The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

**Destination**

**Destination**  Invert match   /    
 **Destination Port Range**       
 From Custom To Custom   
 Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

**Extra Options**

**Log**  Log packets that are handled by this rule   
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

**Description**    
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** [Display Advanced](#)


- Etape 2 : On va créer une autre règle pour autoriser les flux vers les ressources.

On va se rendre dans l'interface OpenVpn est créé une nouvelle règle. Nous devons créer une ou plusieurs règles en fonction des ressources auxquelles vos utilisateurs doivent accéder via le VPN, en limitant les flux au maximum mais ici nous allons autoriser le flux de tout le LAN serveur pour l'instant

The screenshot shows the 'Edit Firewall Rule' configuration page. The 'Action' is set to 'Pass'. The 'Interface' is 'OpenVPN'. The 'Address Family' is 'IPv4' and the 'Protocol' is 'Any'. The 'Source' is set to 'any'. The 'Destination' is set to 'Network' with the address '172.16.20.0 / 24'. The 'Log' checkbox is unchecked. The 'Description' field is empty. The 'Advanced Options' section is collapsed. The 'Rule Information' section shows the Tracking ID as 1697400589, created on 10/15/23 at 22:09:49 by admin@172.16.20.45, and updated on 10/15/23 at 22:53:56 by admin@10.10.10.6.

## A. Importation des configurations sur le poste client

**Etape 1** : Sur le pc client, on récupère le client OpenVPN proposé directement dans pfsense

 `openvpn-pfSense-UDP4-1194-VPN.Assumer.fr-install-2.5.8-l604-amd64 (2)`

---

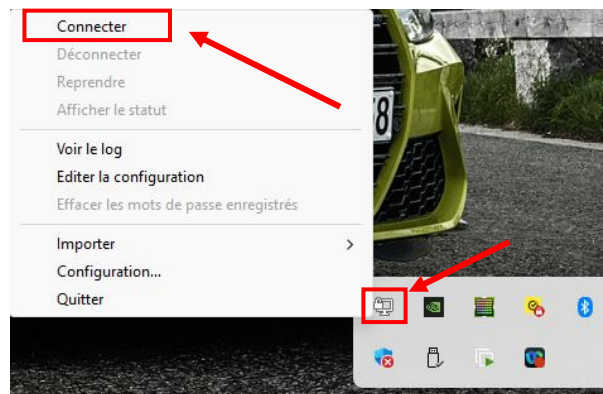
## VI. TEST

---

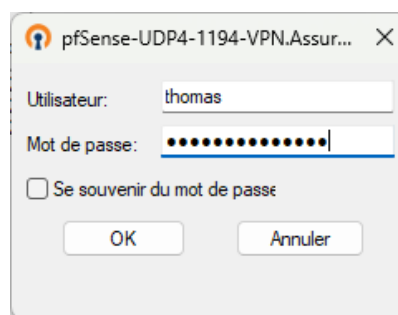
Nous sommes bien connectés à un Wifi domestique pour effectuer ce test



On va tester une connexion en faisant un clic droit sur l'icône VPN et cliquer sur « Connecter »



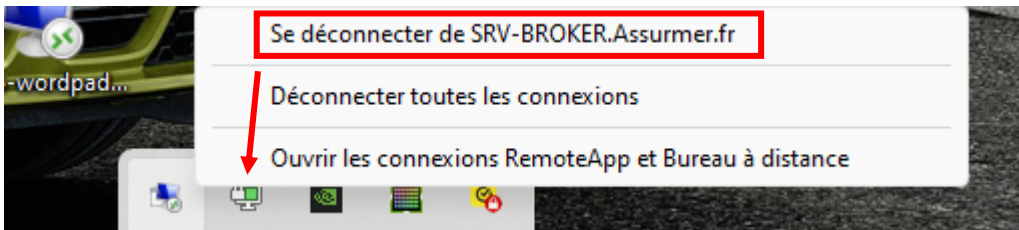
On se connecte avec un utilisateur du domaine



Une fois connecter on récupère bien la configuration réseau du tunnel VPN

```
Carte inconnue OpenVPN TAP-Windows6 :  
Suffixe DNS propre à la connexion. . . : Assurmer.fr  
Adresse IPv6 de liaison locale. . . . . : fe80::a15:44d:9541:3755%61  
Adresse IPv4. . . . . : 10.10.10.6  
Masque de sous-réseau. . . . . : 255.255.255.252  
Passerelle par défaut. . . . . :
```

Nous pouvons voir que nous avons réussie à se connecter à nos serveur RDS depuis un réseau externe en utilisant le VPN d'entreprise



**Résultat :** La connexion externe a fonctionné avec une liaison LDAP actif