

## Interconnexion AD, Pfsense et OpenVPN

**Ce document a pour but de décrire les étapes à réaliser pour se connecter à OpenVPN du Pfsense avec un utilisateur de l'Active Directory**



**Référence : EF-MS-AD&VPN**

**Auteur(s) :**

Dorian Manzanares

**Destinataire(s) :**

Easyformer

Date de modification : 10/12/21

Version : 1

# Sommaire

page

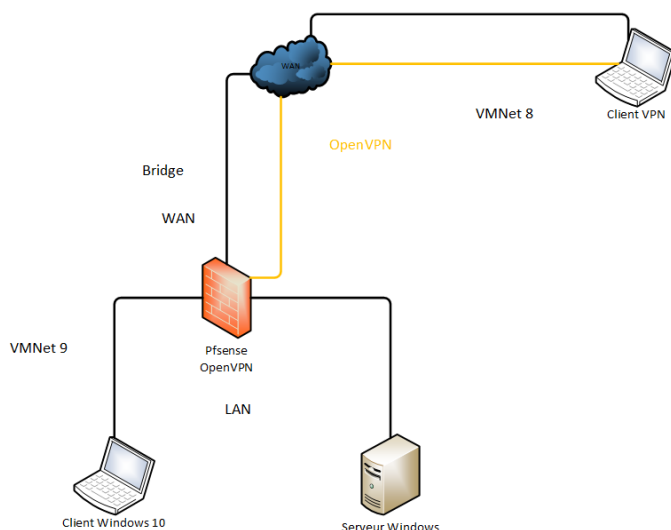
<b>1</b>	<b>PREREQUIS ACTIVE DIRECTORY ET PFSENSE.....</b>	<b>3</b>
1.1	GESTION DE L'ANNUAIRE.....	3
1.1.1	Topologie.....	3
1.1.2	Créations d'utilisateurs.....	3
1.2	GESTION DE PFSENSE .....	4
1.2.1	Création de L'authentification avec AD.....	4
1.2.2	Gérer les droits et connexion au pare-feu avec un utilisateur de l'AD (facultatif) .....	6
1.2.3	Tests de liaison au serveur LDAP .....	7
<b>2</b>	<b>MISE EN PLACE DE OPEN VPN .....</b>	<b>9</b>
2.1	LES CERTIFICATS .....	9
2.1.1	Création d'une autorité de certification et d'un certificat pour le VPN .....	9
2.2	TUNNEL OPENVPN.....	11
2.2.1	Configuration du tunnel .....	11
2.3	EXPORTER LA CONFIGURATION OPENVPN .....	14
2.3.1	Installation du package .....	14
2.4	REGLES DE FIREWALL .....	15
2.4.1	Gestion des règles pour le VPN.....	15
<b>3</b>	<b>CONNEXION AU TUNNEL VPN .....</b>	<b>16</b>
3.1	INSTALLATION ET TESTS .....	16
3.1.1	Utiliser l'assistant OpenVPN.....	16



# 1 Prérequis Active directory et Pfsense

## 1.1 Gestion de l'annuaire

### 1.1.1 Topologie



### 1.1.2 Créations d'utilisateurs

Le but de ce TP sera de mettre en place un VPN client to site avec OpenVPN et associer pfSense à l'active directory.

Les utilisateurs créés pourront se connecter en VPN avec leurs identifiants de l'AD.

Tout d'abord, il faudra se rendre dans « Utilisateurs et ordinateurs Active Directory » au niveau de notre Windows Server, puis dans « Users ».

Ici nous allons créer deux utilisateurs et un groupe.

Racine de la console		Nom	Type	Description
Utilisateurs et ordinateurs Active Directory [DC]		Admin	Utilisateur	
Requêtes enregistrées		Administrateur	Utilisateur	Compte d'utilisateur d'a...
empire.contratak		Administrateurs clés	Groupe de séc...	Les membres de ce grou...
Builtin		Administrateurs clés Entreprise	Groupe de séc...	Les membres de ce grou...
Computers		Administrateurs de l'entreprise	Groupe de séc...	Administrateurs désigné...
Domain Controllers		Administrateurs du schéma	Groupe de séc...	Administrateurs désigné...
Entrepri...		admin-pfsense	Groupe de séc...	
ForeignSecurityPrincipals		Admins du domaine	Groupe de séc...	Administrateurs désigné...
Machines		Bind	Utilisateur	
Managed Service Accounts		Contrôleurs de domaine	Groupe de séc...	Tous les contrôleurs de ...
pfSense		Contrôleurs de domaine clon...	Groupe de séc...	Les membres de ce grou...
Users				

Maintenant, nous allons créer un compte grâce auquel Pfsense pourra récupérer les informations de la base de données active directory.

- Créer un utilisateur nommé Bind
- Créer un groupe nommé « admin-pfsense »
- Ajouter l'utilisateur « Admin » au groupe « admin-pfsense »



## 1.2 Gestion de Pfsense

### 1.2.1 Création de L'authentification avec AD

Dans pfSense on se rendra dans « System » puis « User manager » et on choisira l'onglet « authentication Server » puis, on clique sur add.

Server Settings	
Descriptive name	ADDS
Type	LDAP

LDAP Server Settings	
Hostname or IP address	192.168.9.200 <small>NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.</small>
Port value	389
Transport	TCP - Standard
Peer Certificate Authority	Global Root CA List <small>This CA is used to validate the LDAP server certificate when 'SSL' or 'STARTTLS' Transport is active. This CA must match the CA used by the LDAP server.</small>
Protocol version	3
Server Timeout	25 <small>Timeout for LDAP operations (seconds)</small>
Search scope	Level Entire Subtree  Base DN DC=empire,DC=contratak
Authentication containers	CN=Users,DC=empire,DC=contratak <small>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</small>
Extended query	<input type="checkbox"/> Enable extended query
Bind anonymous	<input type="checkbox"/> Use anonymous binds to resolve distinguished names

Bind credentials	CN=bind,CN=Users,DC=empire,DC=contratak
User naming attribute	samAccountName
Group naming attribute	cn
Group member attribute	memberOf
RFC 2307 Groups	<input type="checkbox"/> LDAP Server uses RFC 2307 style group membership <small>RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).</small>
Group Object Class	posixGroup <small>Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".</small>
UTF8 Encode	<input type="checkbox"/> UTF8 encode LDAP parameters before sending them to the server. <small>Required to support international characters, but may not be supported by every LDAP server.</small>
Username Alterations	<input type="checkbox"/> Do not strip away parts of the username after the @ symbol <small>e.g. user@host becomes user when unchecked.</small>



- Dans Hostname or IP address Il faut renseigner l'IP du serveur.
- La base DN signifie le nom de domaine "DC=empire,DC=contratak  
C'est le nom de domaine que j'ai choisi pour mon Windows Server.
- Pour l'authentification containers, il faut choisir un compte dont le mot de passe n'expirera pas car sinon les authentifications ne pourront pas se faire cela peut poser de gros problèmes si ce compte devient indisponible. Donc ça sera le compte « Bind » crée plus haut.

Une fois que tous les champs sont bien remplis, on peut cliquer sur save.



### 1.2.2 Gérer les droits et connexion au pare-feu avec un utilisateur de l'AD (facultatif)

Il faut ajouter le groupe « admin-pfsense » créé dans l'AD sur pfsense avec le même nom dans l'onglet System\user manager.

Il faut choisir un type « remote »

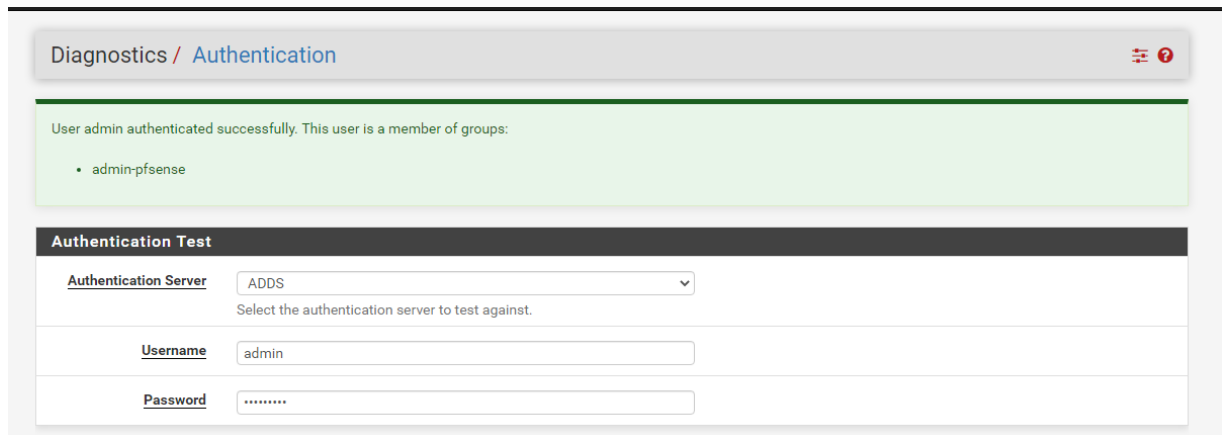
The screenshot shows the 'Group Properties' page in pfSense. The 'Group name' is 'admin-pfsense'. The 'Scope' is set to 'Remote', with a warning message: 'Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.' The 'Description' is 'Groupe des services AD'. The 'Group membership' section shows two lists: 'Not members' and 'Members'. The 'Members' list contains the user 'admin'. There are buttons to 'Move to "Members"' and 'Move to "Not members"'. A note at the bottom says: 'Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.'



### 1.2.3 Tests de liaison au serveur LDAP

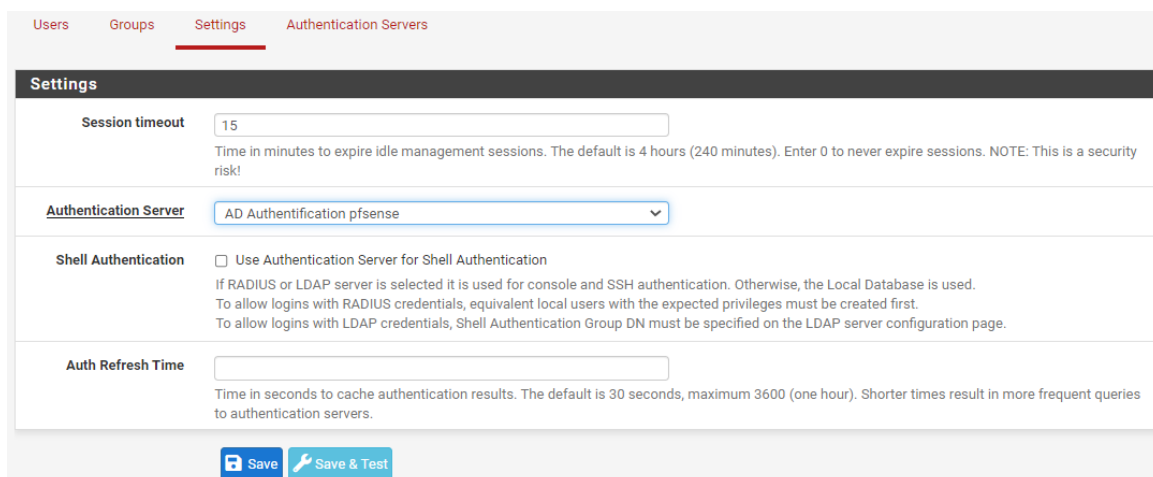
On peut maintenant tester l'authentification d'un utilisateur de mon domaine au niveau de Pfsense.

Pour cela, il faut se rendre dans l'onglet « Diagnostic » puis dans « Authentication ».



The screenshot shows the 'Diagnostics / Authentication' page in Pfsense. At the top, a green message box states: 'User admin authenticated successfully. This user is a member of groups: • admin-pfsense'. Below this is the 'Authentication Test' section. It contains three input fields: 'Authentication Server' (a dropdown menu currently showing 'ADDS'), 'Username' (a text box containing 'admin'), and 'Password' (a masked text box showing '\*\*\*\*\*').

Après un test réussi au niveau de notre utilisateur, nous allons pouvoir tester la bonne liaison de Pfsense avec l'Active Directory, pour se faire, il faut se rendre dans le menu « Settings » et renseigner la base de donnée LDAP.



The screenshot shows the 'Settings' page for 'Authentication Servers' in Pfsense. The 'Settings' tab is selected. The page includes several configuration options: 'Session timeout' (a text box with '15'), 'Authentication Server' (a dropdown menu showing 'AD Authentication pfsense'), 'Shell Authentication' (a checkbox labeled 'Use Authentication Server for Shell Authentication' which is unchecked), and 'Auth Refresh Time' (a text box). At the bottom, there are two buttons: 'Save' and 'Save & Test'.

**Save and test** permet de vérifier que la synchro pfsense et AD fonctionne bien.



## LDAP settings

## Test results

Attempting connection to	192.168.9.200	OK
Attempting bind to	192.168.9.200	OK
Attempting to fetch Organizational Units from	192.168.9.200	OK
Organization units found		
OU=Compta,OU=Entreprise,DC=empire,DC=contratak		
OU=Direction,OU=Entreprise,DC=empire,DC=contratak		
OU=Domain Controllers,DC=empire,DC=contratak		
OU=Entreprise,DC=empire,DC=contratak		
OU=Gestion,OU=Entreprise,DC=empire,DC=contratak		
OU=Info,OU=Entreprise,DC=empire,DC=contratak		
OU=Machines,DC=empire,DC=contratak		
OU=pfsense,DC=empire,DC=contratak		
CN=Users,DC=empire,DC=contratak		

Le résultat du test confirmera que notre configuration est valide.





## 2 Mise en place de open VPN





### 2.1 Les certificats


#### 2.1.1 Création d'une autorité de certification et d'un certificat pour le VPN

J'ai choisi d'appeler mon autorité de certificat CA-PFSense

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA-PFSense	✓	self-signed	1	ST=IDF, O=EF, L=Paris, CN=CA-VPN, C=FR Valid From: Tue, 07 Dec 2021 21:51:39 +0000 Valid Until: Fri, 17 Dec 2021 21:51:39 +0000	OpenVPN Server	 

Et mon certificat utilisateur pour OpenVPN nommé Pfsense-certif

Certificates				
Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (61ad2db19b497) Server Certificate CA: No Server: Yes	self-signed	O=pfsense webConfigurator Self-Signed Certificate, CN=pfsense-61ad2db19b497 Valid From: Sun, 05 Dec 2021 21:22:57 +0000 Valid Until: Sat, 07 Jan 2023 21:22:57 +0000		 
Pfsense-certif Server Certificate CA: No Server: Yes	CA-PFSense	ST=IDF, O=EF, L=Paris, CN=serveur-pfsense, C=FR Valid From: Tue, 07 Dec 2021 21:53:43 +0000 Valid Until: Fri, 05 Dec 2021 21:53:43 +0000	OpenVPN Server	 

 Add/Sign



Bien que j'utilise l'annuaire LDAP pour me connecter au VPN, il faut tout de même créer un utilisateur.

Dans User certificat, il faudra cliquer sur **add**, on sera alors redirigé vers une page pour créer un certificat.

Il faudra ensuite uniquement vérifier que le type de certificat « User » soit bien sélectionné.

VPN-USER User Certificate CA: <b>No</b> Serveur: <b>No</b>	CA-Pfsense ST=IDF, O=EF, L=Paris, CN=toto, C=FR  Valable depuis: <b>Thu, 09 Dec 2021 21:28:25 +0000</b> Valable jusqu'au: <b>Sun, 07 Dec 2031 21:28:25 +0000</b>	Certificat utilisateur     
---	---	--



## 2.2 Tunnel OpenVPN

### 2.2.1 Configuration du tunnel

Nous allons maintenant configurer le tunnel VPN, c'est-à-dire paramétrer le serveur (Pfsense).

The screenshot shows the 'General Information' tab for an OpenVPN server configuration. The settings are as follows:

- Disabled:** ☐ Disable this server. Set this option to disable this server without removing it from the list.
- Server mode:** Remote Access ( SSL/TLS + User Auth )
- Backend for authentication:** ADDS (Local Database is also visible in the dropdown)
- Protocol:** UDP on IPv4 only
- Device mode:** tap - Layer 2 Tap Mode. Notes: "tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2).
- Interface:** WAN. Note: The interface or Virtual IP address where OpenVPN will receive client connections.
- Local port:** 1194. Note: The port used by OpenVPN to receive client connections.
- Description:** Accès OpenVPN. Note: A description may be entered here for administrative reference (not parsed).

Ci-dessus il faut préciser que le VPN recevra ses clients depuis l'interface WAN et que le port de réception sera le port 1194, il est important de donner une description.

Là j'ai choisi l'autorité de certificat que j'ai créé auparavant pour les échanges sécurisés.

The screenshot shows the 'Peer Certificate Authority' configuration page. The settings are as follows:

- Peer Certificate Authority:** CA-Pfsense
- 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:** Pfsense-VPN (Server: Yes, CA: CA-Pfsense, In Use)
- DH Parameter Length:** 2048 bit. Note: Diffie-Hellman (DH) parameter set used for key exchange.
- ECDH Curve:** Use Default. Note: The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.
- Data Encryption Negotiation:** ☒ Enable Data Encryption Negotiation. Note: This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.
- Data Encryption Algorithms:**
  - AES-128-CBC (128 bit key, 128 bit block)
  - AES-128-CFB (128 bit key, 128 bit block)
  - AES-128-CFB1 (128 bit key, 128 bit block)
  - AES-128-CFB8 (128 bit key, 128 bit block)
  - AES-128-GCM (128 bit key, 128 bit block)
  - AES-128-OFB (128 bit key, 128 bit block)
  - AES-192-CBC (192 bit key, 128 bit block)
  - AES-192-CFB (192 bit key, 128 bit block)
  - AES-192-CFB1 (192 bit key, 128 bit block)
  - AES-192-CFB8 (192 bit key, 128 bit block)
  - AES-128-GCM
  - AES-256-CBC



Là le réseau IPV4 du tunnel VPN et renseigné en tant que : 10.10.10.0/24 c'est-à-dire que lorsque quelqu'un se connectera en VPN, il fera partie de ce réseau.

Tunnel Settings	
IPv4 Tunnel Network	<input type="text" value="10.10.10.0/24"/> <small>This is the IPv4 virtual network 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>
IPv6 Tunnel Network	<input type="text"/> <small>This is the IPv6 virtual network 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>
Bridge DHCP	<input type="checkbox"/> Allow clients on the bridge to obtain DHCP.
Bridge Interface	<input type="text" value="none"/> <small>The interface to which this TAP instance will be bridged. This is not done automatically. This interface must be assigned and the bridge created separately. This setting controls which existing IP address and subnet mask are used by OpenVPN for the bridge. Setting this to 'none' will cause the Server Bridge DHCP settings below to be ignored.</small>
Server Bridge DHCP Start	<input type="text"/> <small>When using TAP mode as a multi-point server, a DHCP range may optionally be supplied to use on the interface to which this TAP instance is bridged. If these settings are left blank, DHCP will be passed through to the LAN, and the interface setting above will be ignored.</small>
Server Bridge DHCP End	<input type="text"/>
Redirect IPv4 Gateway	<input checked="" 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.
IPv6 Local network(s)	<input type="text"/>

Là précise que lorsque l'utilisateur sera connecté en VPN il aura accès au réseau inscrit pour ajouter un autre réseau il suffit de rajouter un point-virgule.

Ce champ renseigne la limitation connexion simultanée avec un compte en VPN

IPv4 Local network(s)	<input type="text" value="10.0.0.0/24"/> <small>IPv4 networks that will be accessible from the remote endpoint. Expresses blank if not adding a route to the local network through this tunnel on the remote machine.</small>
Concurrent connections	<input type="text" value="10"/> <small>Specify the maximum number of clients allowed to concurrently connect to this server.</small>

Ce champ facilite le changement d'adresse IP du client lorsqu'ils se connectent en VPN en effet cela peut causer certains problèmes lorsque le client se connectent plusieurs fois avec plusieurs adresses IP publique différentes ce champ remédie à ce problème.

Dynamic IP	<input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.
------------	--

Advanced Client Settings	
DNS Default Domain	<input checked="" type="checkbox"/> Provide a default domain name to clients
DNS Default Domain	<input type="text" value="empire.contratak"/>
DNS Server enable	<input checked="" type="checkbox"/> Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	<input type="text" value="192.168.8.201"/>



L'option suivante permet de résoudre un bug Windows qui empêche la résolution de nom DNS lorsque que le VPN est activé, en effet il utilise DNS local au lieu du VPN.

**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.

Cette option permet de supprimer le cache de connexion ce qui limite les risques d'attaque.

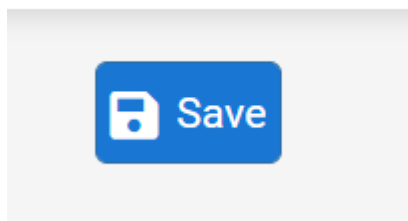
## Need Configuration

### Custom options

auth-nocache

Enter any additional options to add to the OpenVPN server configuration here  
EXAMPLE: push "route 10.0.0.0 255.255.255.0"

Une fois la configuration effectuée, il est temps de la sauvegarder.



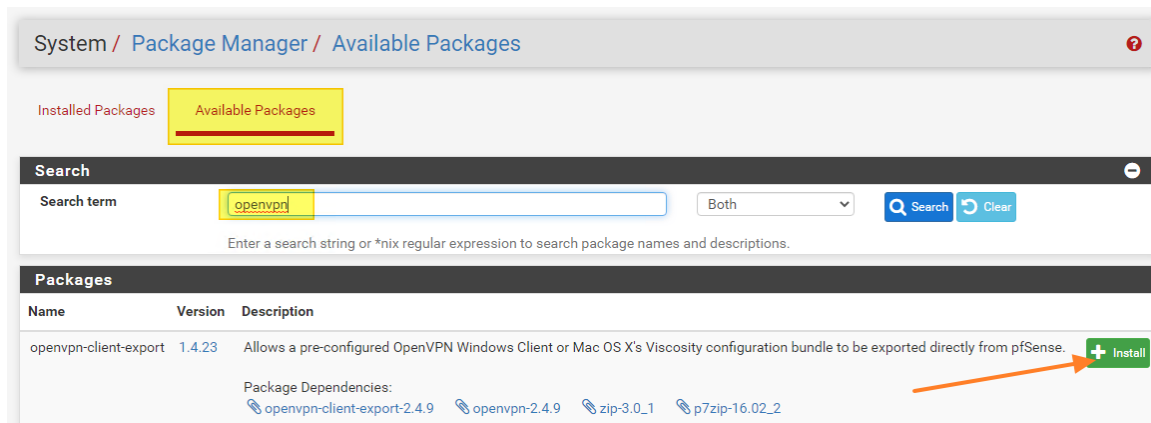
## 2.3 Exporter la configuration OpenVPN

### 2.3.1 Installation du package

Pour télécharger la configuration, il est nécessaire d'installer un paquet supplémentaire sur notre pare-feu.

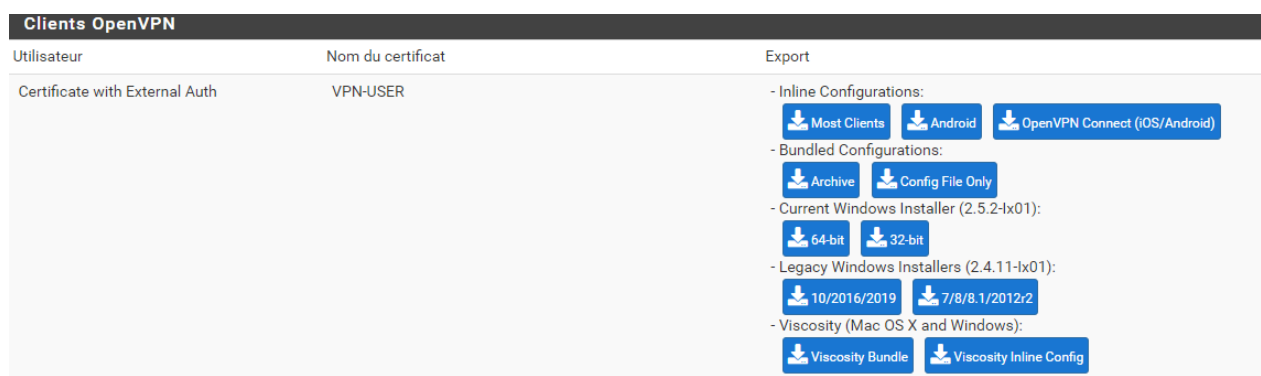
Rendez-vous dans le menu suivant : System > Package Manager > Available Packages.

Il faudra ici installer le paquet « openvpn-client-export ».



Il faudra ensuite se rendre dans : VPN/OpenVPN/Servers puis dans client export

Cliquez sur archive qui téléchargera la configuration tu certificats open VPN de fichier sera un zip à décompresser, le lien de téléchargement est disponible choisir en fonction de son système d'exploitation. Et lancer les fichiers avec open VPN.



On peut voir ici que Pfsense considère mon authentification comme « externe » soit l'ADDS.

Il faut télécharger et installer « Current Windows Installer 64 bits », sur la machine Windows.



## 2.4 Règles de firewall

### 2.4.1 Gestion des règles pour le VPN

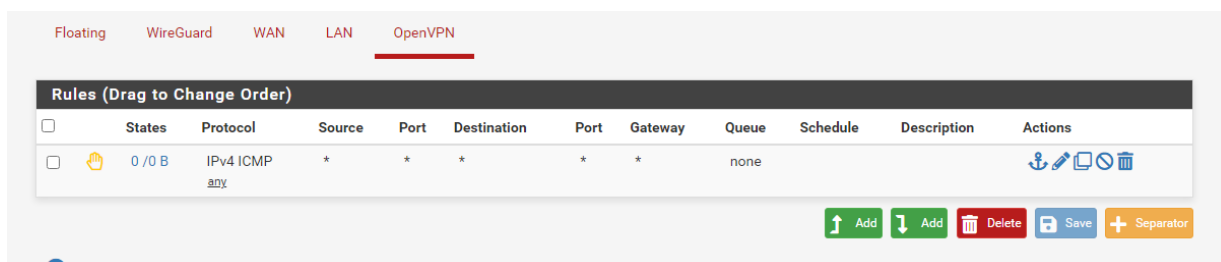
Les règles de firewall sont à fixer en fonction de vos besoins ou de ceux de l'entreprise.



The screenshot shows the 'WAN' tab selected in the Pfsense Firewall Rules configuration. The table lists one rule with the following details:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	WAN address	1194 (OpenVPN)	*	*	*	none	OpenVPN-Distant	

Et ensuite sur l'onglet OpenVPN :



The screenshot shows the 'OpenVPN' tab selected in the Pfsense Firewall Rules configuration. The table lists one rule with the following details:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0 / 0 B	IPv4 ICMP any	*	*	*	*	*	none		

Below the table, there are buttons for 'Add' (up and down arrows), 'Delete', 'Save', and 'Separator'.

On peut par exemple ici remarquer que pour l'interface OpenVPN (qui est créée automatiquement lors de la création du VPN), je vais bloquer l'ICMP.

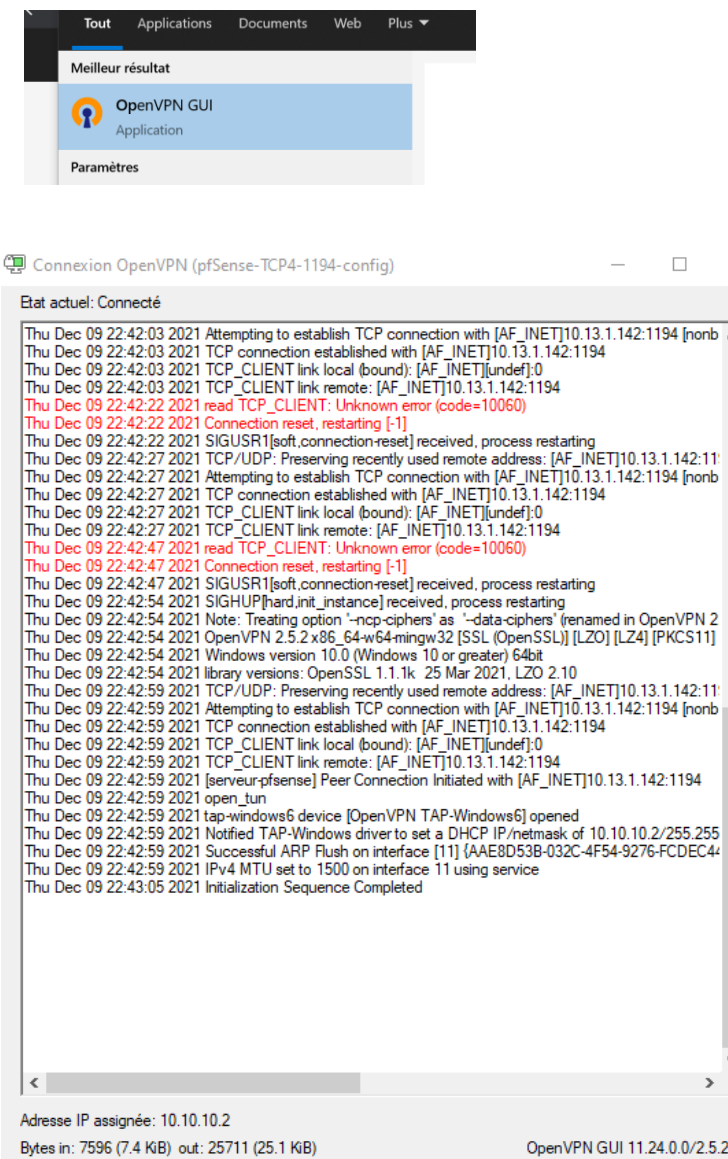


## 3 Connexion au tunnel VPN

### 3.1 Installation et tests

#### 3.1.1 Utiliser l'assistant OpenVPN

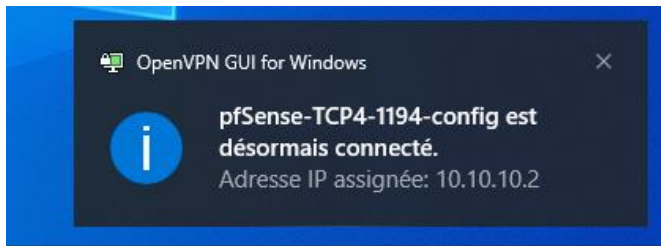
On lance OPENVPN, on va ici se connecter avec l'utilisateur « Admin » créée sur notre Active Directory.



On on peut voir que j'ai une adresse IP en 10.10.10.0/24 comme défini au préalable, le DHCP du pfSense m'a bien fourni une adresse IP.







```
C:\Windows\system32\cmd.exe

Carte inconnue OpenVPN Wintun :

  Statut du média. . . . . : Média déconnecté
  Suffixe DNS propre à la connexion. . . :

Carte Ethernet Ethernet0 :

  Suffixe DNS propre à la connexion. . . : localdomain
  Adresse IPv6 de liaison locale. . . . : fe80::2050:e5e5:17c8:f6fd%3
  Adresse IPv4. . . . . : 10.13.1.124
  Masque de sous-réseau. . . . . : 255.255.255.0
  Passerelle par défaut. . . . . : 10.13.1.254

Carte inconnue OpenVPN TAP-Windows6 :

  Suffixe DNS propre à la connexion. . . : empire.contratak
  Adresse IPv6 de liaison locale. . . . : fe80::2165:dc46:6bfd:7341%11
  Adresse IPv4. . . . . : 10.10.10.2
  Masque de sous-réseau. . . . . : 255.255.255.0
  Passerelle par défaut. . . . . :
```

Sur pfsense, on peut voir le tunnel créé via « Status/OpenVPN »

Status / OpenVPN

Server TCP4:1194 Client Connections: 1

Common Name	Real Address	Virtual Address	Connected Since	Bytes Sent	Bytes Received	Cipher
toto admin	10.13.1.124:49642	10.10.10.2	2021-12-09 22:27:11	5 KiB	6 KiB	AES-128-GCM

Status: Actions:

Voilà, votre tunnel est configuré, et vous vous êtes connecté avec un utilisateur du domaine

