

# **TP4 : OpenVPN**

## **Pfsense**

**Fait par DEPRADE ELIOTT**

# SOMMAIRE

But du TP .....	2
Configuration dans Pfsense .....	3
Création certificat serveur .....	3
Création d'un utilisateur.....	5
Configuration du VPN.....	7
Export de la configuration .....	9
Configuration du client VPN (machine physique) .....	10
Derniers tests .....	11
Vérification de l'interface .....	12

## But du TP

Un client nomade (ordinateur personnel) doit pouvoir se connecter à distance au réseau local derrière pfSense, comme s'il y était physiquement connecté.

La connexion doit être chiffré en UDP.

## Configuration dans PfSense

### Création certificat serveur

Dans un premier temps on va créer le certificat du serveur en allant dans System > Certificates > Authorities :

The screenshot shows the pfSense Community Edition web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main menu on the left has 'System /' selected, with sub-options like Advanced, Certificates, General Setup, High Availability, Package Manager, Register, Routing, Setup Wizard, Update, User Manager, and Logout (admin). The 'Authorities' option is highlighted with a red underline. The central content area is titled 'Authorities' and contains a search bar with fields for 'Search term' and dropdowns for 'Both' and 'Search'. Below the search bar is a note: 'This is set to the default value. Change the password in the User Manager.' A large green button at the bottom right says '+ Add'.

Cliquons sur “Add”.

The screenshot shows two main sections of the pfSense configuration interface:

**Create / Edit CA** (Top Section):

- Descriptive name:** OpenVPN
- Method:** Import an existing Certificate Authority
- Trust Store:**  Add this Certificate Authority to the Operating System Trust Store
- Randomize Serial:**  Use random serial numbers when signing certificates

**Existing Certificate Authority** (Bottom Section):

- System / Certificate / Authorities**
- Authorities** tab is selected.
- Search** bar: Search term (empty), Both dropdown, Search button, Clear button.
- Certificate Authorities** table:

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
OpenVPN	✓	self-signed	0	CN=pfSense.cs.cr <small>i</small> Valid From: Sat, 06 Dec 2025 23:16:46 +0000 Valid Until: Tue, 04 Dec 2035 23:16:46 +0000		<small>edit</small> <small>key</small> <small>cert</small> <small>archive</small>

On choisit la méthode **Method: Create an Internal Certificate Authority**

Et dans le **Common Name** on renseigne **le nom de domaine**, exemple pour ici :  
pfSense.cs.cr

Ensuite, passez à l'onglet **Certificates** et créez un nouveau certificat de serveur en cliquant sur Add/Sign. Choisissez Create an internal certificate, nommez-le (p.ex. OpenVPN-remote-access), sélectionnez la CA créée précédemment et entrez comme Common Name le nom du serveur (par ex. pfSense.cs.cr). Dans Certificate Type, sélectionnez Server Certificate. Cliquez sur Save.



**WARNING:** The 'admin' account password is set to the default value. Change the password in the User Manager.

## System / Certificates / Certificates



Created internal certificate OpenVPN-remote-access



Authorities   Certificates   Certificate Revocation

### 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
GUI default (6922fac4d31d4) <i>Server Certificate</i>	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-6922fac4d31d4		
CA: No Server: Yes		Valid From: Sun, 23 Nov 2025 12:15:01 +0000 Valid Until: Sat, 26 Dec 2026 12:15:01 +0000		
OpenVPN-remote-access <i>Server Certificate</i>	OpenVPN	CN=pfSense.cs.cr		
CA: No Server: Yes		Valid From: Sat, 06 Dec 2025 23:22:48 +0000 Valid Until: Tue, 04 Dec 2035 23:22:48 +0000		

Add/Sign

## Création d'un utilisateur

Allez ensuite dans System>User Manager>Users>Edit.

The screenshot shows the pfSense User Manager Edit screen. At the top, there is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the breadcrumb navigation shows "System / User Manager / Users / Edit". The main form is titled "User Properties" and contains the following fields:

- Defined by: USER
- Disabled:  This user cannot login
- Username: [Input field]
- Password: [Input field] Confirm Password: [Input field]
- Full name: [Input field]  
User's full name, for administrative information only
- Expiration date: [Input field]  
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY
- Custom Settings:  Use individual customized GUI options and dashboard layout for this user.
- Group membership:
  - Not member of: [Input field] [Move to "Member of" list](#)
  - Member of: [Input field] [Move to "Not member of" list](#)
- Certificate:  Click to create a user certificate

Créer votre utilisateur et cochez la case “Create User Certificate”.

The screenshot shows the pfSense User Manager Edit screen with three tabs visible: "Effective Privileges", "User Certificates", and "Keys".

- Effective Privileges:** A table with columns "Inherited from", "Name", "Description", and "Action". There is one row with a green "+ Add" button.
- User Certificates:** A table with columns "Name" and "CA". It shows a row for "alice" with "OpenVPN" as the CA, along with a delete icon and a green "+ Add" button.
- Keys:** A section titled "Authorized SSH Keys" with a text input field.

Utilisez le CA que vous venez de créer.

Parfait, votre utilisateur devrait être maintenant visible dans vos Users.

The screenshot shows the pfSense User Manager interface. At the top, there are tabs for 'Users', 'Groups', 'Settings', and 'Authentication Servers'. The 'Users' tab is selected. Below it is a table titled 'Users' with columns: Username, Full name, Status, Groups, and Actions. Two users are listed: 'admin' (System Administrator) and 'alice'. The 'Status' column shows a checkmark for both. The 'Groups' column shows 'admins' for both. The 'Actions' column for each user has a pencil icon for edit and a trash bin icon for delete. At the bottom right of the table are buttons for '+ Add' and 'Delete'.

Passons à la configuration du VPN

## Configuration du VPN

Allez dans VPN > OpenVPN > Wizard

The screenshot shows the pfSense OpenVPN Remote Access Server Setup wizard. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. A red box highlights the 'VPN' dropdown menu, which is open to show options: 'IPsec', 'L2TP', and 'OpenVPN'. The main content area is titled 'OpenVPN Remote Access Server Setup' and contains instructions: 'This wizard will provide guidance through an OpenVPN Remote Access Server Setup.' and 'The wizard may be stopped at any time by clicking the logo image at the top of the screen.' Below this is a section titled 'Select an Authentication Backend Type' with a dropdown menu set to 'Local User Access'. A note below the dropdown says: 'NOTE: If unsure, leave this set to "Local User Access."'. At the bottom is a blue '» Next' button.

**Type de serveur** = Local User Access

**Autorité CA et certificat serveur** = choisissez la CA interne créée et le certificat serveur (OpenVPN remote-access) déjà générés.

**Adresse WAN du serveur** = indiquez l'IP WAN actuelle du pfSense (ici 192.168.1.130)

Choisissez une adresse différente de votre Wan ou Lan pour votre **Tunnel**

**Local Network** = spécifiez le réseau LAN local à rendre accessible par le VPN

**Advanced Client Settings** = entrez DNS Default Domain = votre domaine, DNS Server 1 = (IP LAN) et DNS Server 2 = (IP WAN/pfSense)

Tunnel Settings	
IPv4 Tunnel Network	<input type="text" value="192.168.200.0/24"/> This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation. The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.
Redirect IPv4 Gateway	<input type="checkbox"/> Force all client generated traffic through the tunnel.
IPv4 Local Network	<input type="text" value="10.10.10.0/24"/> This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not connecting through this tunnel on the remote machine. This is generally set to the LAN network.
Concurrent Connections	<input type="text"/>
	Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression	<input type="text" value="Refuse any non-stub compression (Most secure)"/> <input type="button" value="▼"/>
	Allow compression to be used with this VPN instance, which is potentially insecure.
Compression	<input type="text" value="Disable Compression [Omit Preference]"/> <input type="button" value="▼"/>
	Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects packets not being compressed efficiently.
Type-of-Service	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication	<input type="checkbox"/> Allow communication between clients connected to this server.
Duplicate Connections	<input type="checkbox"/> Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.
Duplicate Connection Limit	<input type="text"/> Limit the number of concurrent connections from the same user.
Advanced Client Settings	
DNS Default Domain	<input type="text" value="cs.cr"/> Provide a default domain name to clients.
DNS Server 1	<input type="text" value="10.10.10.1/24"/> DNS server IP to provide to connecting clients.
DNS Server 2	<input type="text" value="8.8.8.8"/> DNS server IP to provide to connecting clients.
DNS Server 3	<input type="text"/> DNS server IP to provide to connecting clients.
DNS Server 4	<input type="text"/> DNS server IP to provide to connecting clients.
NTP Server	<input type="text"/> Network Time Protocol server to provide to connecting clients.
NTP Server 2	<input type="text"/> Network Time Protocol server to provide to connecting clients.
NetBIOS Options	<input type="checkbox"/> Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
NetBIOS Node Type	<input type="text" value="none"/> Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).
NetBIOS Client IP	<input type="text"/>

Le Wizard propose ensuite d'ajouter automatiquement des règles de pare-feu. Validez les options Add a firewall rule et Add an OpenVPN rule pour autoriser le trafic VPN entrant. Terminez le Wizard. Un serveur OpenVPN est alors créé, mais nous devons affiner certains réglages.

Dans “**advanced configuration**” ajoutez la ligne push “route LAN MASK” dans Custom Option

The screenshot shows the "Advanced Configuration" section of a software interface. At the top, there is a "Custom options" field containing the command "push \"route 10.10.10.0 255.255.255.0\"". Below this, a note says: "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\"". There are two main configuration sections:

- Username as Common Name:** A checked checkbox labeled "Use the authenticated client username instead of the certificate common name (CN)". A note below it states: "When a user authenticates, if this option is enabled then the username of the client will be used in place of the such as determining Client Specific Overrides".
- UDP Fast I/O:** An unchecked checkbox labeled "Use fast I/O operations with UDP writes to tun/tap. Experimental". A note below it states: "Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platform bandwidth limiting".

Votre VPN est normalement fin prêt :

The screenshot shows the "OpenVPN Servers" list. At the top, there are tabs for "Servers", "Clients", "Client Specific Overrides", and "Wizards", with "Servers" being the active tab. The list table has columns: "Interface", "Protocol / Port", "Tunnel Network", "Mode / Crypto", "Description", and "Actions". One entry is listed:

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	192.168.200.0/24	Mode: Remote Access ( SSL/TLS + User Auth ) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits		

At the bottom right of the list area, there is a green button with a plus sign and the word "Add".

## Export de la configuration

Installez le paquet **openvpn-client-export** via **System > Packages**. Ensuite, retournez dans VPN > OpenVPN, onglet Client Export. Sélectionnez l'utilisateur alice et cliquez sur **Most Clients** pour générer un fichier .ovpn (il contient automatiquement le certificat utilisateur et la CA) . Téléchargez ce profil sur le poste client.

The top screenshot shows the 'Available Packages' page in the pfSense Package Manager. A search term 'openvpn-client-export' has been entered in the search bar. The results table shows one package:

Name	Version	Description
openvpn-client-export	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.

Below the table, it says 'Package Dependencies:' followed by a list of packages: openvpn-client-export-2.6.7, openvpn-2.6.8\_1, zip-3.0\_1, and 7-zip-23.01. There is a green 'Install' button next to the package row.

The bottom screenshot shows the 'OpenVPN Clients' page for user 'alice'. It lists the certificate name 'alice' and provides download links for various clients and configurations. The available options include:

- Inline Configurations:
  - [Most Clients](#)
  - [Android](#)
  - [OpenVPN Connect \(iOS/Android\)](#)
- Bundled Configurations:
  - [Archive](#)
  - [Config File Only](#)
- Current Windows Installers (2.6.7-ix001):
  - [64-bit](#)
  - [32-bit](#)
- Previous Windows Installers (2.5.9-ix601):
  - [64-bit](#)
  - [32-bit](#)
- Legacy Windows Installers (2.4.12-ix601):
  - [10/2016/2019](#)
  - [7/8/8.1/2012/2](#)
- Viscosity (Mac OS X and Windows):
  - [Viscosity Bundle](#)
  - [Viscosity Inline Config](#)

A note at the bottom of the page states: 'Only OpenVPN-compatible user certificates are shown'.

## Configuration du client VPN (machine physique)

Sur la machine physique (située sur le réseau WAN), installez un client OpenVPN adapté à l'OS

Sous Windows, installez OpenVPN Connect puis importez le fichier .ovpn :



Vous serez ensuite connecté à votre pfSense grâce aux identifiants de l'utilisateur créé précédemment.

## Derniers tests

Essayez de pinger votre LAN depuis votre machine en WAN :

```

Microsoft Windows [version 10.0.19045.6575]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\depra>ping 10.10.10.10

Envoi d'une requête 'Ping' 10.10.10.10 avec 32 octets de données :
Réponse de 10.10.10.10 : octets=32 temps<1ms TTL=63
Réponse de 10.10.10.10 : octets=32 temps=1 ms TTL=63
Réponse de 10.10.10.10 : octets=32 temps=1 ms TTL=63
Réponse de 10.10.10.10 : octets=32 temps=1 ms TTL=63

Statistiques Ping pour 10.10.10.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\depra>

```

Si ce test ne fonctionne pas, vérifiez votre pare-feu psSense voir s'il n'y a pas de règles trop strictes.

En faisant ipconfig/all votre pc devrait avoir une interface dans la plage de l'IP choisie plus tôt :

## Vérification de l'interface

139 213_4943101	fe80::7188:e82b:b58a:55c3	ffff:1:10	102 Standard query 0x00000 PING _B
137 215_495430	192.168.200.2	224.0.0.251	82 Standard query 0x00000 PTR _B
138 215_495844	fe80::7188:e82b:b58a:55c3	ff02::fb	102 Standard query 0x00000 PTR _B
139 218_962569	00:ff:4f:97:78:42	Broadcast	42 Who has 192.168.200.1? Tell _B
140 218_962579	00:ff:50:97:78:42	00:ff:4f:97:78:42	60 192.168.200.1 is at 00:ff:50:97:78:42
141 219_418510	fe80::7188:e82b:b58a:55c3	ff02::1:2	DHCPv6 STEADYDISCOVER
142 224_280377	192.168.200.2	192.168.200.255	147 Solicit XID: 0xbdd2570 CID: 0
143 224_699183	192.168.200.2	10.10.10.10	280 Client Status from TH00R/Mal:
144 224_699993	10.10.10.10	192.168.200.2	74 Echo (ping) request id=0x0000
145 225_701332	192.168.200.2	10.10.10.10	74 Echo (ping) reply id=0x0000
146 225_702380	10.10.10.10	192.168.200.2	74 Echo (ping) request id=0x0000
147 226_703242	192.168.200.2	10.10.10.10	74 Echo (ping) reply id=0x0000
148 226_704277	10.10.10.10	192.168.200.2	74 Echo (ping) request id=0x0000
149 227_706576	192.168.200.2	10.10.10.10	74 Echo (ping) reply id=0x0000
150 227_707687	10.10.10.10	192.168.200.2	74 Echo (ping) request id=0x0000
151 235_419577	fe80::7188:e82b:b58a:55c3	ff02::1:2	74 Echo (ping) reply id=0x0000
			147 Solicit XID: 0xbdd2570 CID: 0

On peut voir que j'utilise bien l'interface 192.168.200.2 (le tunnel)

Et sur l'interface wan cela se traduit par du traffic en UDP chiffré :

81	3.532075	192.168.1.33	192.168.1.4	WireGuard	138 Transport Data, receiver=0x400FC7C4, counter=657, data1
82	3.532637	192.168.1.4	192.168.1.33	WireGuard	138 Transport Data, receiver=0x400F9E81, counter=415, data1
83	3.533000	192.168.1.33	192.168.1.4	WireGuard	122 Transport Data, receiver=0x400FC7C4, counter=658, data1
84	3.533393	192.168.1.33	192.168.1.4	WireGuard	1354 Transport Data, receiver=0x400FC7C4, counter=659, data1
85	3.533367	192.168.1.33	192.168.1.4	WireGuard	682 Transport Data, receiver=0x400FC7C4, counter=660, data1
86	3.533878	192.168.1.4	192.168.1.33	WireGuard	122 Transport Data, receiver=0x2024E9E81, counter=416, data1
87	3.534200	192.168.1.4	192.168.1.33	WireGuard	1354 Transport Data, receiver=0x400FC7C4, counter=661, data1
88	3.535472	192.168.1.4	192.168.1.33	WireGuard	714 Transport Data, receiver=0x400F9E81, counter=418, data1
89	3.535687	192.168.1.33	192.168.1.4	WireGuard	122 Transport Data, receiver=0x400FC7C4, counter=661, data1
90	3.535845	192.168.1.33	192.168.1.4	WireGuard	134 Transport Data, receiver=0x400FC7C4, counter=662, data1
91	3.535898	192.168.1.33	192.168.1.4	WireGuard	122 Transport Data, receiver=0x400FC7C4, counter=663, data1
92	3.536228	192.168.1.4	192.168.1.33	WireGuard	122 Transport Data, receiver=0x2024E9E81, counter=419, data1
93	3.536489	192.168.1.33	192.168.1.4	WireGuard	122 Transport Data, receiver=0x400FC7C4, counter=664, data1

