

## PfSense 2.8.1 // OpenVPN

LA STRUCTURE PKI (Public Key Infrastructure).....	2
L'Autorité de Certification (CA).....	2
CRÉATION DU CERTIFICAT SERVEUR (L'Oracle).....	5
GESTION UTILISATEUR (L'Accès Client).....	8
CONFIGURATION DU SERVEUR OPENVPN (Le Tunnel).....	11
LA SÉCURITÉ (Firewall Rules).....	18
La Porte d'Entrée (WAN).....	18
La Liberté de Mouvement (Interface OpenVPN).....	21
DÉPLOIEMENT CLIENT (Le Package Magique).....	24
Installation de l'outil.....	24
Configuration de l'Export.....	26
TEST FINAL (L'Injection Debian).....	29
Installation d'OpenVPN.....	29
Lancement du tunnel.....	30

# LA STRUCTURE PKI (Public Key Infrastructure)

*L'Architecte de la confiance. Sans ça, c'est juste deux ordinateurs qui se crient des chiffres aléatoires.*

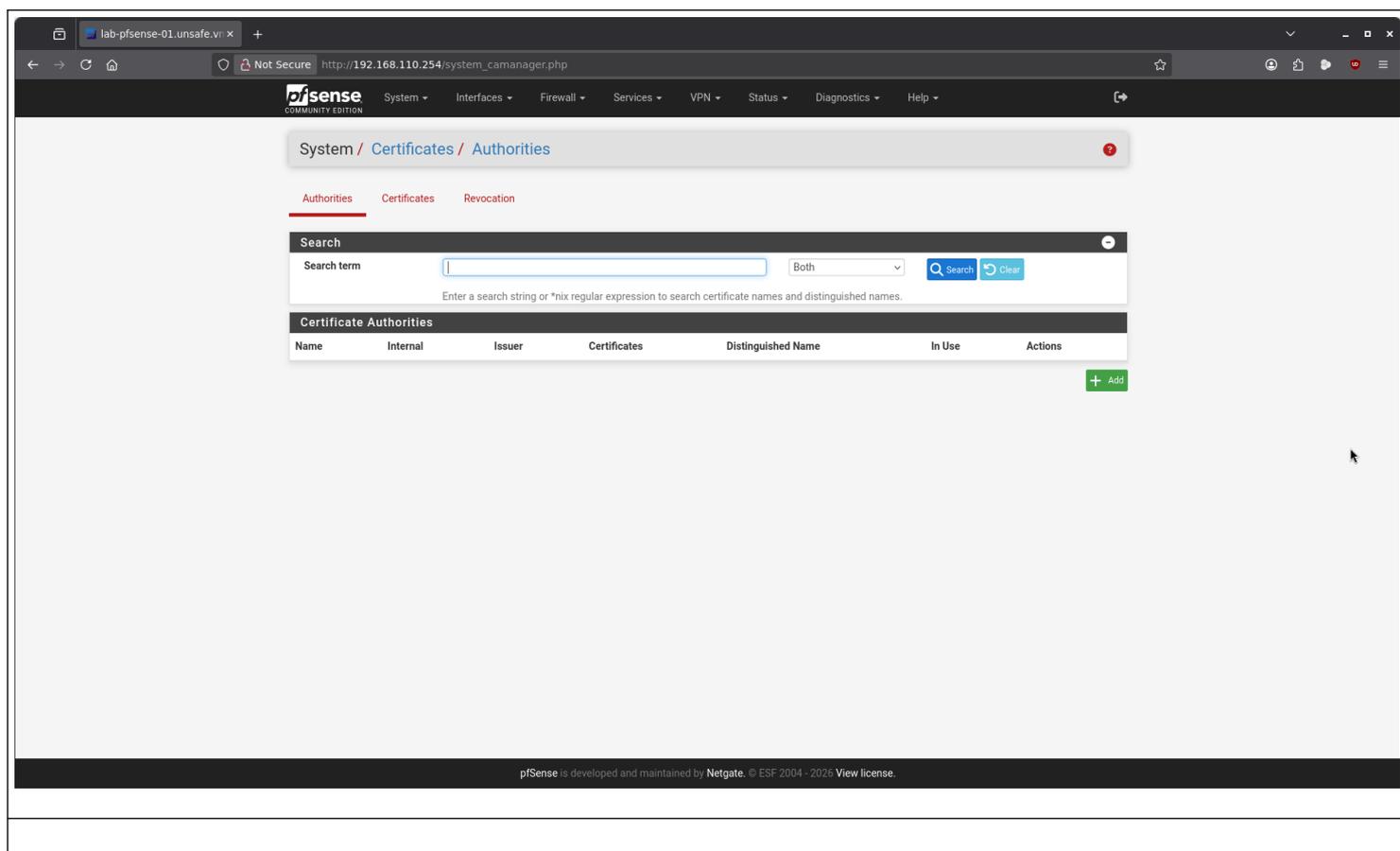
Avant de tunneliser quoi que ce soit, nous devons établir une chaîne de confiance.

## L'Autorité de Certification (CA)

C'est le Dieu de votre VPN. Il signe tout.

**Menu :** System > Cert. Manager > **Authorities.**

**Action :** + Add.



The screenshot shows the pfSense web interface for creating a new Certificate Authority (CA). The breadcrumb trail is 'System / Certificates / Authorities / Edit'. The form is titled 'Create / Edit CA' and has several sections:

- Descriptive name:** CA-OpenVPN-UnSafe. A note below states: '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: ?, >, <, &, /, \, '.'
- Method:** Create an internal Certificate Authority.
- Trust Store:** A checkbox 'Add this Certificate Authority to the Operating System Trust Store' is unchecked. A note says: 'When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.'
- Randomize Serial:** A checkbox 'Use random serial numbers when signing certificates' is unchecked. A note says: '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
  - Key Length:** 4096. A note says: '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. A note says: 'The digest method used when the CA is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.'
  - Lifetime (days):** 3650
  - Common Name:** internal-ca-unsafe
  - A note below states: 'The following certificate authority subject components are optional and may be left blank.'
  - Country Code:** None
  - State or Province:** Occitanie
  - City:** Auzat
  - Organization:** CA-OpenVPN-UnSafe
  - Organizational Unit:** Root Security

A 'Save' button is located at the bottom of the form.

pfSense is developed and maintained by Netgate. © ESF 2004 - 2020. [View license.](#)

<b>Descriptive Name</b>	CA-OpenVPN-UnSafe	
<b>Method</b>	Create an internal CA	
<b>Key Type</b>	RSA / 4096	<b>Niveau de paranoïa : Élevé.</b> 2048 suffisait amplement, mais avec 4096, même un ordinateur quantique prendra une RTT avant de casser ça. C'est lourd, c'est lent, c'est solide. C'est validé.
<b>Digest Algo</b>	SHA256	
<b>Lifetime</b>	3650 (Jours)	10 ans. L'optimisme pur de croire que ce serveur (ou nous) existera encore dans une décennie.
<b>Common Name</b>	internal-ca-unsafe	
<b>Location</b>	Occitanie / Auzat	La Silicon Valley de l'Ariège.
<b>Organizational Unit</b>	Root Security	

**Note :** Une fois sauvegardée, cette CA devient la racine de confiance. Si vous perdez la clé privée de cette CA (stockée dans pfSense), tous les futurs certificats clients/serveurs deviennent inutiles. Ne supprimez jamais cette entrée.

The screenshot shows the pfSense web interface for managing Certificate Authorities. The browser address bar shows the URL `http://192.168.110.254/system_camanager.php`. The page title is "System / Certificates / Authorities". There are three tabs: "Authorities" (selected), "Certificates", and "Revocation". A search bar is present with a "Search term" input field, a "Both" dropdown, and "Search" and "Clear" buttons. Below the search bar, a table titled "Certificate Authorities" displays the following data:

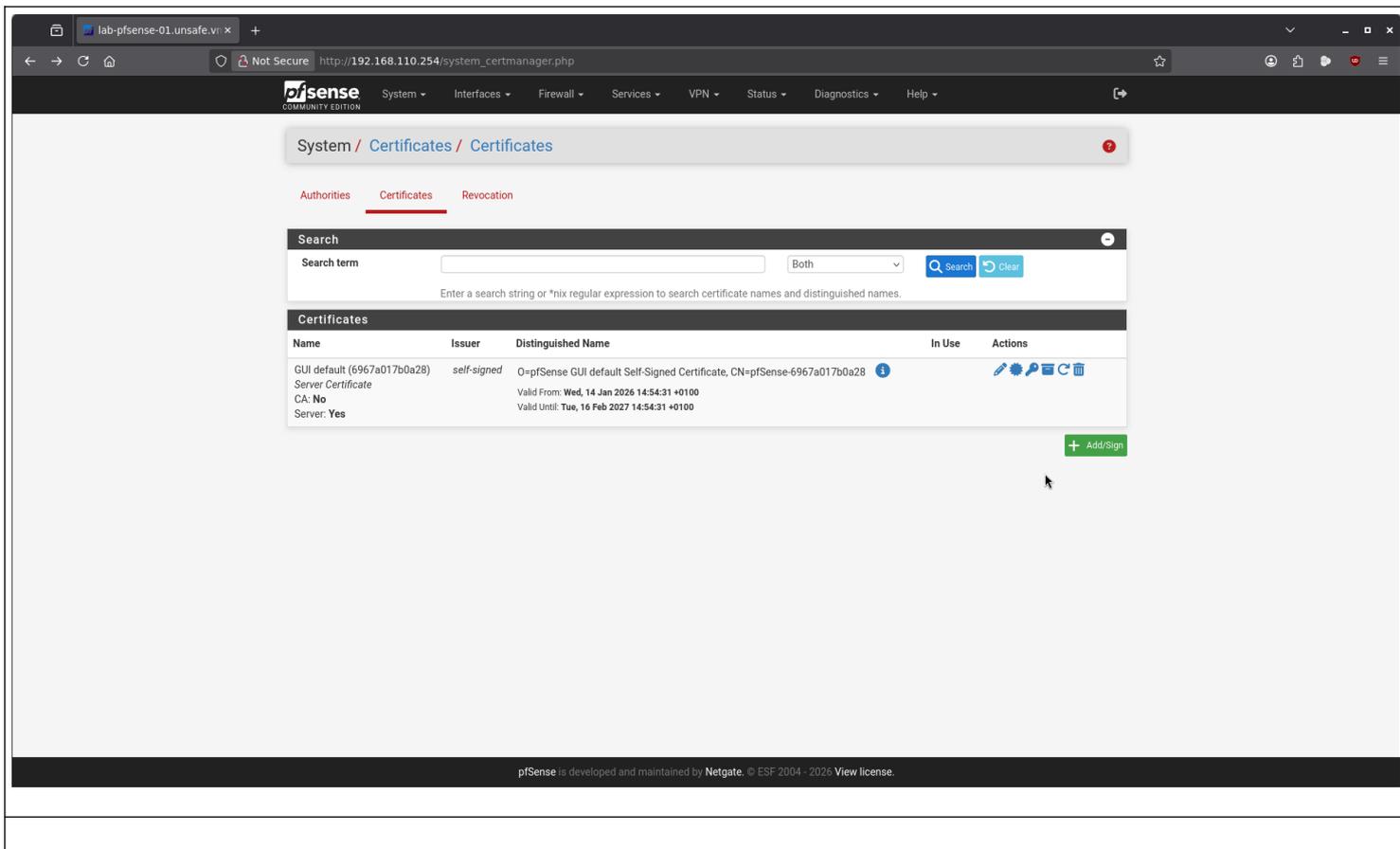
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA-OpenVPN-Unsafe	✓	self-signed	0	ST=Occitanie, OU=Root Security, O=CA-OpenVPN-Unsafe, L=Auzat, CN=internal-ca <small>Valid From: Fri, 23 Jan 2026 17:54:07 +0100 Valid Until: Mon, 21 Jan 2036 17:54:07 +0100</small>		

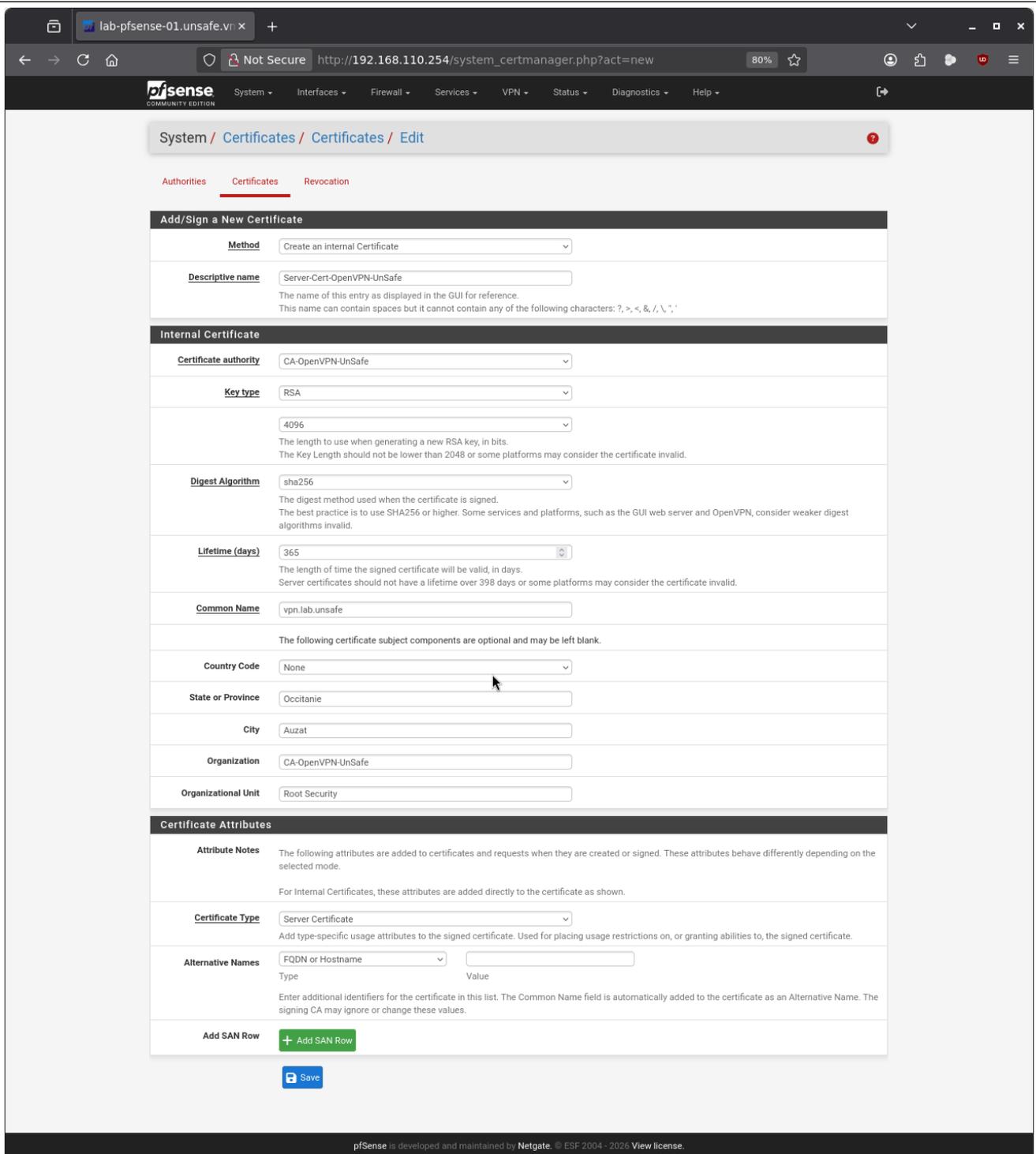
A green "+ Add" button is located at the bottom right of the table. At the bottom of the page, a footer states: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2026 View license."

# CRÉATION DU CERTIFICAT SERVEUR (L'Oracle)

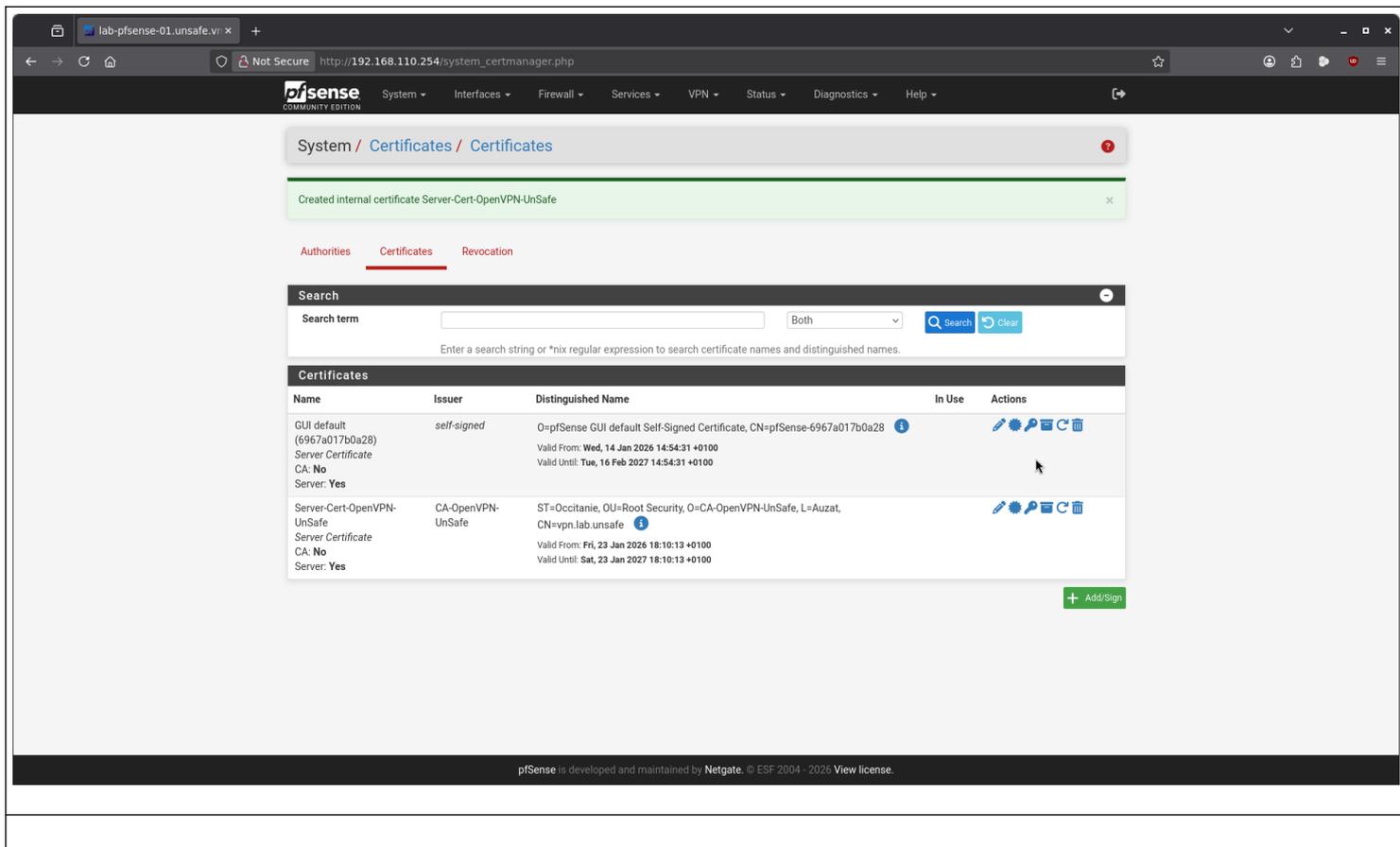
Menu : System > Cert. Manager > Certificates.

Action : + Add.





<b>Method</b>	Create an internal Certificate	
<b>Descriptive Name</b>	Server-Cert-OpenVPN-UnSafe	
<b>Certificate Authority</b>	CA-OpenVPN-UnSafe	<b>CRITIQUE.</b> On sélectionne notre CA créée juste avant. C'est elle qui valide.
<b>Key Type</b>	RSA / 4096	On reste cohérent avec la CA. Si le patron est parano (4096), l'employé doit l'être aussi.
<b>Digest Algorithm</b>	SHA256	
<b>Common Name (CN)</b>	vpn.lab.unsafe	C'est le nom de domaine complet (FQDN) du serveur. En lab, on invente. En prod, ça doit correspondre au DNS public.
<b>Certificate Type</b>	Server Certificate	<b>ALERT ROUGE.</b> Si vous laissez "User", le serveur aura une crise d'identité et le service ne démarrera pas.
<b>Alternative Names</b>	(Laisser vide)	Pas nécessaire pour ce lab, sauf si vous voulez accéder au VPN par plusieurs noms (IP et DNS).



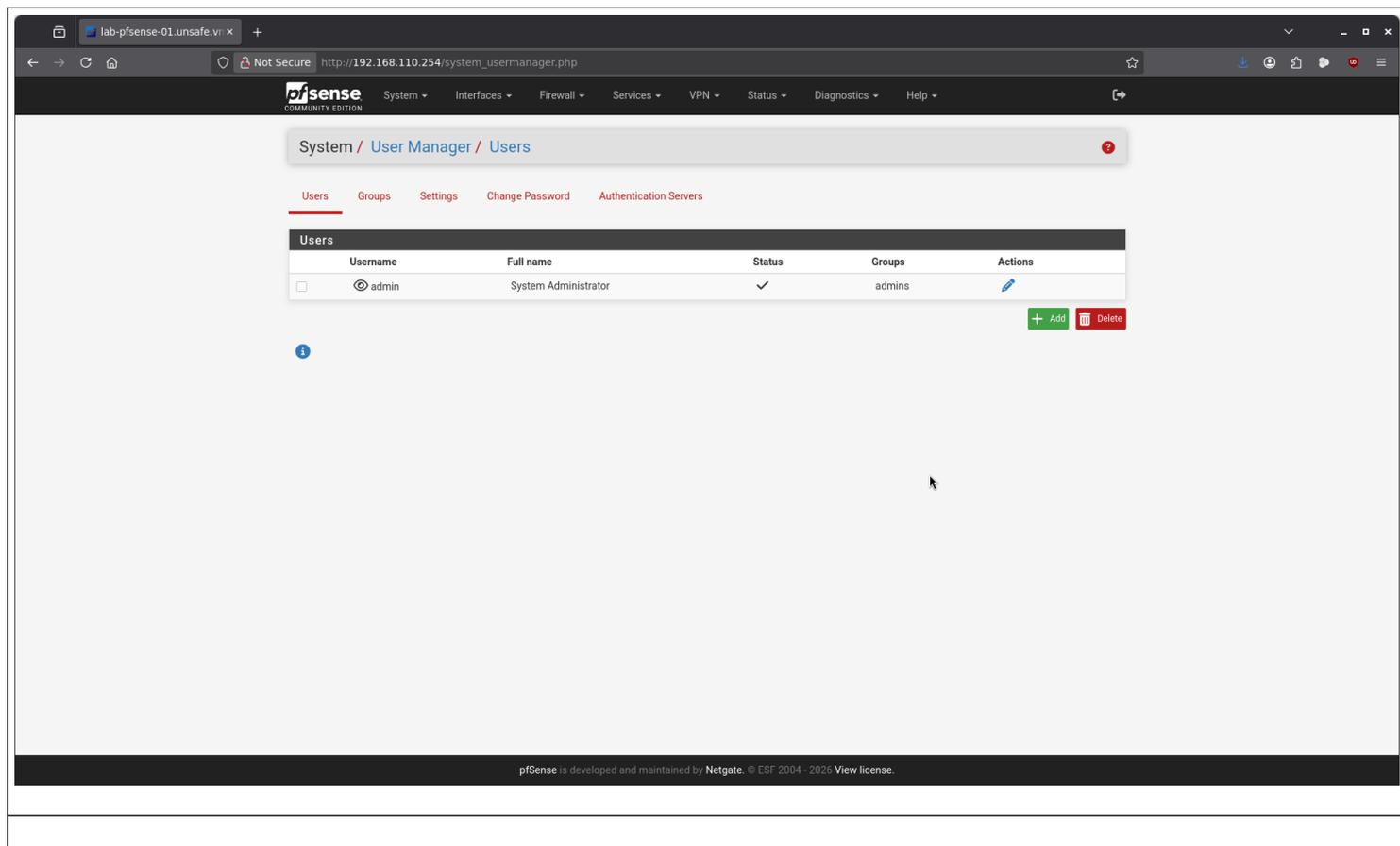
The screenshot shows the pfSense web interface for managing certificates. At the top, there is a navigation menu with options like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The current page is titled 'System / Certificates / Certificates'. A green notification bar at the top indicates 'Created internal certificate Server-Cert-OpenVPN-UnSafe'. Below this, there are tabs for 'Authorities', 'Certificates', and 'Revocation', with 'Certificates' being the active tab. A search bar is present with a search term field, a dropdown menu set to 'Both', and 'Search' and 'Clear' buttons. Below the search bar, a table lists the certificates. The table has columns for Name, Issuer, Distinguished Name, In Use, and Actions. Two certificates are listed: 'GUI default (6967a017b0a28) Server Certificate' and 'Server-Cert-OpenVPN-UnSafe Server Certificate'. Each row has an 'In Use' column with a status icon and an 'Actions' column with icons for edit, refresh, and delete. A green '+ Add/Sign' button is located at the bottom right of the table area. At the very bottom of the page, a footer states 'pfSense is developed and maintained by Netgate. © ESF 2004 - 2026. View license.'

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (6967a017b0a28) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-6967a017b0a28 Valid From: Wed, 14 Jan 2026 14:54:31 +0100 Valid Until: Tue, 16 Feb 2027 14:54:31 +0100		
Server-Cert-OpenVPN-UnSafe Server Certificate CA: No Server: Yes	CA-OpenVPN-UnSafe	ST=Occitanie, OU=Root Security, O=CA-OpenVPN-UnSafe, L=Auzat, CN=vpn.lab.unsafe Valid From: Fri, 23 Jan 2026 18:10:13 +0100 Valid Until: Sat, 23 Jan 2027 18:10:13 +0100		

# GESTION UTILISATEUR (L'Accès Client)

Menu : System > User Manager > Users.

Action : + Add.



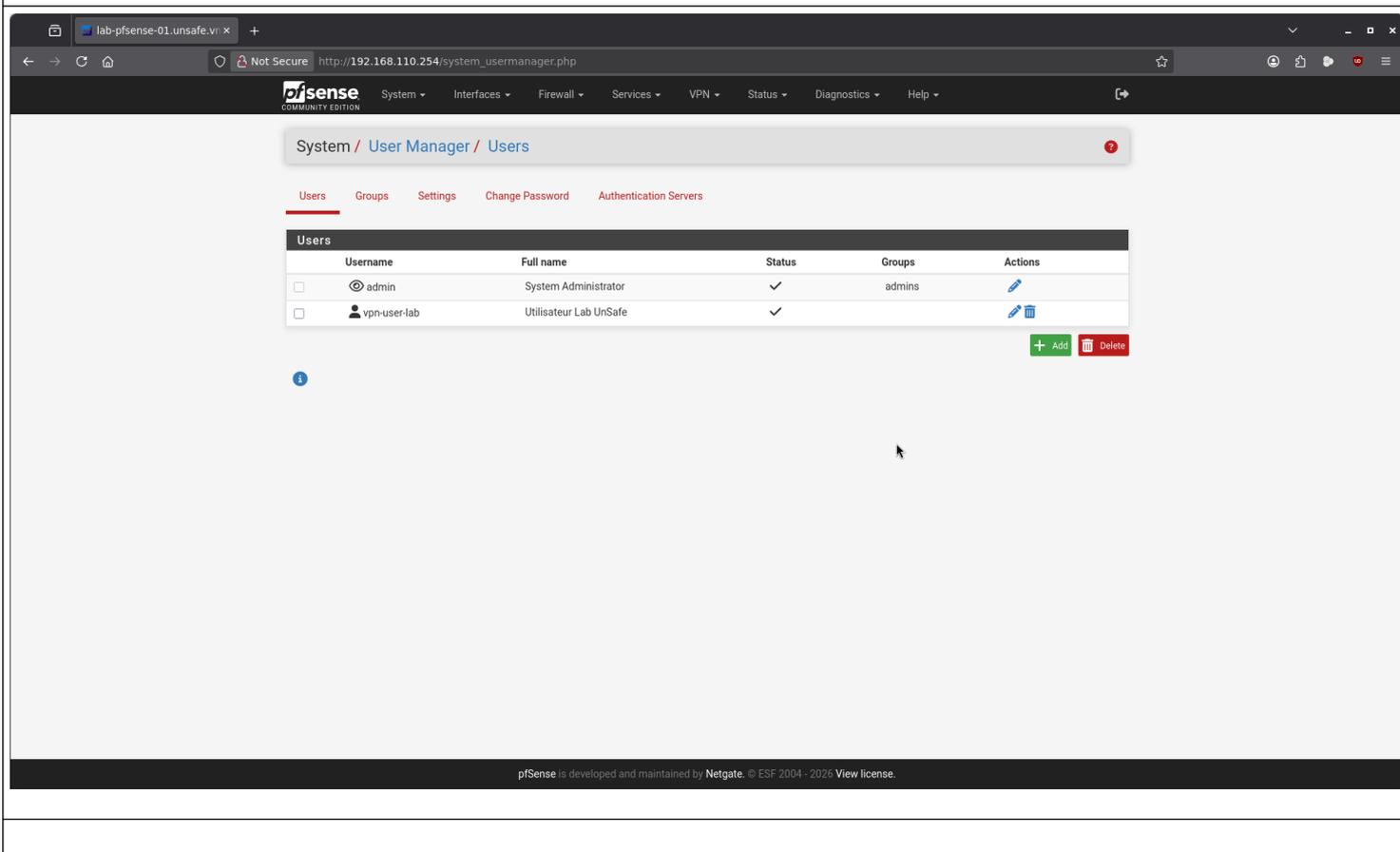
The screenshot displays the pfSense web interface for editing a user in the User Manager system. The browser address bar shows the URL `http://192.168.110.254/system_usermanager`. The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The breadcrumb trail is System / User Manager / Users / Edit.

The main content area is divided into several sections:

- User Properties:** Includes fields for Username (vpn-user-lab), Password (with a confirmation field), Full name (Utilisateur Lab UnSafe), Expiration date, Custom Settings, Group membership (admins), and Certificate (checked).
- Create Certificate for User:** Includes fields for Descriptive name (Cert-OpenVPN-User-Lab-UnSafe), Certificate authority (CA-OpenVPN-UnSafe), Key type (RSA), Key length (2048), Digest Algorithm (sha256), and Lifetime (3650).
- Keys:** Includes a field for Authorized SSH Keys and a field for IPsec Pre-Shared Key.
- Shell Behavior:** Includes a checkbox for Keep Command History.

A blue Save button is located at the bottom of the form.

<b>Username</b>	vpn-user-lab	
<b>Password</b>		Pas de "123456". Si vous mettez ça, Skynet gagnera.
<b>Full Name</b>	Utilisateur Lab UnSafe	
<b>Certificate</b>	[COCHER LA CASE]	<b>CRITIQUE.</b> Cochez "Click to create a user certificate". C'est le bouton magique qui évite de faire 15 clics ailleurs.
<b>Descriptive Name</b>	Cert-OpenVPN-User-Lab-UnSafe	Le nom du fichier de clé.
<b>Certificate Authority</b>	CA-OpenVPN-UnSafe	Toujours le Patron. C'est lui qui signe le laissez-passer.
<b>Key Length</b>	2048	Ici, 2048 suffit pour un client. Mais si vous êtes en mode "Forteresse", mettez 4096 pour être raccord avec le serveur.

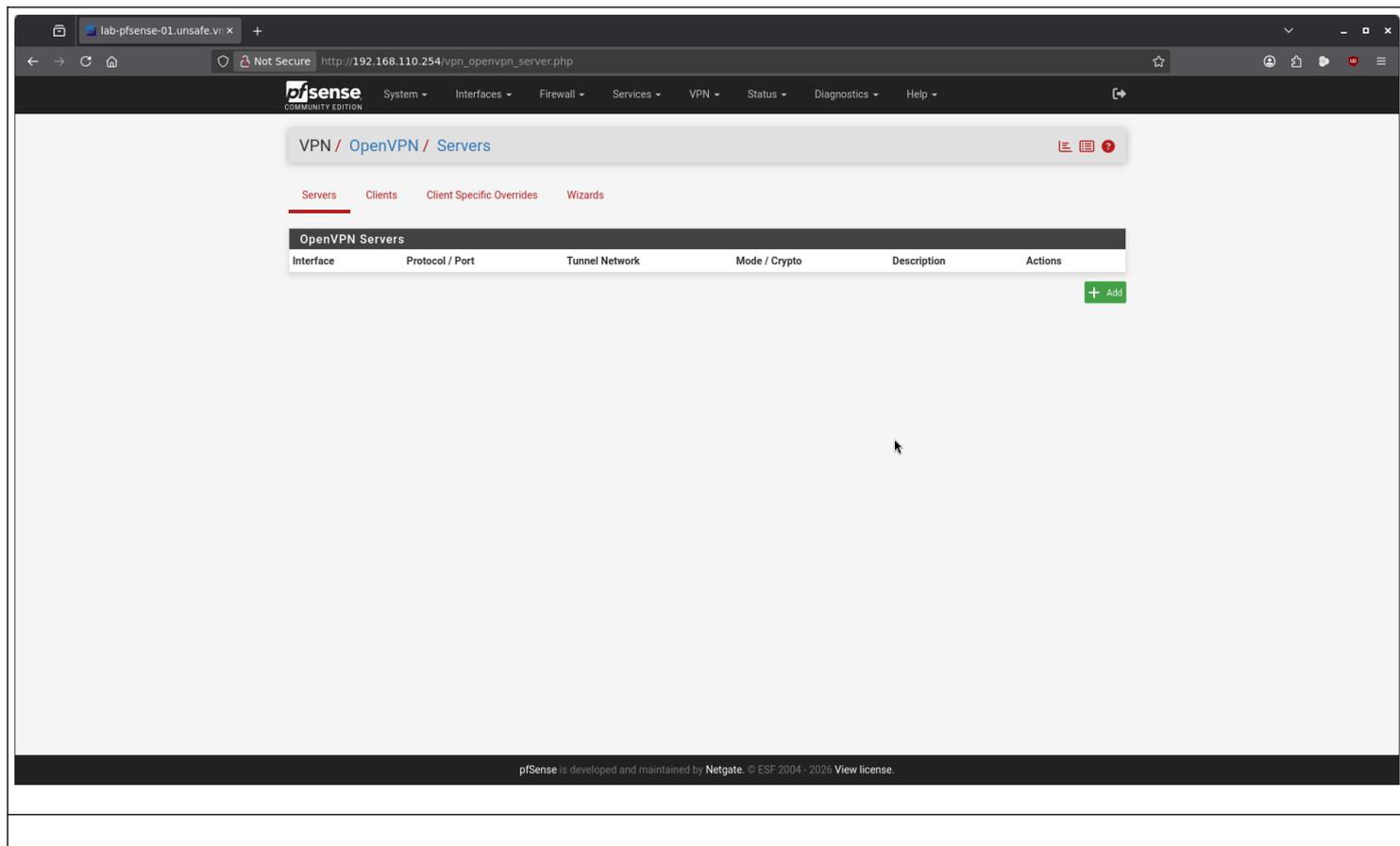


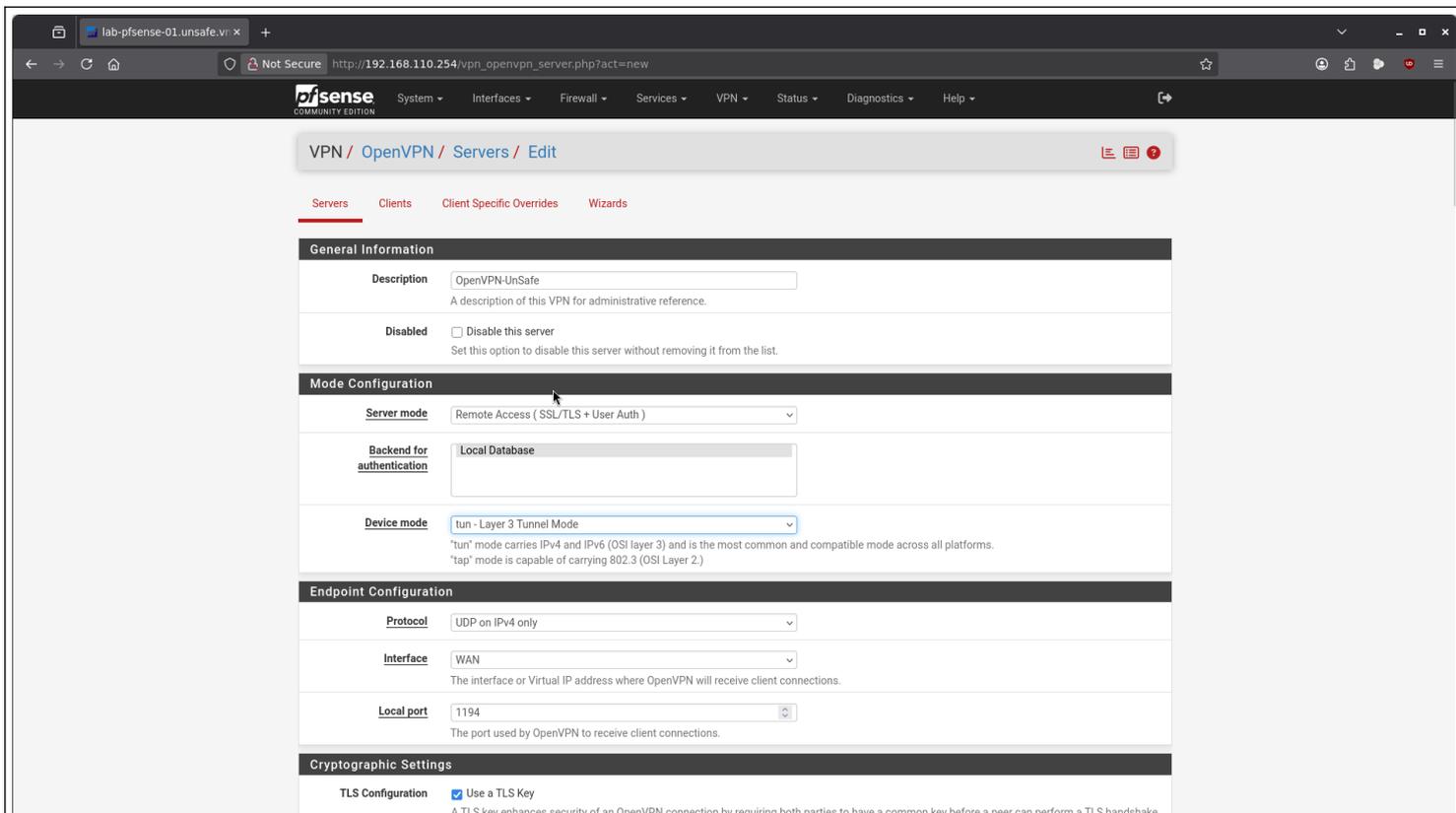
## CONFIGURATION DU SERVEUR OPENVPN (Le Tunnel)

Menu : VPN > OpenVPN > Servers.

Action : + Add.

C'est le cœur du réacteur. Suivez ces instructions à la lettre. Une erreur ici et votre VPN sera aussi utile qu'un pare-feu en papier mâché.





<b>Description</b>	OpenVPN-UnSafe	
<b>Server Mode</b>	Remote Access (SSL/TLS + User Auth)	Ceinture et bretelles. On veut le certificat de la machine <b>ET</b> le mot de passe de l'humain. Sécurité maximale.
<b>Backend for Authentication</b>	Local Database	On utilise la base locale (là où vit notre ami vpn-user-lab).
<b>Device Mode</b>	tun - Layer 3 Tunnel Mode	
<b>Protocol</b>	UDP on IPv4 only	<b>UDP</b> est vital pour la vitesse. TCP sur TCP, c'est l'enfer de la latence (le fameux "TCP Meltdown").
<b>Interface</b>	WAN	C'est la porte d'entrée publique.
<b>Local Port</b>	1194	Le classique.

The screenshot shows the OpenVPN configuration page for a server. The 'Local port' is set to 1194. Under 'Cryptographic Settings', 'Use a TLS Key' and 'Automatically generate a TLS Key' are checked. 'Peer Certificate Authority' is set to 'CA-OpenVPN-UnSafe'. 'Server certificate' is set to 'Server-Cert-OpenVPN-UnSafe'. 'DH Parameter Length' is 2048 bit. 'ECDH Curve' is 'Use Default'. Under 'Data Encryption Algorithms', several algorithms are listed, with 'AES-256-GCM' and 'AES-128-GCM' selected in the 'Allowed' list. 'Fallback Data Encryption Algorithm' is 'AES-256-CBC'. 'Auth digest algorithm' is 'SHA256'. 'Certificate Depth' is 'One (Client+Server)'. 'Strict User-CN Matching' is unchecked. 'Client Certificate Key Usage Validation' is checked. The 'Tunnel Settings' section shows 'IPv4 Tunnel Network' is empty.

<b>Peer Certificate Authority</b>	CA-OpenVPN-UnSafe	On dit au serveur : "Fais confiance uniquement aux gens qui ont un badge signé par le Patron".
<b>Server Certificate</b>	Server-Cert-OpenVPN-UnSafe	<b>ATTENTION</b> : ne selectionner pas le certificats de l'utilisateur !
<b>DH Parameter Length</b>	2048	
<b>Auth Digest Algorithm</b>	SHA256	

The screenshot shows the configuration page for an OpenVPN server. The browser address bar shows the URL: `http://192.168.110.254/vpn_openvpn_server.php?act=new`. The page is divided into several sections:

- Client Certificate Key Usage Validation:** A checkbox labeled 'Enforce key usage' is checked. Below it, a note states: 'Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").'
- Tunnel Settings:**
  - IP4 Tunnel Network:** Input field contains '10.0.8.0/24'. A descriptive note explains this is the virtual network for private communications.
  - IPv6 Tunnel Network:** An empty input field.
  - Redirect IPv4 Gateway:** A checkbox 'Force all client-generated IPv4 traffic through the tunnel.' is unchecked.
  - Redirect IPv6 Gateway:** A checkbox 'Force all client-generated IPv6 traffic through the tunnel.' is unchecked.
  - IPv4 Local network(s):** Input field contains '192.168.110.0/24'. A note explains this is the LAN network accessible from the remote endpoint.
  - IPv6 Local network(s):** An empty input field.
  - Concurrent connections:** A dropdown menu is set to '5'. A note specifies the maximum number of clients.
  - Allow Compression:** A dropdown menu is set to 'Refuse any non-stub compression (Most secure)'. A note explains the security implications of compression.
  - Push Compression:** A checkbox 'Push the selected Compression setting to connecting clients.' is unchecked.
  - Type-of-Service:** A checkbox 'Set the TOS IP header value of tunnel packets to match the encapsulated packet value.' is unchecked.
  - Inter-client communication:** A checkbox 'Allow communication between clients connected to this server' is unchecked.
  - Duplicate Connection:** A checkbox 'Allow multiple concurrent connections from the same user' is unchecked. A note explains that this is discouraged for security reasons.
- Client Settings:**
  - Dynamic IP:** A checkbox 'Allow connected clients to retain their connections if their IP address changes.' is unchecked.
  - Topology:** A dropdown menu is set to 'Subnet - One IP address per client in a common subnet'. A note explains this method for supplying virtual adapter IP addresses.

<b>IP4 Tunnel Network</b>	10.0.8.0/24	C'est le réseau virtuel à l'intérieur du VPN. Il <b>DOIT</b> être différent de votre LAN. Si vous mettez 192.168.110.0/24 ici, tout va planter (conflit de routage).
<b>IP4 Local Network(s)</b>	192.168.110.0/24	C'est le réseau LAN auquel vous voulez accéder. C'est la "récompense" une fois connecté.
<b>Concurrent Connections</b>	5	
<b>Allow Compression</b>	Refuse any non-stub compression (Most secure)	

Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.

### 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".

### Ping settings

**Inactivity Timeout**    
Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device. Activity is based on the last incoming or outgoing tunnel packet. A value of 0 disables this feature. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.

**Ping method**    
keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows:  
ping = interval  
ping-restart = timeout\*2  
push ping = interval  
push ping-restart = timeout

**Interval**    
**Timeout**

### Advanced Client Settings

**DNS Default Domain**  Provide a default domain name to clients

**DNS Server enable**  Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.

**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

**NetBIOS enable**  Enable NetBIOS over TCP/IP   
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

### 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"

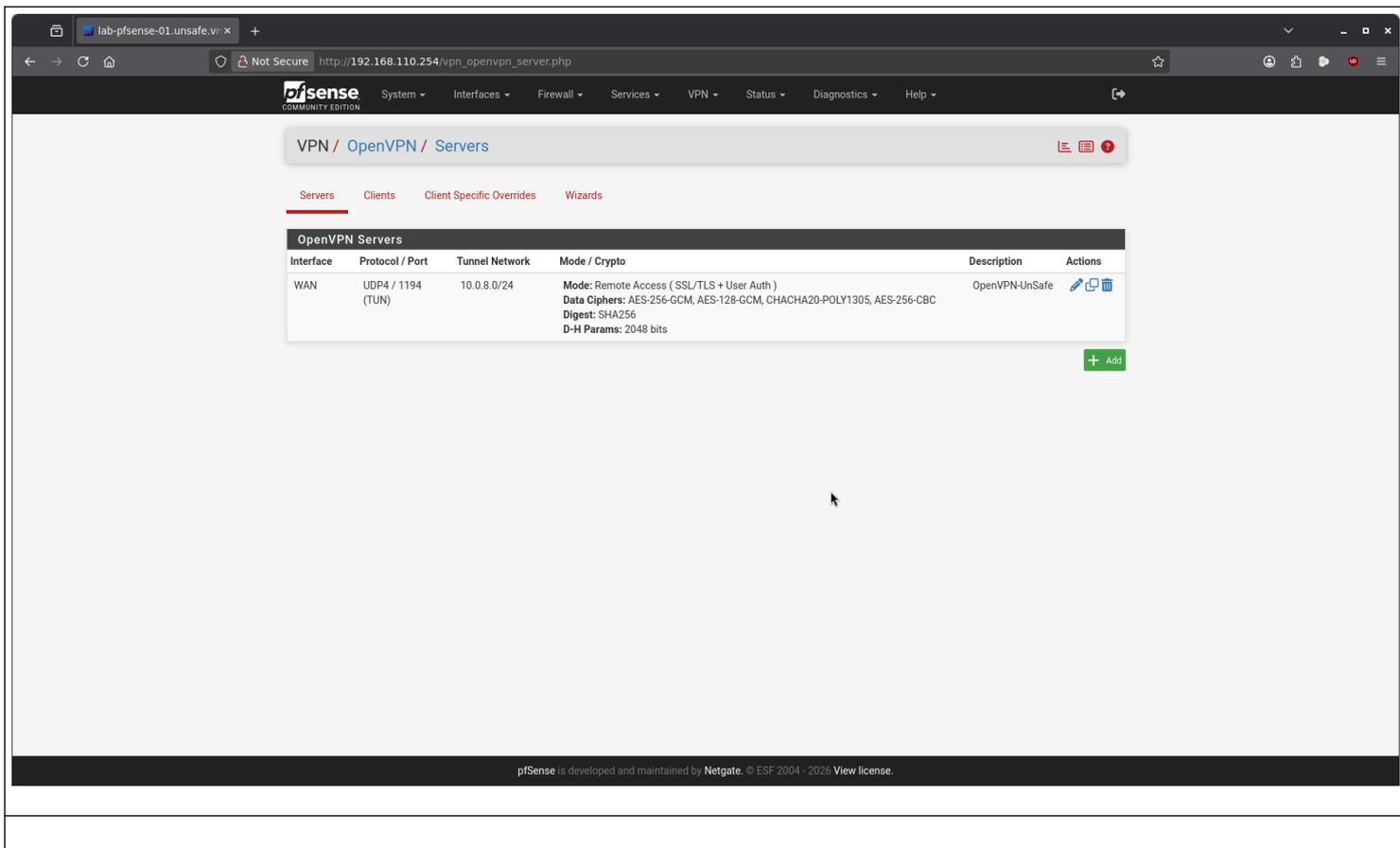
**Username as Common Name**  Use the authenticated client username instead of the certificate common name (CN).   
When a user authenticates, if this option is enabled then the username of the client will be used in place of the certificate common name for purposes

The screenshot shows the 'Advanced Configuration' section of the OpenVPN server configuration in pfSense. The configuration options are as follows:

- DNS Server enable:**  Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
- 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.
- NetBIOS enable:**  Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
- Advanced Configuration:**
  - Custom options:** A text area for additional options, separated by semicolon. Example: "push 'route 10.0.0.0 255.255.255.0'".
  - Username as Common Name:**  Use the authenticated client username instead of the certificate common name (CN). When a user authenticates, if this option is enabled then the username of the client will be used in place of the certificate common name for purposes such as determining Client Specific Overrides.
  - UDP Fast I/O:**  Use fast I/O operations with UDP writes to tun/tap. Experimental. Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.
  - Exit Notify:** A dropdown menu set to "Reconnect to this server / Retry once". Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.
  - Send/Receive Buffer:** A dropdown menu set to "Default". Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KIB and test higher and lower values.
  - Gateway creation:** Radio buttons for "Both" (selected), "IPv4 only", and "IPv6 only". If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.
  - Verbosity level:** A dropdown menu set to "default". Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.
    - None: Only fatal errors
    - Default through 4: Normal usage range
    - 5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
    - 6-11: Debug info range

A blue "Save" button is located at the bottom of the configuration area.

Pour le reste gardez exactement ce que vous avez à l'écran.  
Descendez tout en bas.  
Cliquez sur **Save**.



The screenshot shows the pfSense web interface for configuring OpenVPN servers. The browser address bar shows the URL `http://192.168.110.254/vpn_openvpn_server.php`. The page title is "VPN / OpenVPN / Servers". There are navigation tabs for "Servers", "Clients", "Client Specific Overrides", and "Wizards". The "Servers" tab is active, displaying a table of OpenVPN servers. The table has columns for "Interface", "Protocol / Port", "Tunnel Network", "Mode / Crypto", "Description", and "Actions". One server is listed with the following details:

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.0.8.0/24	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	OpenVPN-UnSafe	 

Below the table is a green "+ Add" button. At the bottom of the page, a footer states: "pfSense is developed and maintained by Netgate. © ESF 2004 - 2026 View license."

# LA SÉCURITÉ (Firewall Rules)

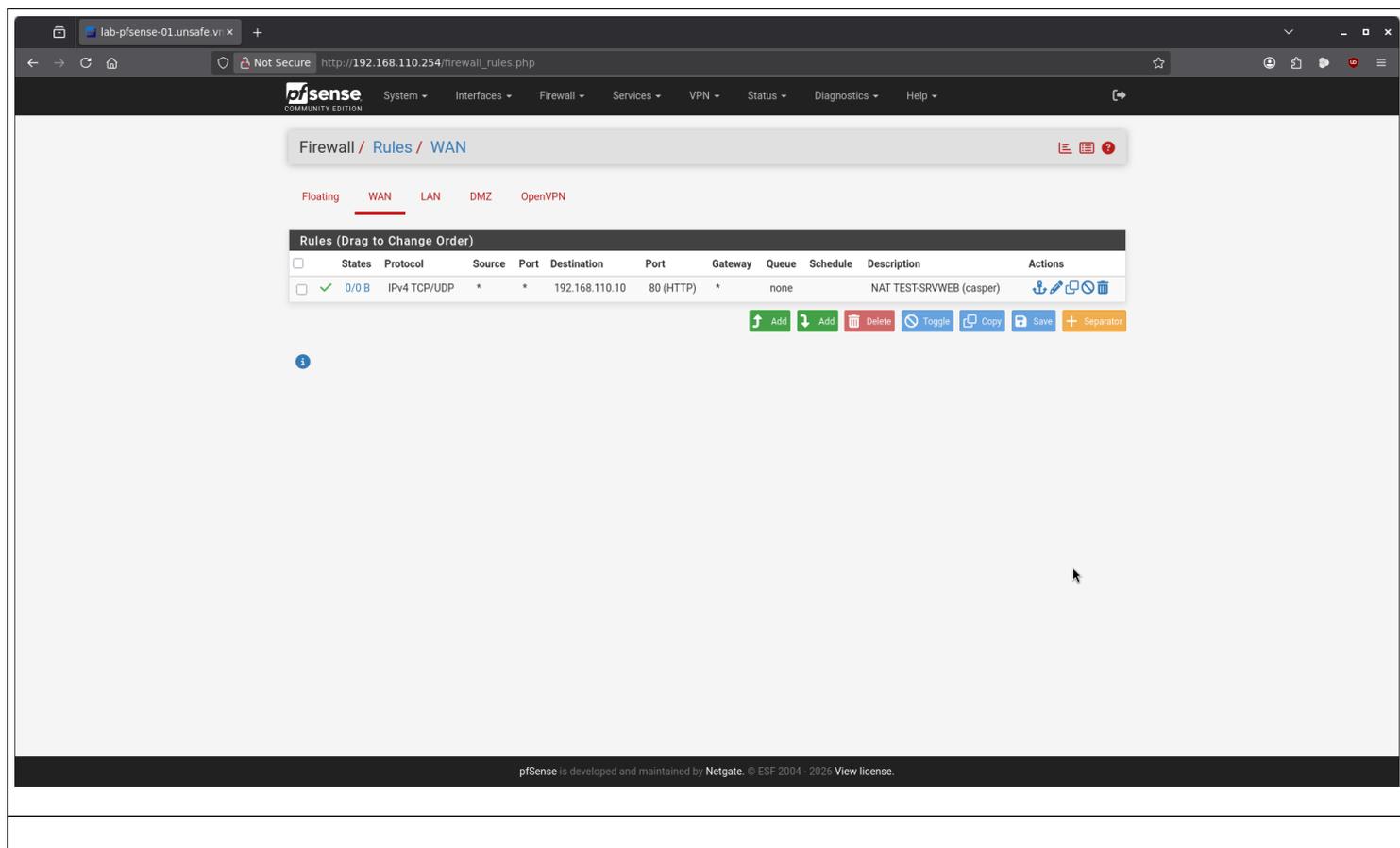
L'ouverture des vannes.

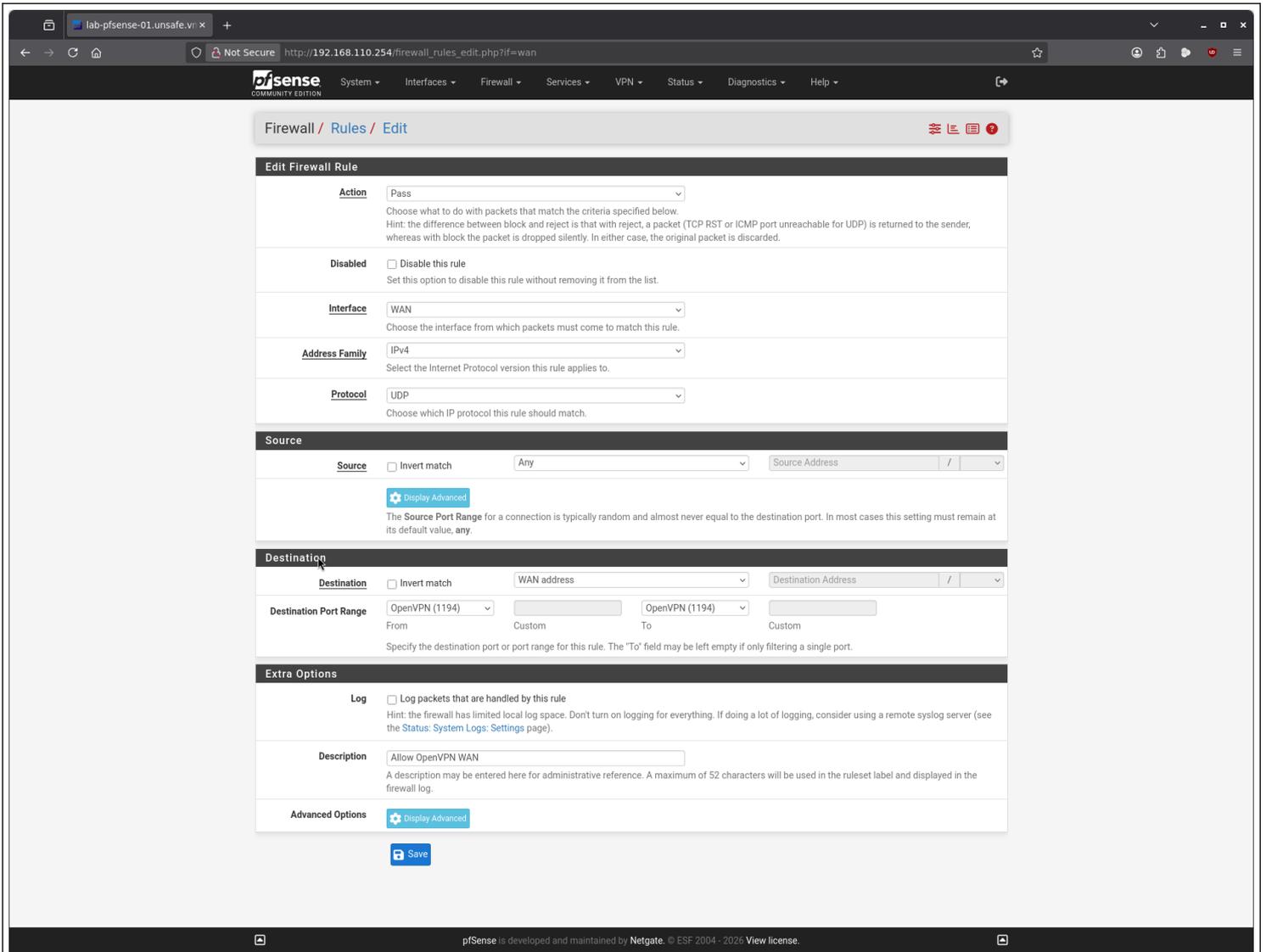
## La Porte d'Entrée (WAN)

Il faut autoriser les paquets chiffrés à toucher le service OpenVPN.

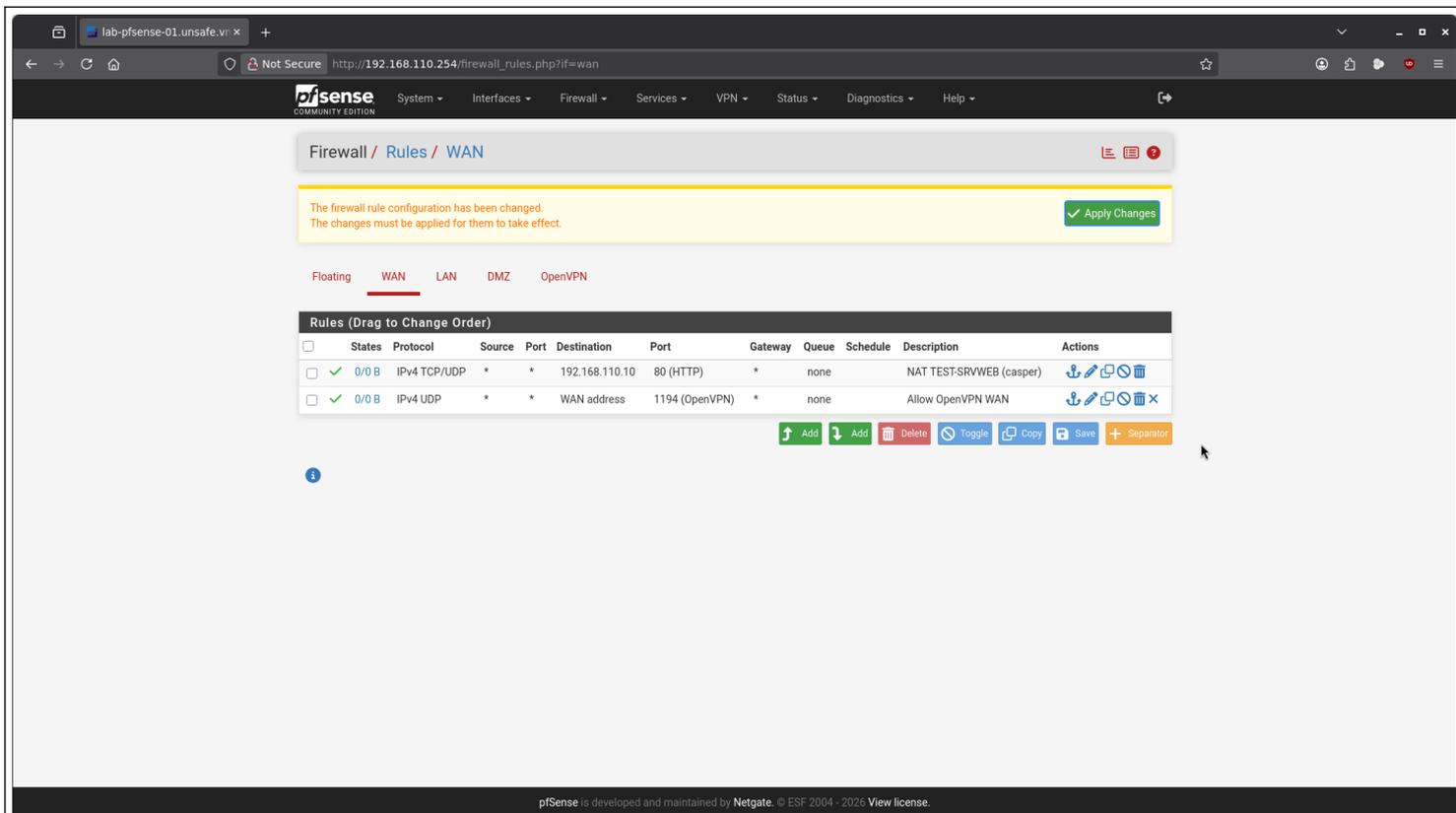
Menu : Firewall > Rules > WAN.

Action : + Add (Flèche vers le bas pour mettre à la fin, ou haut, peu importe en Lab).

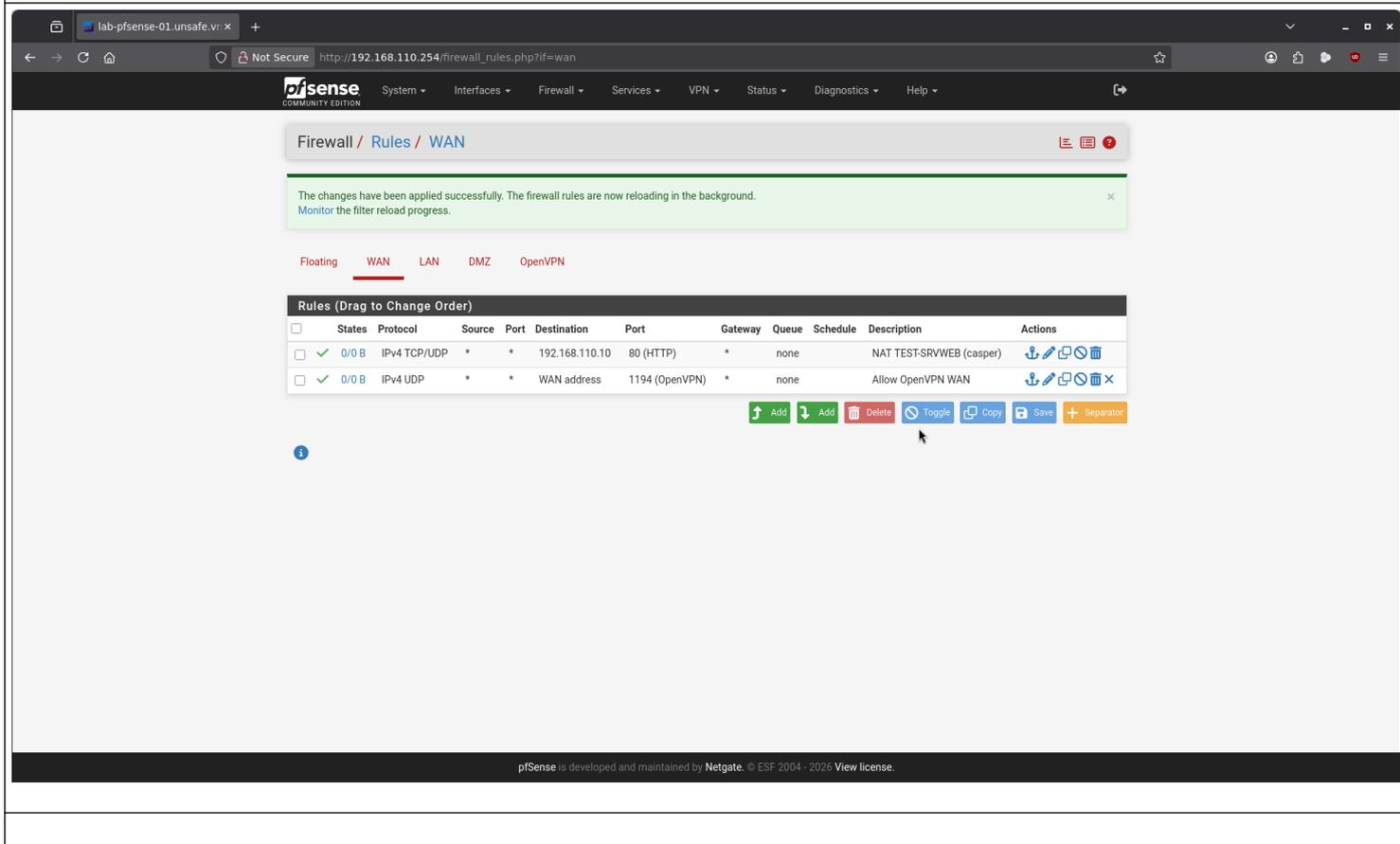




<b>Action</b>	Pass	On laisse entrer.
<b>Interface</b>	WAN	Logique.
<b>Address Family</b>	IPv4	On reste simple.
<b>Protocol</b>	UDP	<b>Vital.</b> Si vous mettez TCP ici alors que le serveur est en UDP, ça ne marchera jamais.
<b>Source</b>	Any	N'importe qui sur internet (ou votre réseau amont) peut tenter sa chance.
<b>Destination</b>	WAN address	
<b>Destination Port Range</b>	1194 (From) / 1194 (To)	Tapez "1194" ou cherchez "OpenVPN" dans la liste.
<b>Log</b>		
<b>Description</b>	Allow OpenVPN WAN	Pour se souvenir pourquoi on a ouvert ce port.



On n'oublie pas d'appliquer les changements !

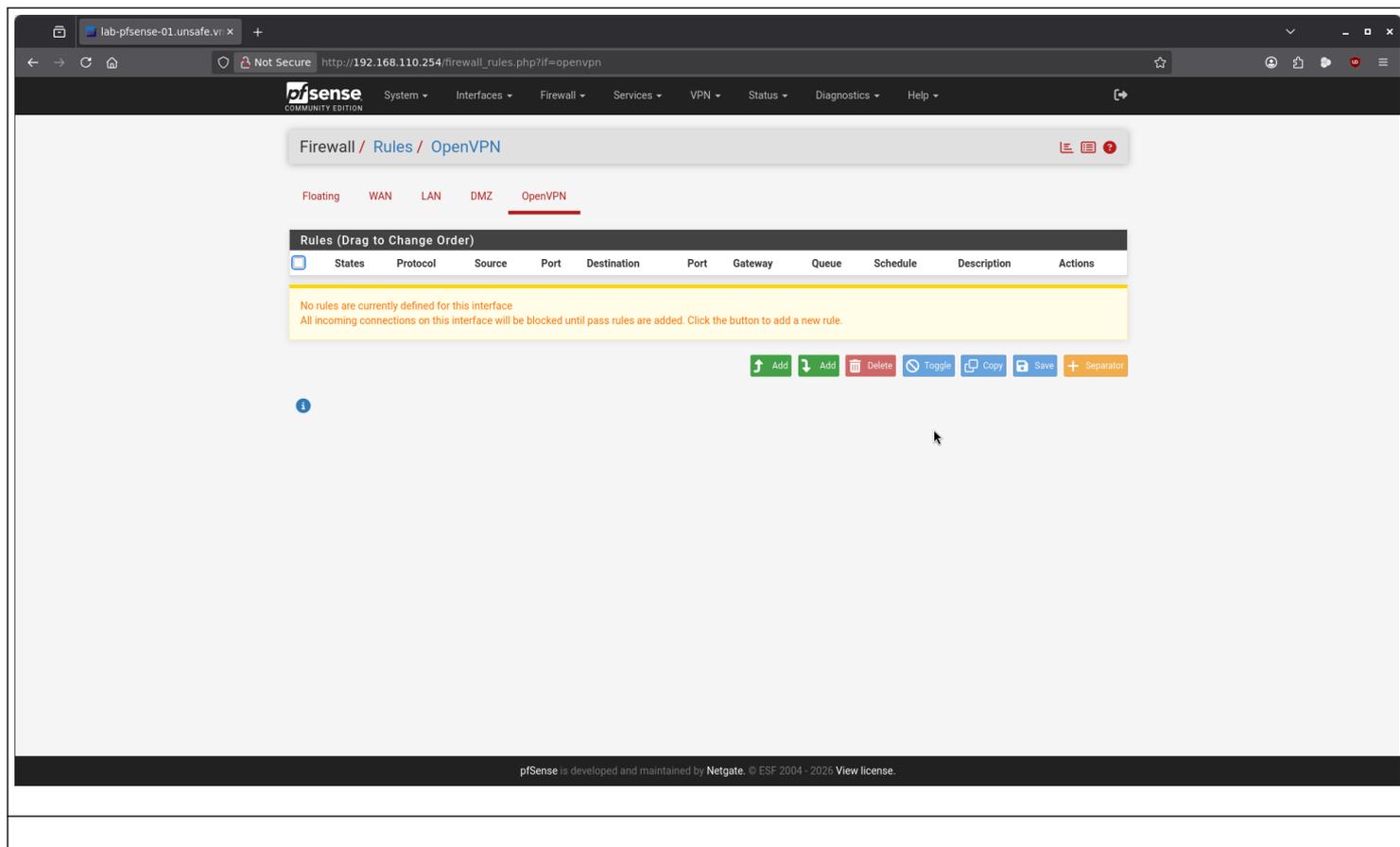


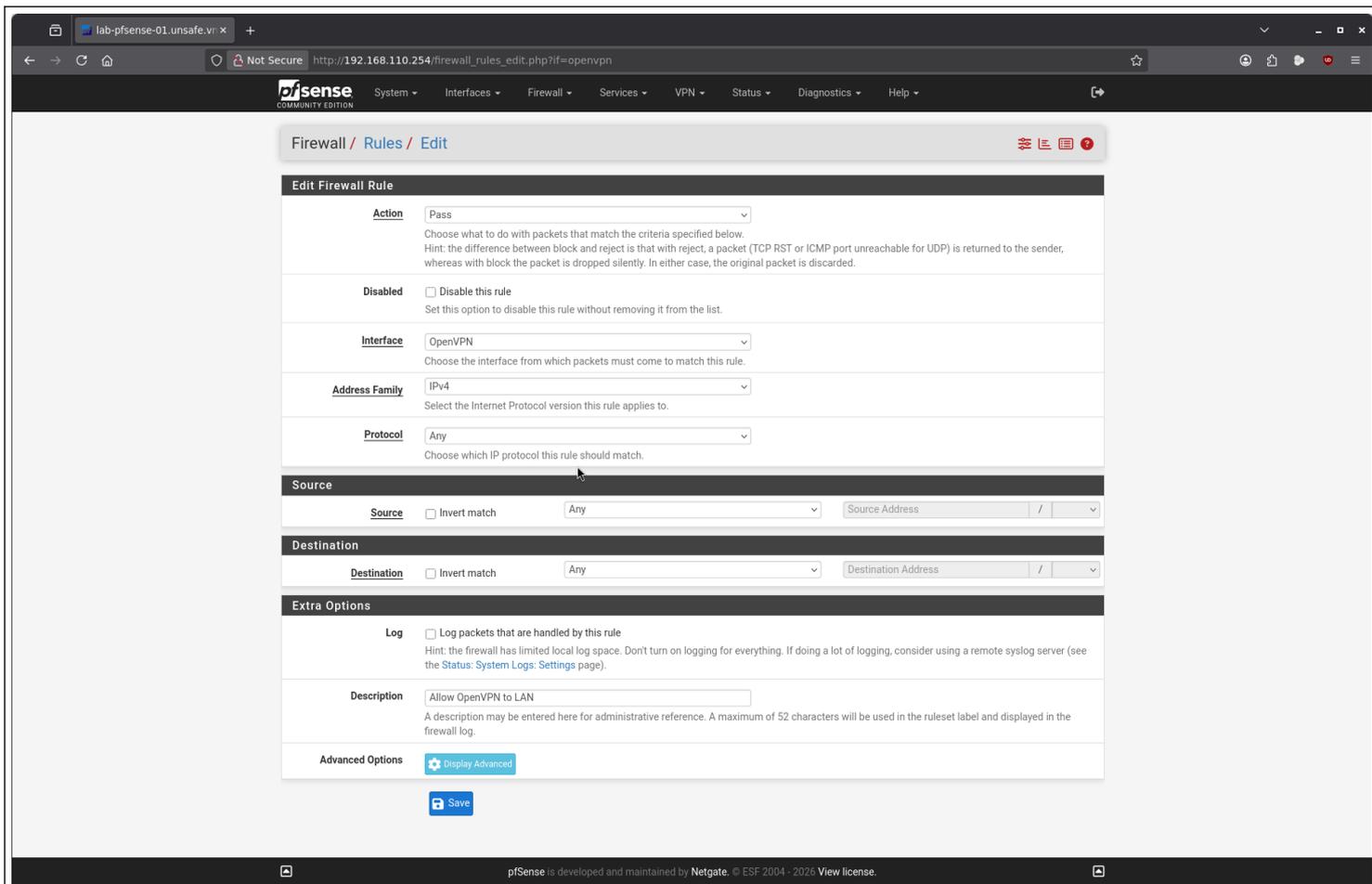
## La Liberté de Mouvement (Interface OpenVPN)

Une fois le client connecté et authentifié, il est "dans" le tunnel. Mais pfSense bloque tout par défaut à l'intérieur aussi. Il faut lui donner le droit de parler au LAN.

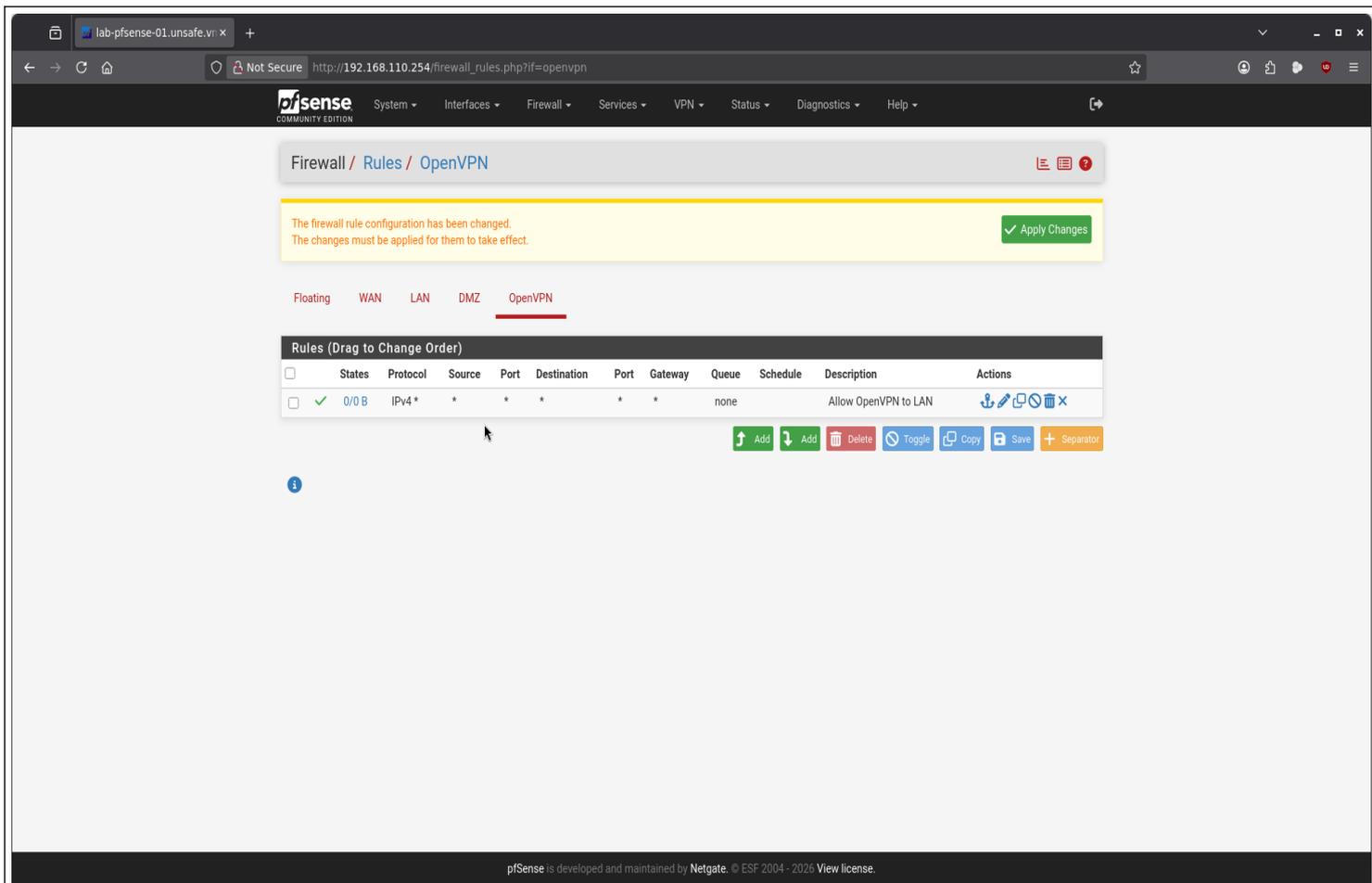
**Menu :** Firewall > Rules > **OpenVPN**.

**Action :** + Add.

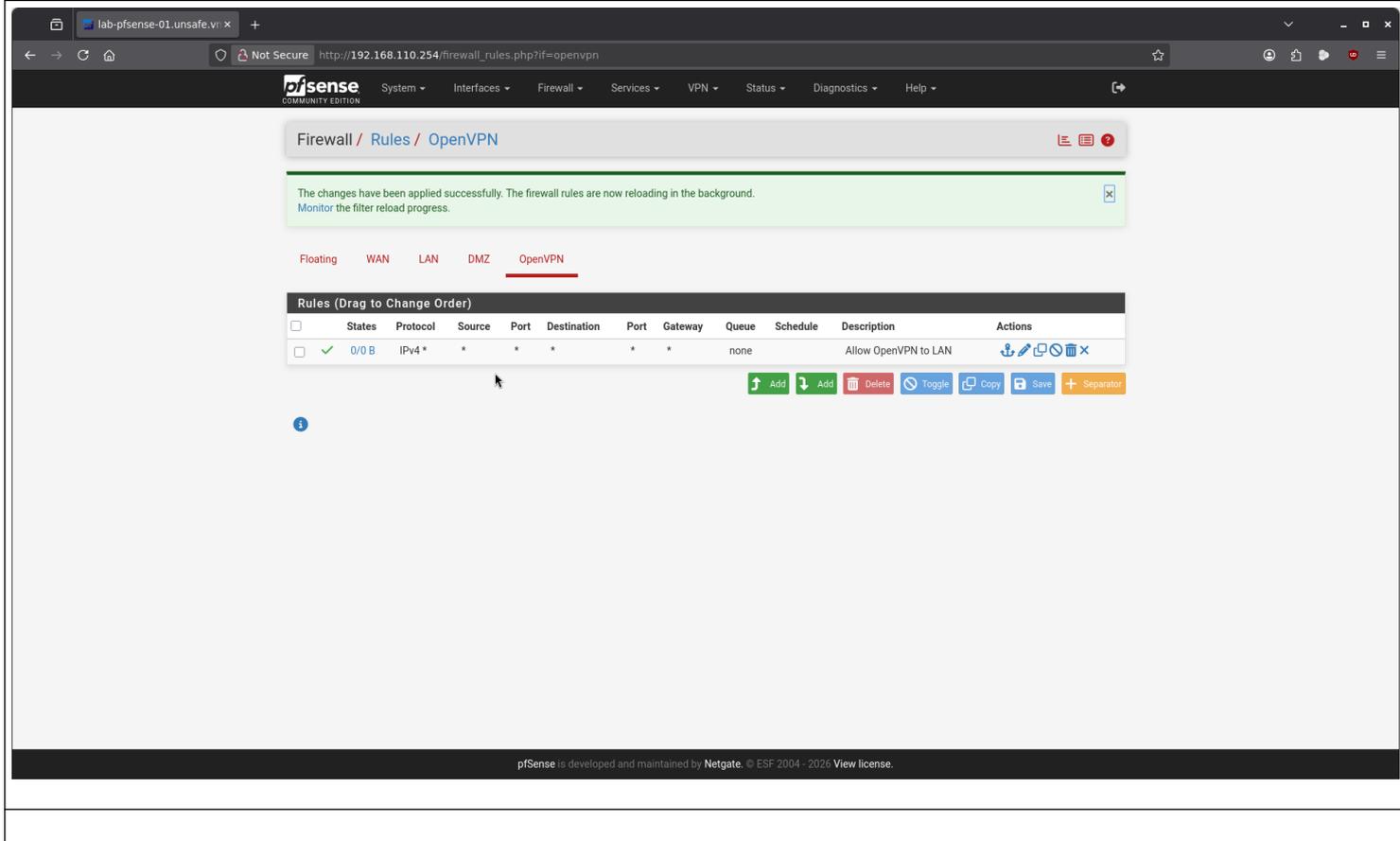




<b>Action</b>	Pass	
<b>Interface</b>	OpenVPN	C'est l'onglet magique qui apparaît quand on crée un serveur.
<b>Protocol</b>	Any	On laisse tout passer (TCP, UDP, ICMP...).
<b>Source</b>	Any	
<b>Destination</b>	Any	
<b>Description</b>	Allow OpenVPN to LAN	<b>Mode Lab.</b> En production, on restreindrait l'accès à des IP précises. Ici, on est des cow-boys, on ouvre tout ("Any / Any").



On n'oublie pas d'appliquer les changements !



# DÉPLOIEMENT CLIENT (Le Package Magique)

Exportation de la charge utile pour l'agent de terrain.

Pour éviter de copier-coller des clés RSA de 4096 bits à la main (et de faire une erreur de syntaxe à la ligne 342), nous utilisons l'outil d'exportation.

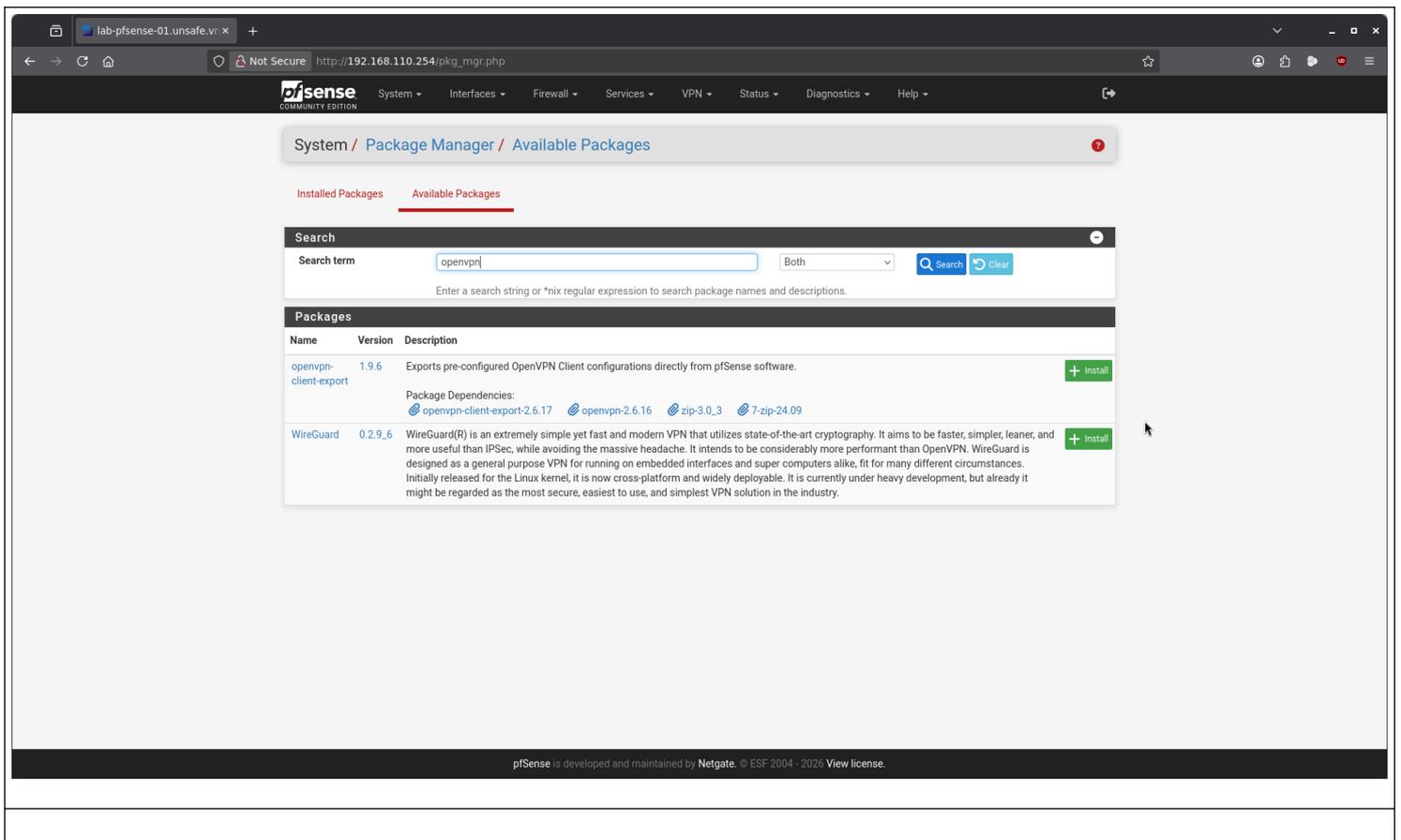
## Installation de l'outil

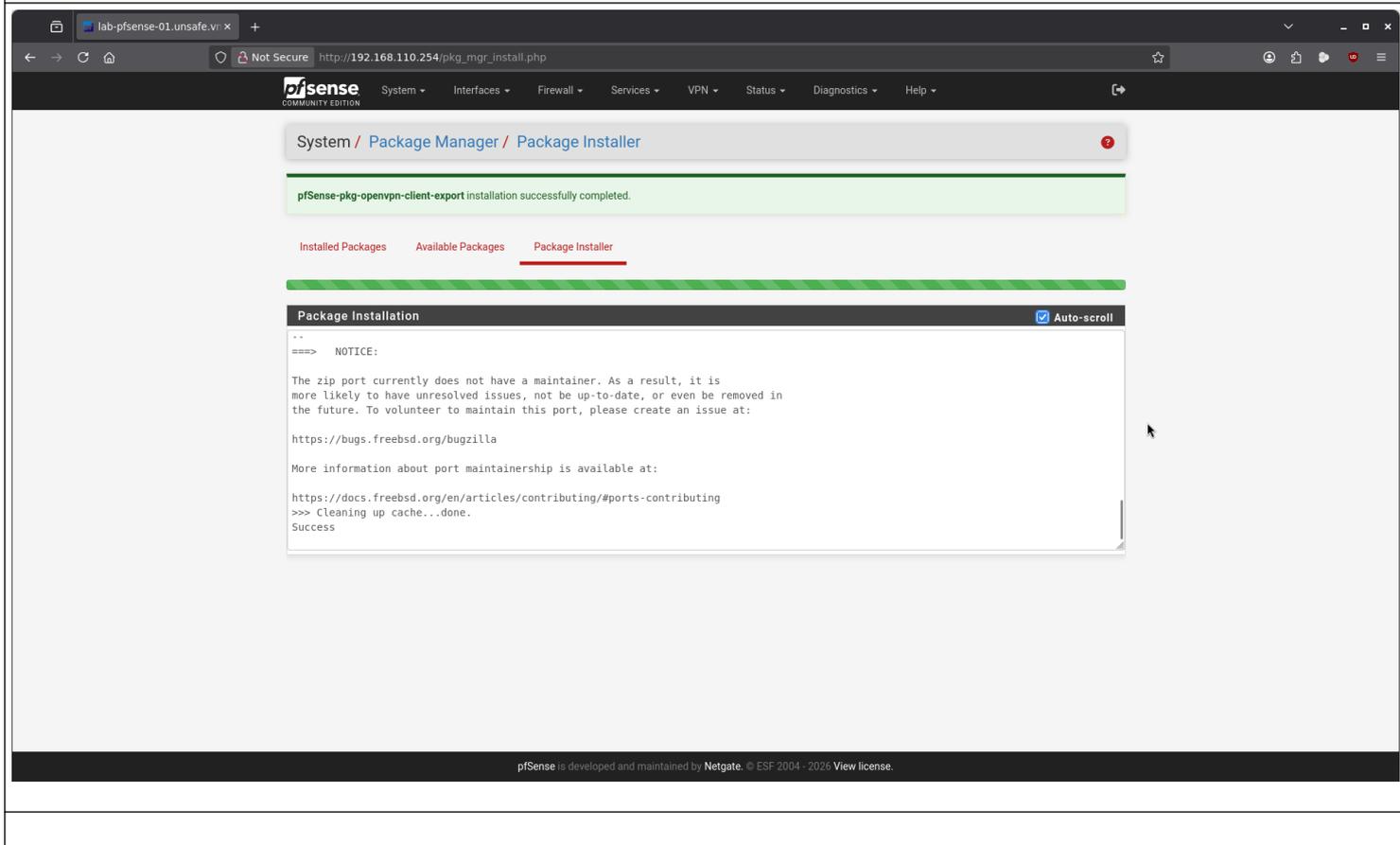
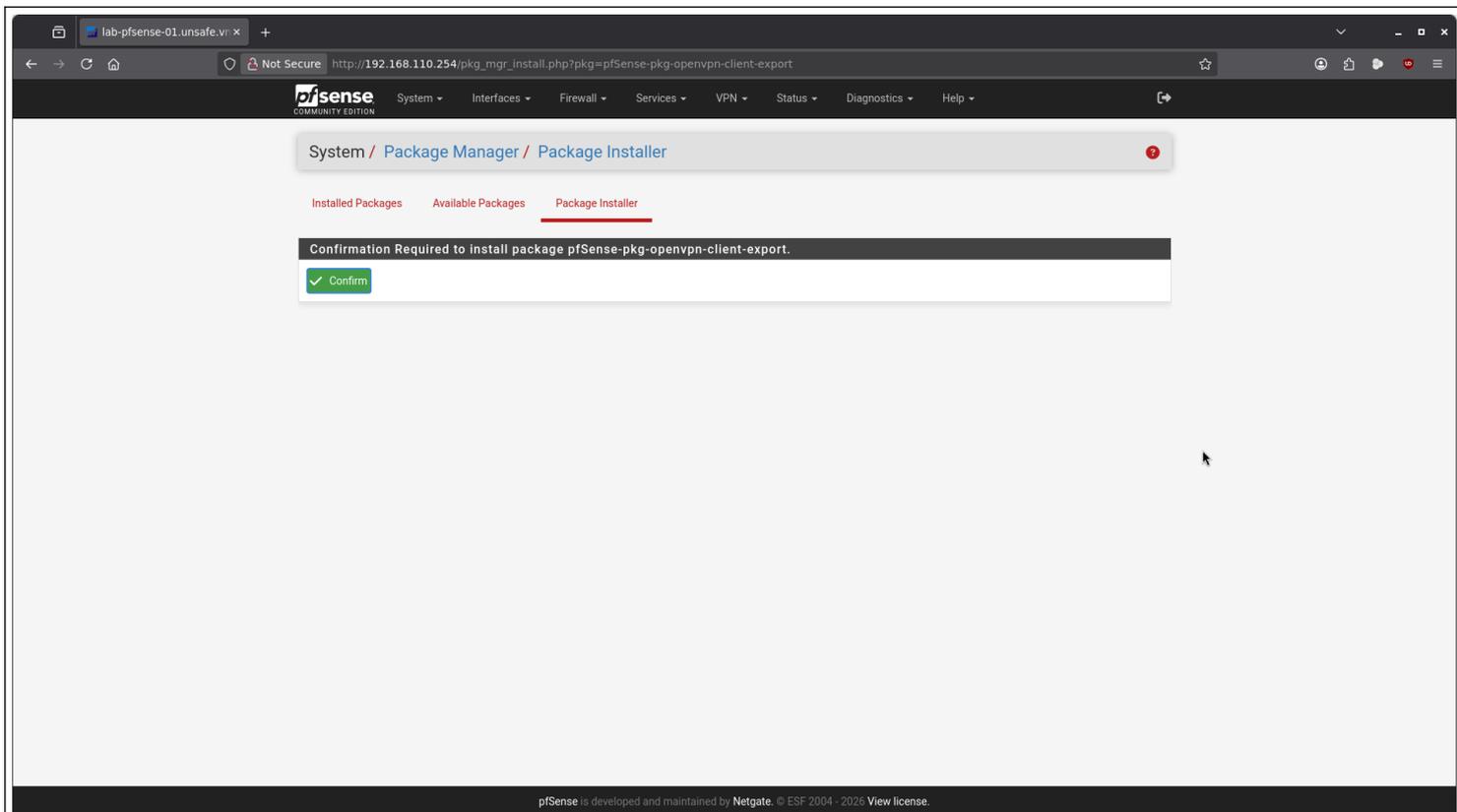
**Menu** : System > Package Manager > Available Packages.

**Recherche** : openvpn-client-export.

**Action** : Cliquez sur Install > Confirm.

Attendez que pfSense finisse de mâchouiller les fichiers (Success).



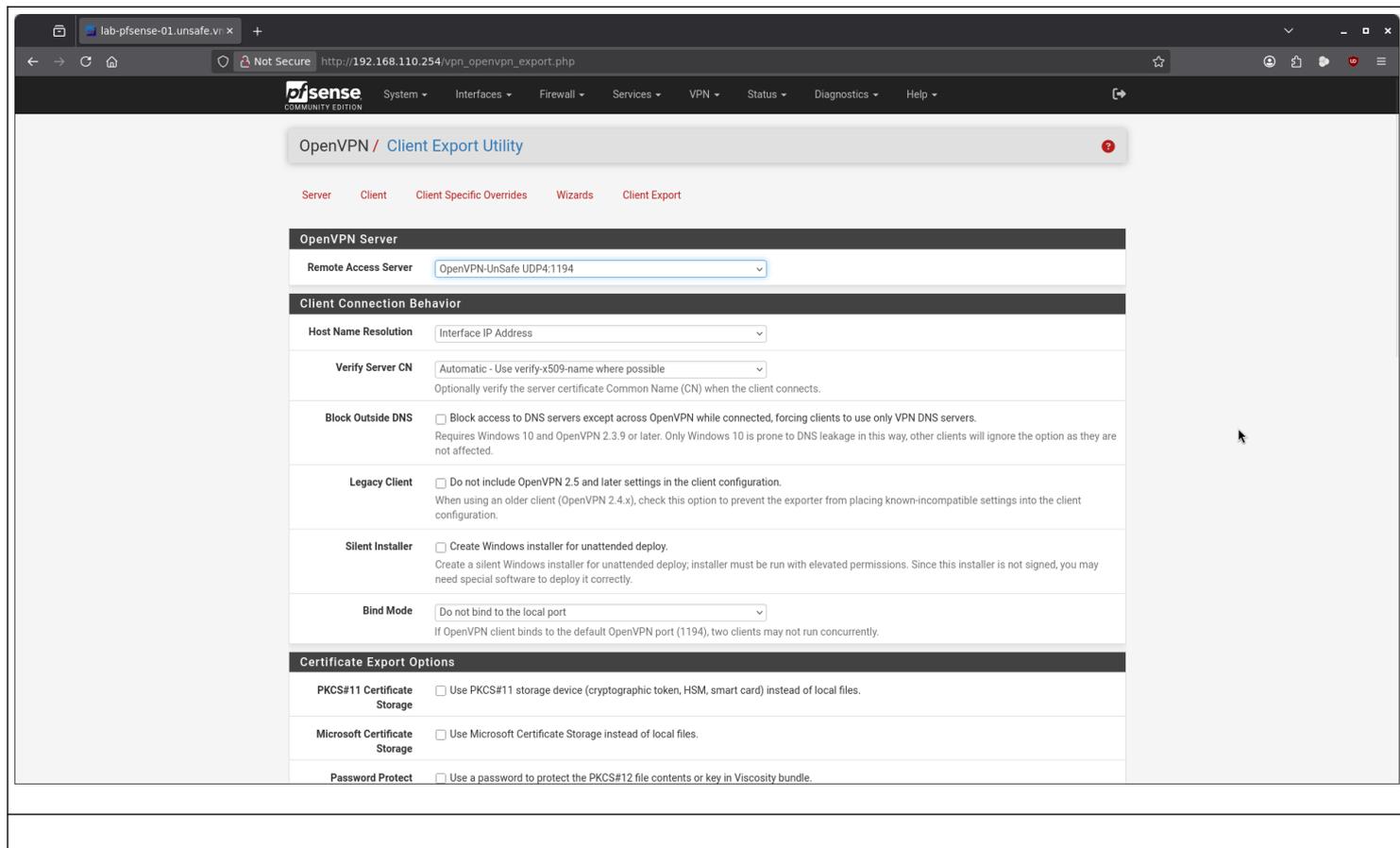


## Configuration de l'Export

Une fois installé, un nouvel onglet apparaît.

Menu : VPN > OpenVPN > **Client Export**.

C'est ici qu'on prépare le fichier .ovpn.



OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards Client Export

**OpenVPN Server**

Remote Access Server: OpenVPN-UnSafe 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.

Silent Installer:  Create Windows installer for unattended deploy. Create a silent Windows installer for unattended deploy; installer must be run with elevated permissions. Since this installer is not signed, you may need special software to deploy it correctly.

Bind Mode: Do not bind to the local port  
If OpenVPN client binds to the default OpenVPN port (1194), two clients may not run concurrently.

**Certificate Export Options**

PKCS#11 Certificate Storage:  Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.

Microsoft Certificate Storage:  Use Microsoft Certificate Storage instead of local files.

Password Protect Certificate:  Use a password to protect the PKCS#12 file contents or key in Viscosity bundle.

PKCS#12 Encryption: High: AES-256 + SHA256 (pfSense Software, FreeBSD, Linux, Window)  
Select the level of encryption to use when exporting a PKCS#12 archive. Encryption support varies by Operating System and program.

**Proxy Options**

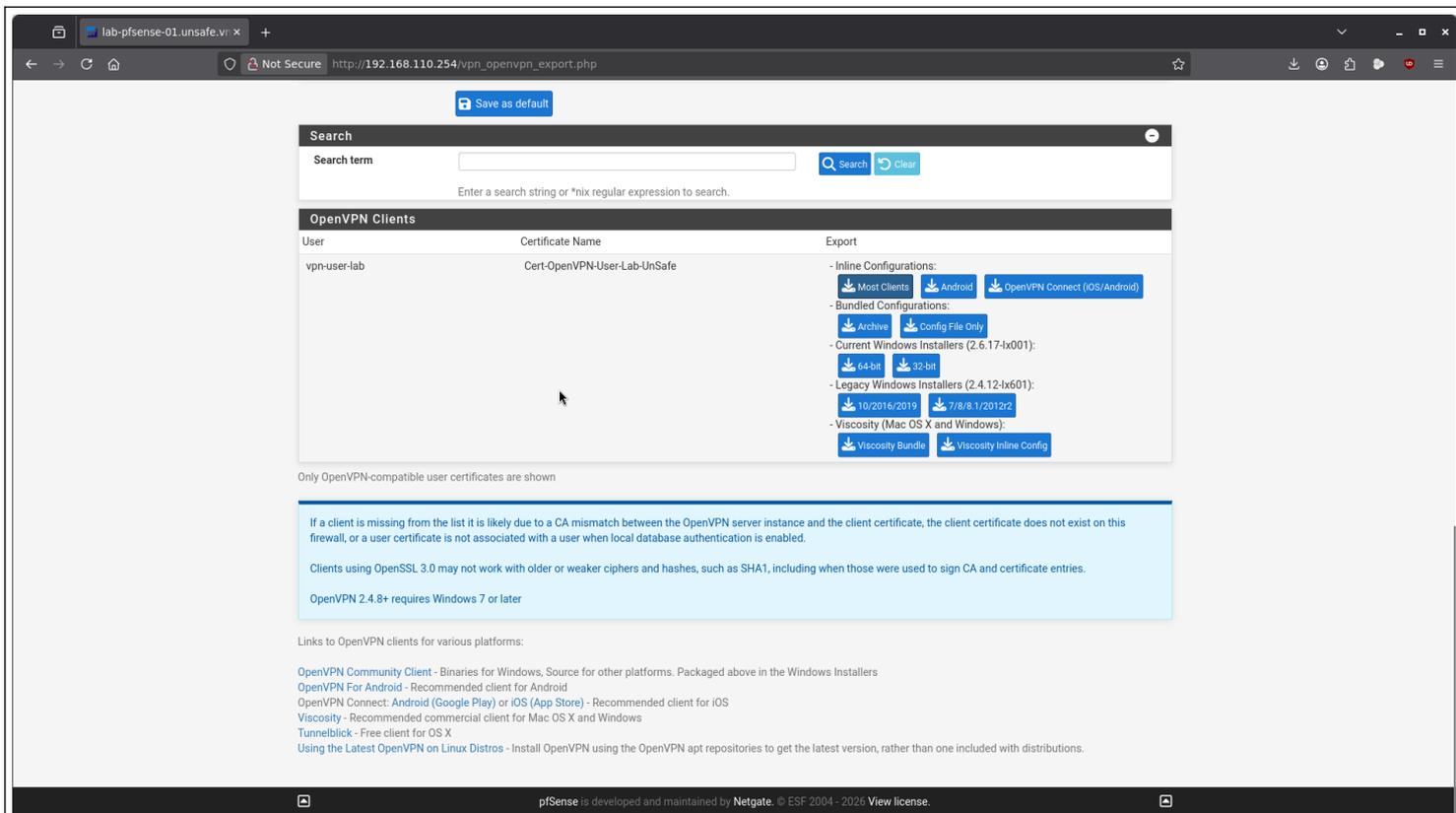
Use A Proxy:  Use proxy to communicate with the OpenVPN server.

**Advanced**

Additional configuration options:   
Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.  
EXAMPLE: remote-random;

Search:

Remote Access Server	OpenVPN-UnSafe UDP4:1194	Vérifiez que c'est bien votre serveur qui est sélectionné.
Host Name Resolution	Interface IP Address	
Verify Server CN	Automatic	



<b>Bouton Download</b>	Localisez votre utilisateur <b>vpn-user-lab</b> en bas.	
<b>Type de fichier</b>	Most Clients (ou Inline Configurations)	Cela télécharge un fichier unique .ovpn qui contient TOUT (CA, Cert, Clé, Config). C'est le "Happy Meal" du VPN.
	<p>The screenshot shows a file manager window titled 'Library'. It displays a list of files, with one file selected: 'lab-pfsense-01-UDP4-1194-vpn-user-lab-config.ovpn'. The file size is 6.9 KB, and it was downloaded from 192.168.110.254 at 7:20 PM. The file manager interface includes a search bar, navigation arrows, and a sidebar with options like 'Organize', 'Clear Downloads', 'History', 'Downloads', 'Tags', and 'All Bookmarks'.</p>	

## TEST FINAL (L'Injection Debian)

*Le moment de vérité.*

Transférez le fichier .ovpn téléchargé vers votre VM Debian (via scp, dossier partagé, ou clé USB virtuelle).

```
jesus@legion:~$ scp Downloads/lab-pfsense-01-UDP4-1194-vpn-user-lab-config.ovpn admin@192.168.100.142:~/
admin@192.168.100.142's password:
lab-pfsense-01-UDP4-1194-vpn-user-lab-config.ovpn
100% 7019    15.2MB/s   00:00
```

```
admin@lab-debian-54:~$ ls -l
total 8
-rw-rw-r-- 1 admin admin 7019 Jan 23 19:35 lab-pfsense-01-UDP4-1194-vpn-user-lab-config.ovpn
```

## Installation d'OpenVPN

```
admin@lab-debian-54:~$ sudo apt update && sudo apt install openvpn
[sudo] password for admin:
Hit:1 http://deb.debian.org/debian trixie InRelease
Get:2 http://security.debian.org/debian-security trixie-security InRelease [43.4 kB]
Get:3 http://deb.debian.org/debian trixie-updates InRelease [47.3 kB]
Get:4 http://security.debian.org/debian-security trixie-security/main Sources [119 kB]
Get:5 http://security.debian.org/debian-security trixie-security/main amd64 Packages [97.9 kB]
Get:6 http://security.debian.org/debian-security trixie-security/main Translation-en [62.5 kB]
Fetched 370 kB in 0s (1,760 kB/s)
5 packages can be upgraded. Run 'apt list --upgradable' to see them.
Installing:
  openvpn

Installing dependencies:
  easy-rsa  libduktape207  liblzo2-2  libnl-genl-3-200  libpkcs11-helper1t64  libpolkit-gobject-1-0  openc-
pkcs11  polkitd  xml-core
  libccid  libeac3  libnl-3-200  libpcsclite1  libpolkit-agent-1-0  openc  pcscd
  sgml-base

Suggested packages:
  pcmciautils  resolvconf  openvpn-dco-dkms  openvpn-systemd-resolved  sgml-base-doc  debhelper

Summary:
  Upgrading: 0, Installing: 18, Removing: 0, Not Upgrading: 5
  Download size: 2,902 kB
  Space needed: 9,438 kB / 22.3 GB available

Continue? [Y/n]
```

## Lancement du tunnel

```
admin@lab-debian-54:~$ sudo openvpn --config lab-pfsense-01-UDP4-1194-vpn-user-lab-config.ovpn
2026-01-23 19:42:00 OpenVPN 2.6.14 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11]
[MH/PKTINFO] [AEAD] [DCO]
2026-01-23 19:42:00 library versions: OpenSSL 3.5.4 30 Sep 2025, LZO 2.10
2026-01-23 19:42:00 DCO version: N/A
Enter Auth Username: vpn-user-lab <-- Le Username de notre Utilisateur crée sur PfSense !
Enter Auth Password: ..... <-- Son Password (j'espère que vous l'avez noté)
2026-01-23 19:42:24 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.100.254:1194
2026-01-23 19:42:24 UDPv4 link local: (not bound)
2026-01-23 19:42:24 UDPv4 link remote: [AF_INET]192.168.100.254:1194
2026-01-23 19:42:24 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to
prevent this
2026-01-23 19:42:24 [vpn.lab.unsafe] Peer Connection Initiated with [AF_INET]192.168.100.254:1194
2026-01-23 19:42:25 TUN/TAP device tun0 opened
2026-01-23 19:42:25 net_iface_mtu_set: mtu 1500 for tun0
2026-01-23 19:42:25 net_iface_up: set tun0 up
2026-01-23 19:42:25 net_addr_v4_add: 10.0.8.2/24 dev tun0
2026-01-23 19:42:25 Initialization Sequence Completed
```

# Une fois que vous avez le message "Completed", ne fermez pas cette fenêtre. Ouvrez un deuxième terminal sur la Debian et testez la vision à travers le tunnel !

```
admin@lab-debian-54:~$ ip a show tun0
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
link/none
inet 10.0.8.2/24 scope global tun0
    valid_lft forever preferred_lft forever
inet6 fe80::eb65:e069:489c:246a/64 scope link stable-privacy proto kernel_ll
    valid_lft forever preferred_lft forever
```

# Pinger l'adresse IP interne du VPN (à travers le tunnel)

```
admin@lab-debian-54:~$ ping 10.0.8.1 -c 3
PING 10.0.8.1 (10.0.8.1) 56(84) bytes of data.
64 bytes from 10.0.8.1: icmp_seq=1 ttl=64 time=0.505 ms
64 bytes from 10.0.8.1: icmp_seq=2 ttl=64 time=1.07 ms
64 bytes from 10.0.8.1: icmp_seq=3 ttl=64 time=1.18 ms

--- 10.0.8.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.505/0.920/1.183/0.296 ms
```

# et des que l'ont coupe la connexion au vps (avec un ctrl+C) ...

```
^C2026-01-23 19:54:33 event_wait : Interrupted system call (fd=-1,code=4)
2026-01-23 19:54:33 SIGTERM received, sending exit notification to peer
2026-01-23 19:54:34 net_addr_v4_del: 10.0.8.2 dev tun0
2026-01-23 19:54:34 SIGTERM[soft,exit-with-notification] received, process exiting
admin@lab-debian-54:~$
```

```
admin@lab-debian-54:~$ ping 10.0.8.1 -c 3
PING 10.0.8.1 (10.0.8.1) 56(84) bytes of data.

--- 10.0.8.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2055ms
```

# Si vous avez ce résultat, votre VPN fonctionne parfaitement.