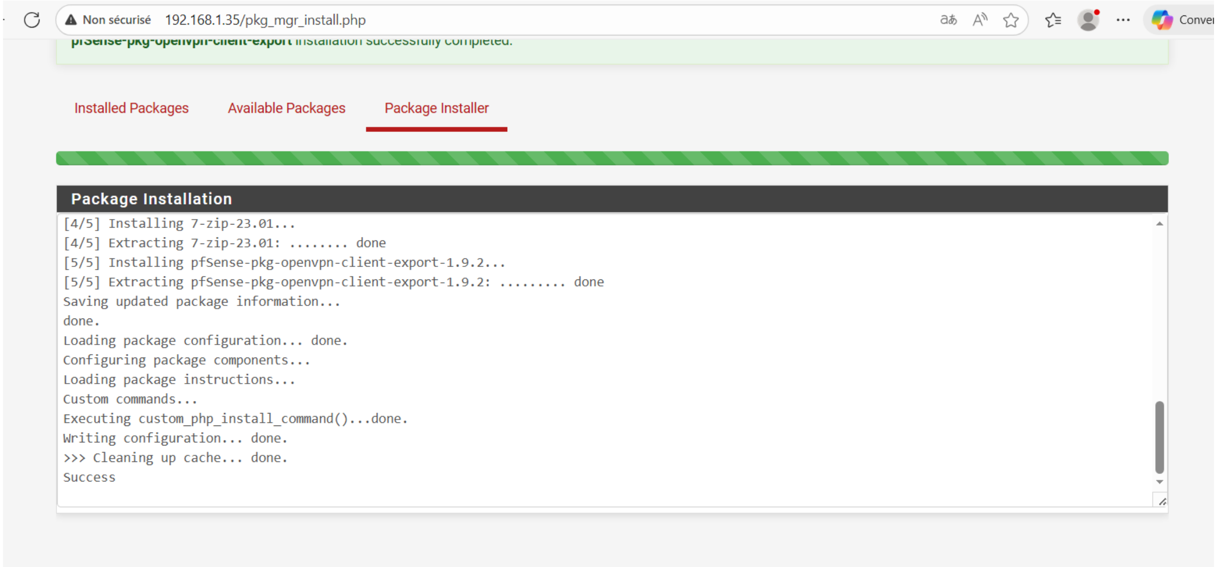
Mise en place d'un VPN

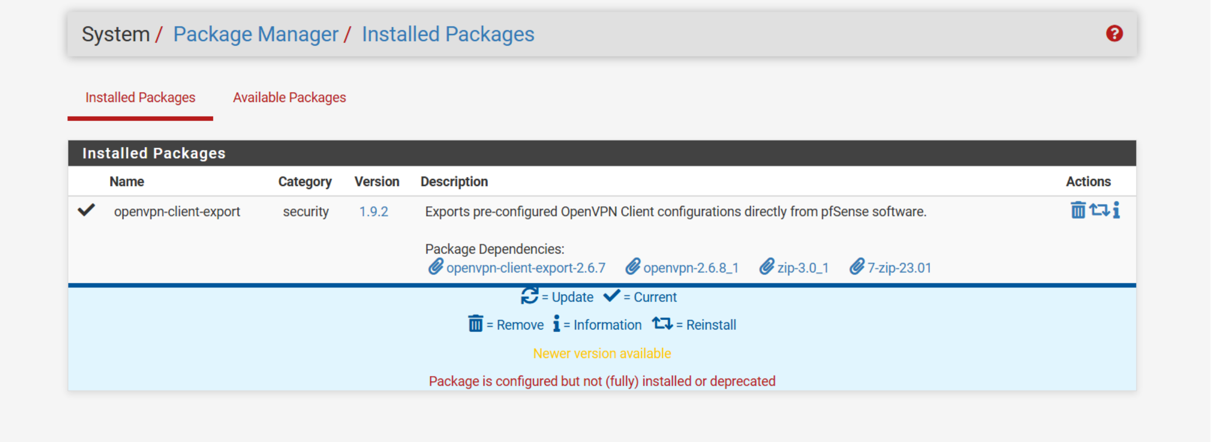
1. Connectez-vous à l'interface web de pfSense
2. Allez dans **System → Package Manager**
3. Cliquez sur l'onglet **Available Packages**
4. Recherchez **"openvpn-client-export"**
5. Cliquez sur **Install** puis confirmez



pfSense-pkg-openvpn-client-export installation successfully completed.

Package Installation

```
[4/5] Installing 7-zip-23.01...
[4/5] Extracting 7-zip-23.01: ........ done
[5/5] Installing pfSense-pkg-openvpn-client-export-1.9.2...
[5/5] Extracting pfSense-pkg-openvpn-client-export-1.9.2: ......... done
Saving updated package information...
done.
Loading package configuration... done.
Configuring package components...
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Writing configuration... done.
>>> Cleaning up cache... done.
Success
```



Installed Packages

	Name	Category	Version	Description	Actions
✓	openvpn-client-export	security	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software. Package Dependencies: openvpn-client-export-2.6.7 openvpn-2.6.8_1 zip-3.0_1 7-zip-23.01	

= Update ✓ = Current

= Remove = Information = Reinstall

Newer version available

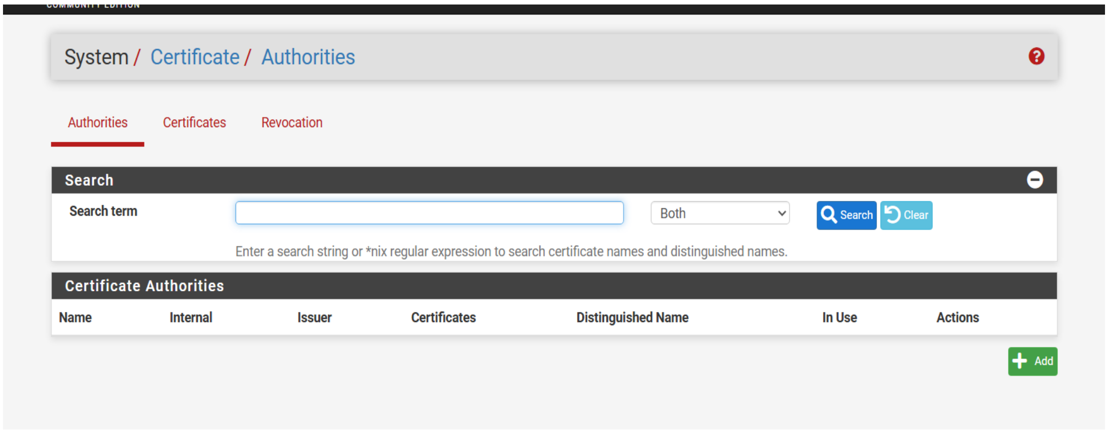
Package is configured but not (fully) installed or deprecated

L'installation est fini.

1. Allez dans **System → Cert Manager**

2. Onglet **CAs**

3. Cliquez sur **Add**



System / Certificate / Authorities

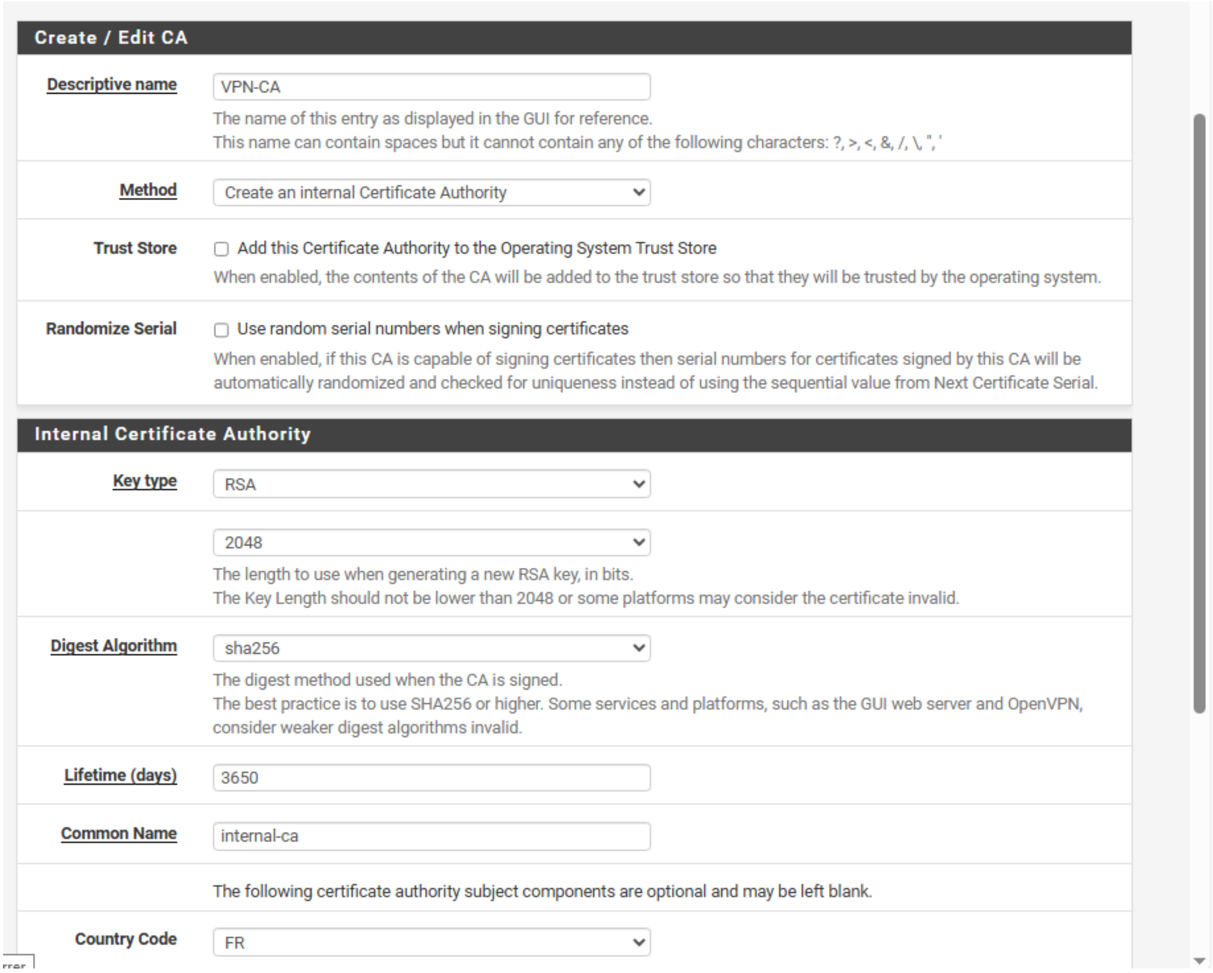
Search term

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

Remplissez les champs suivants :



Create / Edit CA

Descriptive name VPN-CA
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 □ Add this Certificate Authority to the Operating System Trust Store
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 □ Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

Key type RSA

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

Digest Algorithm sha256
The digest method used when the CA is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days) 3650

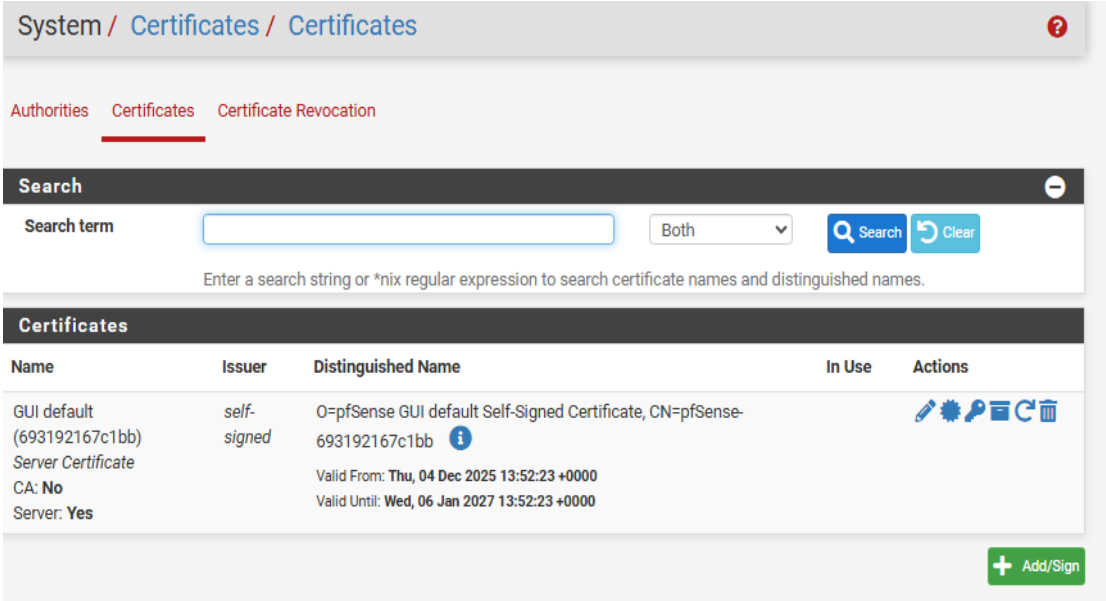
Common Name internal-ca

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

Country Code FR

Puis cliquer sur Save

1. Dans **System → Cert Manager**
2. Onglet **Certificates**
3. Cliquez sur **Add/Sign**



System / Certificates / Certificates

Search

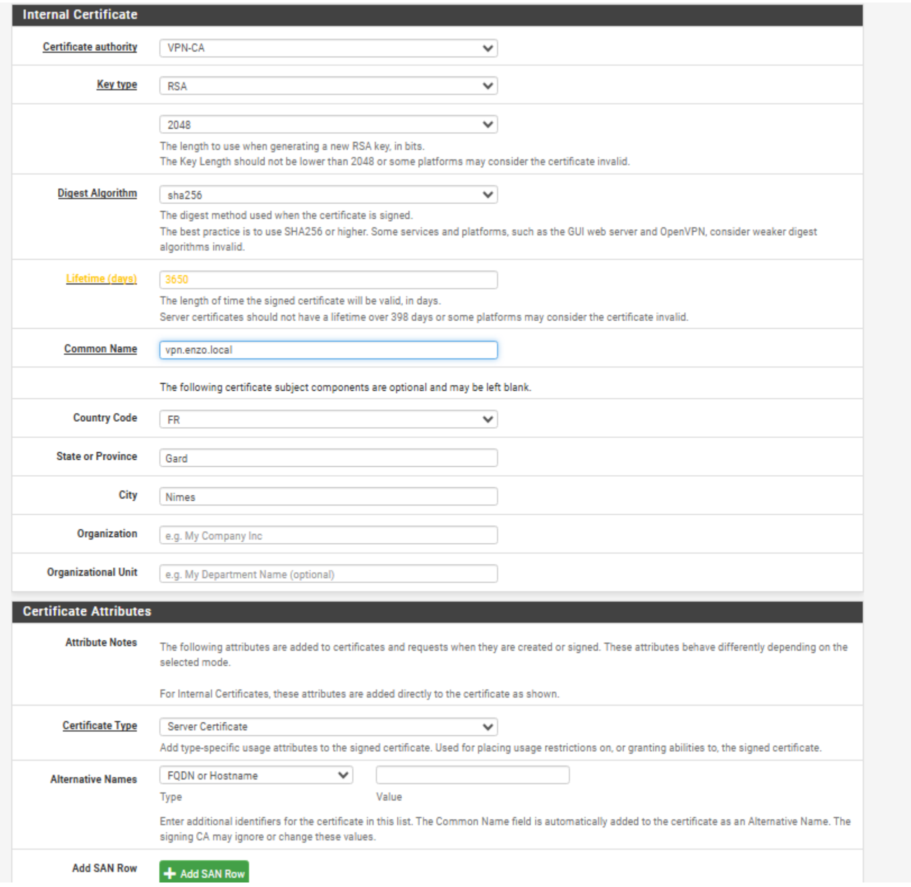
Search term: Both — Search — Clear

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 (693192167c1bb) *Server Certificate* CA: **No** Server: **Yes**	*self-signed*	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-693192167c1bb Valid From: **Thu, 04 Dec 2025 13:52:23 +0000** Valid Until: **Wed, 06 Jan 2027 13:52:23 +0000**		

Configurez le certificat :



Internal Certificate

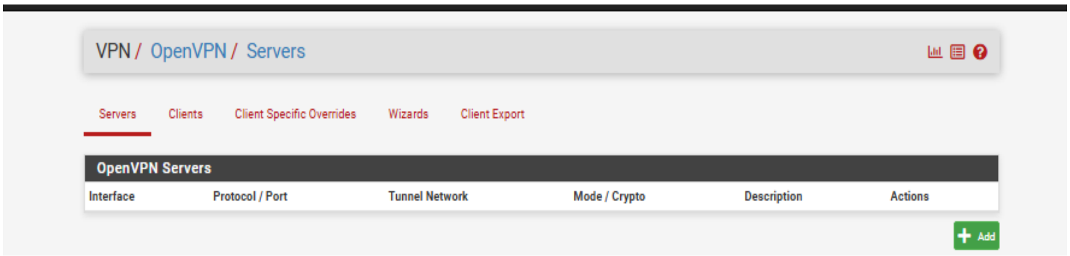
Certificate authority	VPN-CA
Key type	RSA
	2048 The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm	sha256 The digest method used when the certificate is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.
Lifetime (days)	3650 The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.
Common Name	vpn.enzo.local
	The following certificate subject components are optional and may be left blank.
Country Code	FR
State or Province	Gard
City	Nimes
Organization	e.g. My Company Inc
Organizational Unit	e.g. My Department Name (optional)

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 Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.
Alternative Names	Type: FQDN or Hostname — Value: Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.
Add SAN Row	Add SAN Row

Cliquer sur Save

1. Allez dans **VPN → OpenVPN**
2. Onglet **Servers**
3. Cliquez sur **Add**

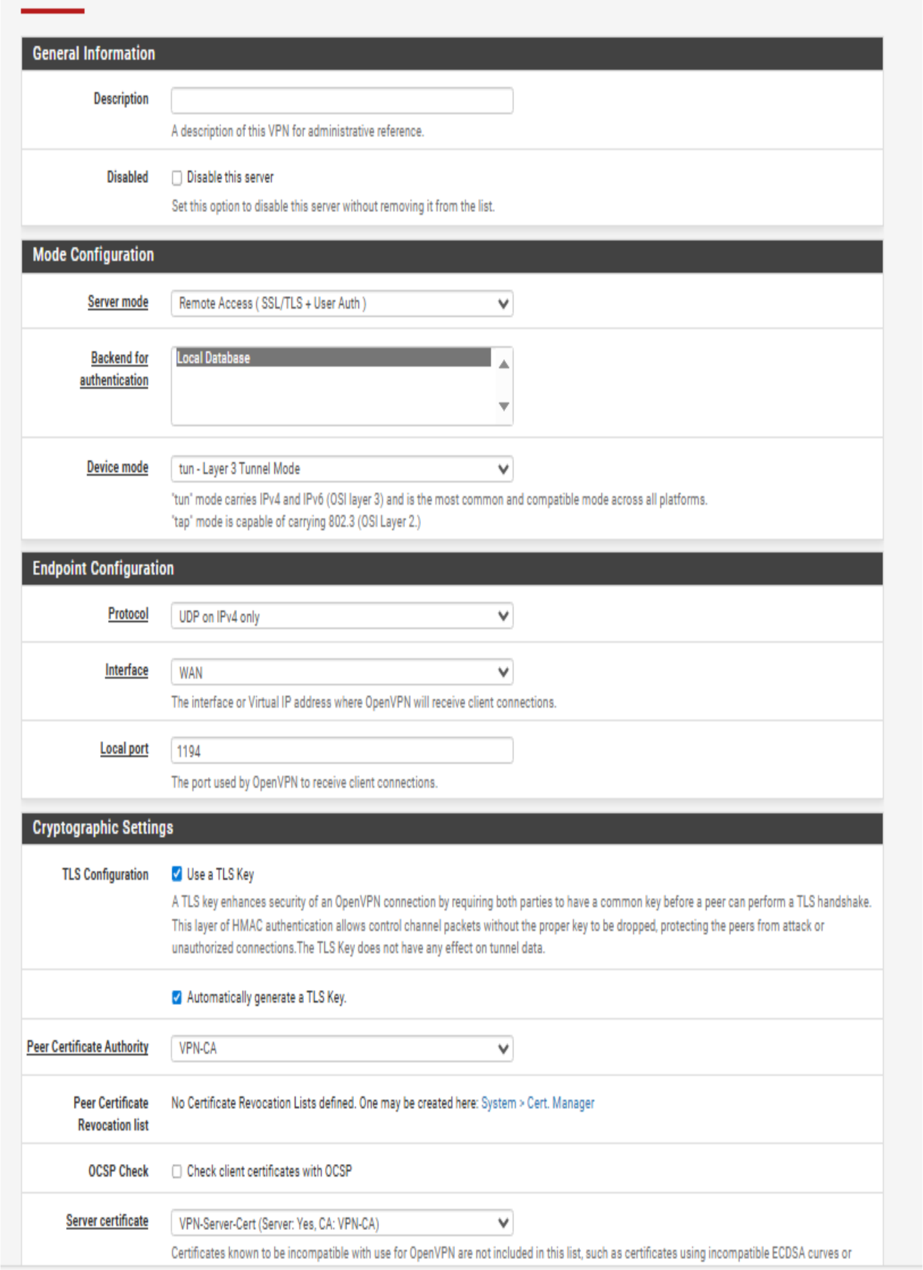


VPN / OpenVPN / Servers

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions

Configuration générale :



General Information

Description:
A description of this VPN for administrative reference.

Disabled: □ Disable this server
Set this option to disable this server without removing it from the list.

Mode Configuration

Server mode: Remote Access (SSL/TLS + User Auth)

Backend for authentication: Local Database

Device mode: tun - Layer 3 Tunnel Mode
'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.)

Endpoint Configuration

Protocol: UDP on IPv4 only

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

Local port: 1194
The port used by OpenVPN to receive client connections.

Cryptographic Settings

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

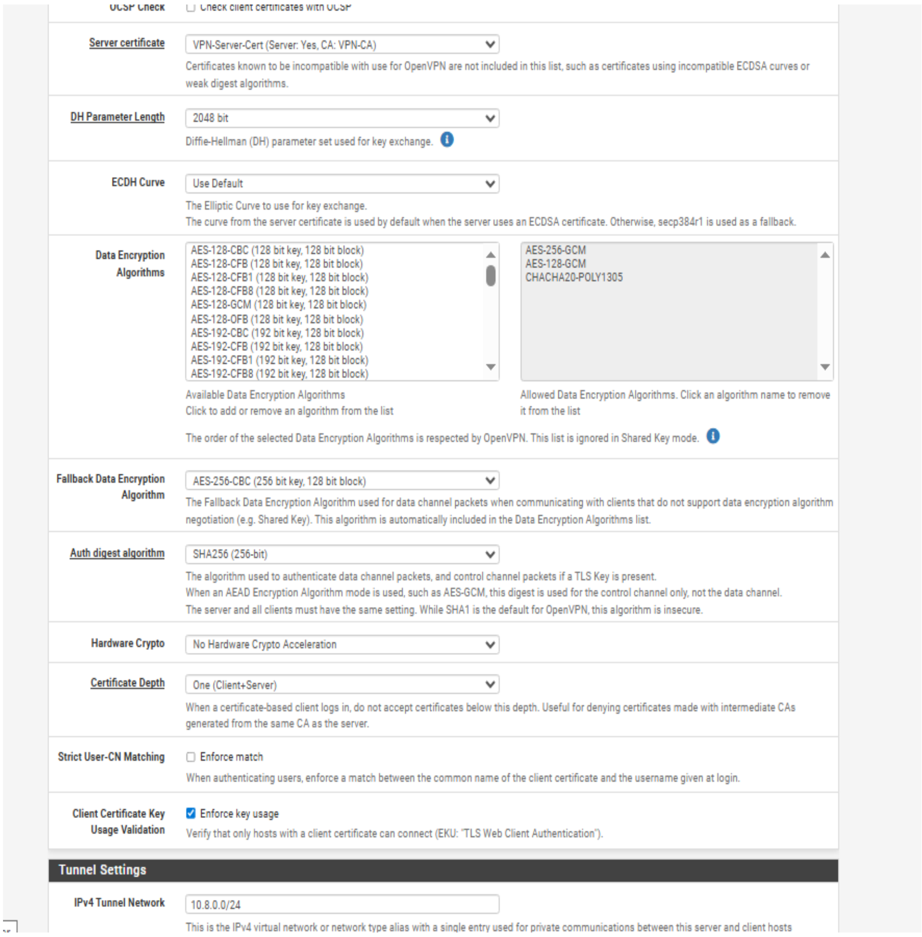
☑ Automatically generate a TLS Key.

Peer Certificate Authority: VPN-CA

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: VPN-Server-Cert (Server: Yes, CA: VPN-CA)
Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or



OCSP Check □ Check client certificates with OCSP

Server certificate VPN-Server-Cert (Server: Yes, CA: VPN-CA)

Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

DH Parameter Length 2048 bit

Diffie-Hellman (DH) parameter set used for key exchange.

ECDH Curve Use Default

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 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)

Available Data Encryption Algorithms
Click to add or remove an algorithm from the list

AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305

Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode.

Fallback Data Encryption Algorithm AES-256-CBC (256 bit key, 128 bit block)

The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.

Auth digest algorithm SHA256 (256-bit)

The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.

Hardware Crypto No Hardware Crypto Acceleration

Certificate Depth One (Client+Server)

When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.

Strict User-CN Matching □ Enforce match

When authenticating users, enforce a match between the common name of the client certificate and the username given at login.

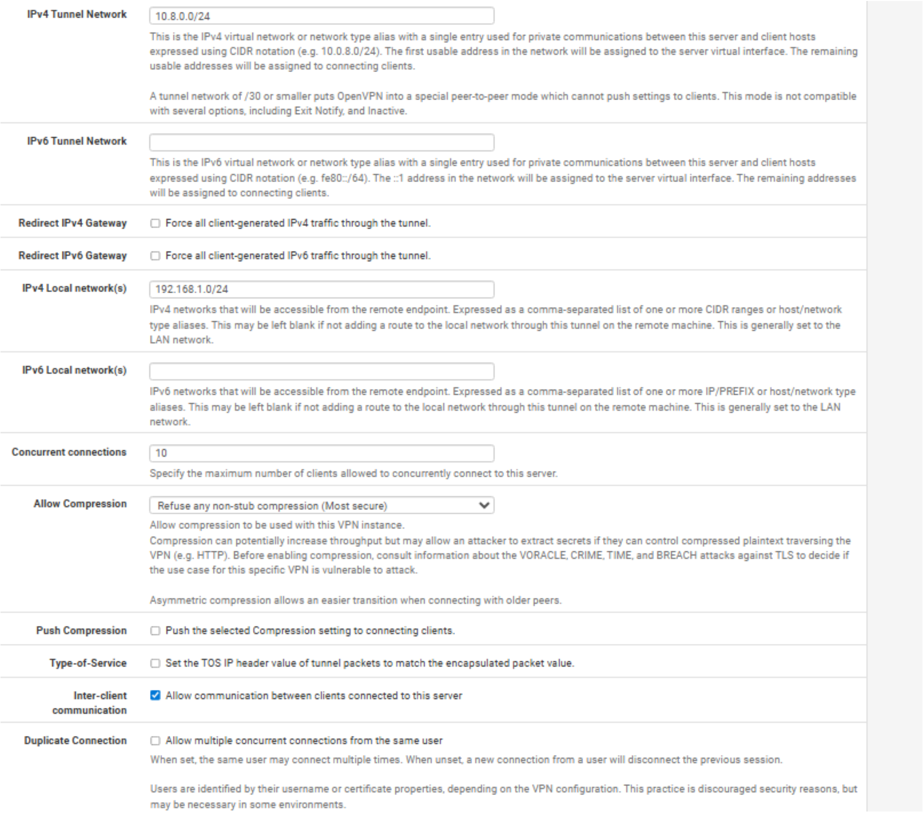
Client Certificate Key Usage Validation ☑ Enforce key usage

Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").

Tunnel Settings

IPv4 Tunnel Network 10.8.0.0/24

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts



IPv4 Tunnel Network 10.8.0.0/24

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

IPv6 Tunnel Network

This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway □ Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway □ Force all client-generated IPv6 traffic through the tunnel.

IPv4 Local network(s) 192.168.1.0/24

IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

IPv6 Local network(s)

IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX 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.

Concurrent connections 10

Specify the maximum number of clients allowed to concurrently connect to this server.

Allow Compression Refuse any non-stub compression (Most secure)

Allow compression to be used with this VPN instance.
Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.

Asymmetric compression allows an easier transition when connecting with older peers.

Push Compression □ Push the selected Compression setting to connecting clients.

Type-of-Service □ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

Inter-client communication ☑ Allow communication between clients connected to this server

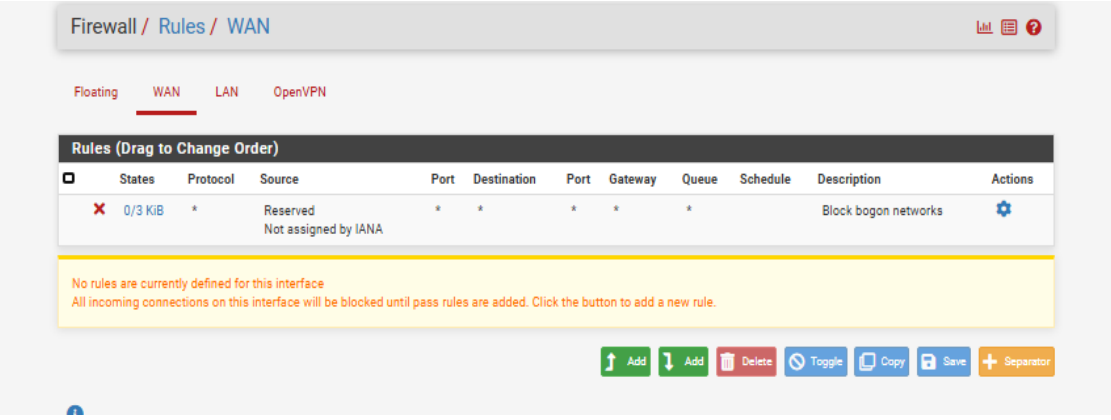
Duplicate Connection □ Allow multiple concurrent connections from the same user

When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.

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.

Cliquez sur **Save**

1. Allez dans **Firewall → Rules**
2. Onglet **WAN**
3. Cliquez sur **Add ↑** (en haut)



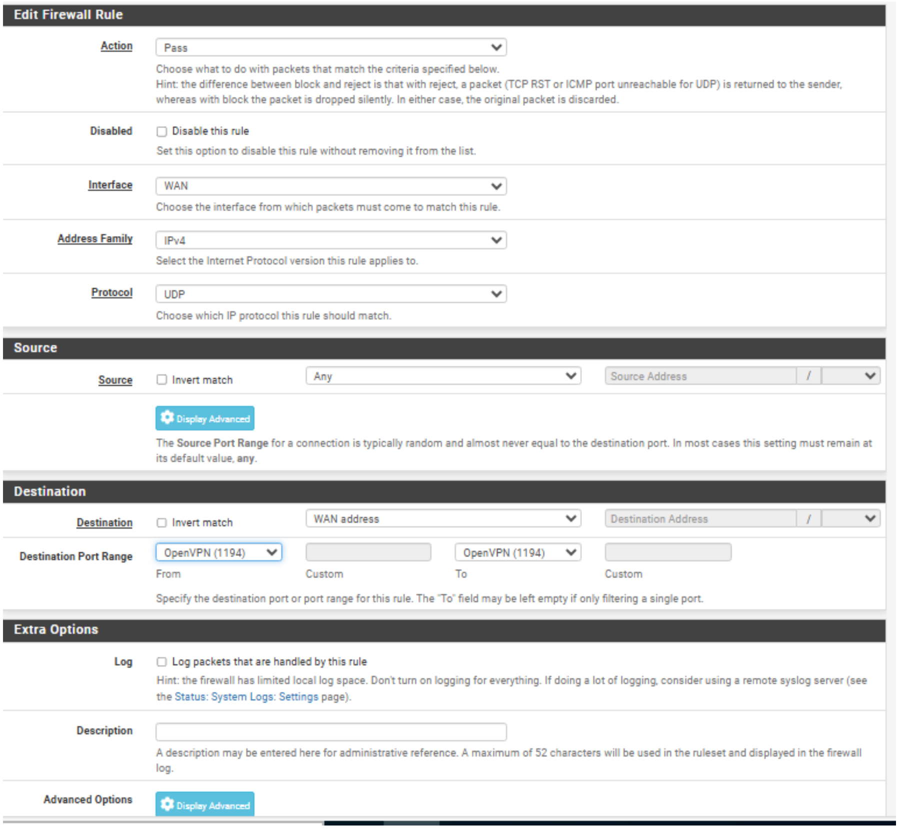
Firewall / Rules / WAN

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0/3 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Configurez la règle :



Edit Firewall Rule

Action: Pass
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: WAN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: UDP
Choose which IP protocol this rule should match.

Source

Source: □ Invert match — Any — Source Address /

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 — WAN address — Destination Address /

Destination Port Range: OpenVPN (1194) — From; Custom; OpenVPN (1194) — 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.

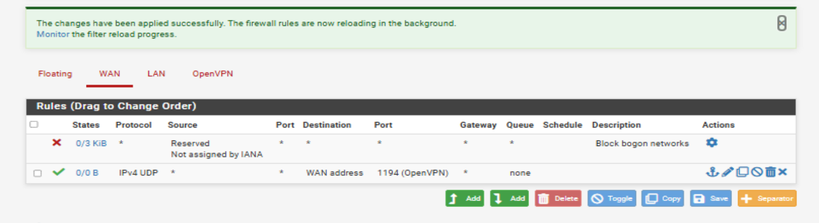
Extra Options

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:

Cliquer ensuite sur Save et Apply changes



The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

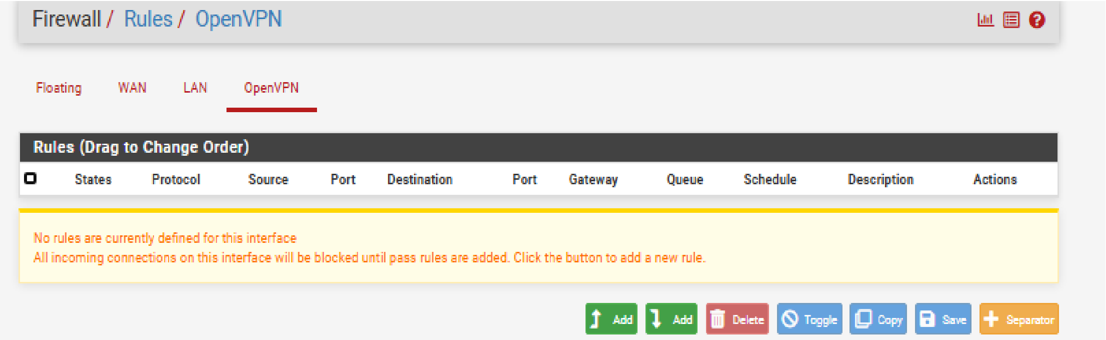
Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0/3 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
□	✓	0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none			

Vous retrouver votre règle ici.

1. Onglet **OpenVPN**

2. Cliquez sur **Add** ↑



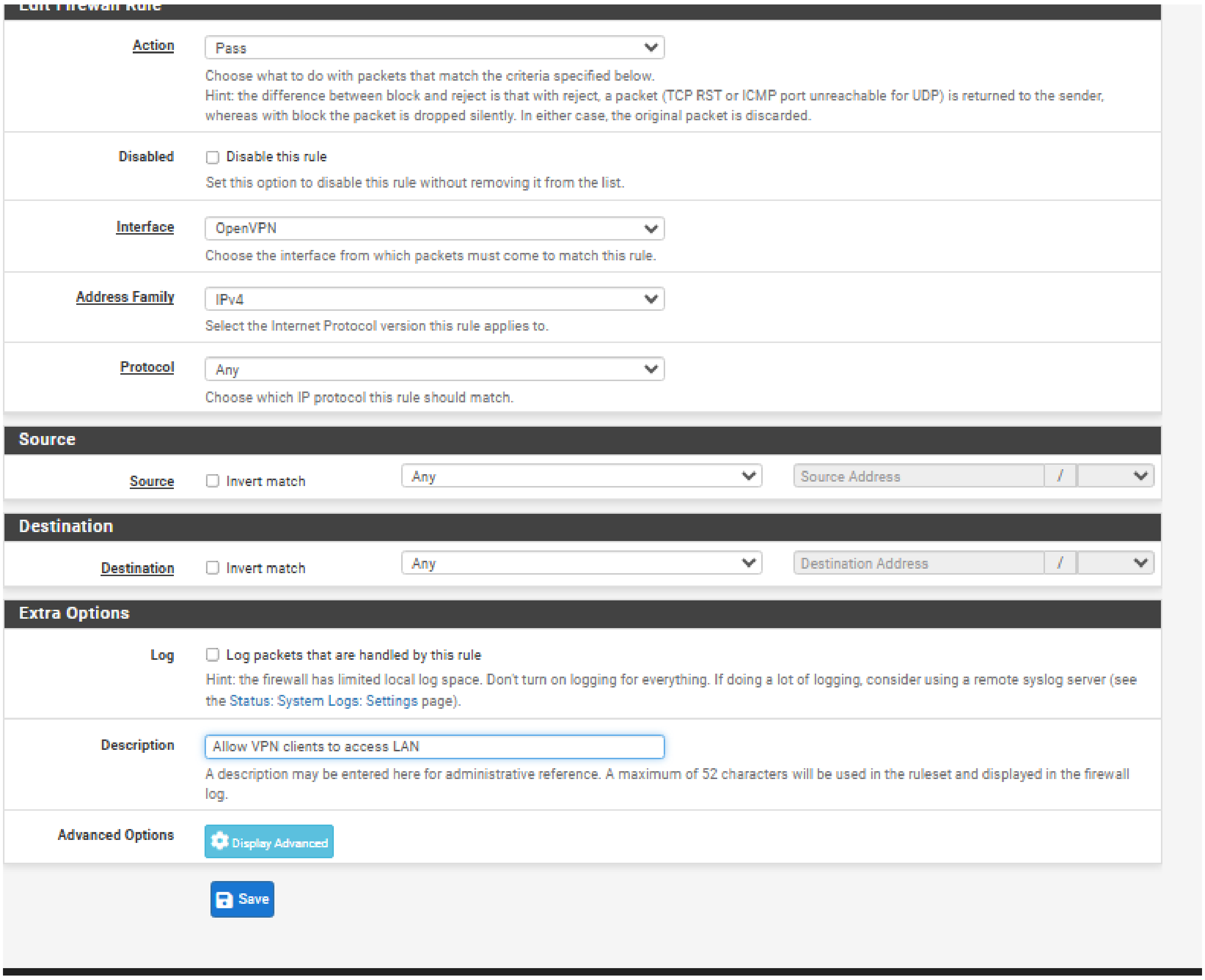
Firewall / Rules / OpenVPN

Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

3. Configurez la règle :



Edit Firewall Rule

Action: Pass
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: OpenVPN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: Any
Choose which IP protocol this rule should match.

Source

Source: ☐ Invert match — Any — Source Address /

Destination

Destination: ☐ Invert match — Any — Destination Address /

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: Allow VPN clients to access LAN
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

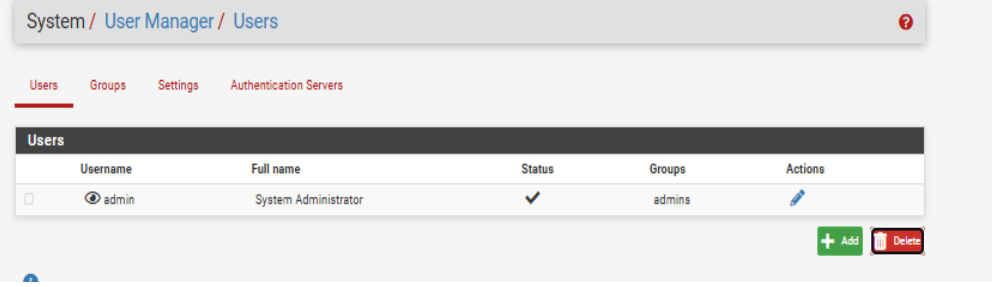
Cliquez sur **Save** puis **Apply Changes**

✅ **Vérification :** Vous devriez avoir au minimum 2 règles (une sur WAN et une sur OpenVPN).

1. Allez dans **System → User Manager**

2. Onglet **Users**

3. Cliquez sur **Add**

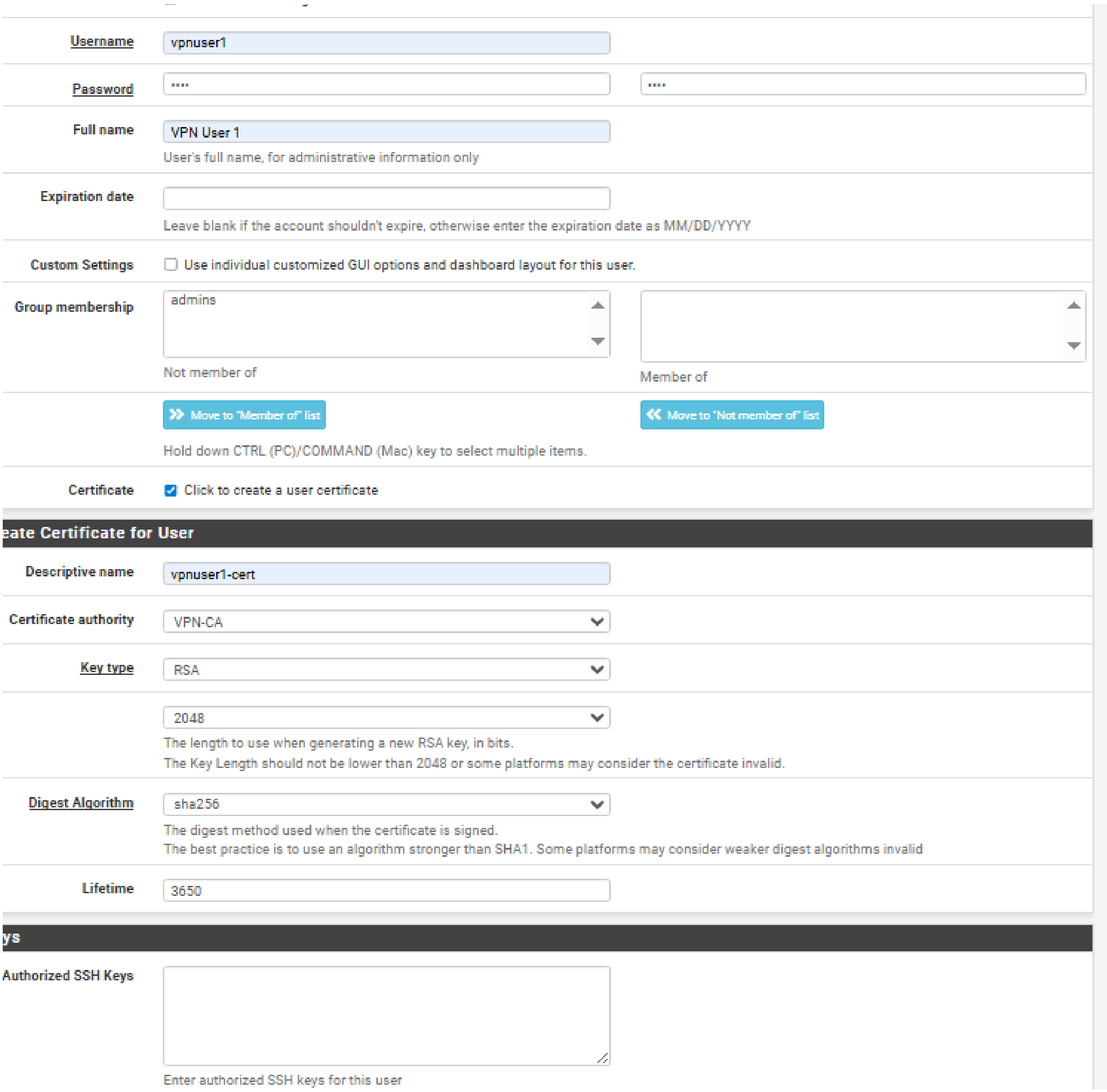


System / User Manager / Users

Users

	Username	Full name	Status	Groups	Actions
□	admin	System Administrator	✓	admins	

4. Remplissez les informations :



Username	vpnuser1	
Password	••••	••••
Full name	VPN User 1 User's full name, for administrative information only	
Expiration date	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	admins Not member of	Member of
	Move to "Member of" list Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.	Move to "Not member of" list
Certificate	☑ Click to create a user certificate	

eate Certificate for User

Descriptive name	vpnuser1-cert
Certificate authority	VPN-CA
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	3650

ys

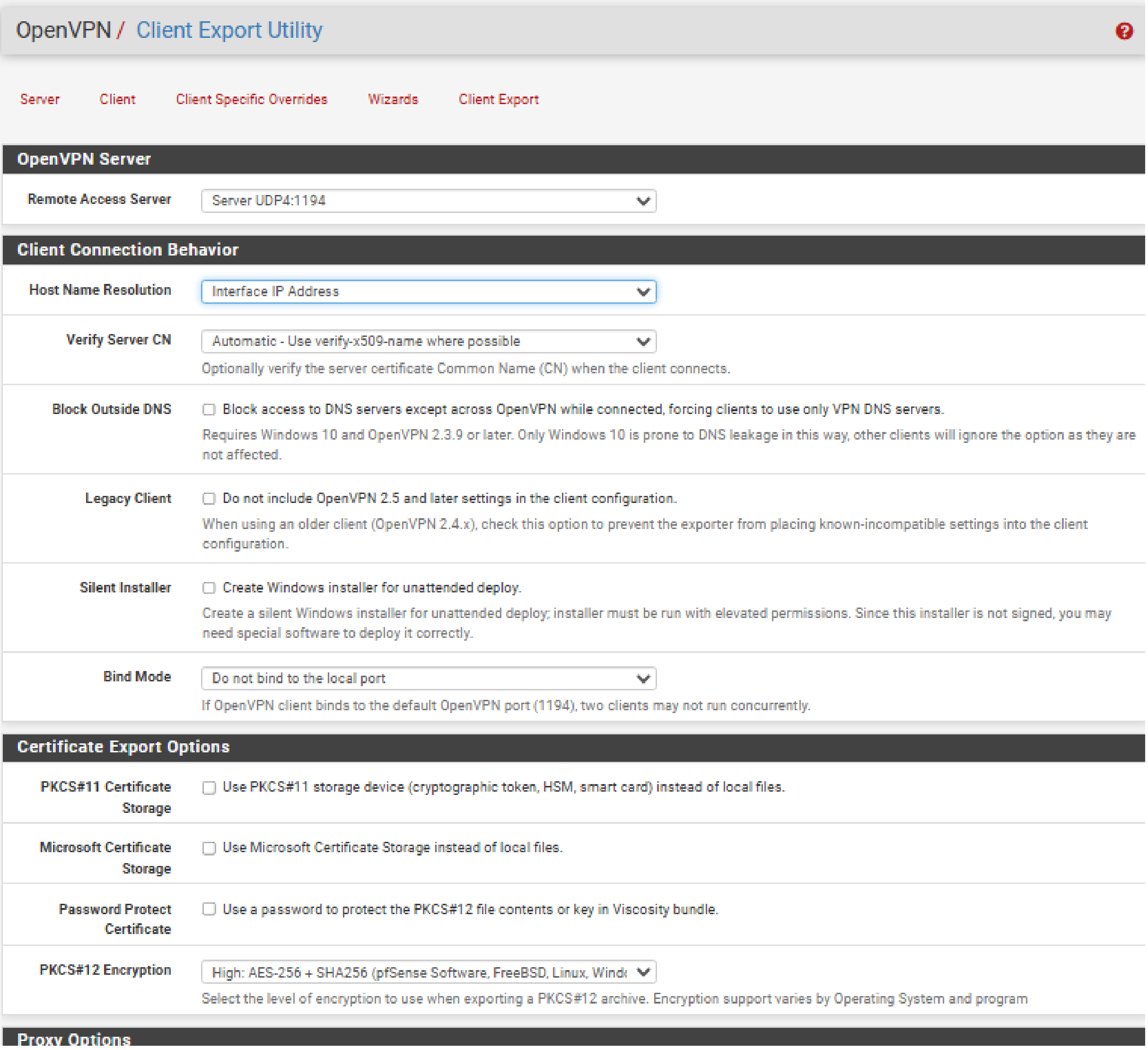
Authorized SSH Keys	Enter authorized SSH keys for this user

Cliquez sur **Save**

1. Allez dans **VPN → OpenVPN**

2. Onglet **Client Export**

3. Configurez les options d'export :



OpenVPN / Client Export Utility

OpenVPN Server

Remote Access Server: Server 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.

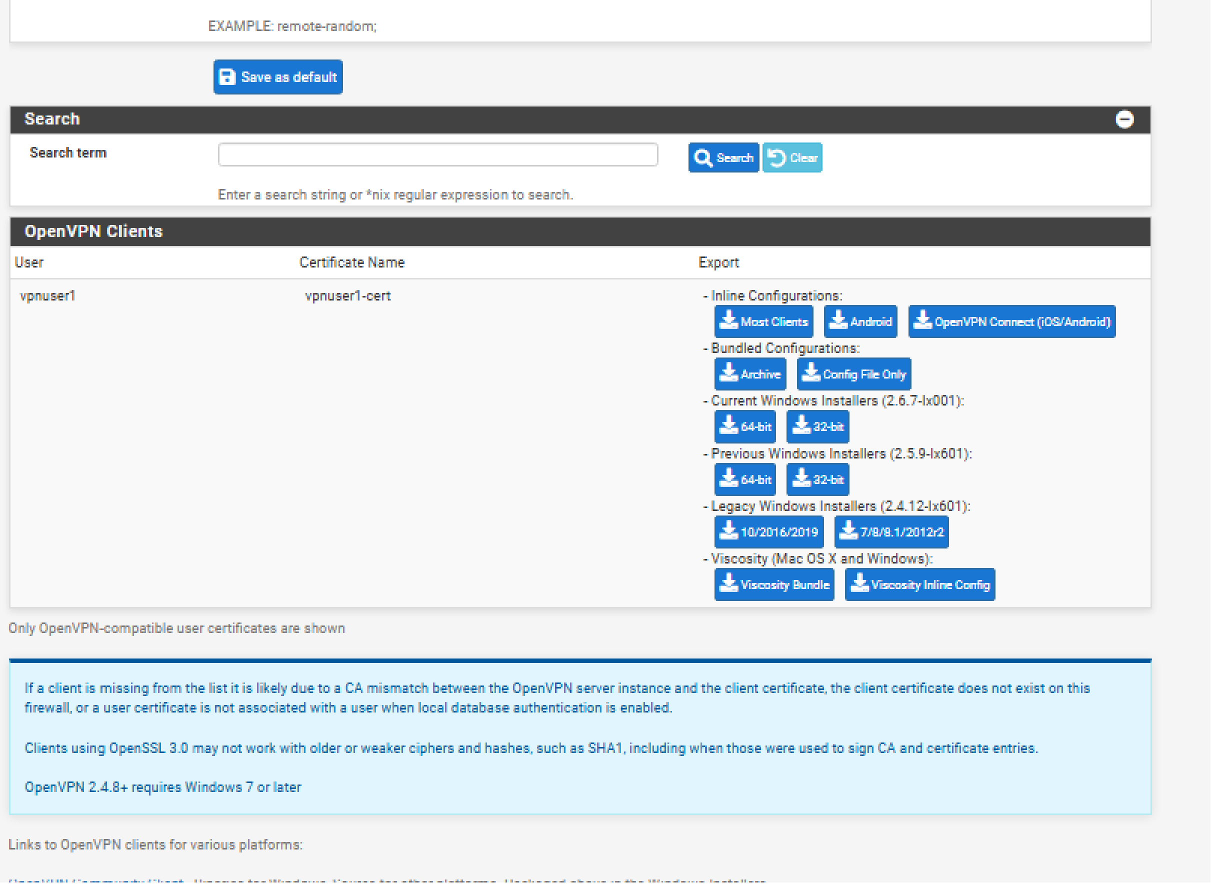
PKCS#12 Encryption: High: AES-256 + SHA256 (pfSense Software, FreeBSD, Linux, Windo
Select the level of encryption to use when exporting a PKCS#12 archive. Encryption support varies by Operating System and program

Proxy Options

4. Descendez jusqu'à la liste des utilisateurs

5. Pour l'utilisateur **vpnuser1**, téléchargez :

• Archive: pour installation complète
• Inline Configuration: fichier .ovpn unique (recommandé)
• Most Clients: pour OpenVPN GUI Windows



EXAMPLE: remote-random;

Search

Search term

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

OpenVPN Clients

User	Certificate Name	Export
vpnuser1	vpnuser1-cert	- Inline Configurations: - Bundled Configurations: - Current Windows Installers (2.6.7-Ix001): - Previous Windows Installers (2.5.9-Ix601): - Legacy Windows Installers (2.4.12-Ix601): - Viscosity (Mac OS X and Windows):

Only OpenVPN-compatible user certificates are shown

If a client is missing from the list it is likely due to a CA mismatch between the OpenVPN server instance and the client certificate, the client certificate does not exist on this firewall, or a user certificate is not associated with a user when local database authentication is enabled.

Clients using OpenSSL 3.0 may not work with older or weaker ciphers and hashes, such as SHA1, including when those were used to sign CA and certificate entries.

OpenVPN 2.4.8+ requires Windows 7 or later

Links to OpenVPN clients for various platforms:

✅ **Fichier obtenu :** vpnuser1-UDP4-1194-config.ovpn (ou similaire)

Test de connexion VPN

Sur Windows :

1. Téléchargez et installez **OpenVPN GUI** depuis openvpn.net
2. Copiez le fichier .ovpn dans C:\Program Files\OpenVPN\config\
3. Lancez OpenVPN GUI (en tant qu'administrateur)
4. Clic droit sur l'icône → Connect
5. Entrez vos identifiants (vpnuser1 / mot de passe)